Network Basics

Computer Organization and Networks 2019

Johannes Feichtner
johannes.feichtner@iaik.tugraz.at

Main Topics

Fundamentals

- History of protocols
- Network Types
- Layers, basic elements
- How to transfer data?

Circuit/Packet Switching, ARPANET, TCP/IP, UDP, HTTP, Web 2.0, Cloud, IPv6, OSI Model, 802.11, LAN/WAN

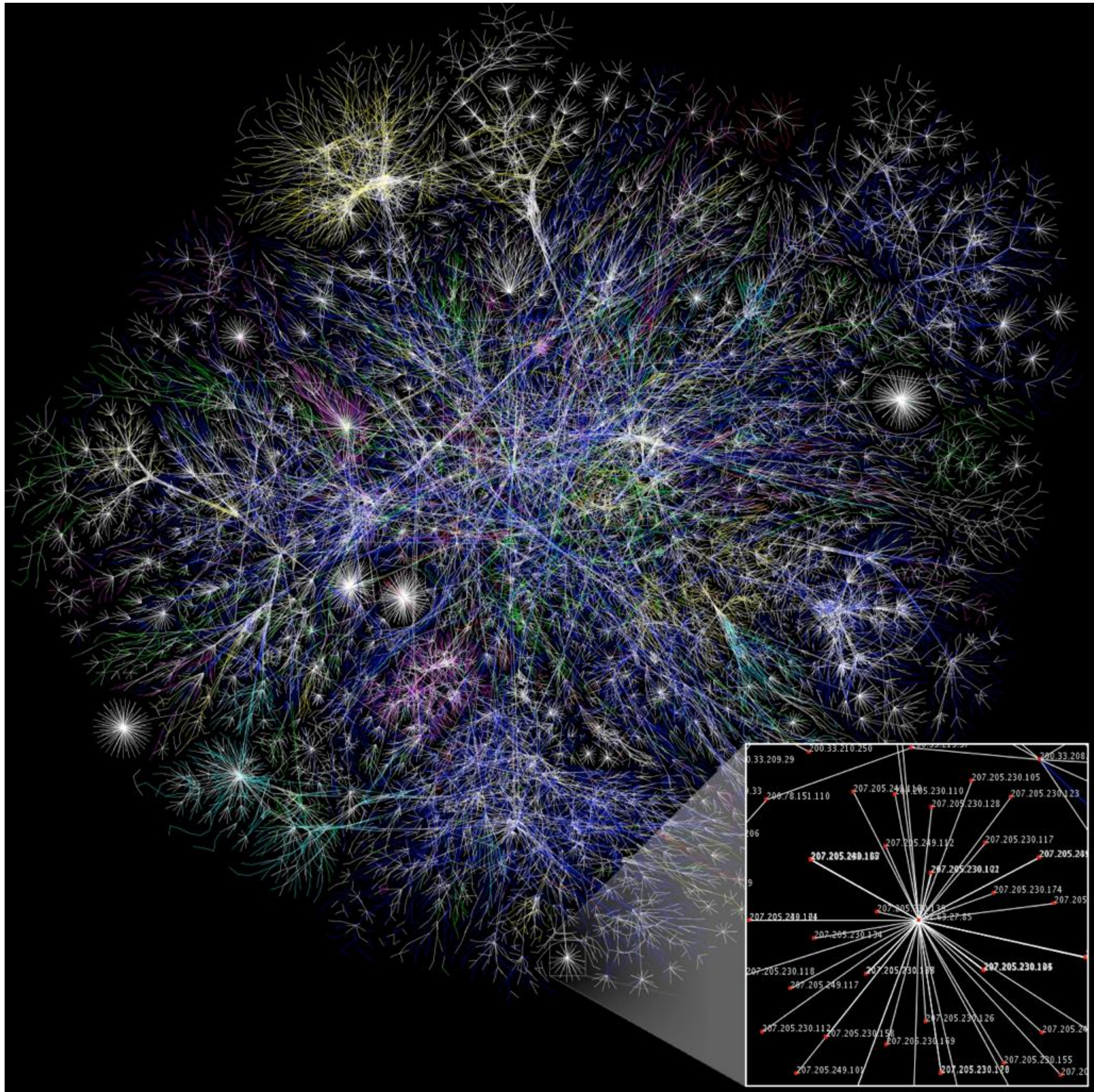
Network Layers

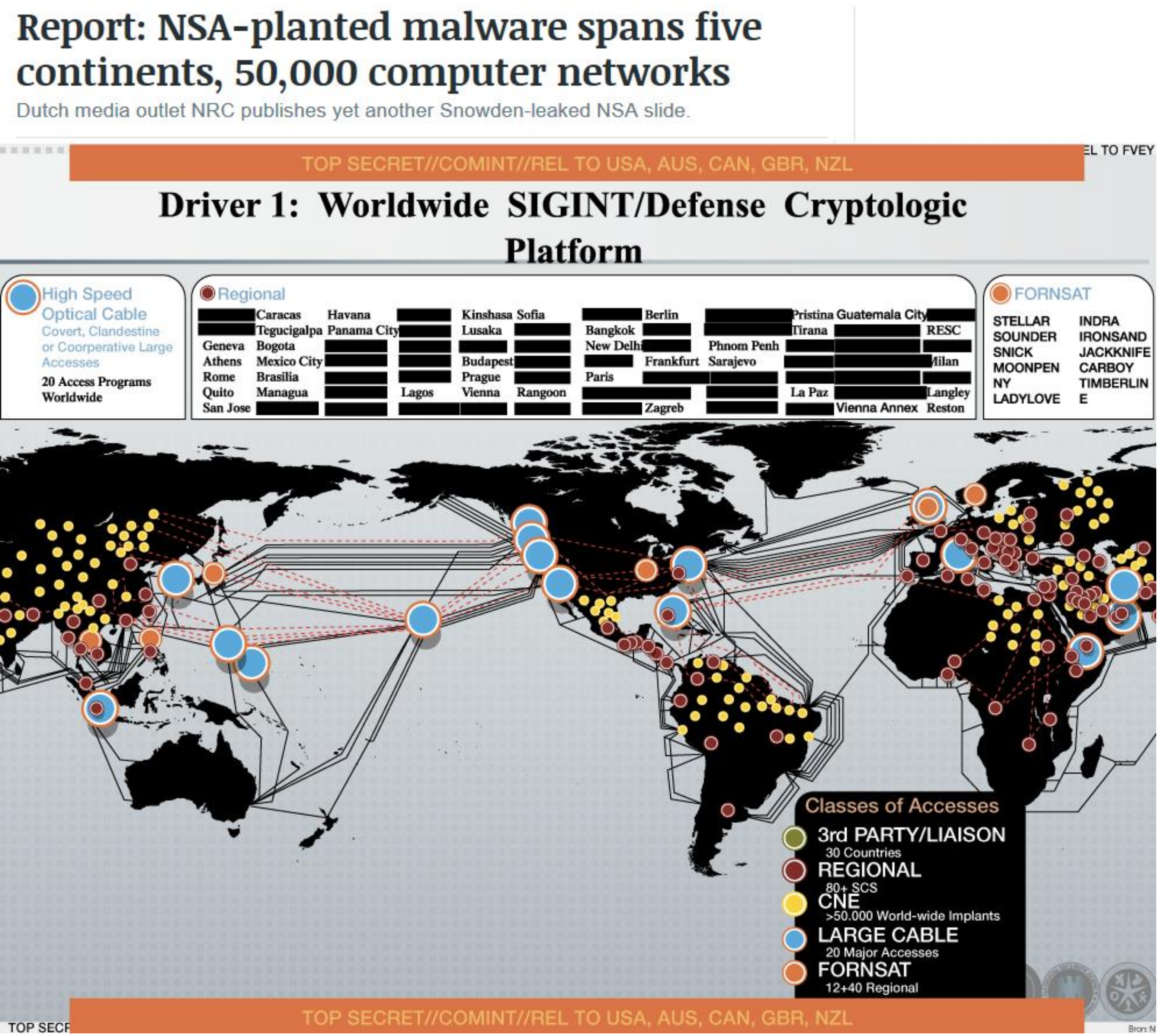
- Link
- Networking
- Transport
- Application

LANs, Switches, Routing, MAC, IPv4/IPv6, VPNs, IPSec, TCP/UDP, HTTP(/2), Congestion control, AJAX, CSS TLS/HTTPS, CSP

Computer Networks – Why?

- More and more things get linked
  - Starting with PCs, Laptops…
  - Smartphones
  - Sensors, Smart Tags, SCADA
  - Internet of Things (IoT)
- Rapid communication
  - Think of high-speed stock trading
  - Crypto coin mining
- „New“ application scenarios
  - Cloud, Smart Grid, Smart Home





Source: http://goo.gl/n2ZSef

What?

Computer Networks as source to gather information from targets or enemies

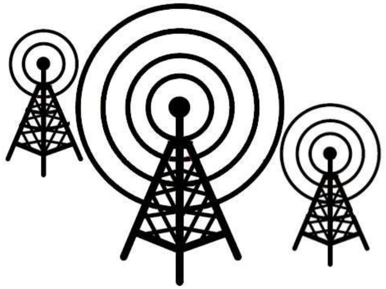
Attacks

- Disrupt / destroy data within computers, networks or both
- Steal data, monitor communication

Defenses

- Protect, monitor, analyse, detect, respond to attacks and intrusions

Computer Networks – How?



1) Starting at…

- Information theory
- Cables, Wireless, …
- Physical properties, Transmission (light, electrons, …)

2) Passing at…

ADSL, UMTS, WLANs, LANs, LTE, DNS, TCP, UDP, TLS, IPSec, L2TP, ARP, FTP, ICMP, POP3, … and countless other acrynoms

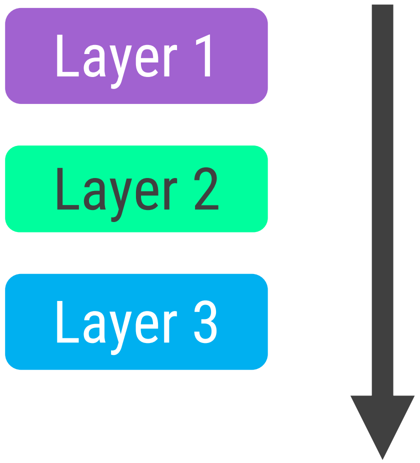
3) Finishing at…

- Connection of Web 2.0, Facebook, Twitter
- Smartphones, Cloud, IoT

Computer Networks – How?

… encapsulate transmission in layers

- Each layer deals with different tasks
- Transmitting data via the Internet
  - Packets, Routing, eventually losing packets?!
- On a higher level…
  - Smartphones talking to the cloud
  - Connections between Web 2.0 apps
  - Secure transmission of data



Scenario 1 – Single Layer

Assumptions

- Two neighbors: Maria and Ann
- Face-to-face communication
- Same language

Any rules to consider?

Source: https://goo.gl/YjMW1d

Scenario 1 – Single Layer

Many rules to follow!

Non-exhaustive list…

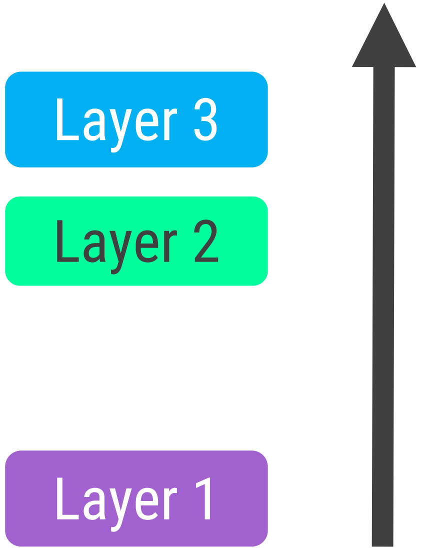
1. Greet each other upon meeting
2. Confine vocabulary to level of friendship
3. Do not speak while other party speaks
4. Communication is dialog → both should be able to speak about same issue
5. Exchange nice words when leaving :-)

→ Conclusions?
Difference to communication between lecturer and students in i13?

