The Medium Access Control Sublayer

Ethernet

- Physical layer
- MAC sublayer protocol
- Ethernet performance
- Switched Ethernet
- Fast Ethernet
- Gigabit Ethernet
- 10 Gigabit Ethernet
- IEEE 802.2: Logical Link Control
- Retrospective on Ethernet

Ethernet

- We have now finished our discussion of channel allocation protocols in the abstract, so it is time to see how these principles apply to real systems.
- Many of the designs for personal, local, and metropolitan area networks have been standardized under the name of IEEE 802.
- The most important of the survivors are 802.3 (Ethernet) and 802.11 (wireless LAN).
- Bluetooth (wireless PAN) is widely deployed but has now been standardized outside of 802.15.
- With 802.16 (wireless MAN), it is too early to tell.

116

Ethernet

- Classical Ethernet
  - which solves the multiple access problem using the techniques we have studied till now
  - Data rate is 3 to 10 Mbps
- Switched Ethernet: in which devices called switches are used to connect different computers.
  - Fast Ethernet (100 Mbps)
  - Gigabit Ethernet (1000 Mbps)
  - 10 gigabit Ethernet (10,000 Mbps)
- In practice, only switched Ethernet is used nowadays.
- Since Ethernet and IEEE 802.3 are identical except for a minor difference many people use the terms ''Ethernet'' and ''IEEE 802.3'' interchangeably.

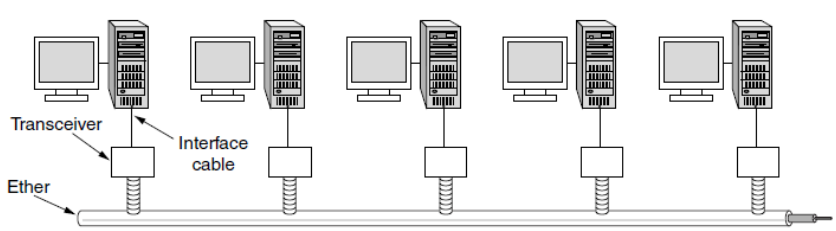
118

Classical Ethernet

- Bob Metcalfe with David Boggs designed and implemented the first local area network in 1976 in Xerox Palo Alto Lab.
- It used a single long thick coaxial cable.
- Speed 3 Mbps.
- **Ethernet** – luminiferous ether, through which electromagnetic radiation was once thought to propagate.
- Successful designed that was later drafted as standard in 1978 by Xerox, DEC, Intel with a 10 Mbps.
- In 1983 it became the IEEE 802.3 standard

119

Classic Ethernet Physical Layer



Architecture of classic Ethernet

120

Classical Ethernet

- Thick Ethernet – a thick cable. Segment could be as long as 500 m. Could be used to connect up to 100 computers.
- Thin Ethernet – BNC connectors. Segment could be no longer than 185 m. Could be used to connect up to 30 computers.
- For a large length connectivity the cables could be connected by repeaters.
- Repeater is a physical layer device that receives, amplifies, and retransmits signals in both directions.

121

Classical Ethernet

- Over each of those cables the signal was coded using Manchester encoding.
- Other restriction was that no two transceivers could be more than 2.5 km apart and no path between any two transceivers could traverse more than four repeaters.
- This limitation was impose due to the MAC protocol used.

122

MAC Sublayer Protocol (1)

The format used to send frames is shown in the figure

Bytes	8	6	6	2	0-1500	0-46	4
(a)	Preamble	Destination address	Source address	Type	Data	Pad	Check-sum
(b)	Preamble | SoF	Destination address	Source address	Length	Data	Pad	Check-sum

(a) Ethernet (DIX). (b) IEEE 802.3.

Classic Ethernet MAC Sublayer Protocol

- Format to send frames is shown in the figure of the previous slide.

1. Preamble – 8 bytes
   - 7 bytes contains 10101010 and 10101011 <- Start of Frame Delimiter (802.3).
   - The Manchester encoding of this pattern produces 10-MHz wave for 6.4 μsec – used for synchronization.
   - The last two bits indicate the start of the frame.

Classic Ethernet MAC Sublayer Protocol

2. Two addresses each 6 bytes – destination + source
   - First bit of the destination address is 0 for ordinary addresses and 1 for group addresses.
   - Group address allow multiple destinations to listen to a single address – **Multicasting**.
   - Special address consisting of all 1 is reserved for **broadcasting**.
   - Uniqueness of the addresses:
     - First 3 bytes are used for (**Organizationally Unique Identifier**)
     - Blocks of 2^{24} addresses are assigned to a manufacturer.
     - Manufacturer assigns the last 3 bytes of the address and programs the complete address into the NIC.

126

MAC Sublayer Protocol

3. Type or Length field.
   - Depending whether the frame is Ethernet or IEEE 802.3
   - Ethernet uses a Type field to tell the receiver what to do with the frame.
   - Multiple network-layer protocols may be in use at the same time on the same machine. So when Ethernet frame arrives, the operating system has to know which one to hand the frame to. The Type field specifies which process to give the frame to. E.g. 0x0800 indicates the frame contains IPv4 packet.

128

MAC Sublayer Protocol

- Length of the field could be carried as well.
- Ethernet length was determined by looking inside the data – a layer violation.
- Added another header for the **Logical Link Control** (LLC) protocol within the data. It uses 8 bytes to convey the 2 bytes of protocol type information.
- Rule: Any number greater than 0x600 can be interpreted a Type otherwise is considered to be Length.

