Computer Networks
Medium Access Control Sublayer

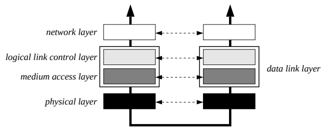
Paolo Costa
costa@cs.vu.nl
`http://www.cs.vu.nl/~costa`

Vrije Universiteit Amsterdam

(Version May 15, 2008)

Notes

Medium Access Sublayer

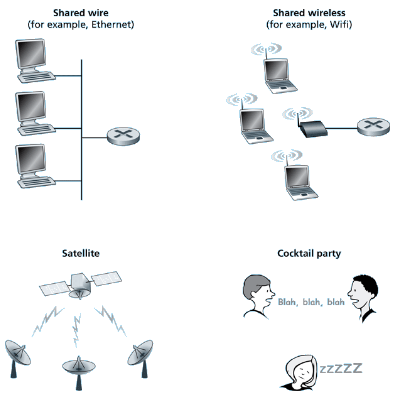


So far: We have discussed the Data Link Layer's functionality and some protocols related to point-to-point communication.

- a large class of networks is built on top of broadcast channels
  - a number of stations that share the same "wire"
  - if one station sends, all the others get to hear it.
- Problem: if you're sharing a channel, then two stations may decide to start frame transmission at the same time
  - frame collision, which means rubbish on the wire.
- Solution: Allocate the channel to one of the competing stations.
  - you'll have to use that same channel to figure out the competition and the allocation.

Notes

Broadcast Channels
Examples



Notes

Medium Access Layer
Strategies

- Three strategies for channel allocation:
  - no control at all
    simply let a station try to use the channel, and do something when a collision happens.
    - applied in contention systems.
  - round-robin technique
    each station in turn is allowed to use the channel.
    - applied in token-based systems
    - the station that has the token may use the channel.
  - reservation for the channel.
    - used in slotted systems.
    - the problem is how to make a reservation.

Notes

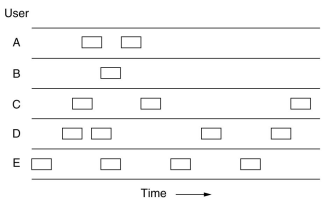
Static Channel Allocation

- Frequency Division Multiplexing (FDM) and Time Division Multiplexing (TDM) can be used to partition a channel's bandwidth among users
  - no collisions and fairness
- However, they have many drawbacks with large number of users and bursty traffic
- TDM
  - transmission rate is limited to R/N even if there is only one node transmitting (being R the total bandwidth and N the number of nodes)
  - a node must always wait its turn even if the network is idle
- FDM
  - bandwidth is not fully used
- In principle, CDMA could be used but there are a number of constraints which makes it difficult to apply in the general case
  - e.g., senders and receivers must know the chip sequence beforehand
  - requires high synchronization

Notes

Dynamic Channel Allocation
Pure ALOHA

- Since none of traditional static protocols work well, we will now explore dynamic protocols
- ALOHA: if you want to send a frame, just do it.
  - if a collision occurs, finish your current transmission and retry later
  - clearly a random waiting time is needed otherwise we would have periodic collisions
  - performace is maximized if all frames have the same size



It's hard to do any worse than this, but efficiency is not really that bad

Notes

Pure ALOHA
Efficiency

- Let S be the average number of new frames submitted during a *frame time* T_{frame} (time needed to transmit a full frame)
  - Poisson distributed
- Let G be the number of old and new frame submissions during a frame time $(G \geq S)$. Also Poisson distributed:

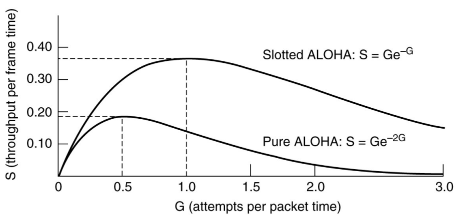
$$\mathcal{P}[k \text{ frames submitted}] = \frac{G^k \cdot e^{-G}}{k!}$$

- Let P_0 be the probability that frame does not suffer from collision $\Rightarrow S = G \cdot P_0$.
- When a frame is being sent, it shouldn't bump into its predecessor, and shouldn't be bumped into by a successor.(vulnerable period = $2T_{frame}$)
  - Probability that a frame will not be damaged during two frame times long is: $P_0 = \mathcal{P}[0] = e^{-2G}$
  - $S = G \cdot e^{-2G}$

Notes

Slotted ALOHA

- We can improve a bit by removing some randomness.
- Slotted ALOHA
  frame transmission can only start at fixed times
- Since the vulnerable period is now halved, $P_0 = e^{-G}$
  $\Rightarrow S = Ge^{-G}$



Notes

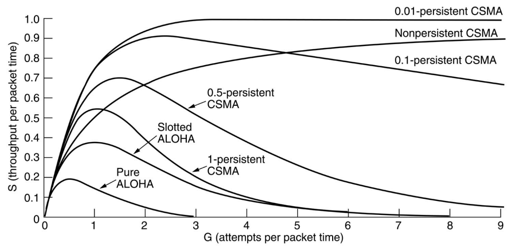
Carrier Sense Multiple Access (CSMA)

CSMA protocols do better than ALOHA: you monitor the channel before and/or during transmission.

- 1-persistent
  Listen whether the channel is free before transmitting. If busy, wait until it becomes free and then immediately start your transmission.
- Nonpersistent
  Less greedy – when the channel is busy, wait a random period of time before trying again. If you wait too long, the channel utilization drops.
- p-Persistent
  Used with slotted systems. If you find the channel idle during the current slot, you transmit with probability p, and defer until next slot with probability $1 - p$.
  - $p = 1$ is not really good
  - $p = 0$ makes you *really* polite.

Notes

Protocol Comparison



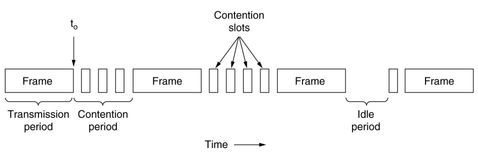
Question

- What are we actually displaying here? Should the conclusion be that p-persistent protocols are really good with $p \approx 0$? Not really. Delay would increase indefinitely.