Scenario 2 – Three Layers

Assumptions

- Anna moves to different city
- Still want to exchange thoughts (via letters)
- Do not want their ideas to be intercepted
  - Agree on encryption/decryption technique
  - Letter cannot be decrypted without key knowledge
- Need a carrier for the letters

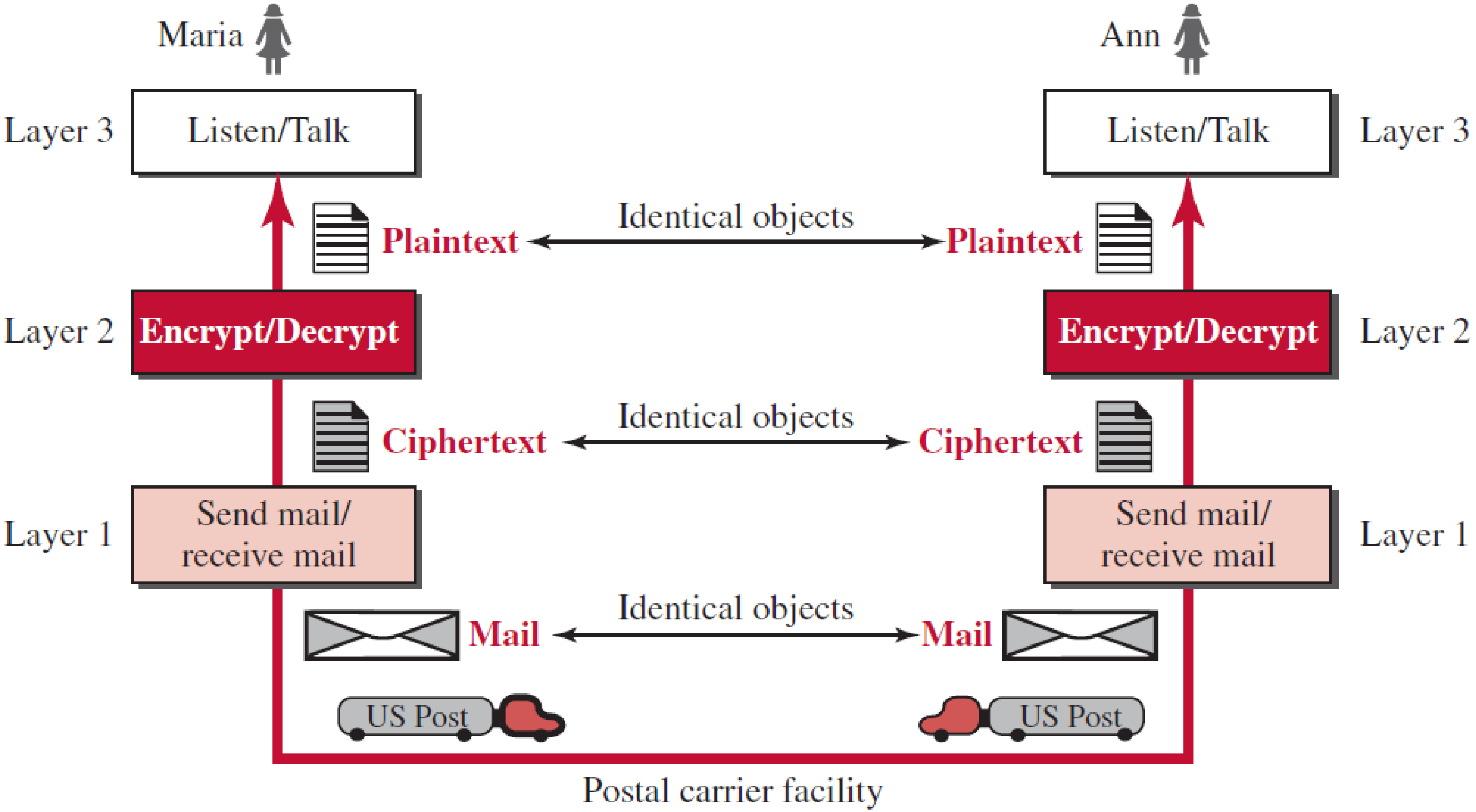


Now what if…

Each of them would have three machines / robots, one per layer…?!

They are using Peer-to-Peer (P2P) connections?

Scenario 2 – Three Layers



Source: https://goo.gl/YjMW1d

Scenario 2 – Conclusions

Why not only 1 machine for 3 tasks?

If encryption / decryption not enough → need to change entire machine

With 3 machines, only need to upgrade / replace layer 2

Modularity!

Layers help to separate services from implementation

→ Receive services from lower layer, pass to upper layer

Two principles

1. If we want bi-directional communication
   → Each layer has to perform two opposite tasks, one per direction
2. At both sides, the objects used by each layer should be identical
   → E.g. at layer 1 Ann sends letter, Maria should receive letter in same format

Scenario 3 – Abstracted Example

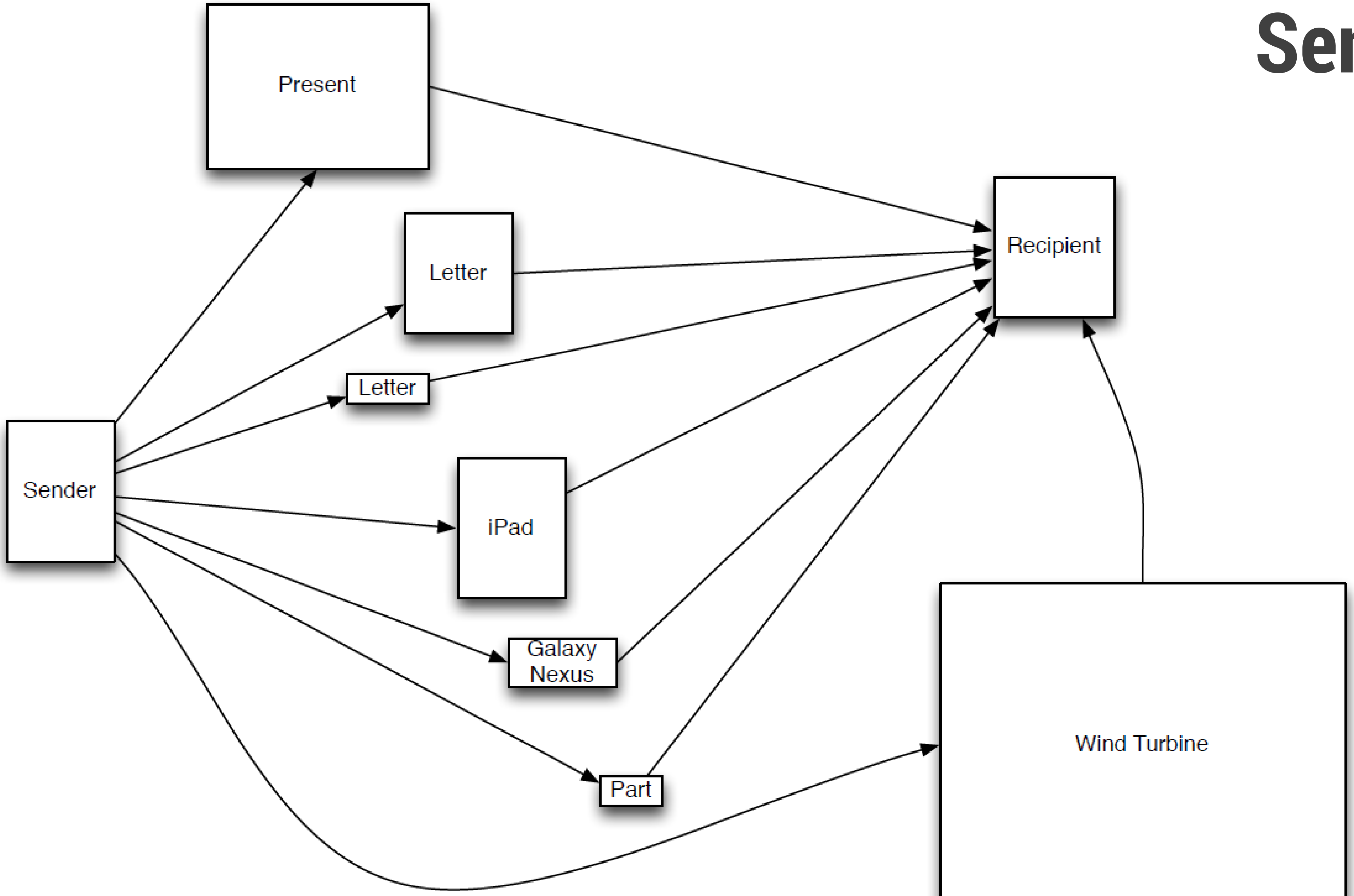
Purpose: *Send arbitrary things (letter, device, car, diamond, …)*

- Real-world sender / receiver
- No delivery infrastructure (e.g. post offices) but transport (cars, trucks, …)

What does it show?

- Need for clearly distinct layers
- Differences between (virtual) circuit / packet switching
- Network hierarchies

Sending...



IAIK TU Graz

Sending...

Worst case

- *No defined protocols*

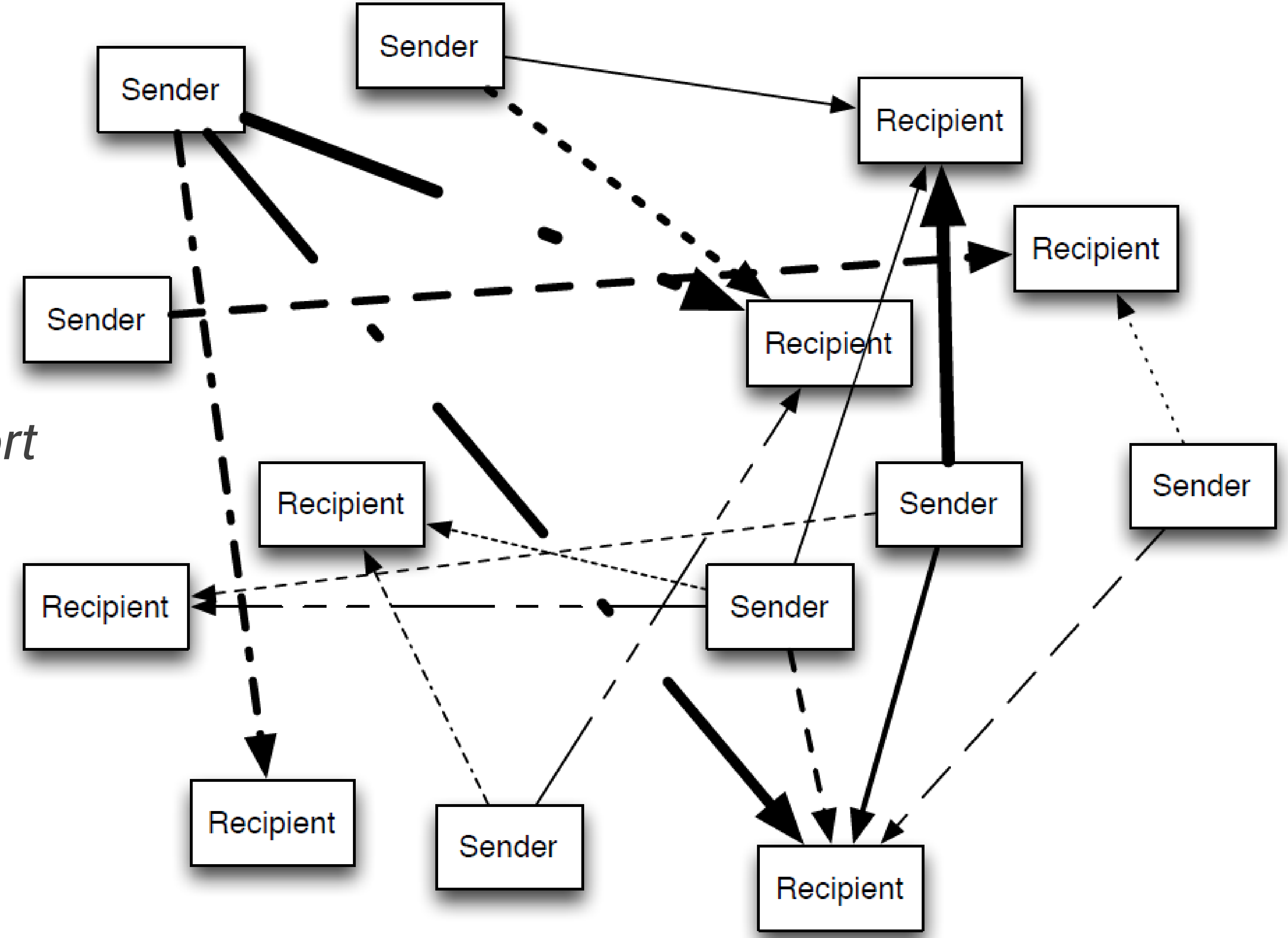
- *No post office*

→ *self-responsible for transport*

- *No resource sharing*

Conclusions?

