Computer Networks

Mohammed El-Hajj

Jacobs University Bremen

October 10, 2021

JACOBS
UNIVERSITY

Course Content

1. Introduction
2. Fundamental Networking Concepts
3. Local Area Networks (IEEE 802)
4. Internet Network Layer (IPv4, IPv6)
5. Internet Routing (RIP, OSPF, BGP)
6. Internet Transport Layer (UDP, TCP)
7. Firewalls and Network Address Translators
8. Domain Name System (DNS)
9. Abstract Syntax Notation 1 (ASN.1)
10. External Data Representation (XDR)
11. Augmented Backus Naur Form (ABNF)
12. Electronic Mail (SMTP, IMAP)
13. Document Access and Transfer (HTTP, FTP)

Part 3: Local Area Networks (IEEE 802)

Section 11: Local Area Networks Overview

LAN Overview

A Local area Network is the data communication system that allows a number of independent devices to communicate directly with each other in a limited geographical area.

LANs are dominated by four architecture:

- Ethernet
- Token Bus
- Token Ring
- Fiber distributed data interface

Token Bus, Token Ring and Ethernet are standards of IEEE and a part of project 802.

IEEE 802 Overview

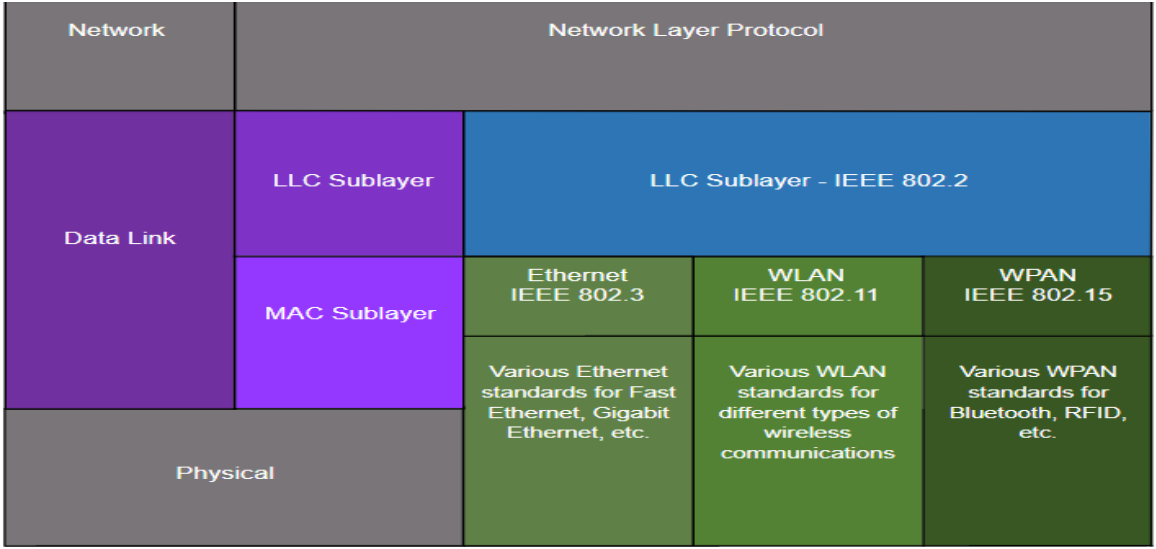
The computer society of the IEEE started a project, called 802 to set up standards to enable intercommunication between equipment from a variety of manufacturers.

Project 802 does not seek to replace any part of the OSI model.

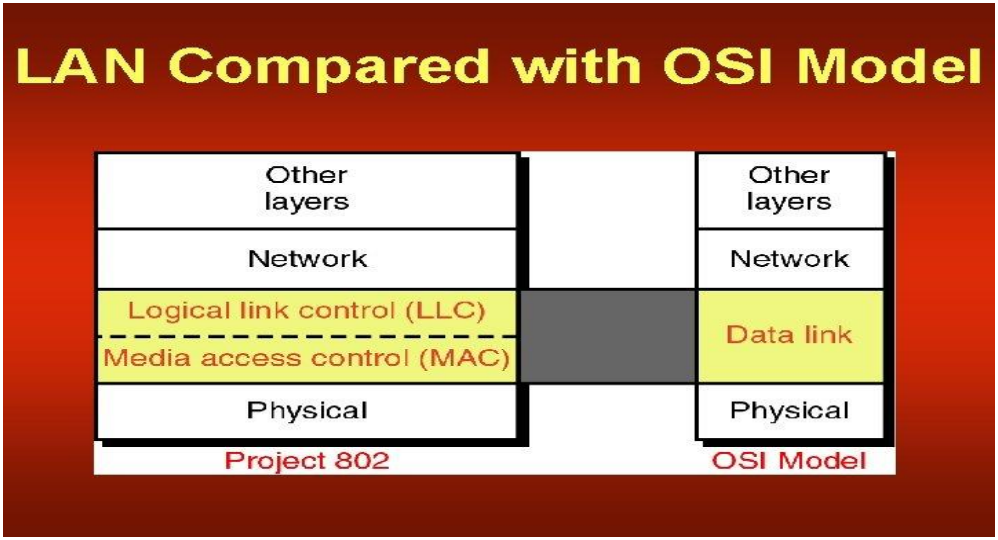
The IEEE has subdivided the data link layer into sub layers:

- Logical link control(LLC)
- Medium access control(MAC)

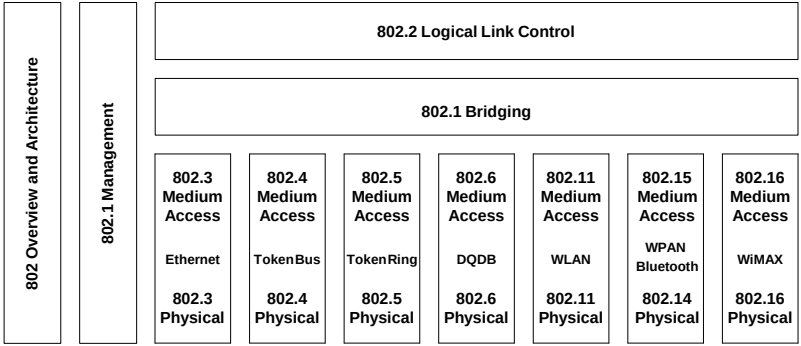
IEEE 802 Overview – Data Link sub layers



OSI Compared to 802 project

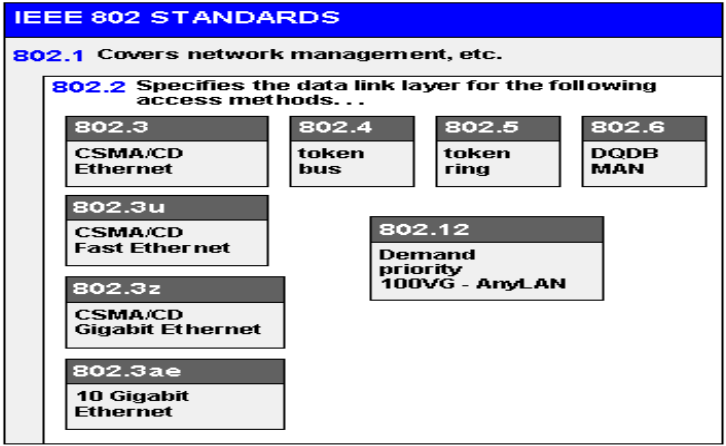


IEEE 802 Overview

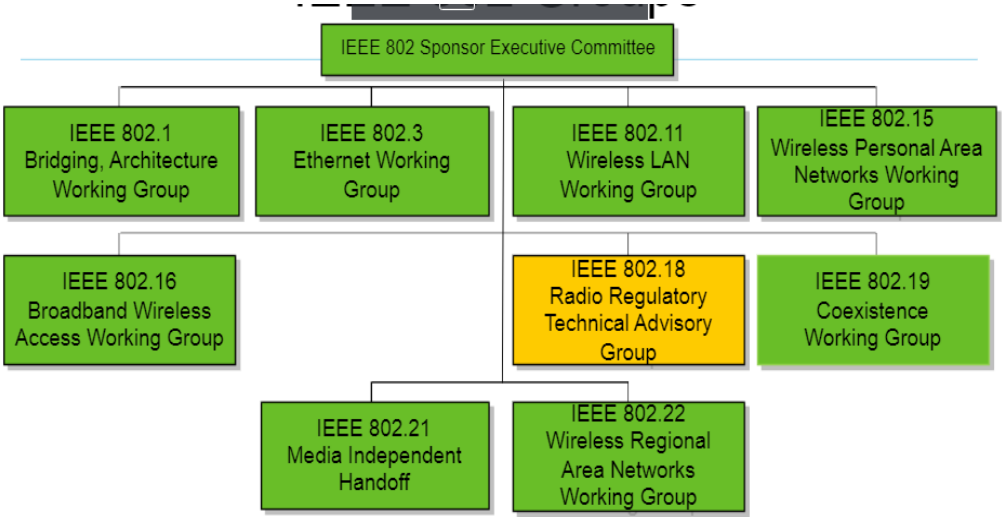


- IEEE 802 standards are developed since the early 1980s
- Dominating technology in local area networks (LANs)