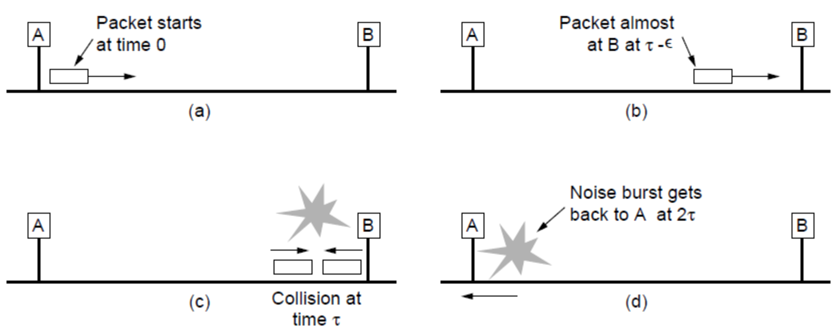
129

MAC Sublayer Protocol

4. Data Field
   - Up to 1500 bytes.
   - Minimum frame length – valid frames must be at least 64 bytes long – from destination address to checksum.
   - If data portion is less than 46 bytes the Pad field is used to fill out the frame to the minimum size.
   - Minimum frame length also serves one very important role – prevents the sender to complete transmission before the first bit arrives at the destination.

130

MAC Sublayer Protocol (2)



Collision detection can take as long as 2τ.

131

MAC Sublayer Protocol

- 10 Mbps LAN with a maximum length of 2500 m and four repeaters the round-trip time has been determined to be nearly 50 μsec in the worst case.
- Shortest allowed frame must take at least this long to transmit.
  - At 10 Mbps a bit takes 100 nsec
  - 500 bits (numbit = 10 Mbps X 100 nsec) rounded up to 512 bits = 64 bytes.

132

MAC Sublayer Protocol

4. Checksum
   - It is a 32-bit CRC of the kind that we have covered earlier.
   - Defined as a generator polynomial described in the textbook.

133

Ethernet Performance

- Examine the performance of classic Ethernet under conditions of heavy and constant load, that is, with k stations always ready to transmit.
- If each station transmits during a contention slot with probability p.
- The probability that some station acquires the channel in that slot *A* is:

$$A = kp(1-p)^{k-1}$$

- *A* is maximized for *p=1/k* with $A \to 1/e$ as $k \to \infty$.

134

Ethernet Performance

- The probability that contention interval has exactly j slots in it is $A(1-A)^{j-1}$.
- Mean number of slots per contention is:

$$\sum_{j=0}^{\infty} jA(1-A)^{j-1} = \frac{1}{A}$$

- Duration of each slot is 2t, the mean contention interval ω is = 2t/A

135

Ethernet Performance

- Assuming optimal p, the mean number of contention slots is never more than e, thus ω is at most $2\tau e \approx 5.4\tau$.

- If the mean frame takes *P* sec to transmit, when many stations have frames to send channel efficiency *E*

$$E = \frac{P}{P + 2\tau/A}$$

136

Ethernet Performance

- Here we see where the maximum cable distanced between any two stations enters into the performance figures.
- The longer the cable the longer the contention interval; This is why the Ethernet standard specifies the maximum cable length.
- It would be instructive to reformulate the equation in the previous slide in term of the frame length *F*, network bandwidth *B* and the cable length *L*, speed of signal propagation *c*, for the optimal case *e* contention slots per frame.

137

Ethernet Performance

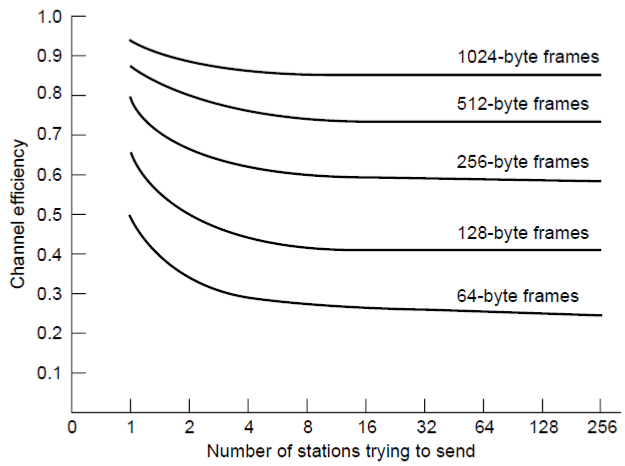
- P = F/B the equation becomes:

$$E = \frac{1}{1 + 2BLe/cF}$$

- When the term $2BLe/cF$ >> 0 the network efficiency becomes very low.
  - Increasing BL; Bandwidth and/or Length of the cable reduces the efficiency.
  - This is contrary to the design criteria to have largest possible bandwidth and longest connections.
  - Classical Ethernet will not be able to provide this.

138

Ethernet Performance



Efficiency of Ethernet at 10 Mbps with 512-bit slot times.

Ethernet Performance

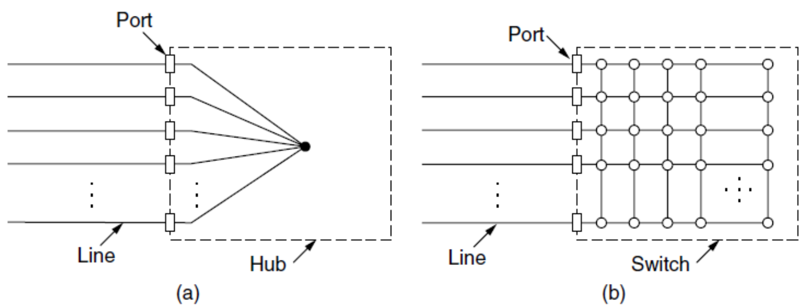
- The theoretical result that Ethernet can not work that efficiently is flowed due to several reasons:
  - Poison distribution of the traffic is not realistic.
  - Research focuses on only several "interesting" cases.
  - Practical results show otherwise that the Ethernet works.