- *Networks in 1950/1960*
- *Dedicated lines*

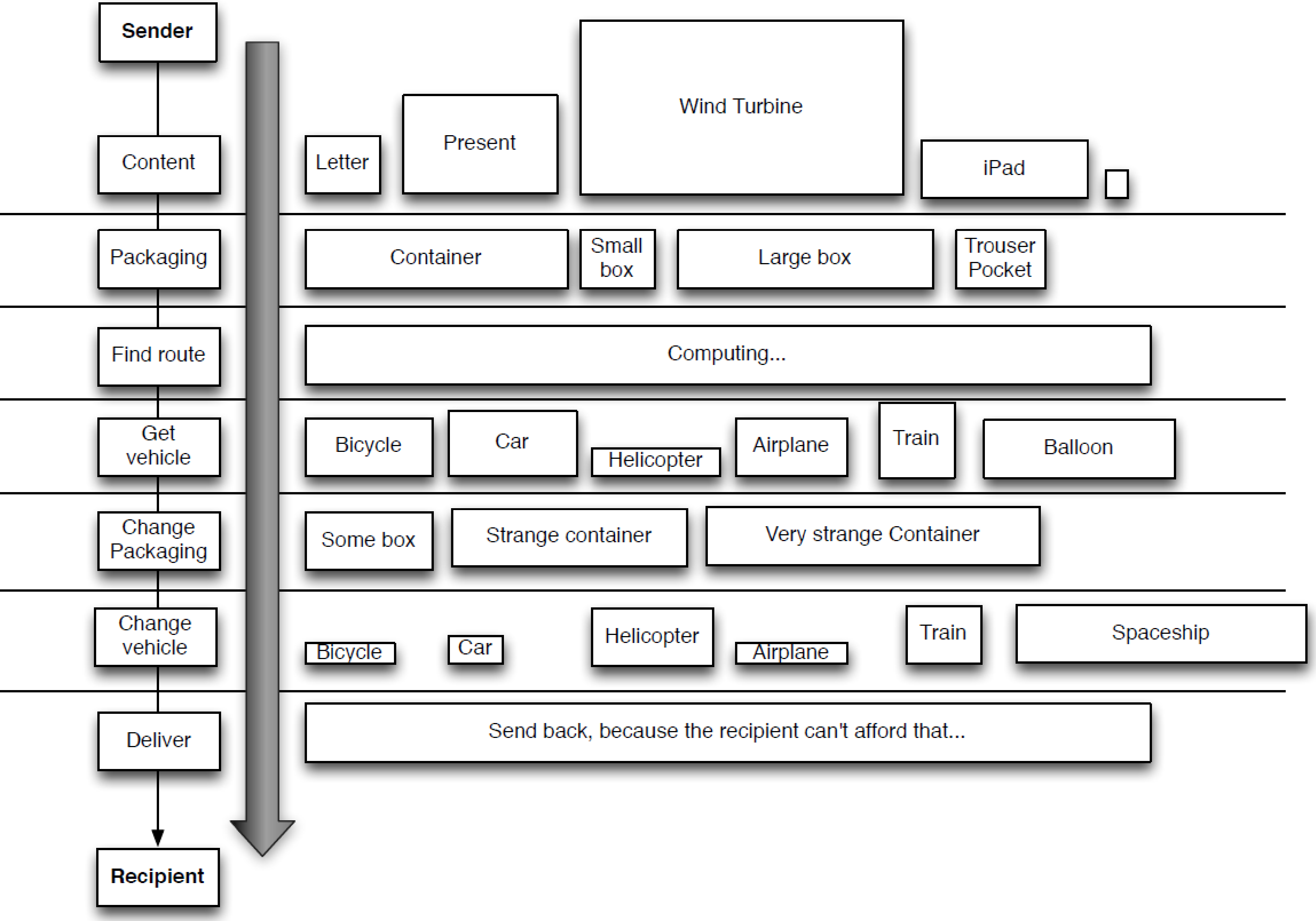


Layers – Abstract View

Approach: *Organize tasks in different abstraction layers*

- Content
  - Letters, devices, parts, big items, small items
- Packaging
  - Wrap content
  - Choose between small/big boxes, containers
  - Sender, recipient address
- Transport
  - Car, truck, train, bicycle, drone, airplane, ship
  - Interpret sender, recipient address of *previous / next destination (hop)*
- Physical
  - Road, water, air

Protocols?



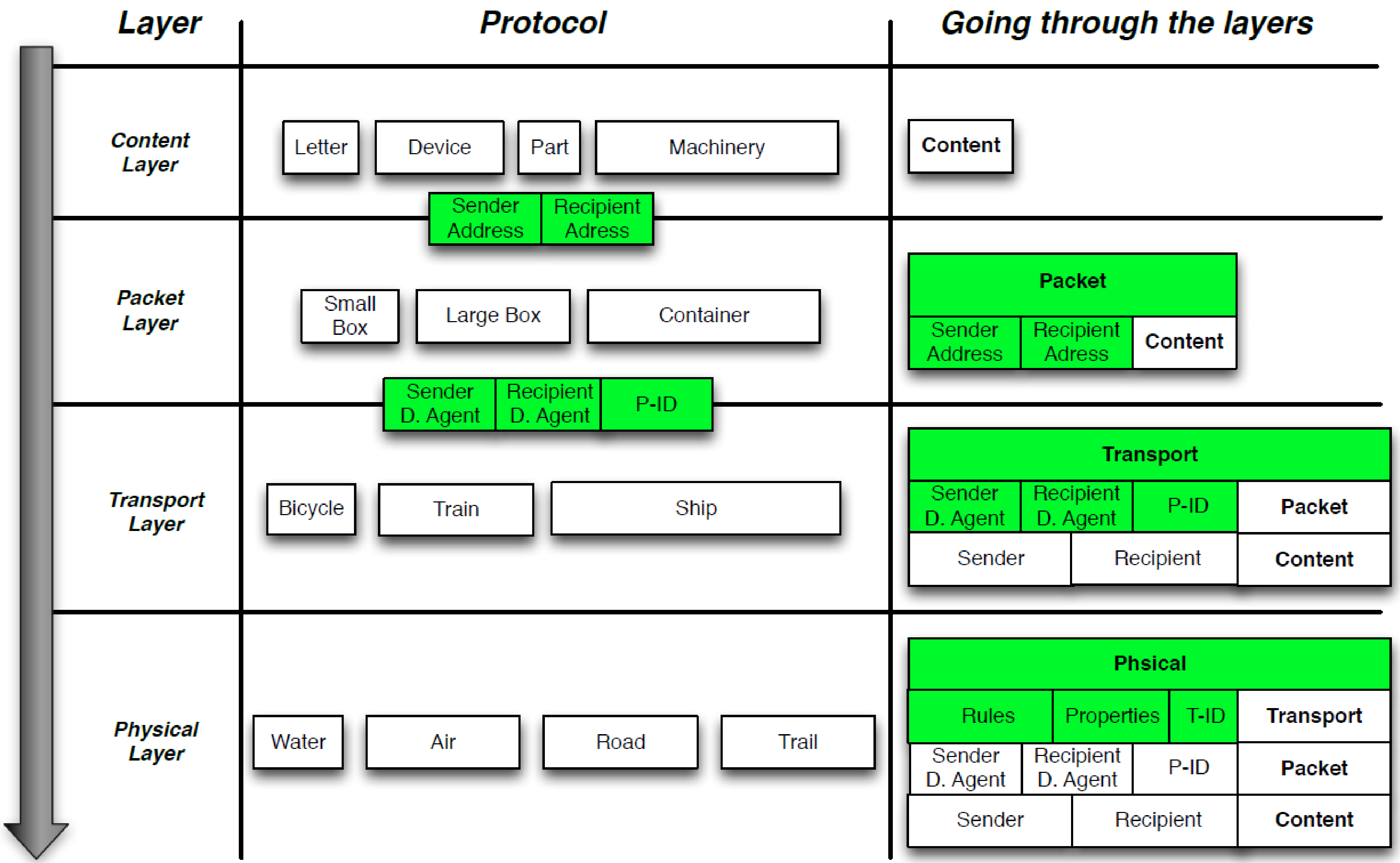
We have the layers but...

- No standards
- No protocols

Consequences

- Send Wind Turbine in trouser pocket?
- Transport iPad with balloon?
- Repackage letter into „strange container“?

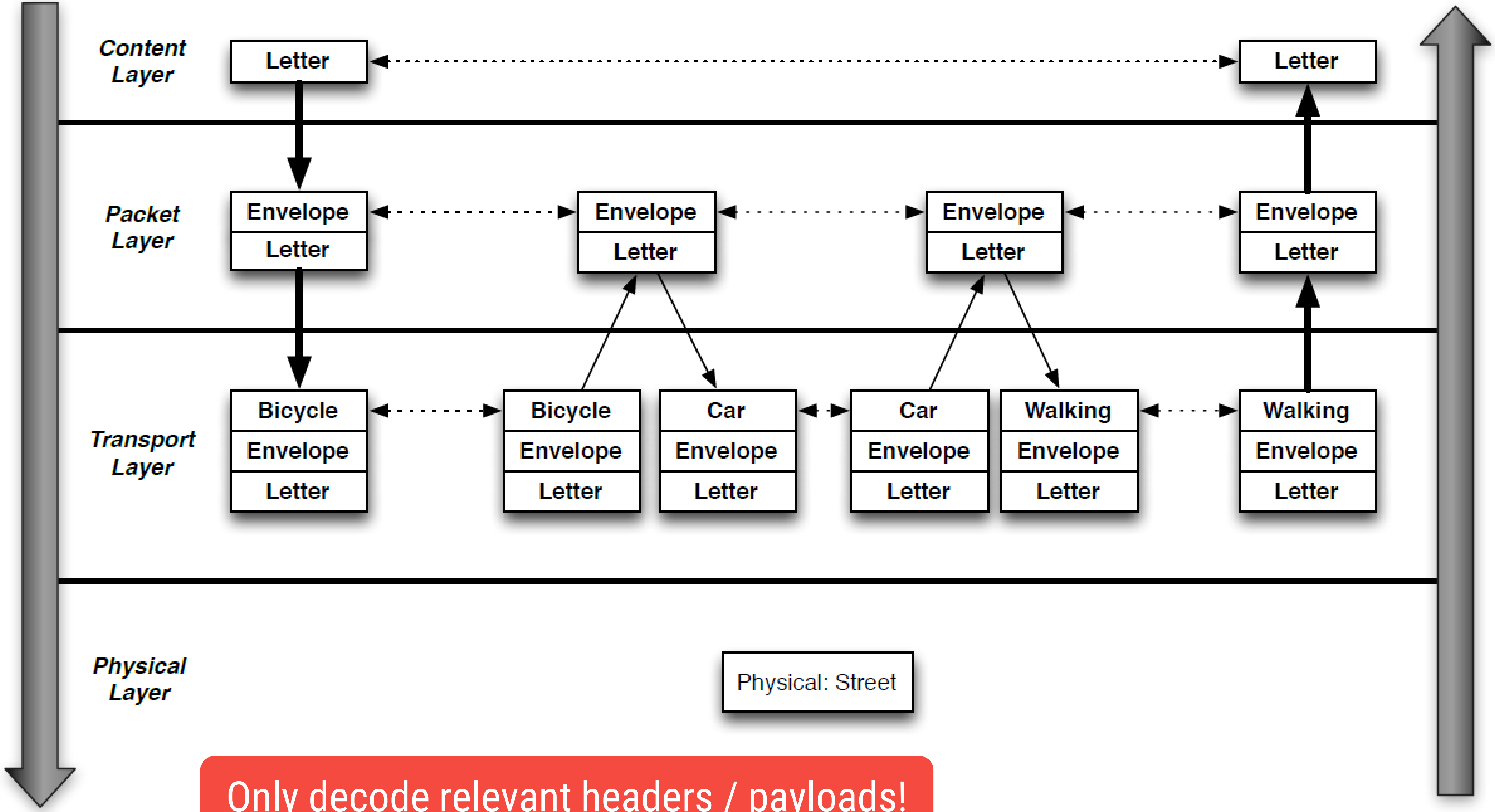
Protocols!