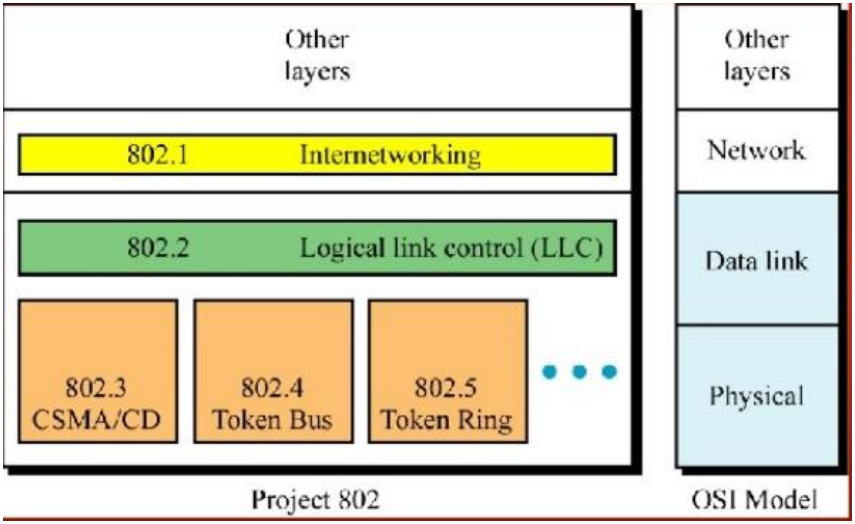
IEEE 802 Overview



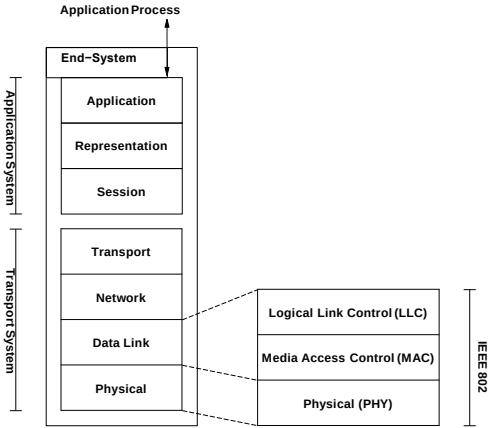
IEEE 802 Overview



IEEE 802 project



IEEE 802 Layers in the OSI Model

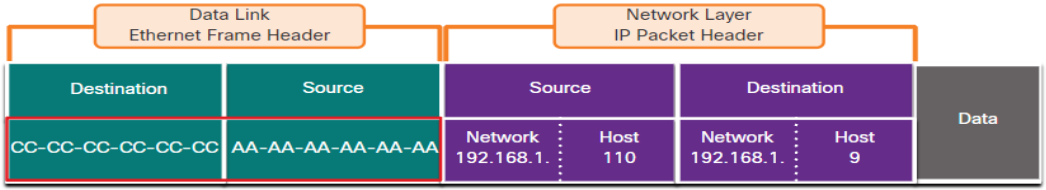


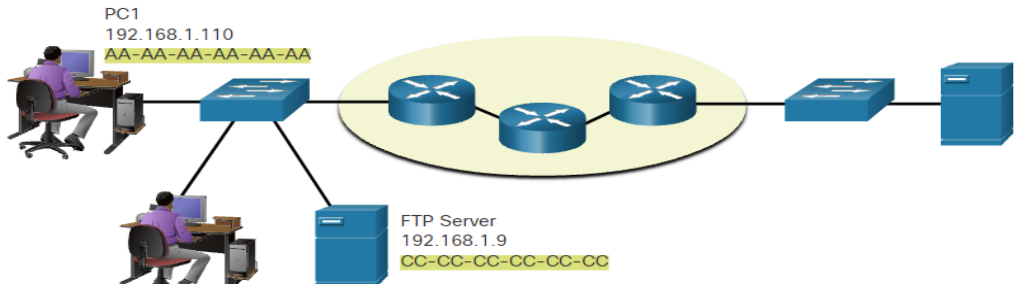
- The Logical Link Control layer provides a common service interface for all IEEE 802 protocols
- The Medium Access Control layer defines the method used to access the transmission media used
- The Physical layer defines the physical properties for the various transmission media that can be used with a certain IEEE 802.x protocol

