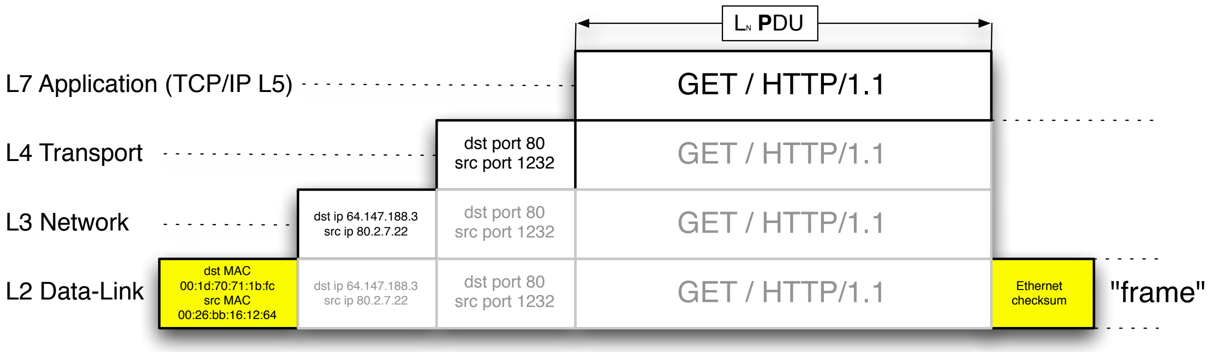
Layer-2 Objectives

- Layer 2 responsibilities
- Layer 2 format
- Layer 2 operation
- Layer 2 Devices: Bridge operation

Layer-2 Stack



L_N PDU

L7 Application (TCP/IP L5)

GET / HTTP/1.1

L4 Transport

dst port 80
src port 1232

GET / HTTP/1.1

L3 Network

dst ip 64.147.188.3
src ip 80.2.7.22

dst port 80
src port 1232

GET / HTTP/1.1

L2 Data-Link

dst MAC
00:1d:70:71:1b:fc
src MAC
00:26:bb:16:12:64

dst ip 64.147.188.3
src ip 80.2.7.22

dst port 80
src port 1232

GET / HTTP/1.1

Ethernet checksum

"frame"

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]
- Error detection using a 32-bit CRC[3]
- Ethernet L2 does *not* assure delivery[4]

[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] err'd frames are simply dropped by bridges, routers, hosts. Ponder about the reason for this. . .

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

L2 Factlets

- messages on a Ethernet LAN are called *frames*
- most abundant LANs/L2-Networks today are 802.3/Ethernet and 802.11/Wireless
- devices for *building* LANs: L1:Hub/Repeater and L2:Bridge/Switch
- devices *interconnecting* LANs to other LANs or the "outside world": L3:Router or L3+:Firewall/Router
- L2 addressing is of *local* [5] interest only!
- a Link/L1 forms a "collision domain", transmissions from different devices may "collide" on a single wire/Hub
- a LAN/L2 denotes a "broadcast domain": `0xFF:FF:FF:FF:FF:FF` destination is sent to all nodes on the LAN[6]
- 802.x/Ethernet is a TDM[7] network

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

[6] it is *limited*, ie it never leaves the LAN via a router

[7] Time Domain Multiplexing

L2 Frame-Header/Metadata

encapsulates – “frames” – a certain[8] amount of data[9] from above layer with metadata:

- **Preamble**: a special synchronize sequence[10]
- **Address**: destination- and source-address of adjacent nodes
- **Type**: identifies encapsulated data (type of SDU/upper-layer), eg 0x0800 for IP
- **Frame Checksum**: allows the destination node to check consistency of data received

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

[9] the “payload” from Layer-3, this is the “SDU” service-data-unit on Layer-2

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

L2 Adressing

- Ethernet L2/MAC addresses consists of 6 Bytes (3 vendor-id[11], 3 serial)
- this allows for (theoretical) $2^{48} \sim$ 256 trillion addresses
- the usual notation for MAC addresses are hex[12] bytes seperated by “:”
- MAC adresses are guaranteed[13] to be unique
- `0xFF:FF:FF:FF:FF:FF` is the *broadcast* [14] destination address
- any address with the `0x_1:__:__:__:__:__` bit set is *multicast* [15]

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

[12] sometimes identified by 0x-prefix

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

[14] “to all”, limited to the LAN of course

[15] eg. to “all routers” in LAN

L2 Interlude

- find your computers MAC address[16]
- find the vendor of your computers NIC[17]
- find other MACs your computer had conversation with[18]
- find the vendor of the router[19] connecting you to the internet[20]
- find the MAC of your neighbours PC[21]
- find the MAC of `www.eff.org`
- listen to the network chit-chat using `tcpdump` (on `netbox`). Try to identify L2-broadcast, multicast and unicast