IAIK TU Graz

Who handles Protocols?

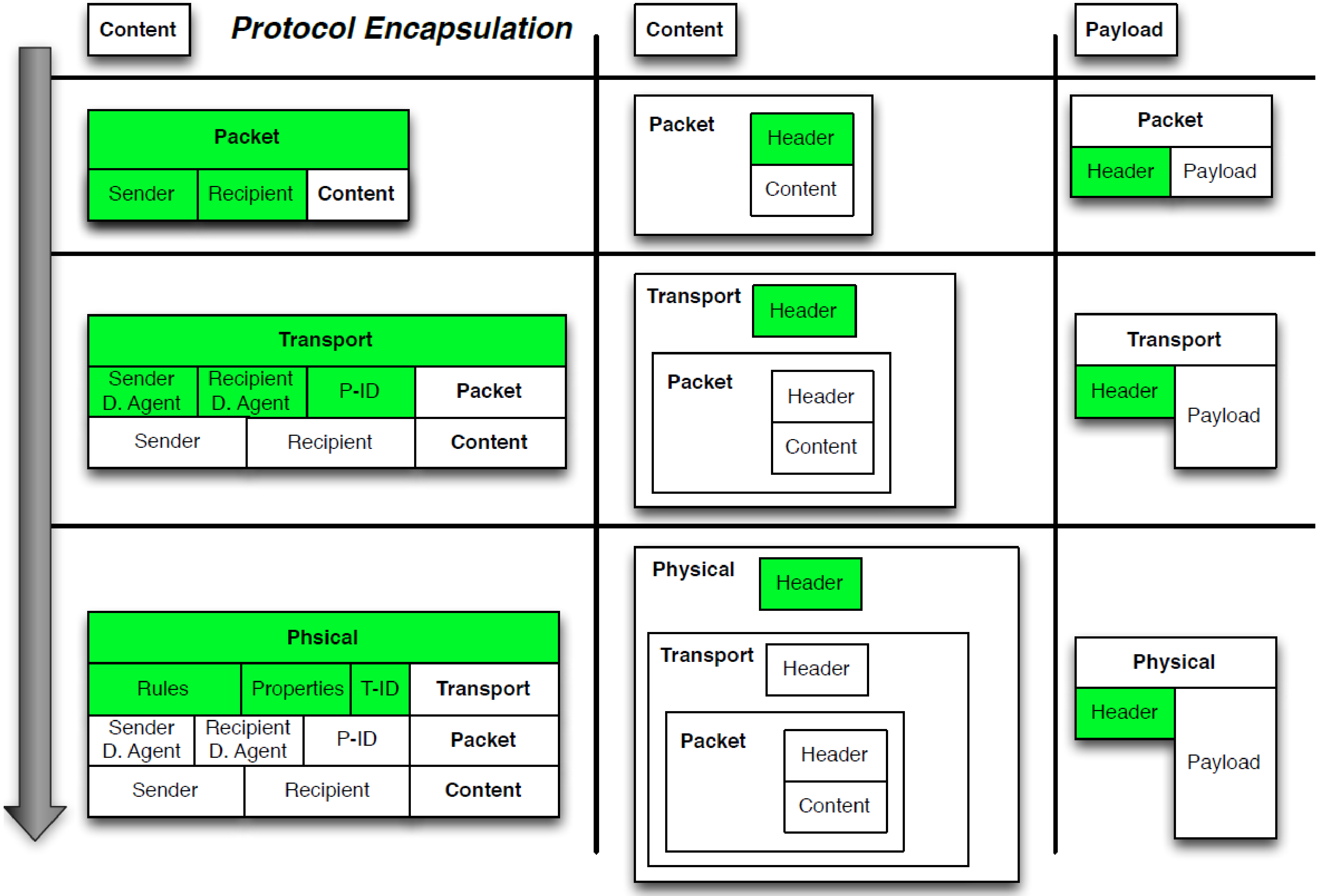
Does every node need to know how to put a letter into an envelope?



Only decode relevant headers / payloads!

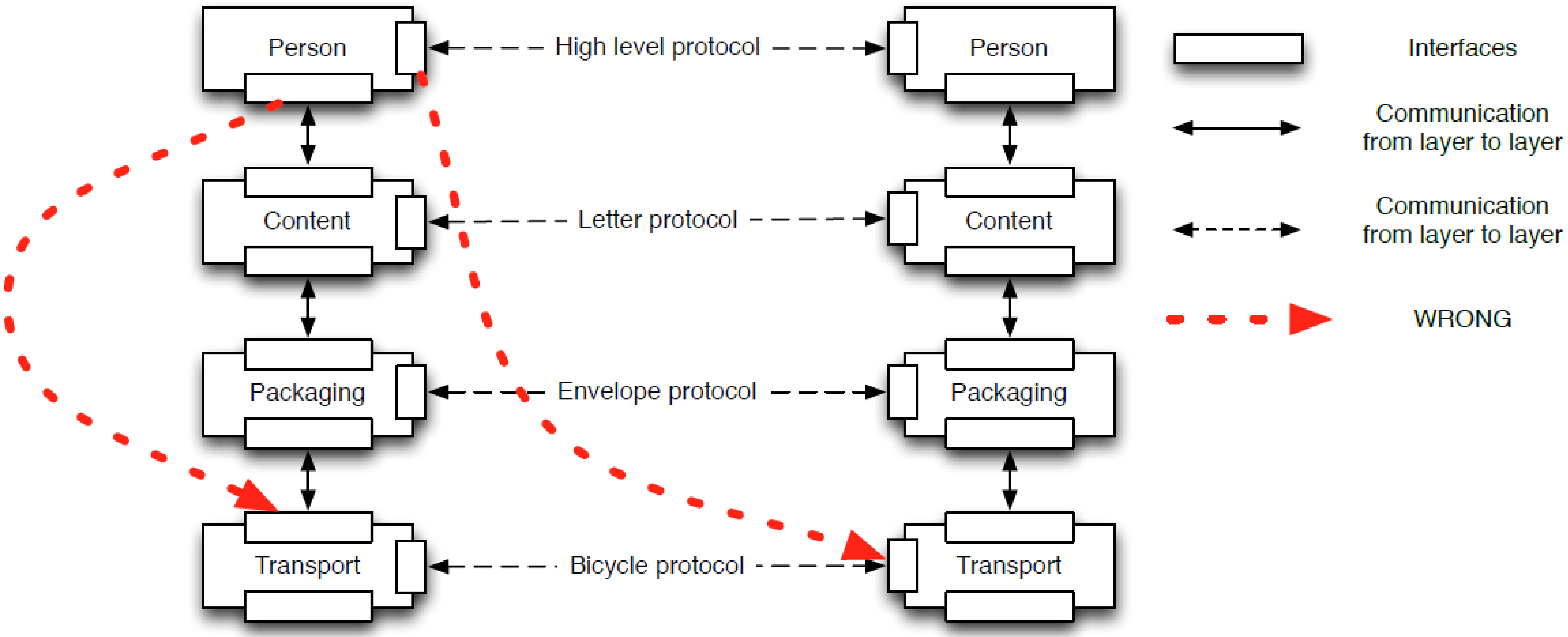
IAIK TU Graz

Layers – Abstraction



Interfaces

- Communication between layers → only with neighbors!
- Via Protocols → only layers at same hierarchy!



IAIK TU Graz

Layers – Why?

- Divide complex task into several smaller (simpler) sub-tasks → layers
- Defining clear interfaces between layers

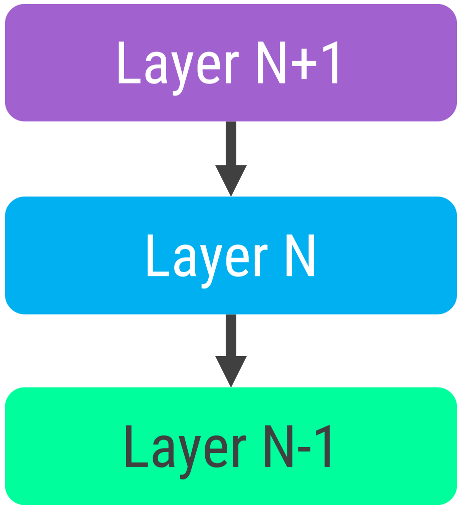
+

- Higher layers represent more abstract concepts → simpler representations
- Communication not always with two end-systems
  – Intermediate systems need some layers but not all (routing)
  – Without layers: Each intermediate as complex as end-system

-

- Probably single layer sometimes simpler
  – E.g. If not needed to provide service to upper layer, give service to lower

Layers – Conclusion



Protocol: *Rules for communication within same layer*

Service: *Abstraction provided to superior layer*
→ API: Concrete way of using the service

Layer N uses services provided by N-1 to implement its protocol and provide its own services!

- Whole set of protocols = protocol stack / suite / set
- Amount of layers (abstraction) depends on purpose of stack

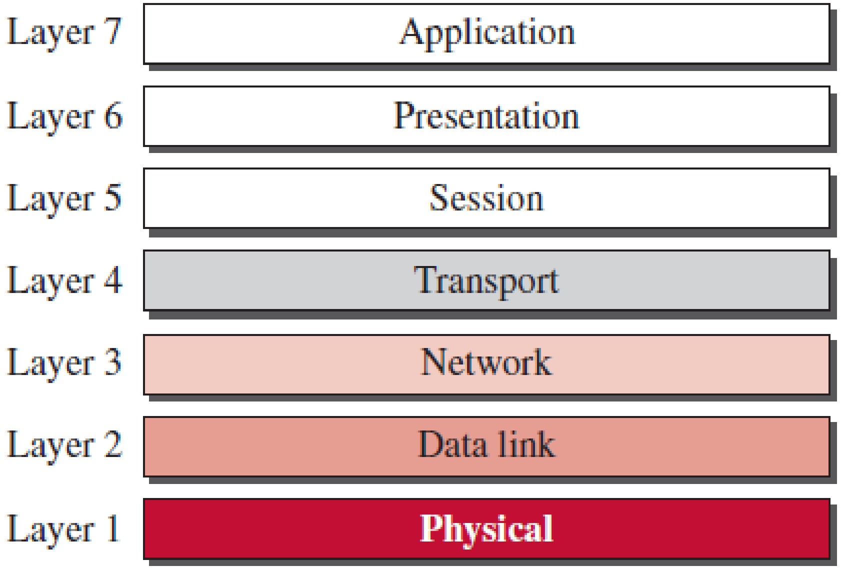
OSI Model

This is not a protocol!