IEEE 802 Addresses

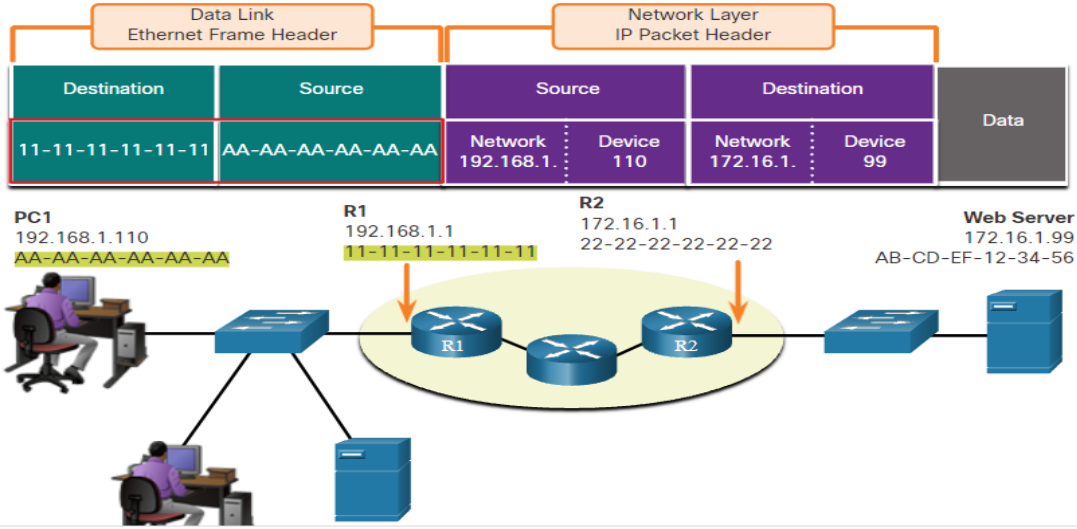
- IEEE 802 addresses (sometimes called MAC addresses or meanwhile also EUI-48 addresses) are 6 octets (48 bit) long
- The common notation is a sequence of hexadecimal numbers with the bytes separated from each other using colons or hyphens (00:D0:59:5C:03:8A or 00-D0-59-5C-03-8A)
- The highest bit indicates whether it is a *unicast* address (0) or a *multicast* address (1). The second highest bit indicates whether it is a *local* (1) or a *global* (0) address
- The *broadcast* address, which represents all stations within a broadcast domain, is
  FF-FF-FF-FF-FF-FF
- Globally unique addresses are created by vendors who apply for a number space delegation by the IEEE

IEEE 802 Addresses in Same Network





IEEE 802 Addresses in remote Network



Section 12: Ethernet (IEEE 802.3)

IEEE 802.3 (Ethernet)

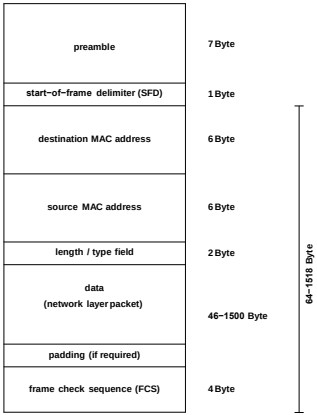
Year	Achievement
1976	Original Ethernet paper published
1990	10 Mbps Ethernet over twisted pair (10BaseT)
1995	100 Mbps Ethernet
1998	1 Gbps Ethernet
2002	10 Gbps Ethernet
2010	100 Gbps Ethernet
2017	400 Gbps Ethernet
2020+	1.6 Tbps Ethernet (predicted)

- Link aggregation allows to “bundle” links, e.g., four 10 Gbps links can be bundled to perform like a single 40 Gbps link

IEEE 802.3 (Ethernet)-LAN Technology Specifications

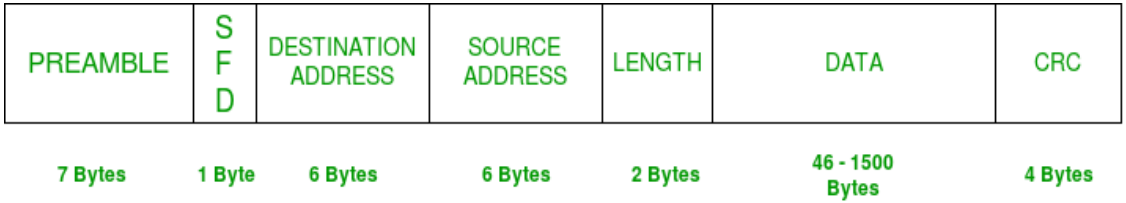
Name	IEEE Standard	Data Rate	Media Type	Maximum Distance
Ethernet	802.3	10 Mbps	10Base-T	100 meters
Fast Ethernet/ 100Base-T	802.3u	100 Mbps	100Base-TX 100Base-FX	100 meters 2000 meters
Gigabit Ethernet/ GigE	802.3z	1000 Mbps	1000Base-T 1000Base-SX 1000Base-LX	100 meters 275/550 meters 550/5000 meters
10 Gigabit Ethernet	IEEE 802.3ae	10 Gbps	10GBase-SR 10GBase-LX4 10GBase-LR/ER 10GBase-SW/LW/EW	300 meters 300m MMF/ 10km SMF 10km/40km 300m/10km/40km