Switched Ethernet

- Wiring was changed from a long cable architecture to a more complex architecture:
  - Each station has a dedicated cable running to a central **hub**. (Fig (a) in the next slide).
  - Adding and removing a station become much easier.
  - Cable length was reduced to 100 m for telephone twisted pair wires and to 200 hundred if Category 5 cable was used.
  - Hubs do not increase capacity – they are equivalent to the single long cable of classic Ethernet.
    - As more stations were added the performance of each station degraded.

141

Switched Ethernet (1)



(a) Hub. (b) Switch.

142

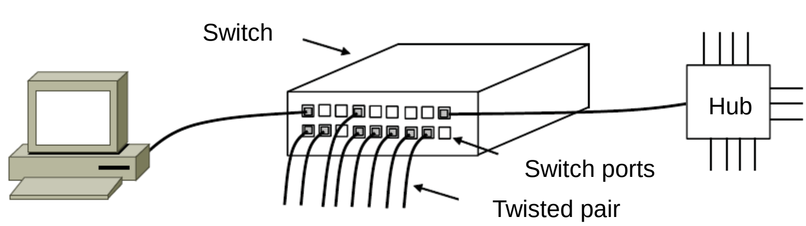
Switched Ethernet

- One could solve this problem by increasing the speech of the basic Ethernet from 1 Mbps to 10 Mbps, 100 Mbps or even 1 Gbps.
- However, multimedia applications requires even higher bandwidths.

- **Switch** is the solution.
  - Switch must be able to determine which frame goes to what station.
  - Security benefits
  - No collision can occur.

143

Switched Ethernet (2)



An Ethernet switch.

144

Fast Ethernet

Name	Cable	Max. segment	Advantages
100Base-T4	Twisted pair	100 m	Uses category 3 UTP
100Base-TX	Twisted pair	100 m	Full duplex at 100 Mbps (Cat 5 UTP)
100Base-FX	Fiber optics	2000 m	Full duplex at 100 Mbps; long runs

The original fast Ethernet cabling.

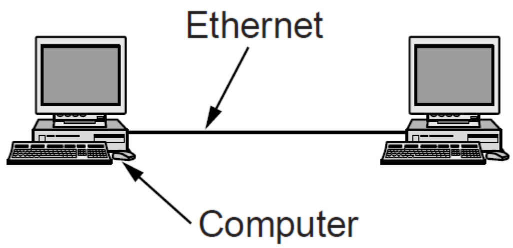
145

GigaBit Ethernet

- After the standard for Fast Ethernet was adopted the work for yet even faster standard started: GigaBit Ethernet
- Goals:
  - Increase performance ten fold over Fast Ethernet.
  - Maintain compatibility with both Classical and Fast Ethernet.
  - Unacknowledged datagram service with both unicast and broadcast.
  - Use the same 48-bit addressing scheme already in use,
  - Maintain the same frame format including minimum and maximum sizes.

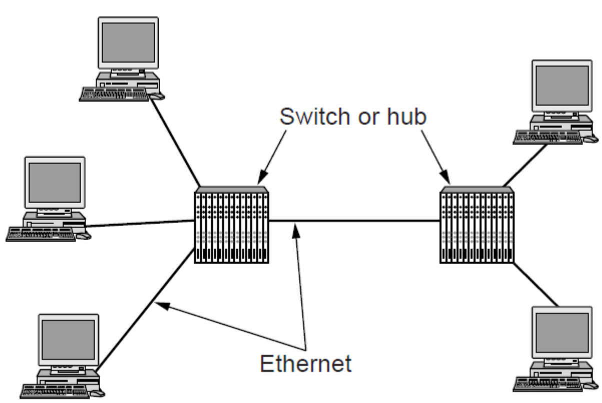
146

Gigabit Ethernet (1)



A two-station Ethernet

Gigabit Ethernet (2)



A two-station Ethernet

Gigabit Ethernet (3)

Name	Cable	Max. segment	Advantages
1000Base-SX	Fiber optics	550 m	Multimode fiber (50, 62.5 microns)
1000Base-LX	Fiber optics	5000 m	Single (10 μ) or multimode (50, 62.5 μ)
1000Base-CX	2 Pairs of STP	25 m	Shielded twisted pair
1000Base-T	4 Pairs of UTP	100 m	Standard category 5 UTP

Gigabit Ethernet cabling.

149

10 Gigabit Ethernet

Name	Cable	Max. segment	Advantages
10GBase-SR	Fiber optics	Up to 300 m	Multimode fiber (0.85μ)
10GBase-LR	Fiber optics	10 km	Single-mode fiber (1.3μ)
10GBase-ER	Fiber optics	40 km	Single-mode fiber (1.5μ)
10GBase-CX4	4 Pairs of twinax	15 m	Twinaxial copper
10GBase-T	4 Pairs of UTP	100 m	Category 6a UTP

Gigabit Ethernet cabling

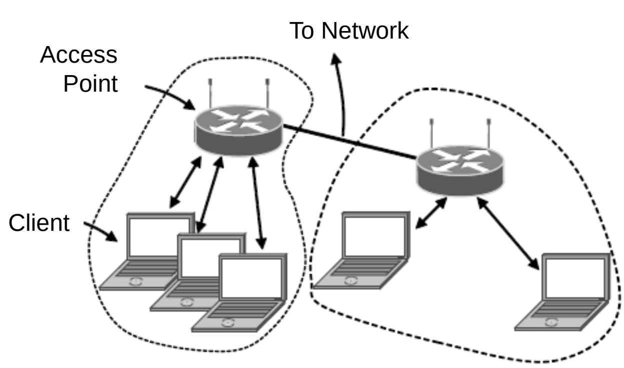
150

Wireless Lans

- 802.11 architecture and protocol stack
- 802.11 physical layer
- 802.11 MAC sublayer protocol
- 802.11 frame structure
- Services