OSI = Open Systems Interconnection

- Layered framework for design of a flexible, robust, and interoperable network architecture

- Design of 7 layers
  - Standard names, interfaces and functions for each
  - Purpose of these functions:
    Defined by investigating existing layers, problems, shortcomings, needs (academic approach)



Source: https://goo.gl/YjMW1d

TCP/IP Model

= Transmission Control / Internet Protocol Suite

- Different layers than OSI model
- Nowadays leading protocol suite
  - ARPANET switched to TCP/IP in 1983
  - Others (DECNET, NCP, SNA) kind of died…
- Initially defined as 4 software layers built upon hardware
  - Nowadays physical component often considered 5th layer

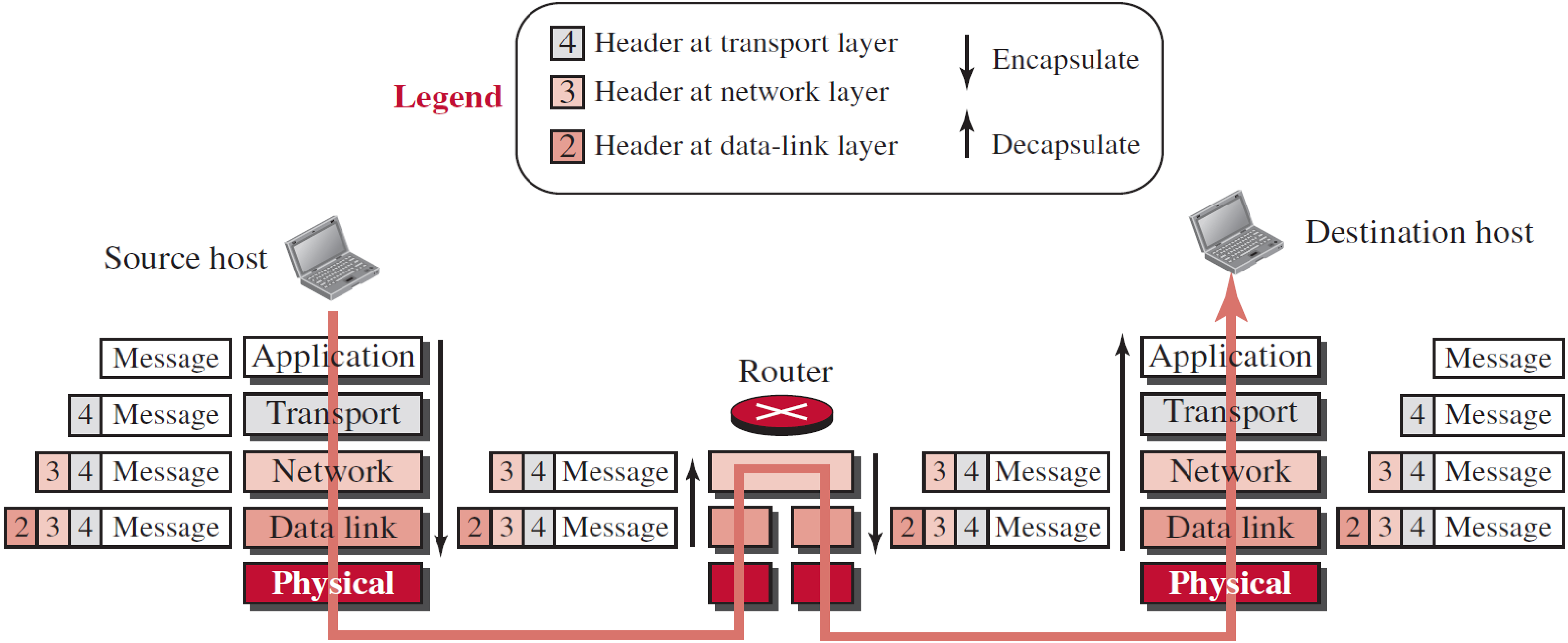
Internet Protocol Suite
Application Layer
BGP · DHCP · DNS · FTP · HTTP · IMAP · IRC · LDAP · MGCP · NNTP · NTP · POP · RIP · RPC · RTP · SIP · SMTP · SNMP · SSH · Telnet · TLS/SSL · XMPP · (more)
Transport Layer
TCP · UDP · DCCP · SCTP · RSVP · ECN · (more)
Internet Layer
IP (IPv4, IPv6) · ICMP · ICMPv6 · IGMP · IPsec · (more)
Link Layer
ARP/InARP · NDP · OSPF · Tunnels (L2TP) · PPP · Media Access Control (Ethernet, DSL, ISDN, FDDI) · (more)
v · d · e

TCP/IP Layers

- Application
  - Everything else (HTTP, user applications, etc.)
- Transport
  - Ensure that sent data arrives (TCP)
- Internet
  - Addressing other nodes, routing of packets (IP)
- Link
  - Type of Network: Wireless, Cables, Protocols, Networks

Internet Protocol Suite
Application Layer
BGP · DHCP · DNS · FTP · HTTP · IMAP · IRC · LDAP · MGCP · NNTP · NTP · POP · RIP · RPC · RTP · SIP · SMTP · SNMP · SSH · Telnet · TLS/SSL · XMPP · (more)
Transport Layer
TCP · UDP · DCCP · SCTP · RSVP · ECN · (more)
Internet Layer
IP (IPv4, IPv6) · ICMP · ICMPv6 · IGMP · IPsec · (more)
Link Layer
ARP/InARP · NDP · OSPF · Tunnels (L2TP) · PPP · Media Access Control (Ethernet, DSL, ISDN, FDDI) · (more)
v·d·e

TCP/IP Example



Source: https://goo.gl/YjMW1d

How to transfer data?

Exchanging Data

Status quo – We have

- Layers
  - Encapsulation / decapsulation
- Protocol suites, models
  - OSI, TCP/IP, …

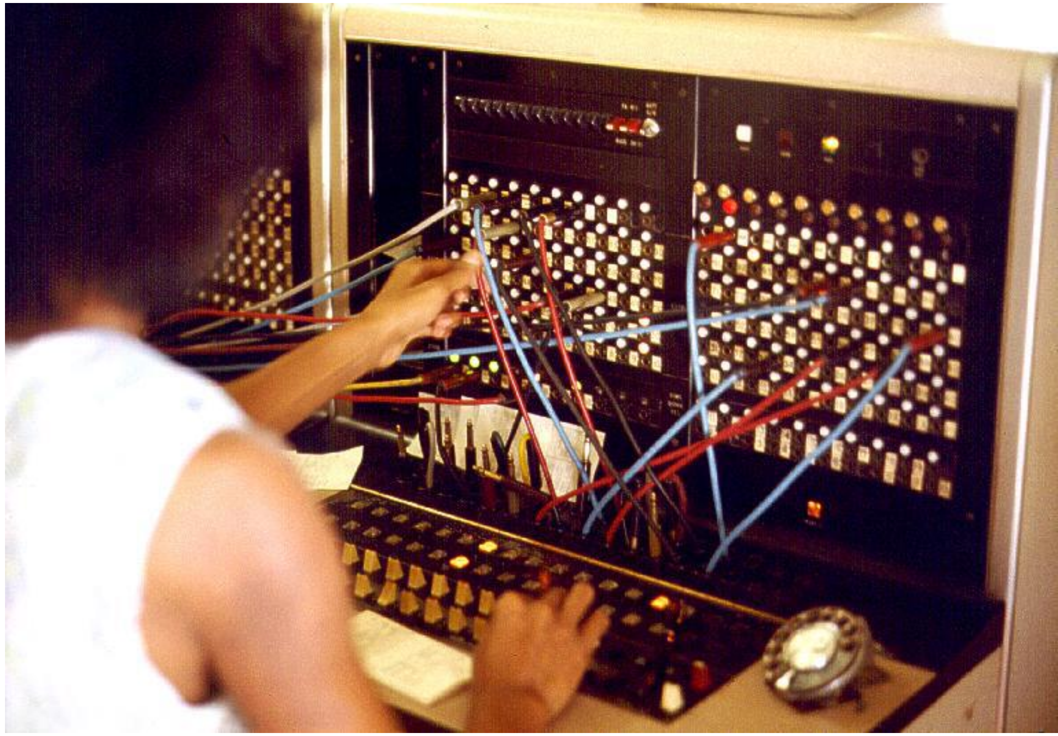
But: *How can we actually transfer information?*

→ *Circuit Switching*
→ *Packet Switching*
→ *Virtual Circuit Switching*

Circuit Switching

Using dedicated line for communication between two partners
→ Early telephone systems!

- **Advantage**
  - Fast and guaranteed capacity when circuit is set up
- **Disadvantage**
  - Waste of resources when channels unused
  - Not suitable for inter-connecting large number of different systems



Source: https://goo.gl/ngYysy

Still used in mobile 2G networks (GPRS, EDGE)!

Packet Switching

- Divide transmitted data into small fragments
  - Packets, frames, cells, …
  - Each fragment carries addressing information in header

- Router / Switch routes each chunk individually
  - Independent routing decisions
  - Dynamic path construction possible, e.g. choose line with least traffic

- Resource sharing (multiplexing) by design

- Flow control
  - Sender has to adapt to speed of receiver
  - Router / Switch needs transmission buffer (input, output)

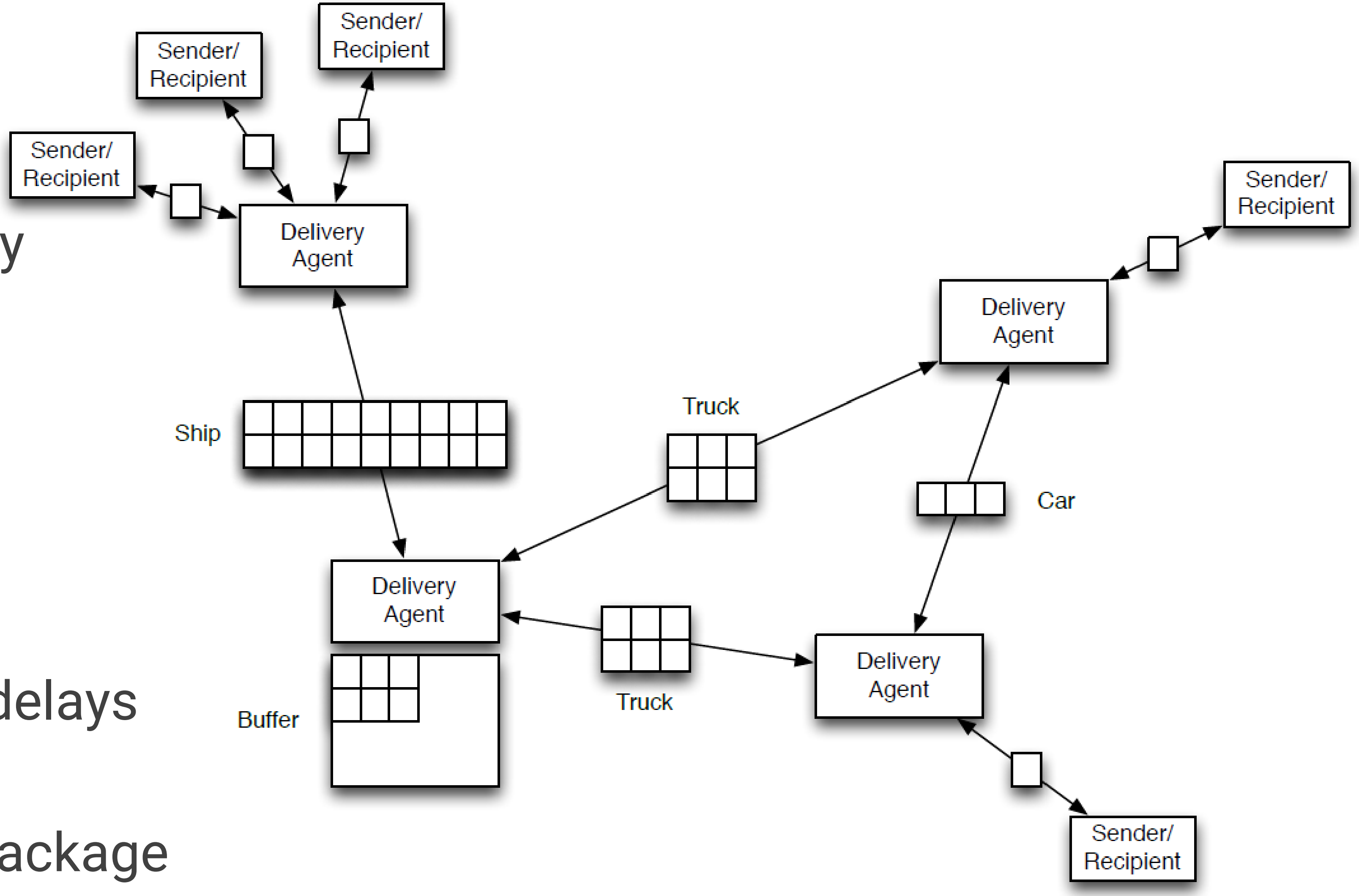
Packet Switching

+

- Very flexible
- High utilization / efficiency
- Bursty traffic handling and shaping possible