Notes

CSMA w/Collision Detection (CSMA/CD)

- CSMA/CD protocols sense the channel, but immediately stop transmission when you detect a collision.
- Ethernet works like this



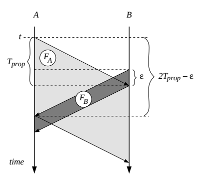
1. Listen to see whether the channel is free.
   - transmission is delayed until the channel is no longer used.
2. During transmission, keep listening in order to detect a collision.
   - if a collision occurs, transmission immediately stops.
3. If a collision occurred, wait a random period of time, and proceed with the first step again.

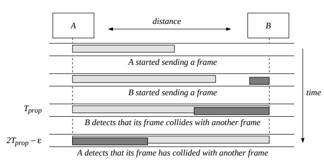
Notes

CSMA w/Collision Detection
Contention Period

- Question: how big should the contention period be?
- The minimum time to detect a collision is just the time it takes the signal to propagate from one station to another (T_{prop})
  - WRONG !!!
- If the second station starts transmitting at $T_{prop} - \varepsilon$, it will immediately detect the collisions but the first station will need $2T_{prop} - \varepsilon$

⇒ The contention interval is therefore $2T_{prop}$





Notes

Collision Free Protocols

- Collisions do still occur in CSMA/CD during the contention period
- These collisions may affect system performance, especially when the cable is long (i.e., T_{prop} is large and frames are small)
- Also, in some cases collision detection is hard to implement (e.g., wireless networks)

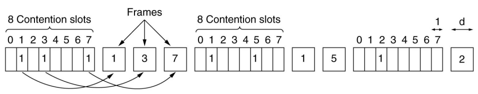
⇒ In the following we'll see some protocols which completely avoid collisions, even during the contention period

Note

- No MAC-sublayer protocol guarantees reliable delivery.
- Even in absence of collisions, the receiver may not have copied the frame correctly for various reasons
  - e.g., lack of space, missed interrupt or external events like a bolt.

Notes

Collision Free Protocols
Bit-map method



- The contention period contains N slots.
- If station k wants to transmit a frame, it transmits a 1 during the k^{th} slot.
- The highest-numbered station goes first.

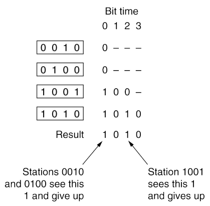
Question

- What is the potential issue of this approach ? It may suffer serious scalability problems with thousands of stations

Notes

Collision Free Protocols
Binary Countdown Protocol

- During contention period a total of $\log_2 N$ bits can be transmitted
- Each host broadcasts its binary address one bit at a time
  - bits transmitted simultaneously are boolean OR'd together
  - this is an electrical property of the bus used
- If a host sent a zero bit but the boolean OR results in a one bit, the host gives up and stops sending
- Whichever host remains after the entire address has been broadcast gets access to the medium



Notes

Comparison

- Contention systems are good when there's not much going on
  - a station can immediately transmit a frame
  - we do some repairing when things go wrong.
- Collision-free systems are good when there's generally a lot of traffic
  - a station first has to get the channel explicitly before frame transmission
  - we do a lot of work avoiding collisions.

What we really want is the contention strategy during light loads, and collision-free strategy during rush hours.

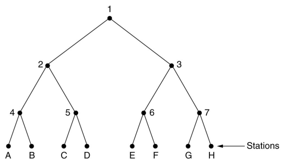
Notes

Limited-Contention Protocols

- Solution: Dynamically regulate the number of competing stations during a contention period.
  - if there's a collision during the k^{th} slot, divide the contenders into two groups.
  - the first group gets to try it again during the next slot ($k+1$)
  - if no collisions occur then, the second group gets a try during the slot after that ($k+2$).
  - otherwise, the first group is split up again.
- If there's not much traffic, the first station will be immediately allowed to transmit a frame.
- With a lot of traffic, the strategy reduces to the bit-map protocol.

Notes

Limited-Contention Protocols
The Adaptive Tree Walk Protocol

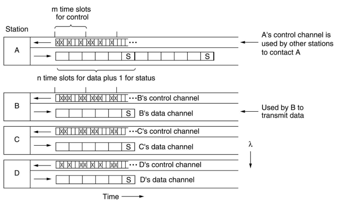


- In the first transmission slot (slot 0) all stations can try to transmit
- If a collision occurs, in slot 1 only nodes falling under node 2 may compete
- If one of them succeeded, in the next slot it will be the turn of node 3's subtree
- Otherwise, it is node 4's turn

Notes

Wavelength Division (1/2)

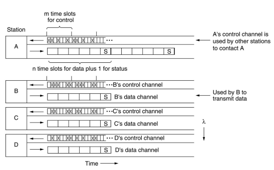
- If you have a lot of bandwidth, just divide the channel into sub-channels, and dynamically allocate the sub-channels.
  - used in fiber optics



- Each station gets two channels: one control channel for handling incoming requests, one for the actual data transfer.
- Each channel repeatedly carries a fixed series of slots.
- The data channel contains a status slot carrying info on free slots in its control channel.

Notes

Wavelength Division (2/2)

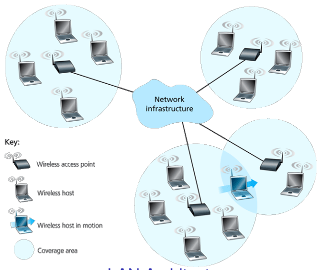


- In order to contact a station A, you first read its status slot from the data channel to see which control slot is unused.
  - you then put a transmission request in a free control slot.
- If the transmission request is accepted, you can send data on your own data channel that will be picked up by A.
  - you put the data in a specific slot, and tell A which slot that is
- There's still a lot of competition.
  - if two senders try to grab the same control slot, neither will get it
  - both will notice a failure and will wait for a random time before retrying

Notes

Wireless Networks

- Often, there are a number of base stations (a.k.a. access points) connected through guided media.
  - a base station can communicate with a mobile computer
  - the mobile computers use radio/infrared signals for communication.
- Nodes can also group together to form an ad hoc network



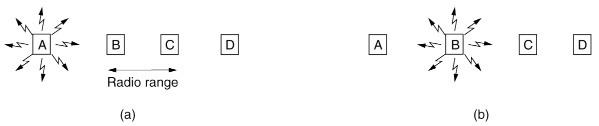
LAN Architecture


Ad Hoc Mode

Notes

Wireless Networks
Interference

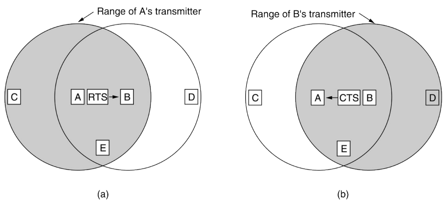
Problem: There can be subtle interference:



- Issue (a)
  How can *C* be prevented from trying to transmit something to *B* ?
  - in that case it will ruin any receipt by *B*
  - hidden station problem
- Issue (b)
  How can we tell *C* that it is allowed to transmit to *D*, because this will not interfere with the communication from *B* to *A* ?
  - exposed station problem

Notes

Multiple Access with Collision Avoidance (MACA)



(a) *A* first sends a Request To Send (RTS).
(b) *B* answers with a Clear To Send (CTS).