IEEE 802.3 Frame Format



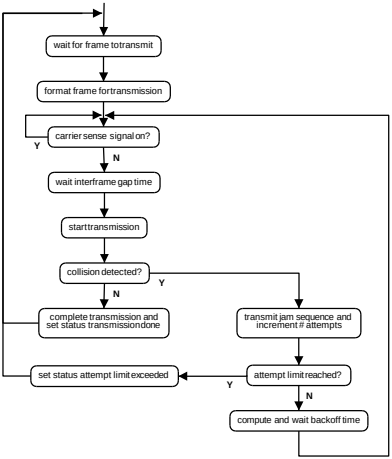
- Classic Ethernet used CSMA/CD and a shared bus
- Today's Ethernet uses a star topology with full duplex links
- Jumbo frames with sizes up to 9000 bytes can be used on dedicated links to improve throughput
- Interface cards capable to segment large chunks of data (e.g., 64k) into a sequence of frames (large segment offload, LSO) improve throughput on the sending side

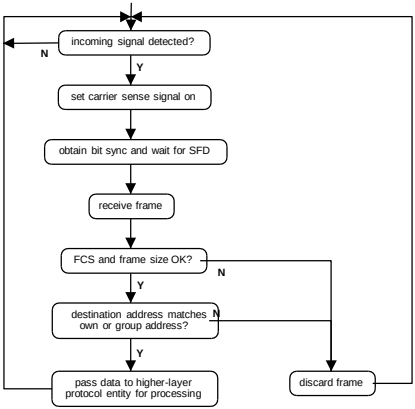
IEEE 802.3 Frame Format



IEEE 802.3 ETHERNET Frame Format

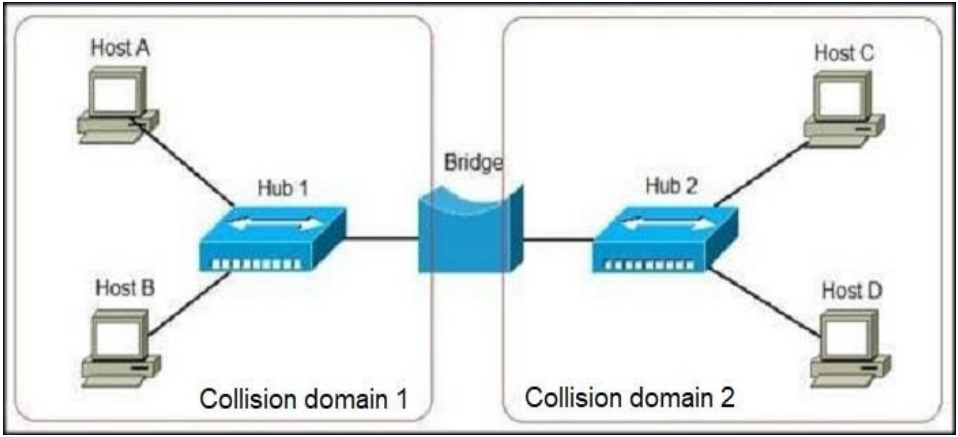
Transmitting and Receiving IEEE 802.3 Frames



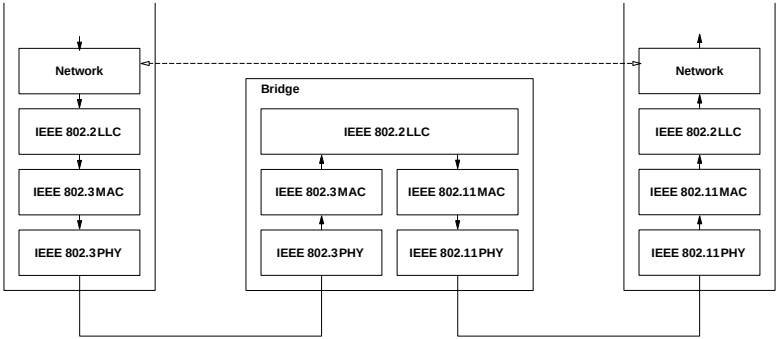


Section 13: Bridges (IEEE 802.1)

Bridged IEEE 802 Networks

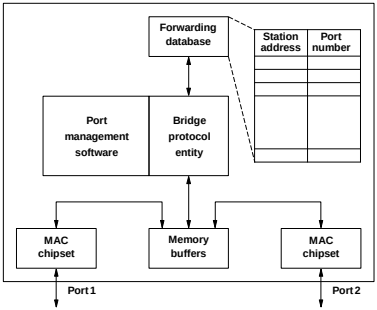


IEEE 802 Bridges



- *Source Routing Bridges*: Sender routes the frame through the bridged network
- *Transparent Bridges*: Bridges are transparent to senders and receivers

Transparent Bridges (IEEE 802.1D)



- Lookup an entry with a matching destination address in the forwarding database and forward the frame to the associated port.
- If no matching entry exists, forward the frame to all outgoing ports except the port from which the frame was received (flooding).