-

- Fairness not automatic
- Highly variable queueing delays
  - Buffers needed
- Different paths for each package
- Lost packets → Congestion!



IAIK TU Graz

Link Layer

Definitions

RFC 1122, RFC 1123

Link Layer

- **Task**: Encapsulate network layer packets into (Ethernet) frames
- Link = Physical inter-connection to other hosts in the network
- Link protocols = Communication standards operating on physical connections

IEEE 802

- Set of standards for LANs and MANs
- Fits into TCP/IP model (and OSI even better)
- Sublayers for Local Area Networks

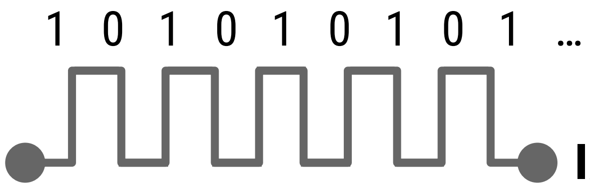
Logical Link Control *(LLC)*

Media Access Control *(MAC)*

Link layer
LAN

Data link

Physical



IEEE 802 Working Groups

Name	Description	
IEEE 802.1	Higher Layer LAN Protocols	active
IEEE 802.2	LLC	disbanded
IEEE 802.3	Ethernet	active
IEEE 802.4	Token bus	disbanded
IEEE 802.5	Defines the MAC layer for a Token Ring	disbanded
IEEE 802.6	MANs (DQDB)	disbanded
IEEE 802.7	Broadband LAN using Coaxial Cable	disbanded
IEEE 802.8	Fiber Optic TAG	disbanded
IEEE 802.9	Integrated Services LAN (ISLAN or isoEthernet)	disbanded
IEEE 802.10	Interoperable LAN Security	disbanded
IEEE 802.11	Wireless LAN (WLAN) & Mesh (Wi-Fi certification)	active
IEEE 802.12	100BaseVG	disbanded
IEEE 802.13	Unused[2]	Reserved for Fast Ethernet development[3]
IEEE 802.14	Cable modems	disbanded
IEEE 802.15	Wireless PAN	active
IEEE 802.15.1	Bluetooth certification	
IEEE 802.15.2	IEEE 802.15 and IEEE 802.11 coexistence	
IEEE 802.15.3	High-Rate wireless PAN (e.g., UWB, etc.)	
IEEE 802.15.4	Low-Rate wireless PAN (e.g., ZigBee, WirelessHART, MiWi, etc.)	
IEEE 802.15.5	Mesh networking for WPAN	
IEEE 802.15.6	Body area network	
IEEE 802.15.7	Visible light communications	
IEEE 802.16	Broadband Wireless Access (WiMAX certification)	
IEEE 802.16.1	Local Multipoint Distribution Service	
IEEE 802.16.2	Coexistence wireless access	
IEEE 802.17	Resilient packet ring	hibernating
IEEE 802.18	Radio Regulatory TAG	
IEEE 802.19	Coexistence TAG	
IEEE 802.20	Mobile Broadband Wireless Access	hibernating
IEEE 802.21	Media Independent Handoff	
IEEE 802.22	Wireless Regional Area Network	
IEEE 802.23	Emergency Services Working Group	
IEEE 802.24	Smart Grid TAG	New (November, 2012)
IEEE 802.25	Omni-Range Area Network	Not yet ratified

Source: https://goo.gl/2kD9vK

IAIK TU Graz

Sublayer – Logical Link Control (LLC)

Packet → Frame

Purpose

- Interface to (higher) network layer
- Encapsulate data packet into frame and vice-versa
- Responsibility: Reliable frame delivery within LAN

Services

- Error control (especially important for WLANs)
  - Detect erroneous packets
  - Cancel faulty packets
- Flow control
  - **Not** used with Ethernet → retransmission happens on higher layers
  - **Not** used with WLAN → bit errors common but handled by MAC protocol

IAIK TU Graz

Sublayer – Media Access Control (MAC)

Frame → Signal

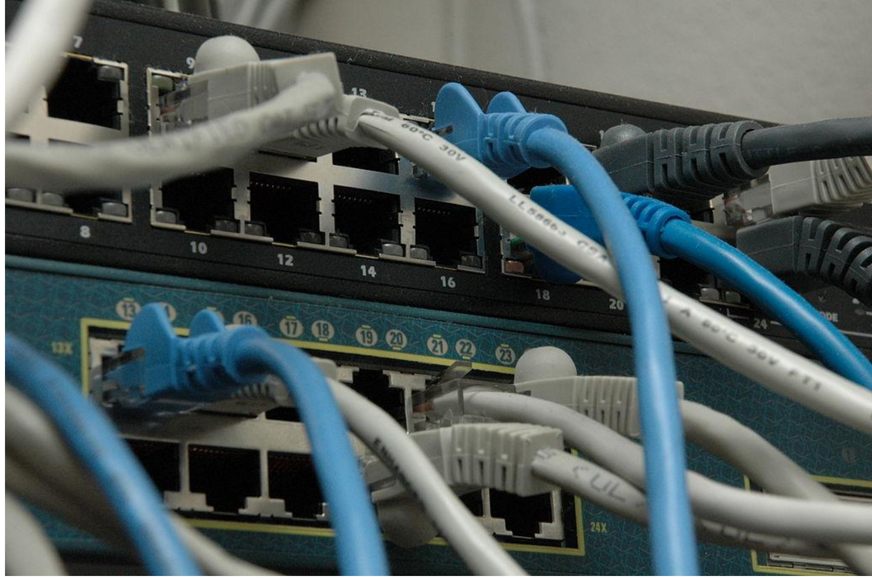
Purpose

- Interface to (lower) physical layer
- Move frames from one network card (NIC) to another via a shared channel

Services

- Physical addressing via MAC address
- Marks begin and end of frames (= frame synchronization)
- Control access to shared medium → collision detection
  - Data packet queueing or scheduling
  - Quality of Service (QoS) control
- Virtual LAN (VLAN)

Local Area Networks



Source: https://goo.gl/Aq7iRP

How it started…

- 1970s: Increasing number of computers in labs and universites → need fast inter-connection
- Design for ~100 nodes
- Connecting to WANs not considered at that time → LANs now need higher levels for that

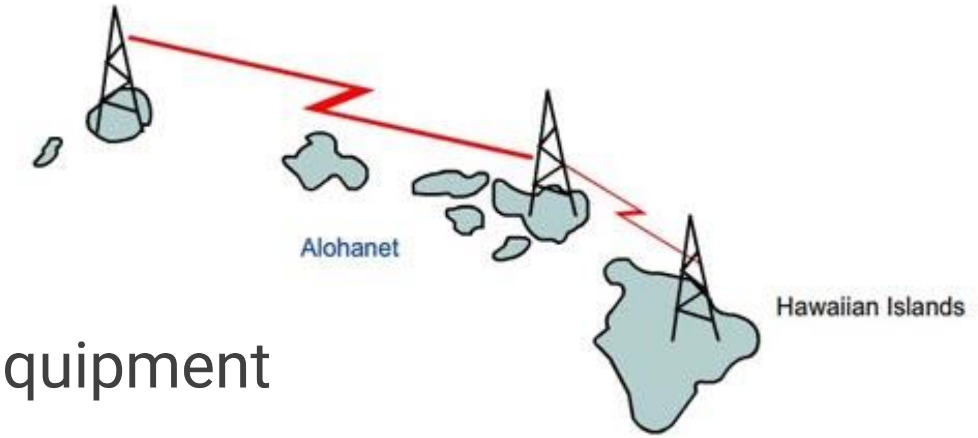
… and it should be „cheap“

- No connections between every computer (point-to-point)
- Minimum amount of expensive cables

→ All linked nodes used a shared medium for transmissions

Example: Wireless networks!

ALOHAnet



Source: http://goo.gl/MDVO05

- Connect different islands using low-cost radio equipment
- All clients talk to a hub on same frequency

→ Who can talk at what time?

The Idea

- Why not just talk and wait for answer?
- Random access
  - Node sends something, waits for ACK from destination
  - If ACK is not seen, resend the frame

  → Dynamic bandwidth allocation

Result: 9600 bits per second, carrier: 400 MHz, bandwidth: 40 KHz

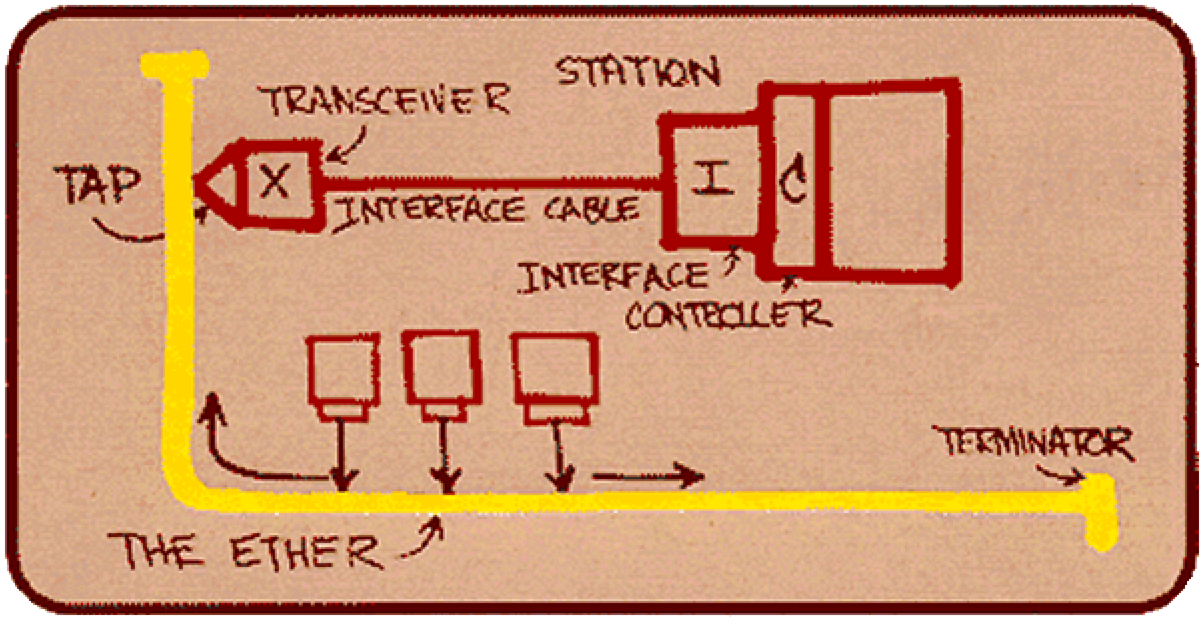
Local Area Networks

On the way to Ethernet…

- Is random access also suited for wired networks?
- 1973: Metcalfe studied ALOHAnet, came up with a concept