151

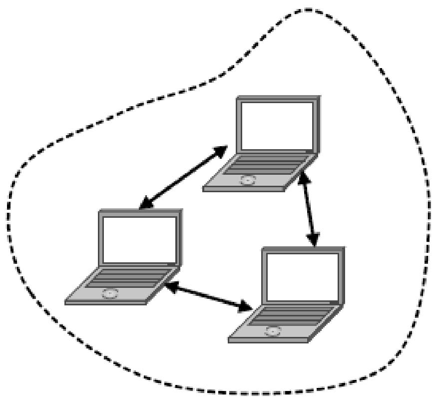
802.11 Architecture and Protocol Stack (1)



802.11 architecture – infrastructure mode

152

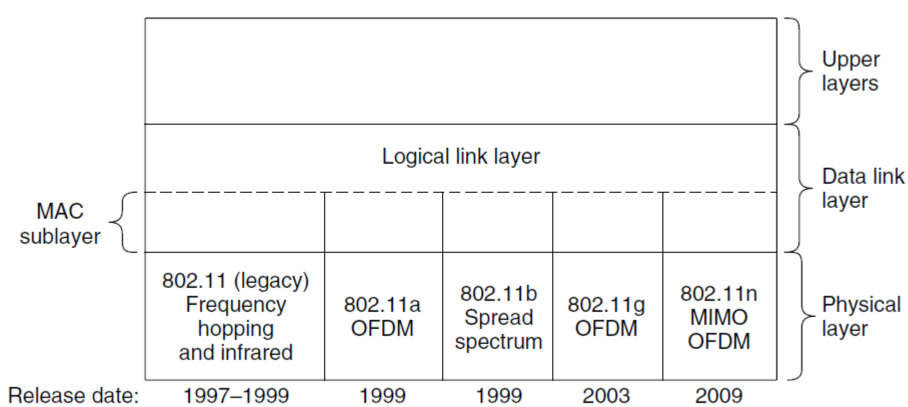
802.11 Architecture and Protocol Stack (2)



802.11 architecture – ad-hoc mode

153

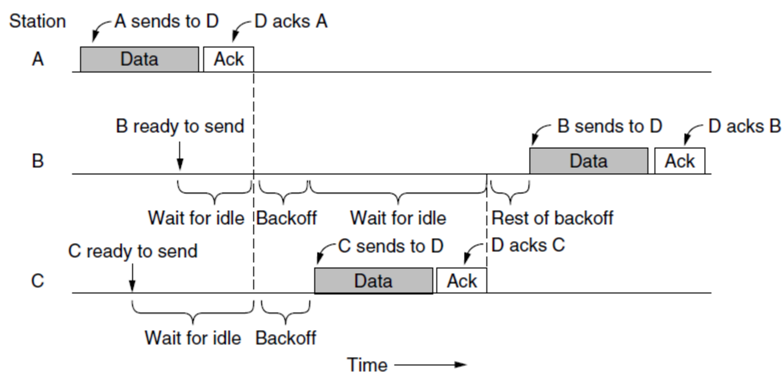
802.11 Architecture and Protocol Stack (3)



Part of the 802.11 protocol stack.

154

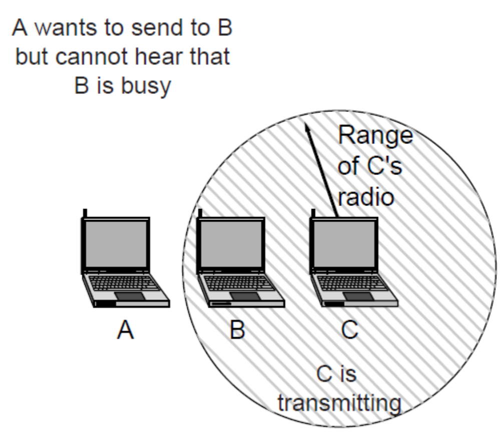
The 802.11 MAC Sublayer Protocol (1)



Sending a frame with CSMA/CA.

155

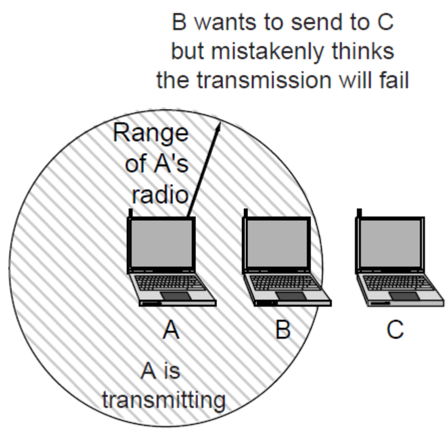
The 802.11 MAC Sublayer Protocol (2)



The hidden terminal problem.

156

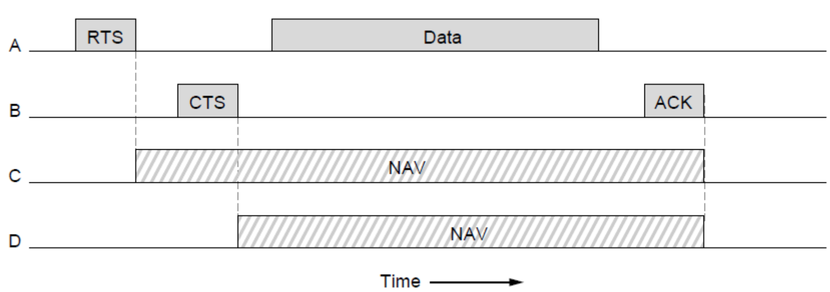
The 802.11 MAC Sublayer Protocol (3)



The exposed terminal problem.