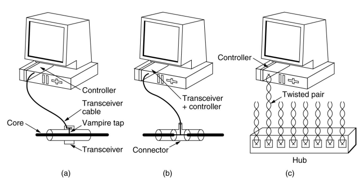
- *C* hears only RTS and can freely transmit, knowing it will not interfere with *A*'s transmission.
  ⇒ solves exposed station problem
- *D* hears only the CTS and keeps still for otherwise it would interfere with *B*'s reception.
  ⇒ solves hidden station problem

Notes

802.3 (or Ethernet)

- Ethernet stands for a near implementation of the IEEE 802.3 protocol.
- It is CSMA/CD based
  - sense the channel, wait until idle, and backoff if collision

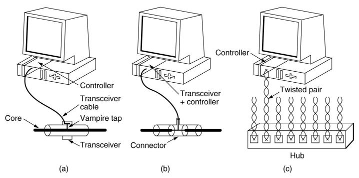
.



Name	Cable	Max. dist.	Nodes/Seg.
10Base5	Thick coax (a)	500 m	100
10Base2	Thin coax (b)	200 m	30
10Base-T	Twisted pair (c)	100 m	1024
10Base-F	Fiber optics	2000 m	1024

Notes

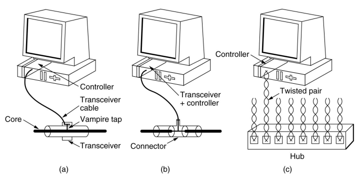
802.3 (or Ethernet)
Cabling (1/2)



- 10Base5 is called so because it operates at 10 Mbps, uses baseband (i.e., digital) signaling, and can support cable up to 500 m
  - a transreceiver is campled around the cable and contains the electronics to handle collision detection
- 10Base2 has just a passive connection to the cable
  - the transreceiver electronics are on the controller board

Notes

802.3 (or Ethernet)
Cabling (2/2)

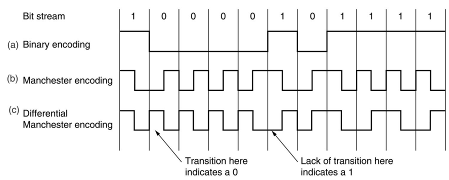


- Cable breaks can be a major problem for both media
  - usually a pulse of known shape is injected and if it is blocked somewhere an echo signal is sent back
- 10BaseT solves the issues with cable breaks
  - all stations have a cable running to a hub, where they are all connected electrically
  - hubs do *not* buffer incoming traffic
  - no (physical) shared cable at all but collisions still occurs at the hub

Notes

Manchester Encoding

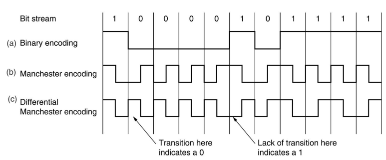
- Problem: We can't just send straight binary codes across the wire, because stations can't distinguish a 0 from an idle line.
- Solution: use an encoding scheme in which a voltage transition occurs during every bit time (Manchester Encoding):



- A binary 1 bit is sent by having the voltage set high during the first interval and low in the second one
  - a binary 0 is just the reverse
- Differential Manchester Encoding
  - a 1 bit is indicated by the absence of a transition at the start
  - a 0 bit is indicated by the presence of a transition

Notes

Machester Encoding
Pros & Cons



Question

- What is an advantageous side-effect of having a transition for every bit? It allows to keep sender/receiver in sync.

Question

- What is a drawback of this encoding compared with Binary encoding ? It requires twice as much bandwidth as binary encoding. For instance, to send 10 Mbps we need to change the signal 20 million times / sec

Notes

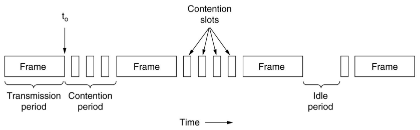
802.3 Frame Layout

Preamble	SoF	Destination address	Source address	Length	Data	Pad	Check-sum

- Preamble: Seven times 10101010 is used to synchronize the receiver's clock with that of the sender
- Start: Just a delimiter to tell that the real info is now coming
- Address: Generally 48-bit fields. Leftmost bit indicates ordinary or group addresses (multicast / broadcast). Second bit indicates global or local address
- Length: Ranges from 0-1500. Frames should always be at least 64 bytes
  - useful for collision detection
- Pad: used to fill out the frame to the minimum size
- Checksum: Calculated over the data field. CRC-based

Notes

Exponential Backoff Algorithm

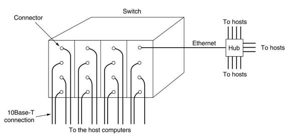


- Ethernet is CSMA/CD based
- After a collision time is divided into discrete slots
  - in the standard they are 51.2 μs long
- Exponential Backoff
  - after the first collision, each station waits either 0 or 1 slot times before trying again
  - after the second collision, each ones picks either 0, 1, 2, or 3 slot times
  - in general, after i collisions, a random number between 0 and $2^i - 1$ is chosen
- It dynamically adapts to the number of stations trying to send

Notes

Switched 802.3 LANs

- Problem: As more stations are added, traffic will go up, and so will the possibility of collisions $\Rightarrow$ the network will saturate.
- Solution: Divide the network into separate sub-LANs and connect them through a switch:



- incoming frames are buffered in the on-board's RAM as they arrive
- each card has its own collision domain
  - collisions are impossible and performance is improved