- 1976: „Ethernet: Distributed Packet Switching For Local Computer Networks“
  - 2.94 Mbit/s Ethernet
  - 8 bit addresses
  - Manchester signal coding
  - 50 Ω coaxial cable

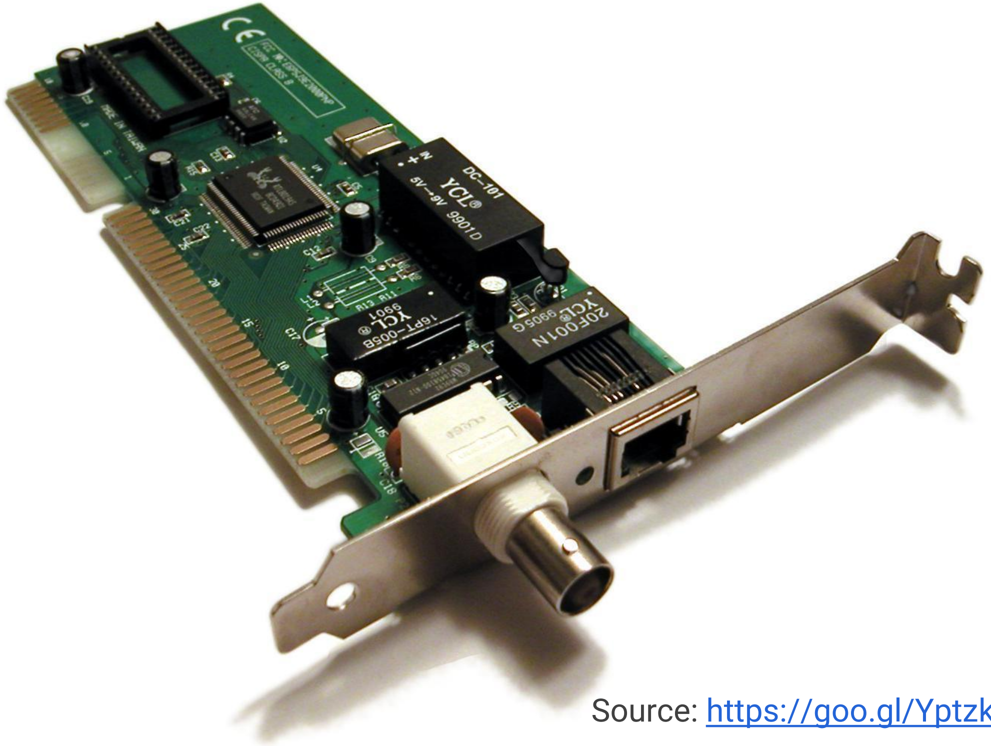
- 1982: Published as standard



Source: http://goo.gl/nu9bWj

Ethernet

Ethernet



Source: https://goo.gl/YptzkF

Ongoing evolution…

- 1981: 10 Mbit/s with 3COM cards
  - Cables: Coaxial, Twisted-pair, Fiber-optic
- 1995: 100 Mbit/s „Fast Ethernet“
- 1999: 1 Gbit/s
- 2002: 10 Gbit/s
  - No more hubs, half duplex mode, collision detection with shared media
- 2010: 100 Gbit/s
- ? 1 Tbit/s
  - Requires different technology, e.g. optical links instead of RJ-45
  - Currently: 400 Gbit/s – Standardized in 12/2017 by IEEE

See: http://goo.gl/80z0tt

Ethernet

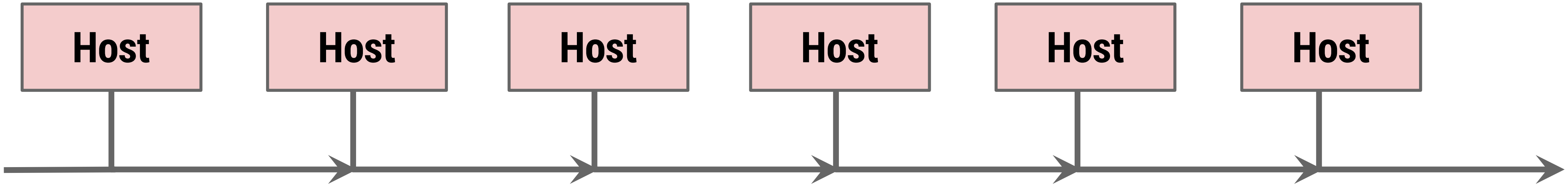
Summarizing the core ideas

- Shared medium (cheap cabling)
- Decentralized: No central instance needed
- Random access for accessing the shared medium

→ *Problem: How to deal with frame collisions?*

→ *Solution: Channel access control*

Important: Only a problem if shared media (hubs) are used!



MAC with Ethernet

Channel access control

= enable it for multiple devices to share one physical medium (e.g. hub)

Mechanism: **Carrier Sense Multiple Access / Collision Detection (CSMA/CD)**

1. *Listen*: Wait while medium is busy
2. *Send*: Transmit frame and meanwhile detect collisions
   Collision occurred? Also inform others using a *jam* signal
3. *Line busy*: Wait certain time (= *backoff period*) and start again at step 1
4. Repeat steps until max. attempt counter reached and end transmission

Nowadays: Usually, we use switches and full-duplex connections

→ Switches isolate each Ethernet segment, no more collisions

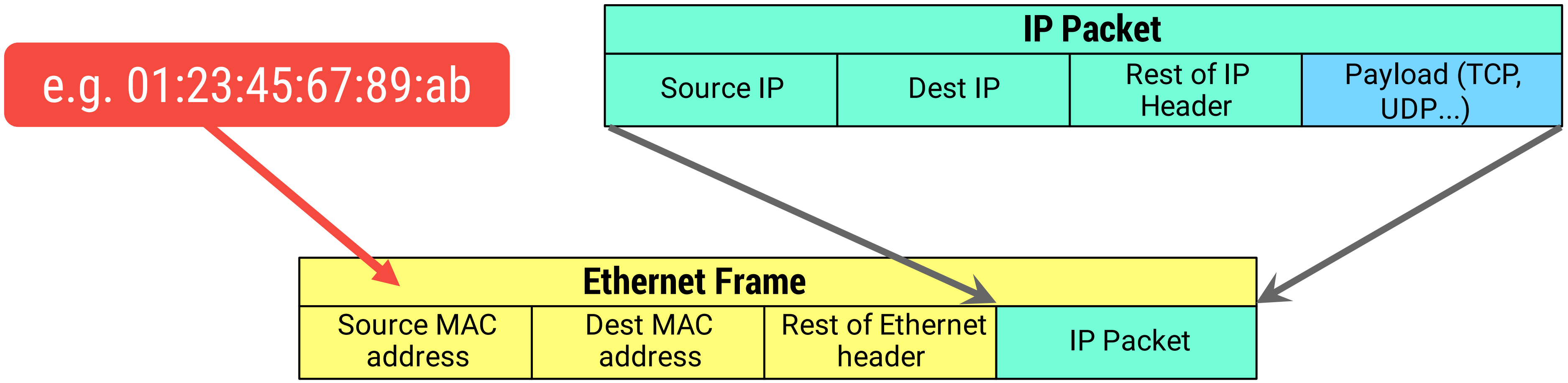
→ CSMA/CD no longer needed

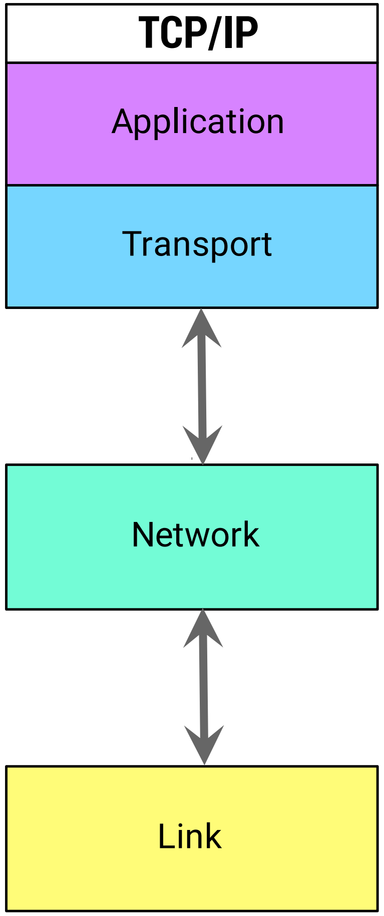
LLC with Ethernet

Principle: Form Ethernet frame from Ethernet header + IP Packet

Ethernet header

- „Source MAC address“ = Source Service Access Point (SSAP)
- „Dest MAC address“ = Destination Service Access Point (DSAP)
- Add remainder: EtherType + CRC checksum
  - E.g. EtherType 0x8000 indicates IPv4 datagram





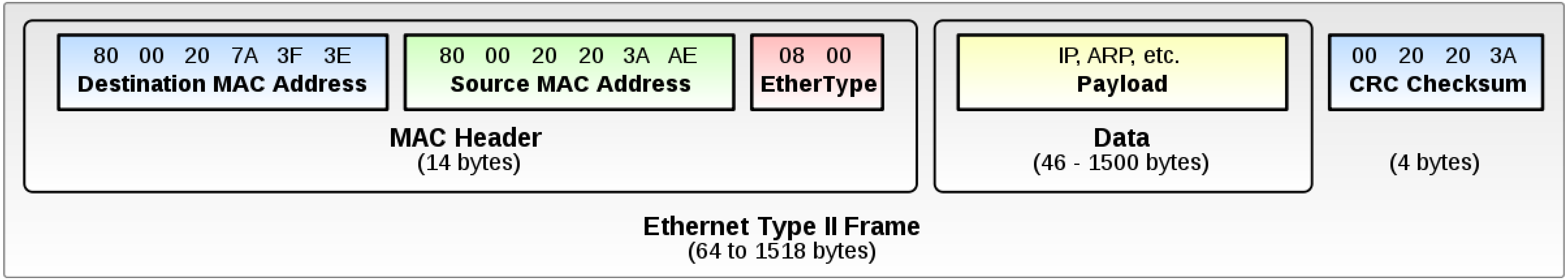
LLC with Ethernet

Conclusion:

Obviously, there is addressing in the link layer

→ Why do we need addressing in IP then?

→ Couldn‘t we use the link layer addresses?



