Layer-2 Objectives

- Layer 2 responsibilities
- Layer 2 format
- Layer 2 operation
- Bridge operation

L2 Responsibilities

- packaging of data for transport over links (ie, between adjacent nodes/LAN[1])
- implementation of *local* destination- and source-addressing in LAN
- Ethernet/IEEE-802.3 allows for multicast- and broadcast destination[2]
- Ethernet L2 does *not* assure delivery[3]

[1] Local Area Network: typical in-house network connected to the Internet via a Router. WAN/Wide Area Network consist of many LANs → Internet

[2] message to some or all nodes on LAN

[3] ie, the layers above must handle lost messages

L2 Factlets

- most abundant LANs/L2-Networks today are 802.3/Ethernet and 802.11/Wireless
- devices for *building* LANs: Hub/Repeater (L1) and Bridge/Switch (L2)
- devices *interconnecting* LANs to other LANs or the "outside world": Router (L3) or Firewall/Router (L3+)
- L2 addressing is of *local* [4] interest only!
- a LAN/L2 is a so called "broadcast domain": `0xFF:FF:FF:FF:FF:FF` destination is limited *not* to the LAN
- 802.x/Ethernet is a TDM[5] network
- messages on a Ethernet LAN are called *frames*

[4] there is no need for your computer to know the L2 address of a webserver in the Internet

[5] Time Domain Multiplexing

L2 Frame-Header/Metadata

encapsulates – "frames" – a certain[6] amount of data[7] from above layer with metadata:

- **Preamble**: a special synchronize sequence[8]
- **Address**: source- and destination address of adjacent nodes
- **Type**: identifies encapsulated data, eg 0x0800 for IP
- **Frame Checksum**: allows the destination node to check consistency of data received

[6] on Ethernet maximum 1518 Bytes - layer-2 metadata, minimum 64 Bytes

[7] the "payload", often somewhat incorrectly refered to as PDU, Protocol Data Unit

[8] http://en.wikipedia.org/wiki/Ethernet_frame

L2 Adressing

- Ethernet L2/MAC addresses consists of 6 Bytes (3 vendor-id[9], 3 serial)
- this allows for (theoretical) $2^{48} \sim 256$ trillion addresses
- the usual notation for MAC addresses are hex[10] bytes seperated by ":"
- MAC adresses are guaranteed[11] to be unique
- `0xFF:FF:FF:FF:FF:FF` is the *broadcast* [12] destination address
- any address with the `0x_1:__:__:__:__:__` bit set is *multicast* [13]

[9] https://db.uga.edu/network/public/vendorcode.cgi

[10] sometimes identified by 0x-prefix

[11] theoretically... most OS/network cards allows you to alter this address and sometimes the vendor just blows it

[12] limited to LAN

[13] eg. to "all routers" in LAN

L2 Interlude

- find your computers MAC address[14]
- find the vendor of your computers NIC[15]
- find other MACs your computer had conversation with[16]
- find the vendor of the router[17] connecting you to the internet[18]
- find the MAC of your neighbours PC[19]
- find the MAC of `www.eff.org`

[14] UNIX: `ifconfig`, Microsoft Windows: `ipconfig /all`

[15] Network Interface Card

[16] `arp -a`, add another `-n` on UNIX for faster responses

[17] "default gateway"

[18] this is actually a L3 theme... use `netstat -rn` to find the routers IP and locate the corresponding MAC in the `arp -a` output

[19] use `ping` *IP* first then issue `arp -a` once again

L2 Bridging

- *bridges* are devices to extend the reach of a LAN. The resulting network is still a single LAN
- multiport[20] bridges are called (L3) *switches*
- bridges *segment* a LAN by analyzing the destination address and send out frames only on ports leading to the target device
- . . . thus providing some "privacy"[21]
- this is achieved by building a MAC-address/port lookup table by storing the *source* MAC-address along with the receiving port number
- as long as a particular destination MAC-address is not known, frames must be *flooded* out to all except the receiving port
- broadcast frames are send out on all ports except on the receiving one

[20] anything with more than a few ports

[21] try yourself: use `wireshark` or `tcpdump` and see if you can spy on your neighbous traffic

L2 CSMA/CD, Collision-Domain

- CSMA: Carrier Sense Multiple Access/Collision Detection
- since the cable/medium[22] allows for at a single transmission only at any given time (TDM), the sender constantly monitors its transmission and cancels it in case of noise: *collision detection*
- such a L2-segment[23] is called a "collision-domain"
- bridged seperates "collision-domains", thus a end-device connected to a switch has its private collision-domain[24]

[22] in case of twisted-pair cables the send/receive lines are physically seperated allowing for full-duplex traffic. Traditional coax-cables are half-duplex only

[23] single broadcast-medium cable (coax) or repeater/hub interconnected

[24] and will never encounter collisions at all if configured correctly

L2 Bridging: Cut-Through vs Store-and-Forward

- traditionally bridges/switches receives a whole frame and forwards it if the frame-checksum matches
- this adds a certain *latency* [25] to the transmission
- some bridges/switches offer a *cut-through* forwarding mode, where the frame is forwarded as soon as the destination-address is received
- this mode allows for a *constant* and minimal latency
- in case of line-noise, the bridge may forward defective frames in cut-through mode
- advanced bridges mitigate this problem by fall-back to store-and-forward mode in presence of errors

[25] a delay, in this case dependent of the frame-length

L2 Briding: Loops and avoidance of

- complex LANs with multiple bridges may form *loops* [26]
- especially broadcast frames may lead to a (broadcast) *storm*
- advanced bridges employ a *spanning-tree* [27] protocol to avoid this

[26] try this at home: "short-circuit" your (auto-crossover) switch by connecting a cable back-to-back

[27] IEE 802.3D STP Spanning Tree Protocol: an application of the Djikstra-Algorithm, we'll study this in L3 OSPF

L2 Bridging: VLAN

- advanced bridges allow for *Virtual LANs* (VLANs)
- VLANs are seperated LAN/L2-segments[28]
- the L2 metadata is extended by a VLAN-identification number
- a physical port on the bridge can be configured to allow for one VLAN only[29] – usually to connect to end-devices
- physical ports may also be configured to operate in *trunking* mode – usually in bridge-to-bridge *aggregated* link or to allow for advanced end-devices to seperate VLANs internally
- typical applications: seperate external-, internal- and server-LAN for security reasons[30]

[28] ie, a router is required to interconnect VLANs

[29] the VLAN-id is *stripped*†from the metadata

[30] this is considered bad practice

L2: References for ND03

- http://en.wikipedia.org/wiki/Ethernet_frame, http://en.wikipedia.org/wiki/Ethernet_II_framing
- http://en.wikipedia.org/wiki/802.3
- http://en.wikipedia.org/wiki/IEEE_802.1D
- http://en.wikipedia.org/wiki/Bridging_(networking) especially the part "bridging makes no assumptions about where in the network a particular address is located" $\rightarrow$ "flooding"
- http://en.wikipedia.org/wiki/Frame_(networking)
- https://db.uga.edu/network/public/vendorcode.cgi, MAC vendor