Question

- What is another nice side-effect ? Privacy issue. Sniffing becomes impossible

Notes

Fast Ethernet

- Problem: Ethernet by itself was too slow, and new alternatives (optics) were just too expensive (they were okay for backbones, but not for basic LAN segments).
- Solution: Upgrade existing base of LANs (i.e. Ethernets) in such a way that the interfaces remain the same, but the capacity goes up
- Fast Ethernet.(100 Mbps)
  - data formats, interfaces, and protocols are all the same.
  - that means that we can only drop the bit time from 100 nsec to 10 nsec.
- Category 3 twisted pair are unable to carry 200 megabaud signal (100 MBps with Manchester Encoding) for 100 m.
  - category 5 cables must be adopted

Notes

Gigabit Ethernet (802.3z)

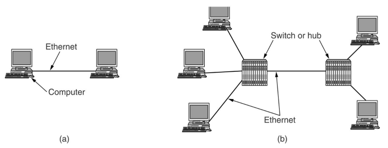
- because Fast Ethernet may not always be fast enough, we simply move the decimal point one position and get Gigabit Ethernet: transfer Ethernet frames at 1000 Mbps.

Name	Cable	Max. range
1000BASE-SX	Fiber	550 m
1000BASE-LX	Fiber	5000 m
1000BASE-CX	Copper	25 m
1000BASE-T	Twisted pair	100 m

- Gigabit Ethernet works only in point-to-point mode
- 10 Gbit: Another step further: point-to-point over fiber, with copper specs being developed.
  - they call it 802.3ae because they run out of letters :)

Notes

Gigabit Ethernet
Specs



- With a switch, there is no need for the CSMA/CD part!
  - maximal cable length is determined by signal strength.
- With a hub, the maximal cable length is restricted to 25 m.
  - this is because the minimum frame size is 64 bytes (details in the book)
- To facilitate longer cables, minimum size is increased to 512 bytes:
  - Carrier extension: let the hardware extend a frame to 512 bytes by using padding (no need to update the software)
  - Frame bursting: let the hardware put several frames into a 512-byte frame (provided that there are more than one frame to send)

Notes

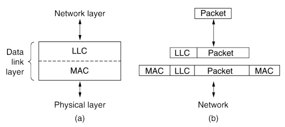
Gigabit Ethernet
Encoding

- Gigabit ethernet uses a different encoding scheme because clocking data in $1ns$ is too difficult on wire
- it uses four category 5 twisted pairs to allow four symbols to be transmitted in parallel.
  - each symbol is encoded using one of five voltage levels.
  - this scheme allows a single symbol to encode 00, 01, 10, 11, or a special value for control purposes
    $\Rightarrow$ there are 2 data bits per twisted pair or 8 data bits per clock cycle.
  - the clock runs at 125 MHz (instead of the required 1Ghz), allowing 1-Gbps operation

Notes

Logical Link Control

- Ethernet and the other 802 protocols offer just a best-effort datagram service
  - no reliable communication
  - suitable e.g., for IP packets (connection-less service)
- Some systems, however, needs an error-controlled, flow-controlled data link protocol

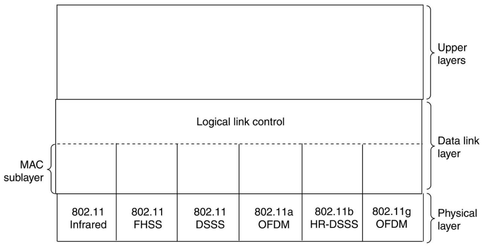


- Logical Link Control (LLC)
  - closely based on the HLDC protocol
  - provides unreliable datagram service, acknowledged datagram service, and reliable connection-oriented service
  - the header contains three fields: destination, source, and a control (acks + seq. numbers) field

Notes

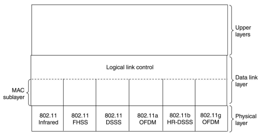
Wireless LANs

- Wireless LANs need to apply special techniques to achieve high bandwidth
- The Data Link Layer is split into two layers:
  - the MAC layer determines how the channel is allocated
  - the LLC hides the difference between all the 802 variants and provides reliable service (if needed)



Notes

Wireless LANs
Physical Layer



- Infrared: Applicable for 1-2 Mbps. Not very popular, also because sunlight degrades performance
- Frequency Hopping Spread Spectrum (FHSS): Use 79 channels, each 1 MHz wide in an unregistered band (i.e., free to be used)
  - frames are sent at different frequencies each time
  - low bandwidth, but good resistance against security attacks and interference from other devices.
- Direct Sequencing Spread Spectrum Similar to CDMA, restricted to 1-2 Mbps
- Orthogonal FDM Akin to ADSL: apply FDM across multiple channels (48 for data, 4 for control). Can reach 54 Mbps
- High Rate Direct Sequencing: Akin to DSS - use 11 million chip sequences to get to 11 Mbps (802.11b)

Notes

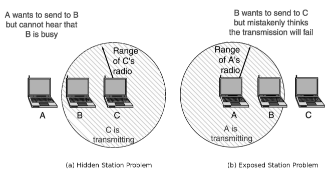
Wireless LANs
The Future: IEEE 802.11n

- IEEE 802.11n is a proposed amendment to the IEEE 802.11 standard to significantly improve network throughput
- It leverages off Space Division Multiplexing (SDM)
  - improves performance by parsing data into multiple streams transmitted through multiple antennas (up to four)
  - a.k.a. multiple-input and multiple-output (MIMO)
  - it also increase power consumption and cost
- In addition the bandwidth of each channel is moved to 40 Mhz (instead of the standard 20 Mhz)
  - total throughput per channel is 150 Mb
- Combining four 40 Mhz channels with MIMO we get a data rate of 600 Mbps
  - in practice, speeds of 100Mbit/sec. to 140Mbit/sec are expected
- The draft is expected to be finalized in March 2009 with publication in December 2009
  - major manufacturers are now releasing 'pre-N', 'draft n' or 'MIMO-based' products (e.g., NETGEAR or Apple)

Notes

Wireless LANs
MAC Layer

- Problem: How do we solve the hidden / exposed station problem ?
  - one way or the other, stations should not be allowed to continuously interfere with each other's transmissions