157

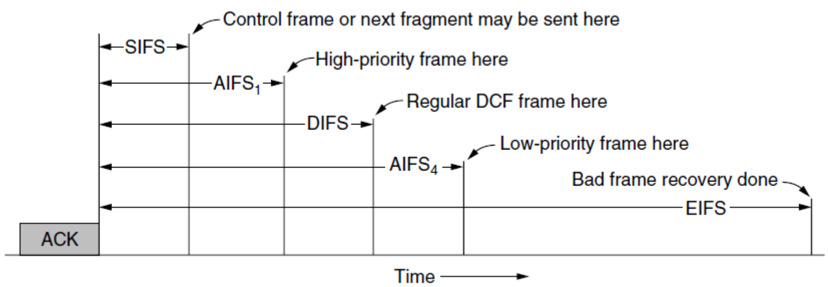
The 802.11 MAC Sublayer Protocol (4)



The use of virtual channel sensing using CSMA/CA.

158

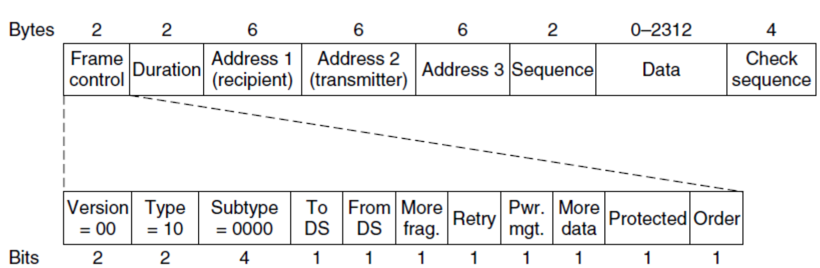
The 802.11 MAC Sublayer Protocol (5)



Interframe spacing in 802.11

159

802.11 Frame Structure



Format of the 802.11 data frame

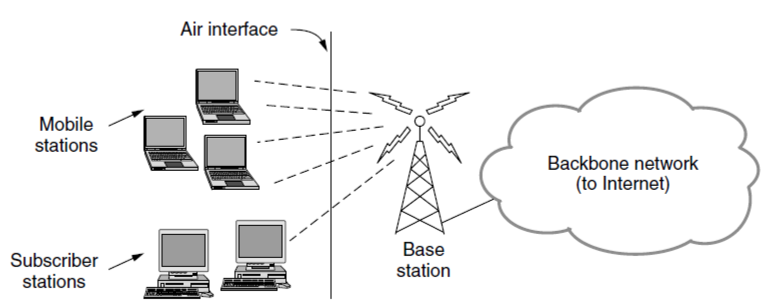
160

Broadband Wireless

- Comparison of 802.16 with 802.11, 3G
- 802.16 architecture and protocol stack
- 802.16 physical layer
- 802.16 frame structure

161

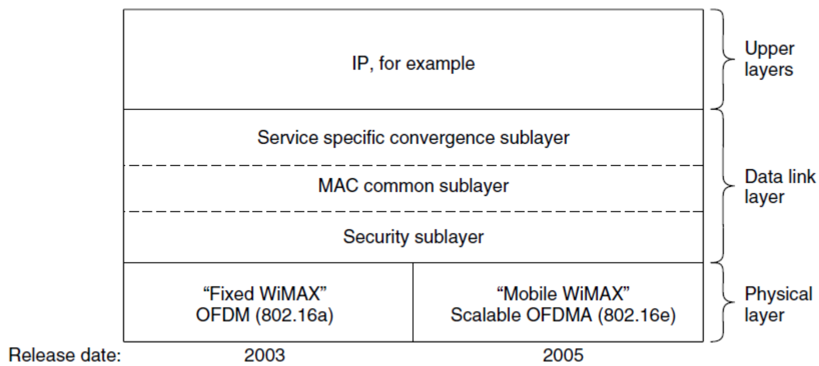
Comparison of 802.16 with 802.11 and 3G



The 802.16 architecture

162

802.16 Architecture and Protocol Stack

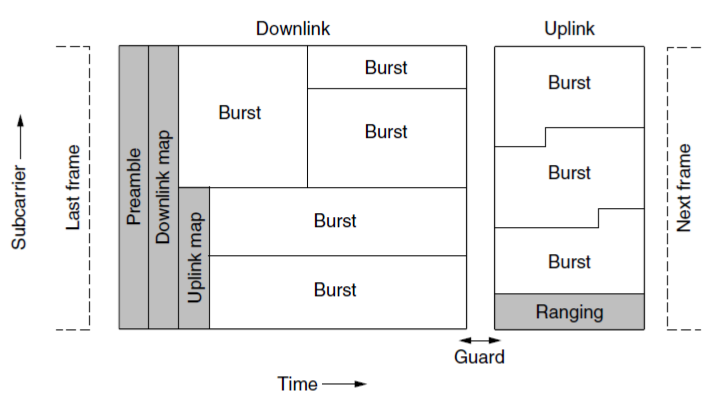


The 802.16 protocol stack

163

802.16 Physical Layer

Frames structure for OFDMA with time division duplexing.