Backward Learning and Flooding

1. The forwarding database is initially empty.
2. Whenever a frame is received, add an entry to the forwarding database (if it does not yet exist) using the frame's source address and the incoming port number.
3. Reinitialize the timer attached to the forwarding base entry for the received frame.
4. Lookup the destination address in the forwarding database.
5. If found, forward the frame to the identified port. Otherwise, send the frame to all ports (except the one from which it was received).
6. Periodically remove entries from the forwarding table whose timer has expired.

- Aging of unsused entries reduces forwarding table size and allows bridges to adapt to topology changes.
- Backward learning and flooding requires a cycle free topology.

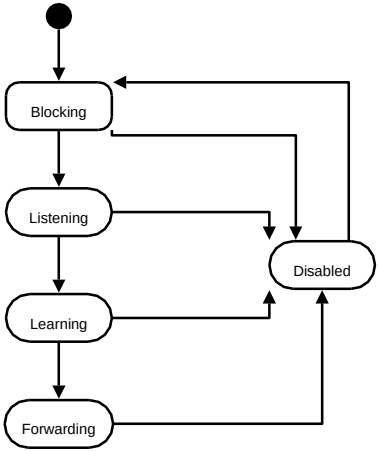
Spanning Tree

1. The root of the spanning tree is selected (root bridge). The root bridge is the bridge with the highest priority and the smallest bridge address.
2. The costs for all possible paths from the root bridge to the various ports on the bridges is computed (root path cost). Every bridge determines which root port is used to reach the root bridge at the lowest costs.
3. The designated bridge is determined for each segment. The designated bridge of a segment is the bridge which connects the segment to the root bridge with the lowest costs on its root port. The ports used to reach designated bridges are called designated ports.
4. All ports are blocked which are not designated ports or root ports. The resulting active topology is a spanning tree.

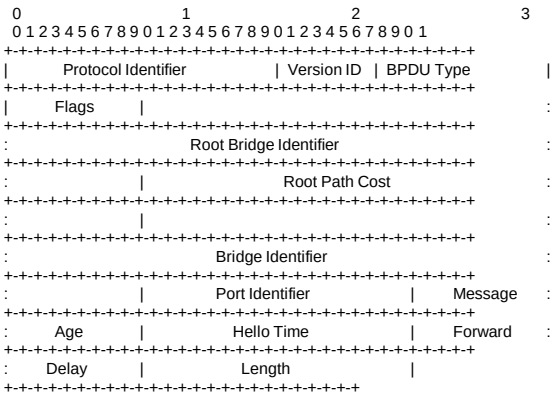
Port States

- Blocking: A port in the blocking state does not participate in frame forwarding.
- Listening: A port in the transitional listening state has been selected by the spanning tree protocol to participate in fame forwarding.
- Learning: A port in the transitional learning state is preparing to participate in frame forwarding.
- Forwarding: A port in the forwarding state forwards frames.
- Disabled: A port in the disabled state does not participate in frame forwarding or the operation of spanning tree protocol.

Port State Transitions



Bridge Protocol PDUs



- BPDUs are sent periodically over all ports (including blocked ports) to a special multicast address
- BPDUs are usually encapsulated in an LLC header (see below)
- Failure to transmit or deliver BPDUs may result in briding errors

Broadcast Domains

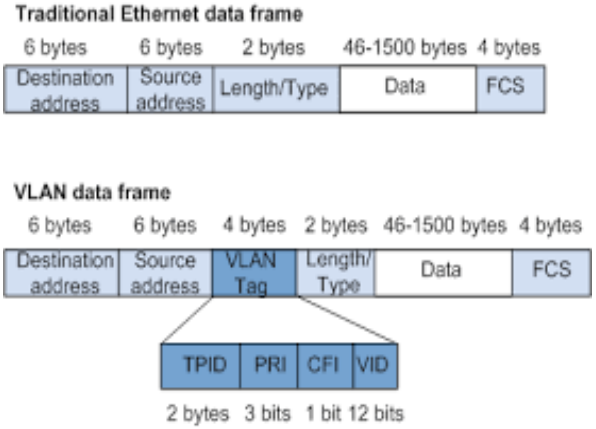
- A bridged LAN defines a single *broadcast domain*:
  - All frames send to the broadcast address are forwarded on all links in the bridged networks.
  - Broadcast traffic can take a significant portion of the available bandwidth.
  - Devices running not well-behaving applications can cause *broadcast storms*.
  - Bridges may flood frames if the MAC address cannot be found in the forwarding table.
- It is desirable to reduce the size of broadcast domains in order to separate traffic in a large bridged LAN.
- Do not confuse a broadcast domain with a collision domain, i.e., segments on which media access collisions can occur.