- IEEE 802.11 provides two methods to deal with this problem:
  - Distributed coordination: let the stations figure it out by using a collision avoidance protocol (CSMA/CA)
  - Point coordination: there's a central base station that controls who goes first
    - (mostly used)

Notes

CSMA/CA

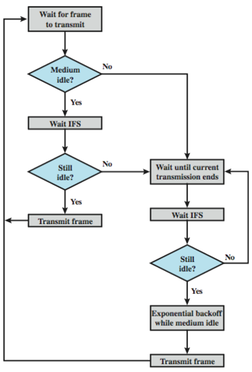
- Collision detection is hard to implement on the wireless medium
  - radios cannot transmit and receive on the same frequency (half-duplex channels)
- Solution: Use collision avoidance protocol
  - name is somewhat inappropriate as all MAC protocols aim at avoiding collisions
- It has two methods operations:
  - Ethernet-like
  - MACAW

Notes

CSMA/CA
Ethernet-like

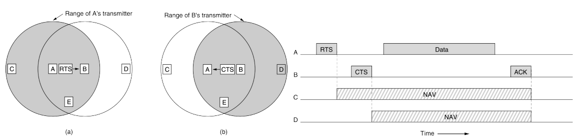
1. When a station wants to transmit, it senses the channel
2. If it is idle,wait for a fixed interval (IFS) and then transmits
3. Otherwise, it waits until the transmission ends, then wait for another IFS and finally wait for a random time before transmitting
   - exponential backoff is used
4. if a collision occurs (i.e., no ack received), the process restarts

- Similar to nonpersistent ALOHA
  - there random time was used before re-sensing the channel when busy
- Nowadays most MAC are reprogrammable by users
  - ⇒ vulnerable to cheating



Notes

CSMA/CA
MACAW

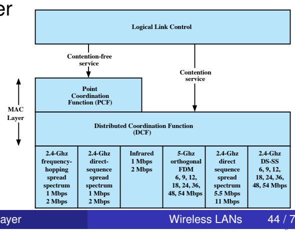


- MACAW: send RTS/CTS packets to see whether you should defer transmission to avoid interference with another transmission
- it is an evolution of the MACA protocol discussed before
  - to improve reliability, ACKs are sent upon successful receipt
- Example: *A* wants to send a message to *B*
  - *C* and *D* listening to the RTS and CTS packets can estimate how long the sequence will take
    - Network Allocation Vector (NAV): it's a virtual channel that a station assigns to itself telling it to shut up
- Note: since *A* has to receive an ACK from B, *C* cannot transmit
  - ⇒ the exposed station problem is *not* solved (but the hidden station problem is)

Notes

CSMA/CA
Point Coordination

- In PCF the base-station polls the other stations, asking them if they have anything to send
- It sends a beacon frame once every 10 or 100 ms.
  - This frame carries information on frequencies and such, and invites stations to sign up for transmission.
- To save battery, a base station can also direct a mobile station to go into sleep state
  - incoming messages will be buffered until it wakes up
- When base station transmits, there can be no hidden terminals
- PCF and DCF can coexist together
  - it works by carefully defining the interframe time interval.
  - first the base station can poll the other stations
  - if nobody replies, any station can acquire the channel



Notes

802.11: Frame Structure (1/3)

Bytes	2	2	6	6	6	2	6	0-2312	4
	Frame control	Dur- ation	Address 1	Address 2	Address 3	Seq.	Address 4	Data	Check- sum

Bits	2	2	4	1	1	1	1	1	1	1	1	
	Version	Type	Subtype	To DS	From DS	MF	Re- try	Pwr	More	W	O	Frame control

- Type: Data, control, or management frame
- Subtype: Are we dealing with RTS, CTS, an ACK, etc.
- DS: Is the frame entering/leaving the current cell?
- MF: Frames are allowed to be fragmented to increase reliability. This bit tells whether more fragments are on their way.

Notes

802.11: Frame Structure (2/3)

Bytes	2	2	6	6	6	2	6	0-2312	4
	Frame control	Dur- ation	Address 1	Address 2	Address 3	Seq.	Address 4	Data	Check- sum

Bits	2	2	4	1	1	1	1	1	1	1	1	
	Version	Type	Subtype	To DS	From DS	MF	Re- try	Pwr	More	W	O	Frame control

- Retry: Is this a retransmission?
- Power: Used by a base station to activate/passivate a station (important in view of power saving)
- More: Additional frames can be expected.
- W: Data is encrypted using the Wired Equivalence Privacy algorithm.
- O: Stick to ordered delivery of frames.

Notes

802.11: Frame Structure (3/3)

Bytes	2	2	6	6	6	2	6	0-2312	4
	Frame control	Dur- ation	Address 1	Address 2	Address 3	Seq.	Address 4	Data	Check- sum

Bits	2	2	4	1	1	1	1	1	1	1	1	
	Version	Type	Subtype	To DS	From DS	MF	Re- try	Pwr	More	W	O	Frame control

- Duration: Tells how long the transmission of this frame will take, allowing other stations to set their NAV accordingly.
- Addresses: Source/destination in a cell; and those of base stations outside the cell when dealing with intercell traffic.
- Sequence: Sequence number of this frame. 4 bits are used to identify a fragment of a frame.

Notes

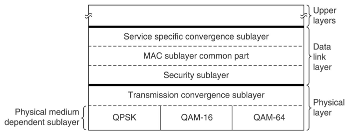
Broadband Wireless

- Goal: Use wireless connection between buildings
  - e.g., avoiding the use of the local loop
- 802.11 is great for indoor networking, but is not that good for wireless communication between buildings:
  1. Buildings do not move, so much of the mobility stuff from 802.11 is not needed
  2. Several computers should be able to make use of the same "connection" (i.e., it should be broadband). 802.11 is intended to support one transmission at a time.
  3. Broadband connections can be supported by powerful radios (money is less of a problem),
     ⇒ full-duplex communication possible
  4. We may need to cross longer distances, up to several kilometers
     ⇒ different modulation schemes are needed
     ⇒ privacy and security issues
  5. More bandwidth is needed: 10-to-66 GHz frequency range
     ⇒ millimiter waves are more error-prone (e.g., rain) but they can be focused in directional beams (IEEE 802.11 is omnidirectional)