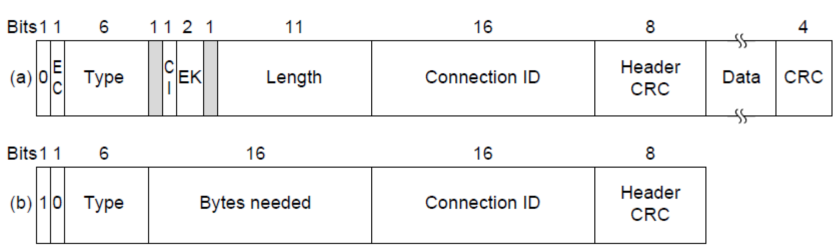
164

802.16 MAC Sublayer Protocol

Classes of service

1. Constant bit rate service.
2. Real-time variable bit rate service.
3. Non-real-time variable bit rate service.
4. Best-effort service.

802.16 Frame Structure



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

Data Link Layer Switching

- Uses of bridges
- Learning bridges
- Spanning tree bridges
- Repeaters, hubs, bridges, switches, routers, and gateways
- Virtual LANs

167

Uses of bridges

- An Organization may have different departments having their own LAN, and later, there is a need for interaction.
  - Multiple LANs come into existence due to the autonomy of their owners.
- The organization may be geographically spread over several buildings separated by considerable distances.
  - It may be cheaper to have separate LANs in each building and connect them with bridges and a few long-distance fiber optic links than to run all the cables to a single central switch.
- It may be necessary to split what is logically a single LAN into separate LANs (connected by bridges) to accommodate the load.
  - There are more computers than ports on any Ethernet hub and more stations than allowed on a single classic Ethernet.

168

Uses of bridges

- Even if it were possible to wire all the workstations together, putting more stations on an Ethernet hub or classic Ethernet would not add capacity.
  - All of the stations share the same, fixed amount of bandwidth. The more stations there are, the less average bandwidth per station.
- However, two separate LANs have twice the capacity of a single LAN.
- Bridges let the LANs be joined together while keeping this capacity.
  - The key is not to send traffic onto ports where it is not needed, so that each LAN can run at full speed.
  - This behavior also increases reliability, since on a single LAN a defective node that keeps outputting a continuous stream of garbage can clog up the entire LAN.
  - By deciding what to forward and what not to forward, bridges act like fire doors in a building.

169

Uses of bridges

- To make these benefits easily available, ideally bridges should be completely transparent.
  - It should be possible to go out and buy bridges, plug the LAN cables into the bridges, and have everything work perfectly, instantly.
  - There should be no hardware changes required, no software changes required, no setting of address switches, no downloading of routing tables or parameters, nothing at all.
  - Just plug in the cables and walk away.
- Furthermore, the operation of the existing LANs should not be affected by the bridges at all.
- As far as the stations are concerned
  - There should be no observable difference whether or not they are part of a bridged LAN.
  - It should be as easy to move stations around the bridged LAN as it is to move them around a single LAN.

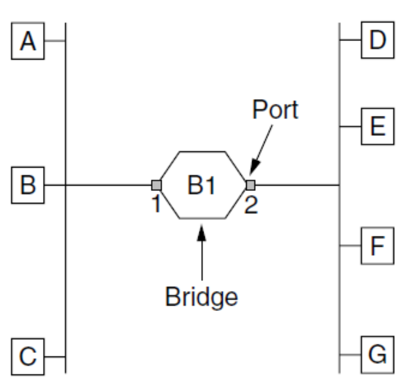
170

Learning Bridges

- Surprisingly enough, it is actually possible to create bridges that are transparent.
- Two algorithms are used:
  - a backward learning algorithm to stop traffic being sent where it is not needed; and
  - a spanning tree algorithm to break loops that may be formed when switches are cabled together willy-nilly.

171

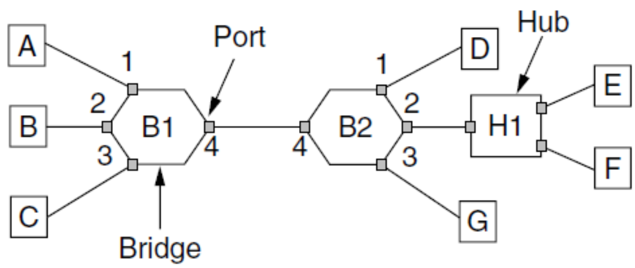
Learning Bridges



Bridge connecting two multidrop LANs

172

Learning Bridges



Bridges (and a hub) connecting seven point-to-point stations.

173

Learning Bridges

- A big (hash) table is maintained inside the bridge to know about the port numbers of all the destination.
- When the bridges are first plugged in, all the hash tables are empty.
- None of the bridges know where any of the destinations are, so they use a flooding algorithm:
  - every incoming frame for an unknown destination is output on all the ports to which the bridge is connected except the one it arrived on.
- As time goes on, the bridges learn where destinations are. Once a destination is known, frames destined for it are put only on the proper port; they are not flooded.
- The algorithm used by the bridges is backward learning.

174

Learning Bridges

- The topology can change as machines and bridges are powered up and down and moved around.
- To handle dynamic topologies, whenever a hash table entry is made, the arrival time of the frame is noted in the entry.
- Whenever a frame whose source is already in the table arrives, its entry is updated with the current time.
- Thus, the time associated with every entry tells the last time a frame from that machine was seen.
- Periodically, a process in the bridge scans the hash table and purges all entries more than a few minutes old.
- In this way, if a computer is unplugged from its LAN, moved around the building, and plugged in again somewhere else, within a few minutes it will be back in normal operation, without any manual intervention.
- This algorithm also means that if a machine is quiet for a few minutes, any traffic sent to it will have to be flooded until it next sends a frame itself.