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

[17] Network Interface Card

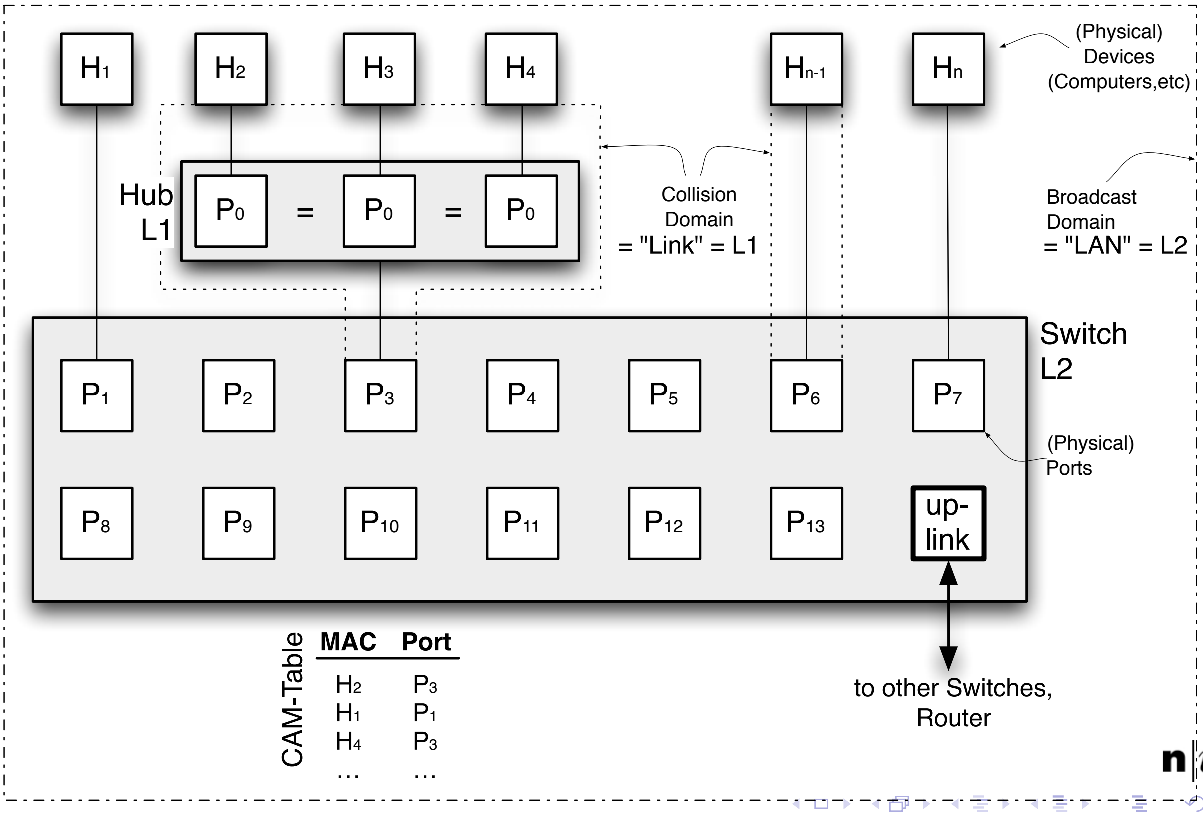
[18] `arp -a`, add another `-n` on UNIX for faster responses

[19] "default gateway"

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

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

L2 Bridging 1/2



MAC	Port
H_2	P_3
H_1	P_1
H_4	P_3
...	...

L2 Bridging 2/2

- *bridges* are devices to extend the reach of a LAN. The resulting network is still a single LAN
- multiport[22] bridges are called (L3) *switches*
- bridges analyze the destination address of a frame and transmit it only on specific port(s)
  - . . . thus providing some “privacy”[23]
  - 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

[22] anything with more than a few ports

[23] 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[24] 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 L1-segment[25] is called a “collision-domain”
- bridged seperates “collision-domains”, thus a end-device connected to a switch has its private collision-domain[26]

[24] 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

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

[26] 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* [27] 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

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

L2 Briding: Loops and avoidance of

- complex LANs with multiple bridges may form *loops* [28]
- especially broadcast frames may lead to a (broadcast) *storm*
- advanced bridges employ a *spanning-tree* [29] protocol to avoid this

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

[29] 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[30]
- 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[31] – 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[32]

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

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

[32] 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" → "flooding"
- http://en.wikipedia.org/wiki/Frame_(networking)
- https://db.uga.edu/network/public/vendorcode.cgi, MAC vendor