Notes

IEEE 802.16
Protocol Stack

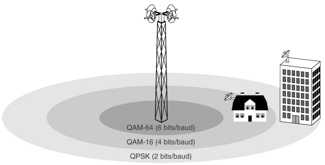
WiMAX (World Interoperability for Microwave Access) is a family of IEEE 802.16 aiming at replacing ADSL and cable modems



- The Transmission Converge Sublayer hides the different modulation schemes
- The Security sublayer deals with security and privacy
  - more crucial for outdoor networks
- MAC: the base station controls the systems by scheduling downstream and upstream channels
  - it is connection-oriented (QoS needed by phone-companies)
- The Service-specific Converge sublayer replaces the usual LLC
  - it has to integrate seamlessly datagram protocols (IP, PPP, and Ethernet) and connection-oriented ones (e.g., ATM)

Notes

IEEE 802.16
Physical Layer

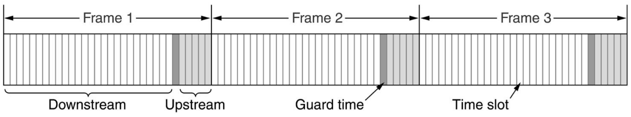


- Millimiter waves (10-to-66 GHz spectrum) travel in straight lines
  - the base station have multiple antennas, each pointing at different areas
- These waves falls off sharply with the distance
  - signal-to-noise ratio also drops
- Different modulation schemes are used
  - QAM-64: 6 bits / baud, 150Mbps
  - QAM-16: 4 bits / baud, 100Mbps
  - QPSK: 2 bits / baud, 50 Mbps
- Hamming codes are used to perform error correction

Notes

IEEE 802.16
MAC Sublayer

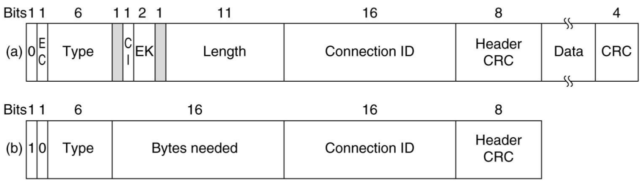
- We need a flexible way to allocate bandwidth for downstream and upstream data
  - just as in ADSL, an asymmetric approach works best.
- Time Division Duplexing (TDD)
  - let the base station send out frames containing time slots:



- Downstream traffic is mapped onto time slots by the base station.
  - The base station is completely in control for this direction
- Upstream traffic is more complex. Three options:
  1. The base-station pre-allocates it (constant bit rate service)
  2. The base-station periodically polls stations (variable bit rate service)
  3. No polling but subscribers have to contend (best-effort service)

Notes

802.16: Frame Structure



(a) A generic frame
(b) A bandwidth request frame

- 802.16 offers connection-oriented services
  - ConnectionID specifies the current connection
- Checksumming the data is optional
  - the physical layer uses error correction techniques
  - no facilities (e.g., sequence numbers) for retransmissions
- Encryption is critical for the system
  - managed at MAC level
  - EK specifies the encryption keys used

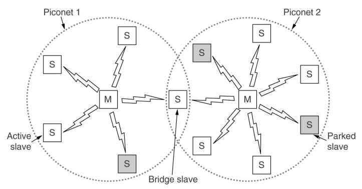
Notes

Bluetooth

- Bluetooth is to allow very different (portable and fixed) devices located in each other's proximity to exchange information:
  - Let very different portable devices (PDA, cellular phone, notebook) set up connections
  - Replace many of the existing cables (headset, keyboard, mouse, printer)
  - Provide better wireless connection (handsfree solutions)
  - Provide wireless access to Internet entry points
  - Relatively high bandwidth: 1 Mbit/second
- Also referred to as IEEE 802.15.1
- It's named after a Viking king who unified Denmark and Norway (940-981)

Notes

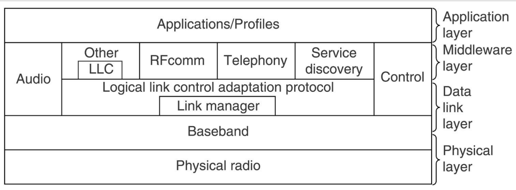
Bluetooth Architecture



- Piconet: Group of devices with one master and multiple slaves.
  - there can as much as 7 active slaves, but a total of 255 parked ones (i.e., in a power-saving state).
- Scatternet: An interconnected collection of piconets
- A piconet is a centralized TDM system with the master determining which device gets to communicate
  - the connection procedure for a non-existent piconet is initiated by any of the devices, which then becomes the master
- The master-slave design facilitates the implementation of Bluetooth chips for under 5$

Notes

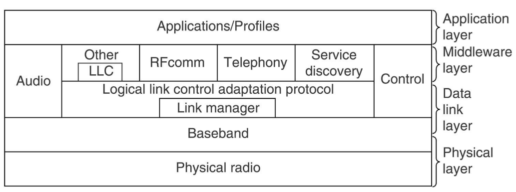
Bluetooth Protocol Stack (1/2)



- Radio: it uses frequency hopping (2.4 GHz band):
  - take data signal and modulate it with a carrier signal that changes frequency in hops.
    - good to minimize interference from other devices (microwave ovens!)
  - hops for Bluetooth: fixed at $2402 + k$ MHz, $k = 0, 1, \ldots, 78$.
  - modulation is frequency shift keying with 1 bit / Hertz
    - ⇒ 1Mbps data rate but much of this is consumed as overhead
- Baseband: Core of the data link layer.
  - determines timing, framing, packets, and flow control.
  - provides synchronous and asynchronous data communication.
  - error correction can be used to provide higher reliability

Notes

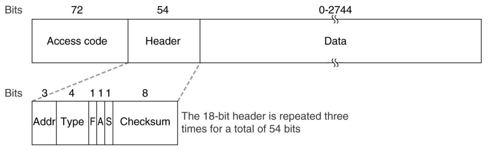
Bluetooth Protocol Stack (2/2)



- Link manager:
  Manages connections, power management
- Logical link control:
  Multiplexing of higher-level protocols, segmentation and reassembly of large packets, device discovery
- Audio:
  Handles streaming for voice-related applications
- RFCOMM:
  Emulate serial cable based on GSM protocol