175

Learning Bridges

- The routing procedure for an incoming frame depends on the port it arrives on (the source port) and the address to which it is destined (the destination address).
- The procedure is as follows.
  - If the port for the destination address is the same as the source port, discard the frame.
  - If the port for the destination address and the source port are different, forward the frame on to the destination port.
  - If the destination port is unknown, use flooding and send the frame on all ports except the source port.
- You might wonder whether the first case can occur with point-to-point links. The answer is that it can occur if hubs are used to connect a group of computers to a bridge.

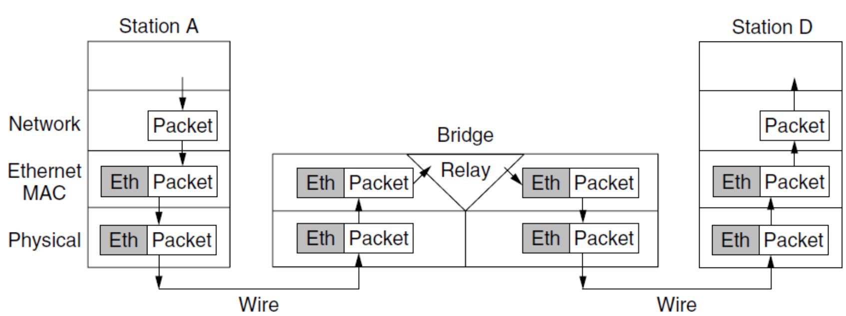
176

Learning Bridges

- As each frame arrives, this algorithm must be applied, so it is usually implemented with special-purpose VLSI chips.
- The chips do the lookup and update the table entry, all in a few microseconds.
- Because bridges only look at the MAC addresses to decide how to forward frames, it is possible to start forwarding as soon as the destination header field has come in, before the rest of the frame has arrived (provided the output line is available, of course).
- This design reduces the latency of passing through the bridge, as well as the number of frames that the bridge must be able to buffer.
- It is referred to as cut-through switching or wormhole routing and is usually handled in hardware.

177

Learning Bridges



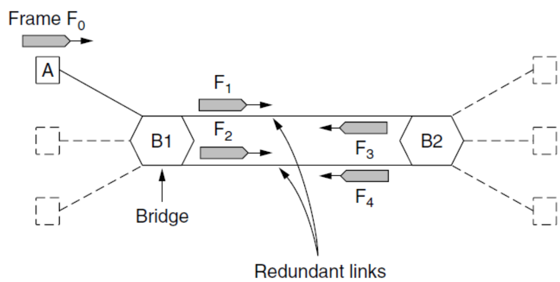
Protocol processing at a bridge.

- Note that a bridge with k ports will have k instances of MAC and physical layers. The value of k is 2 for our simple example.

178

Spanning Tree Bridges

- To increase reliability, redundant links can be used between bridges.
- This design ensures that if one link is cut, the network will not be partitioned into two sets of computers that cannot talk to each other.



Bridges with two parallel links

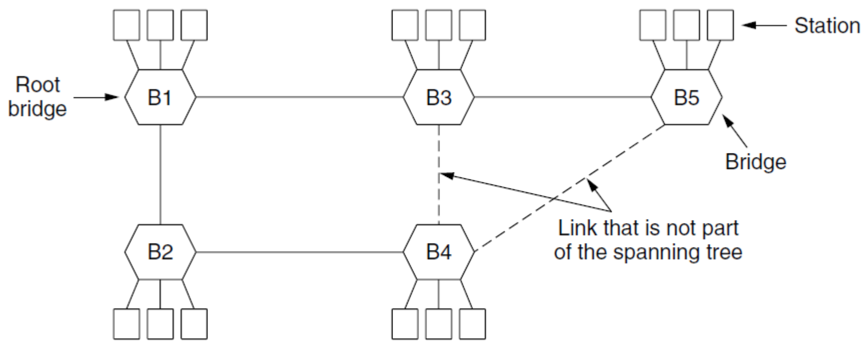
179

Spanning Tree Bridges

- However, this redundancy introduces some additional problems because it creates loops in the topology.
- An example of these problems can be seen by looking at how a frame sent by A to a previously unobserved destination is handled in Fig. of previous slide.
- The solution to this difficulty is for the bridges to communicate with each other and overlay the actual topology with a spanning tree that reaches every bridge.
- In effect, some potential connections between bridges are ignored in the interest of constructing a fictitious loop-free topology that is a subset of the actual topology.

180

Spanning Tree Bridges (2)



A spanning tree connecting five bridges. The dotted lines are links that are not part of the spanning tree.

Spanning Tree Bridges

- This topology can be thought of as a graph in which the bridges are the nodes and the point-to-point links are the edges.
- The graph can be reduced to a spanning tree, which has no cycles by definition, by dropping the links shown as dashed lines in the Figure.
- Using this spanning tree, there is exactly one path from every station to every other station.
- Once the bridges have agreed on the spanning tree, all forwarding between stations follows the spanning tree.
- Since there is a unique path from each source to each destination, loops are impossible.
- To build the spanning tree, the bridges run a distributed algorithm.

Spanning Tree Bridges

- Each bridge periodically broadcasts a configuration message out all of its ports to its neighbors and processes the messages it receives from other bridges, as described next.
  - The bridges must first choose one bridge to be the root of the spanning tree.
  - Next, a tree of shortest paths from the root to every bridge is constructed.
  - To find these shortest paths, bridges include the distance from the root in their configuration messages.
  - Each bridge remembers the shortest path it finds to the root.
  - The bridges then turn off ports that are not part of the shortest path.
- Even after the spanning tree has been established, the algorithm continues to run during normal operation to automatically detect topology changes and update the tree.