Section 14: Virtual Local Area Networks (IEEE 802.1Q)

IEEE 802.1Q Virtual LANs

- VLANs provide a separation of logical LAN topologies from physical LAN topologies
- VLANs are identified by a VLAN identifier (1..4094)
- VLANs allow to separate the traffic on an IEEE 802 network
- A station only receives frames belonging to that VLANs it is a member of
- VLANs can reduce the network load:
  1. VLANs often cover only a certain part of the underlying physical topology
  2. Frames that are targeted to all stations (broadcasts) will only be delivered to the stations connected to the VLAN
- Stations can be a member of multiple VLANs simultaneously (important for shared servers)

IEEE 802.1Q Tagged Frames



- The tag protocol identifier indicates a tagged frame
- Tagged 802.3 frames are 4 bytes longer than original 802.3 frames
- Tagged frames should only appear on links that are VLAN aware

VLAN Membership

- Bridge ports can be assigned to VLANs in different ways:
  - Ports are administratively assigned to VLANs (port-based VLANs)
  - MAC addresses are administratively assigned to VLANs (MAC address-based VLANs)
  - Frames are assigned to VLANs based on the payload contained in the frames (protocol-based VLANs)
  - Members of a certain multicast group are assigned to VLAN (multicast group VLANs)
- The Generic Attribute Registration Protocol (GARP) can (among other things) propagate VLAN membership information.

IEEE 802.1 Q-in-Q Tagged Frames (IEEE 802.1ad)

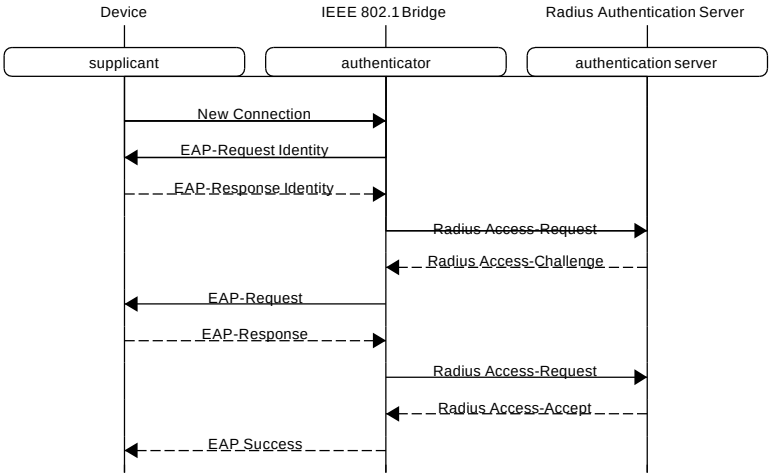
- With two tags, a theoretical limit of $4096 \cdot 4096 = 16777216$ different tags can be achieved (larger tag space)
- A tag stack allows bridges to easily modify the tags since bridges can easily "push" or "pop" tags
- A tag stack creates a mechanism for ISPs to encapsulate customer single-tagged 802.1Q traffic with a single outer tag; the outer tag is used to distinguish traffic from different customers
- Q-in-Q frames are convenient means of constructing layer 2 tunnels, or applying quality of service (QoS) policies
- 802.1ad is upward compatible with 802.1Q and although 802.1ad is limited to two tags, there is no ceiling in the standard allowing for future growth
- Double tagging is relatively easy to add to existing products

Section 15: Port Access Control (IEEE 802.1X)

IEEE 802.1X Port Access Control

- Port-based network access control grants access to a switch port based on the identity of the connected machine.
- The components involved in 802.1X:
  - The *supplicant* runs on a machine connecting to a bridge and provides authentication information.
  - The *authenticator* runs on a bridge and enforces authentication decisions.
  - The *authentication server* is a (logically) centralized component which provides authentication decisions (usually via RADIUS).
- The authentication exchange uses the Extensible Authentication Protocol (EAP).
- IEEE 802.1X is becoming increasingly popular as a roaming solution for IEEE
  802.11 wireless networks.

IEEE 802.1X Sequence Diagram



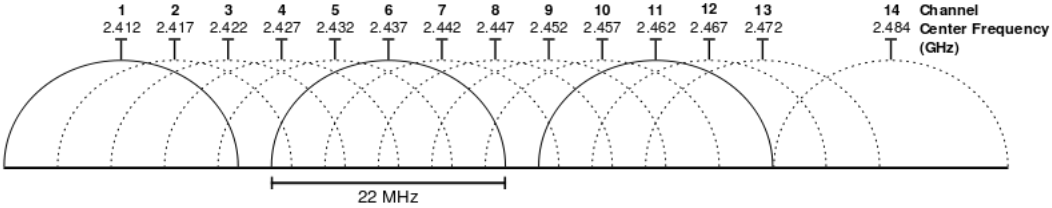
Section 16: Wireless LAN (IEEE 802.11)

IEEE 802.11 Wireless

Protocol	Released	Frequency	Data Rate	Indoor	Outdoor
802.11a	1999	5 GHz	54 Mbps	35*m*	120*m*
802.11b	1999	2.4 GHz	11 Mbps	38*m*	140*m*
802.11g	2003	2.4 GHz	54 Mbps	38*m*	140*m*
802.11n	2009	2.4/5 GHz	248 Mbps	70*m*	250*m*
802.11ac	2014	5 GHz	600 Mbps	70*m*	250*m*

- Very widely used wireless local area network (WLAN).
- As a consequence, very cheap equipment (base stations, interface cards).
- Wired equivalent privacy (WEP) was a disaster (at least for those who believe a wire is secure).
- Recommended is WPA-2 (Wifi Protected Access), in particular in combination with 802.1X and EAP-TLS.