Notes

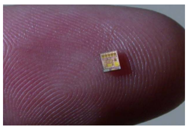
Bluetooth Frame Structure



- Access code identifies the master of the piconet
  - slaves within radio range of two masters do not interfere
- Address identifies the recipient among the eight active devices
- The Flow bit is asserted by a slave when its buffer is full and cannot receive any more data
- The Acknowledgment bit is used to piggyback an ACK
- The Sequence bit is used to number the frames
  - Stop-and-wait protocol is used so 1 bit is enough
- The 18-bit header is repeated three times (54-bit header)
  - On the receiving side, all three copies are examined.
  - if all three are the same, the bit is accepted.
  - if not, the majority opinion wins

Notes

Wireless Sensor Networks

- A wireless network of small devices with sensing and computing cababilities
- Issues:
  - Limited hardware: Each node generally has limited resources (CPU, storage, networking/bandwidth, and energy).
  - Limited networking support: We're dealing with peer-to-peer networks with random topologies. Connectivity is mobile and unreliable. Each node is router and application host.
  - Limited SW development support: There is a strong coupling between application and system layers, which is quite unusual for most developers.
- Sensor networks offer a cheap alternative to fixed infrastructures

Notes

Wireless Sensor Networks
Zigbee

- ZigBee is the name of a specification for a suite of high level communication protocols using small, low-power digital radios
- It has been standardized as IEEE 802.15.4
- Physical Layer:
  - Direct-sequence spread spectrum coding using orthogonal QPSK that transmits two bits per symbol
  - 250 Kbps in the 2.4 GHz band and 20Kbps in the 868Mhz band
- MAC Layer
  - CSMA/CA

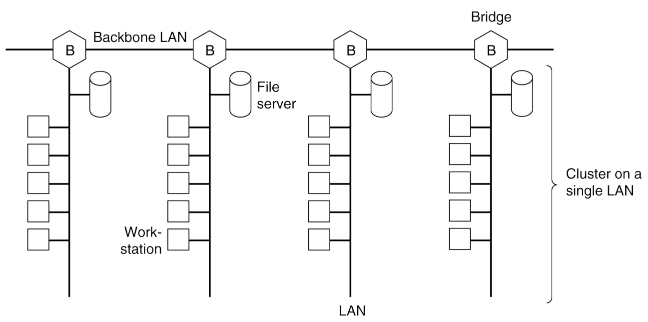
Notes

Data Link Layer (DLL) Switching

- We want to interconnect a number of LANs, rather than having one big one.
- Two LANs are connected through a bridge for several reasons:
  1. You want to let existing LANs (in departments, buildings, etc.) as they are.
     - on the other hand, you do want to connect them.
  2. When an organization is spread over several buildings, it is cheaper to have a different interconnect (e.g., infrared) than coax cable.
     - you may also have no choice.
  3. Splitting things up (rather than just tying things together) may be good for load balancing.
  4. Physical distance sometimes precludes building one big LAN.
     - e.g., UTP 100 Mbps Ethernet can handle cables only up to 100 m.
  5. The reliability can be improved
     - if one part goes down, the other LAN segments may still operate.
  6. Security: Most LAN interfaces have a promiscuous mode in which *all* frames are given to the computer
     - splitting LANs prevent this type of attacks

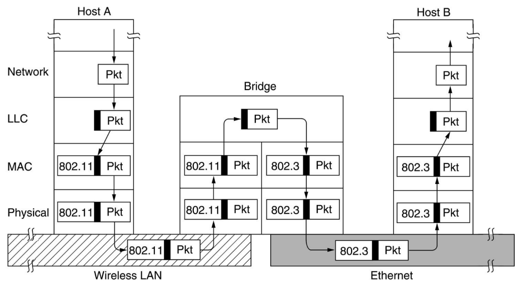
Notes

DLL Switching
Example



Notes

Bridges
Basics

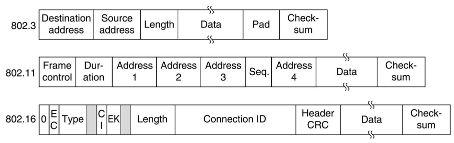


- A packet is passed to the data link layer (LLC part)
- It is then passed to the MAC layer (specific access strategy)
- A bridge converts the stuff above the MAC layer, in the LLC layer

Notes

Bridges
Issues

- Frame format Committees for 802.x invented different formats:



- Different transmission rates: if a higher speed LAN starts pumping frames on a lower speed one, we've got a problem
- Frame Length: 802.x MACs use different frame sizes

Question

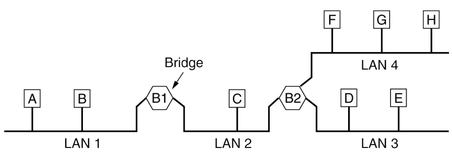
- Splitting a frame into pieces is often out of the question! Why ? There is no way that we can deal with reassembling frames into larger parts. The data link layer can simply not handle that.

- Security: 802.11 and 802.16 support encryption at MAC level but Ethernet does not

Notes

Transparent Bridges

- Issue: Can we develop a bridge that interconnects LANs in a completely transparent way, i.e. seems to turn it into one big LAN?

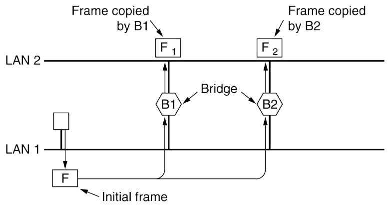


- Backward Learning protocol
  - An incoming frame is simply forwarded to all other LAN segments connected to the bridge
  - Because an incoming frame contains the source address, a bridge can gradually know through which interface it can reach a host.
    - it builds and maintain a routing table
  - Use a timeout mechanism to flush all knowledge a bridge has ⇒ it will gradually build up a fresh view again
    - this accounts for dynamic topologies (e.g., a user moving to a different building)

Notes

Problem

- Sometimes LANs are connected by multiple bridges
  - we no longer have a tree, but a graph containing cycles
  - ⇒ we can't just forward frames anymore.