Spanning Tree Bridges

- The algorithm for constructing the spanning tree was invented by Radia Perlman.
- Her job was to solve the problem of joining LANs without loops.
- She was given a week to do it, but she came up with the idea for the spanning tree algorithm in a day.
- Fortunately, this left her enough time to write it as a poem (Perlman, 1985):

Poem by Radia Perlman (1985) Algorithm for Spanning Tree (1)

I think that I shall never see
A graph more lovely than a tree.
A tree whose crucial property
Is loop-free connectivity.
A tree which must be sure to span.
So packets can reach every LAN.
. . .

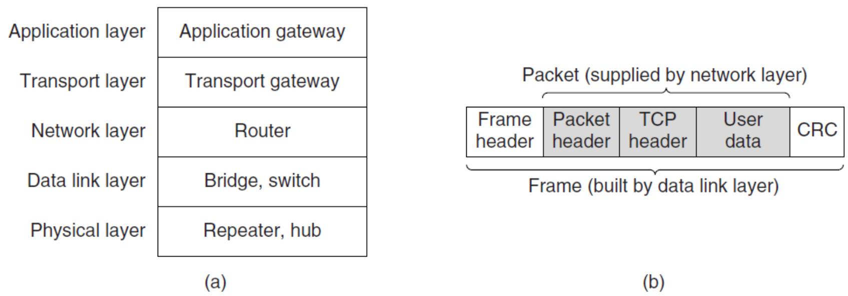
185

Poem by Radia Perlman (1985) Algorithm for Spanning Tree (2)

. . .
First the Root must be selected
By ID it is elected.
Least cost paths from Root are traced
In the tree these paths are placed.
A mesh is made by folks like me
Then bridges find a spanning tree.

186

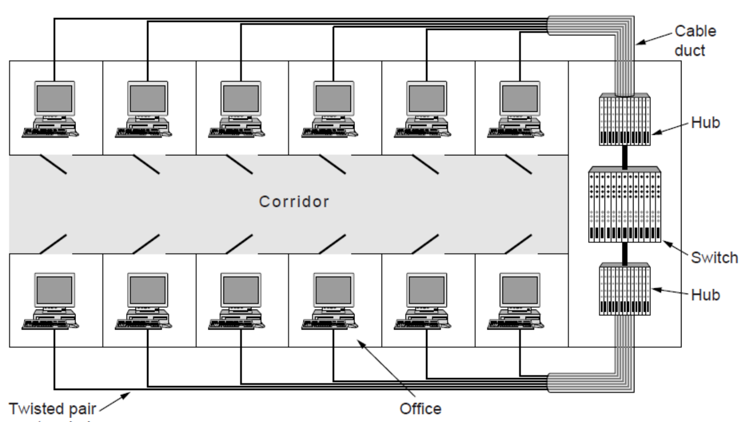
Repeaters, Hubs, Bridges, Switches, Routers, and Gateways



(a) Which device is in which layer.
(b) Frames, packets, and headers.

187

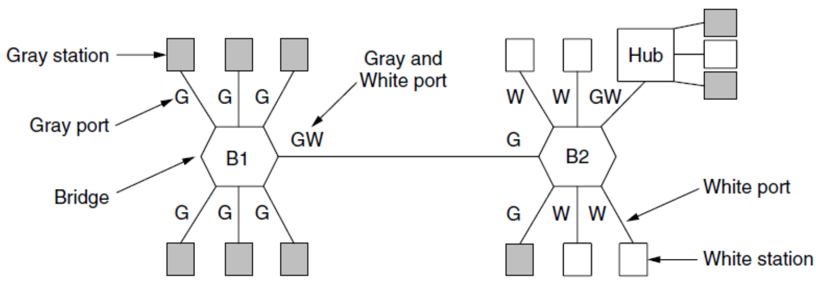
Virtual LANs (1)



A building with centralized wiring using hubs and a switch.

188

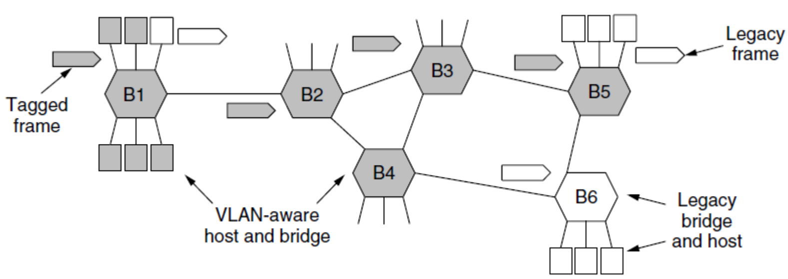
Virtual LANs (2)



Two VLANs, gray and white, on a bridged LAN.

189

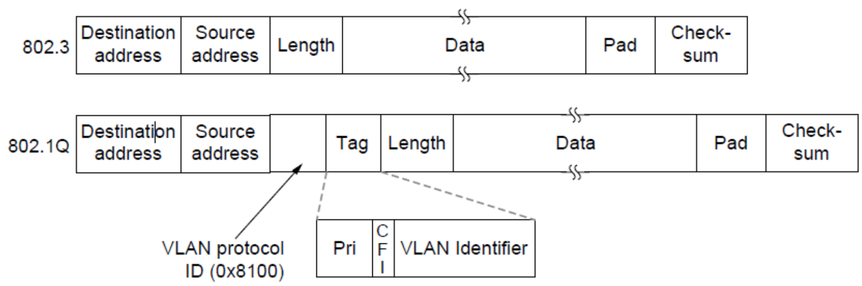
The IEEE 802.1Q Standard (1)



Bridged LAN that is only partly VLAN-aware. The shaded symbols are VLAN aware. The empty ones are not.

190

The IEEE 802.1Q Standard (2)



The 802.3 (legacy) and 802.1Q Ethernet frame formats.

The End