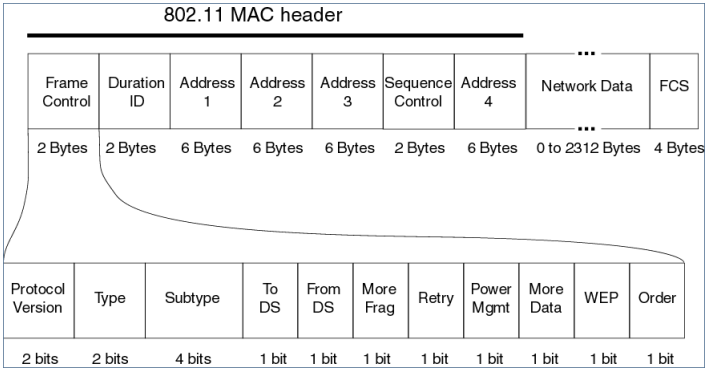
IEEE 802.11 2.4 GHz Channels



IEEE 802.11 Frame Types

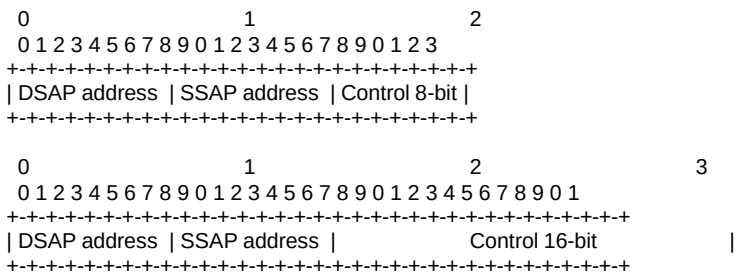
- Data Frames: Carrying “useful” payloads
- Control Frames: Facilitate the exchange of data frames
  - Ready-to-send (RTS) and Clear-to-send (CTS) frames
  - Acknowledgement (ACK) frames
- Management Frames: Maintenance of the network
  - Beacon frames
  - Authentication / deauthentication frames
  - Association / deassociation frames
  - Probe request / response frames
  - Reassociation request / response frames

IEEE 802.11 Frame



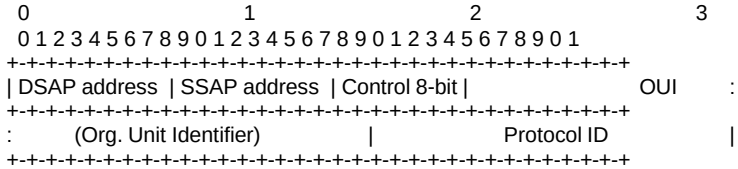
Section 17: Logical Link Control (IEEE 802.2)

IEEE Logical Link Control



- The LLC header follows the MAC frame header (but it is not always used)
- DSAP = Destination Service Access Point
- SSAP = Source Service Access Point
- Control = Various control bits, may indicate subsequent header

IEEE Logical Link Control SNAP Header (8-bit



- The LLC header may be followed by the Subnetwork Access Protocol (SNAP) header (if indicated by the Control field)
- The Organizational Unit Identifier (OUI) identifies an organization defining Protocol ID values
- The Protocol ID identifies the protocol in the following payload
- If the OUI is 0x000000, the Protocol ID contains an Ethernet type value

Referenc

R. M. Metcalfe and D. R. Boggs.
Ethernet: Distributed packet switching for local computer networks.
Communications of the ACM, 19(5):395–404, July 1976.

R. Perlman.
An Algorithm for Distributed Computation of a Spanning Tree in an Extended LAN.
SIGCOMM Computer Communication Review, 15(4), September 1985.

A. F. Benner, P. K. Pepeljugoski, and R. J. Recio.
A Roadmap to 100G Ethernet at the Enterprise Data Center.
IEEE Applications and Practice, 45(3), November 2007.

L. D. Nardis and M.-G. Di Benedetto.
Overview of the IEEE 802.15.4/4a standards for low data rate Wireless Personal Data Networks.
In *Proc. of the 4th IEEE Workshop on Positioning, Navigation and Communication 2007 (WPNC'07)*, Hannover, March 2007. IEEE.