- *B1* would receive the frame *F2* created by *B2* and it would forward it again to LAN1, believing it is a new frame
  - the cycle goes on forever

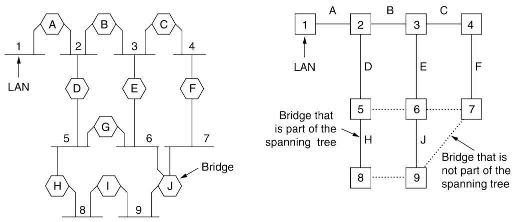
Question

- Why would we need multiple bridges ? Redundancy

Notes

Solution

- Let the bridges construct a spanning tree on their own.



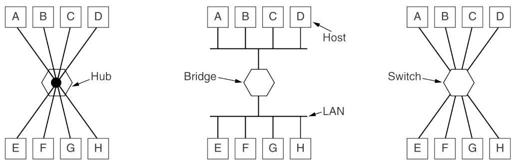
(a) (b)

- each bridge broadcasts its ID across the attached LAN segments.
  - the lowest numbered bridge becomes root for that segment.
- a root bridge for a segment knows it can never be the root for the tree, if it finds out there's a bridge with a lower number.
- bridges advertise their distance to the "real" root
  - ⇒ that's how we build a spanning tree.

Notes

From Repeater to Switch

There's a lot of confusion when it comes to placing "connectors" in reference models:



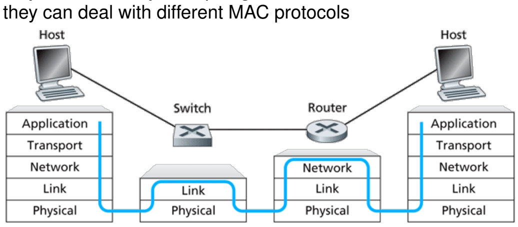
(a) (b) (c)

- Repeater: Amplifies incoming signal
- Hub: Takes an incoming frame and passes it to all other ports
- Switch: Connects several computers (and routes frames between them)
  - it eliminates collisions by buffering simultaneous frames
- Bridge: Connects two or more LANs
  - sometimes bridges and switches are used as synonyms

Notes

From Router to Gateway

- Routers: Placed in "classical" networks, and forwards packets to other routers
  - they can handle cyclic topologies
  - they can deal with different MAC protocols

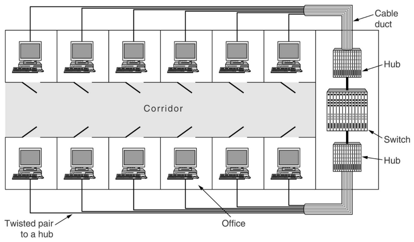


- Transport gateways: Connects two networks at the transport layer: go from a TCP connection to an ATM transport connection.
- Application gateway: Connects two different application protocols, such as sending SMS messages to a Web server, or connecting an X.400 mail system to an Internet-based mail system.

Notes

Virtual LANs (1/2)

- Many LANs are organized according to a physical division of workstations, possibly having multiple LANs connected by bridges
  - ⇒ better management and security

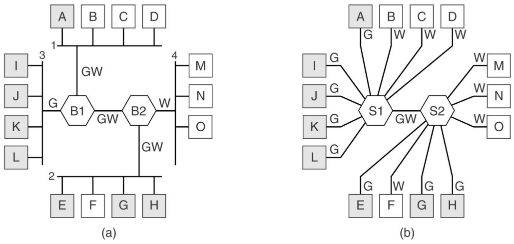


- Problem: The physical organization may not correspond at all with what would seem logically the best organization (e.g., based on membership of a department).
  - we don't want to rewire all cables when an employee move to a different office

Notes

Virtual LANs (2/2)

- Solution: Adjust the bridges and switches such that an incoming frame is forwarded only to those outgoing ports that connect hosts (or LAN segments) belonging to the same logical group as the sending host:

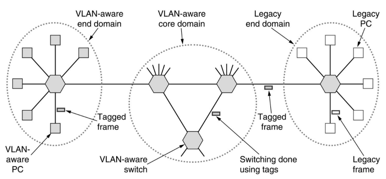


(a) Four physical LANs interconnected by bridges
(b) The same 15 machines organized into two VLANs by bridges

Notes

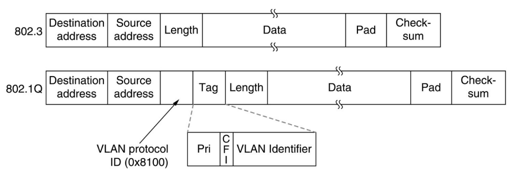
Identifying a VLAN

- Actually it is not necessary to keep a map between hosts and VLAN groups
  - it is sufficient to store information about the VLAN inside the frame
  - ⇒ add a tag to frame headers
- Problem: You don't want existing networks (Ethernet!) to break down.
  - you need to apply a trick so that non-VLAN aware frames can be adjusted to one in which the VLAN is identified by a tag.
- Solution: Let bridges and switches make the adjustment: add the tag when a frame comes in for the first time; remove it when it is sent to a non-VLAN aware host.



Notes

802.1Q: VLAN Ethernet



- VLAN protocol ID: value 0x8100, by which it is automatically interpreted as a type (correct according to the 802.3 standard)
- VLAN ID: This is what it is all about
- CFI: Bit indicating that the payload is an 802.5 frame that is being tunneled (token ring protocol)
- Pri (Priority): So, finally, we can introduce QoS into Ethernet networks.
- The last two fields are not related to 802.1Q but they have been introduced because there are very few opportunities to update the Ethernet frame

Notes

Summary

Method	Description
FDM	Dedicate a frequency band to each station
WDM	A dynamic FDM scheme for fiber
TDM	Dedicate a time slot to each station
Pure ALOHA	Unsynchronized transmission at any instant
Slotted ALOHA	Random transmission in well-defined time slots
1-persistent CSMA	Standard carrier sense multiple access
Nonpersistent CSMA	Random delay when channel is sensed busy
P-persistent CSMA	CSMA, but with a probability of p of persisting
CSMA/CD	CSMA, but abort on detecting a collision
Bit map	Round-robin scheduling using a bit map
Binary countdown	Highest-numbered ready station goes next
Tree walk	Reduced contention by selective enabling
MACA, MACAW	Wireless LAN protocols
Ethernet	CSMA/CD with binary exponential backoff
FHSS	Frequency hopping spread spectrum
DSSS	Direct sequence spread spectrum
CSMA/CA	Carrier sense multiple access with collision avoidance

Notes

Notes

Notes

Notes