Source: https://goo.gl/ZEjfK1

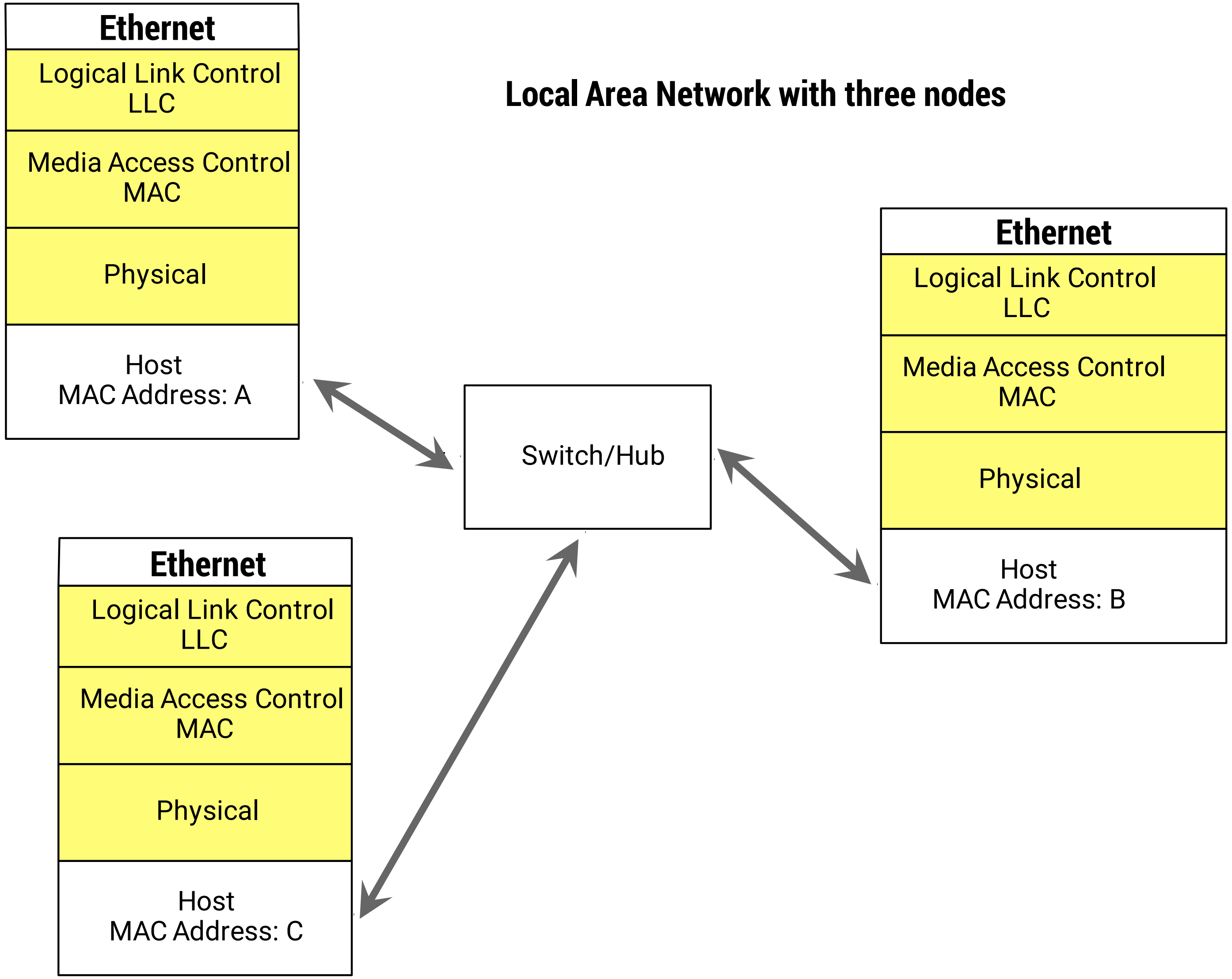
LLC with Ethernet

In LAN:

We could communicate via Ethernet and MAC addresses

Only Ethernet protocols would be needed!

Local Area Network with three nodes

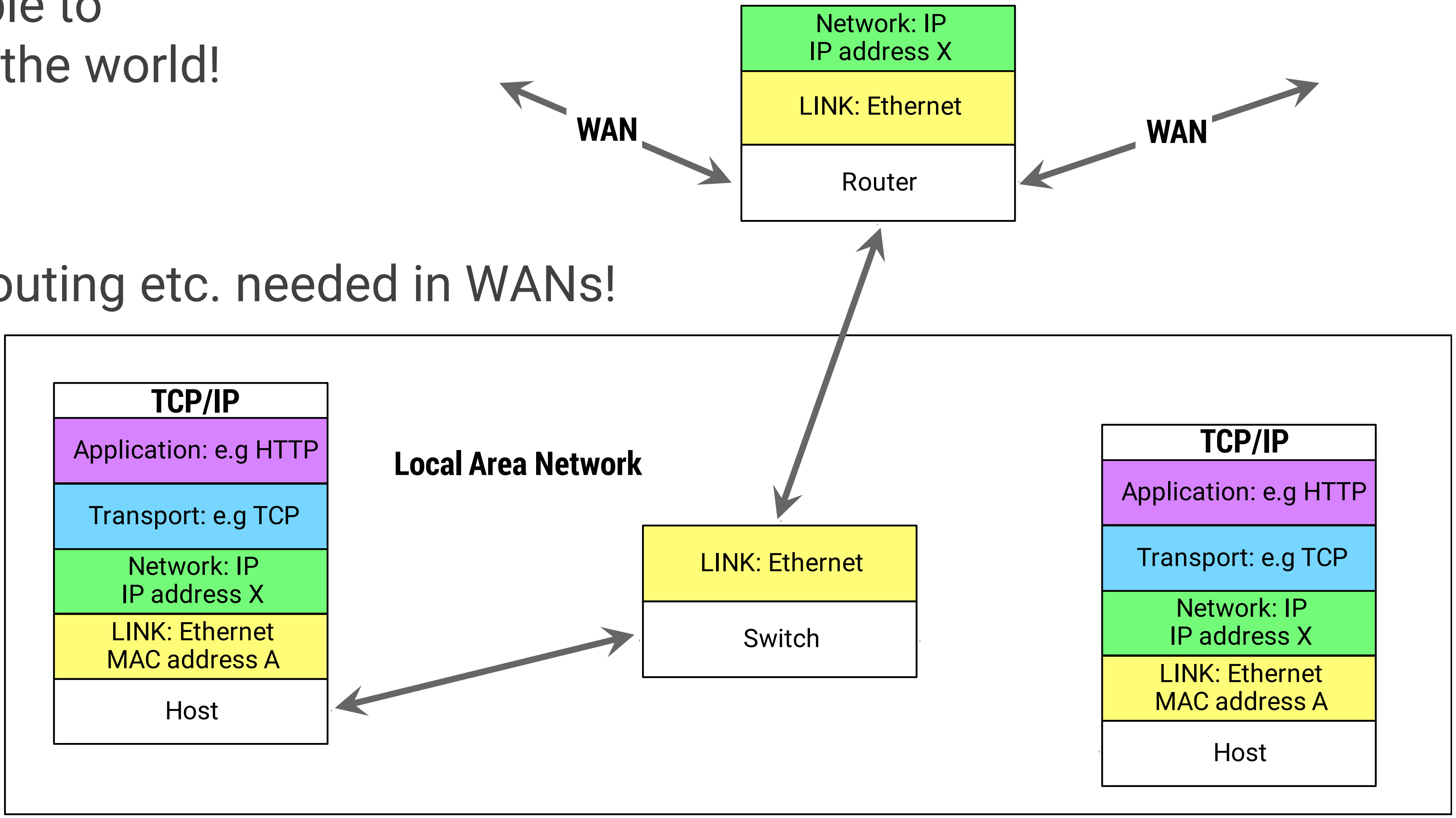


LLC with Ethernet

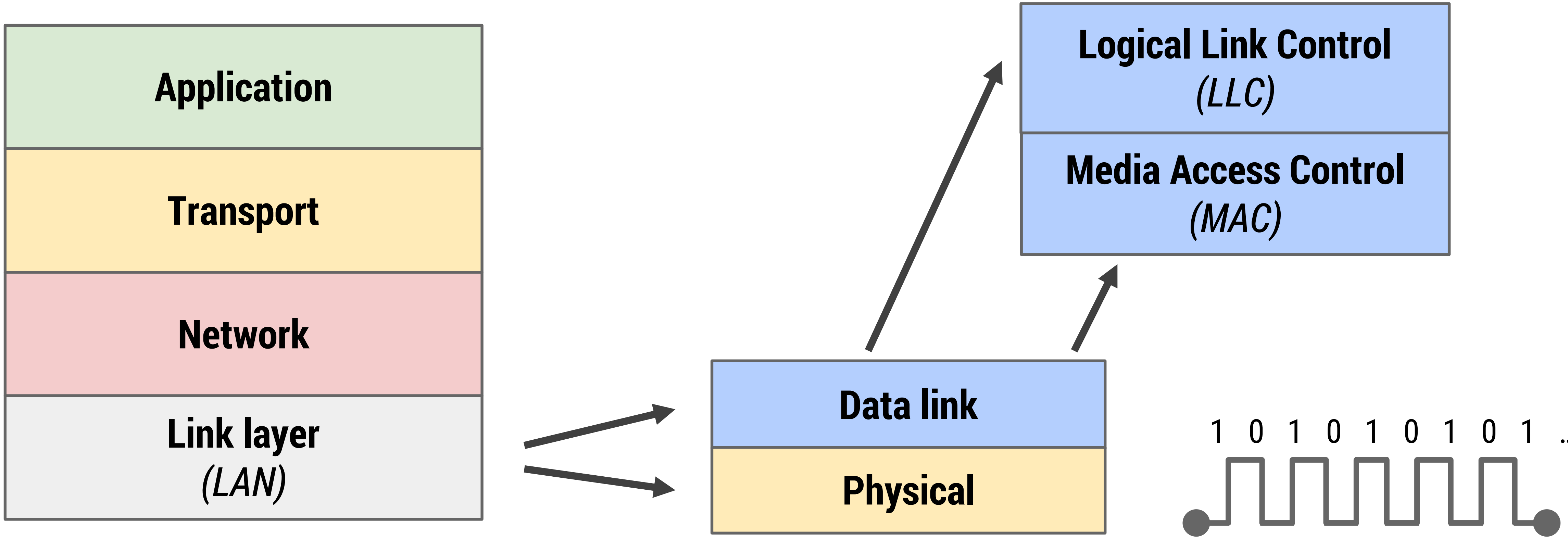
But...

we would not be able to communicate with the world!

→ IP Addressing, routing etc. needed in WANs!



Ethernet Summary



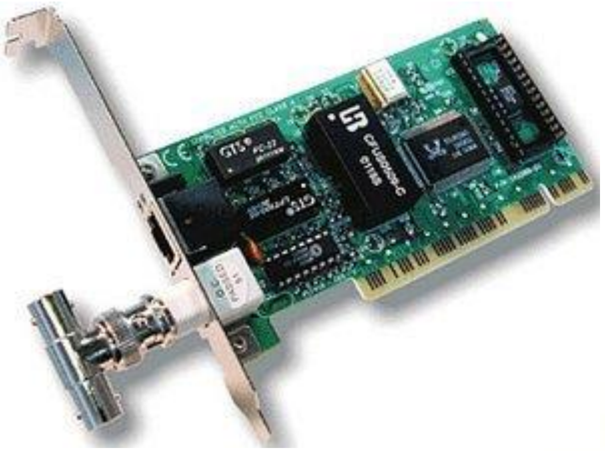
TCP / IP Model

- **LLC layer**: Add Ethernet frame to network (IP) packet
- **MAC layer**: Perform addressing of frames via network cards

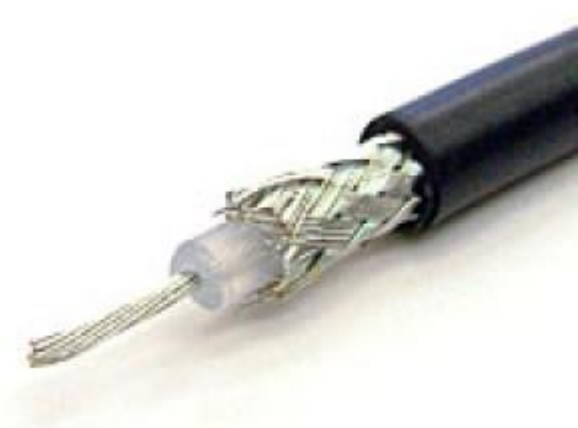
Cables, Hubs, Switches

Ethernet – 10BASE2

„Thin Ethernet“, „Cheapernet“



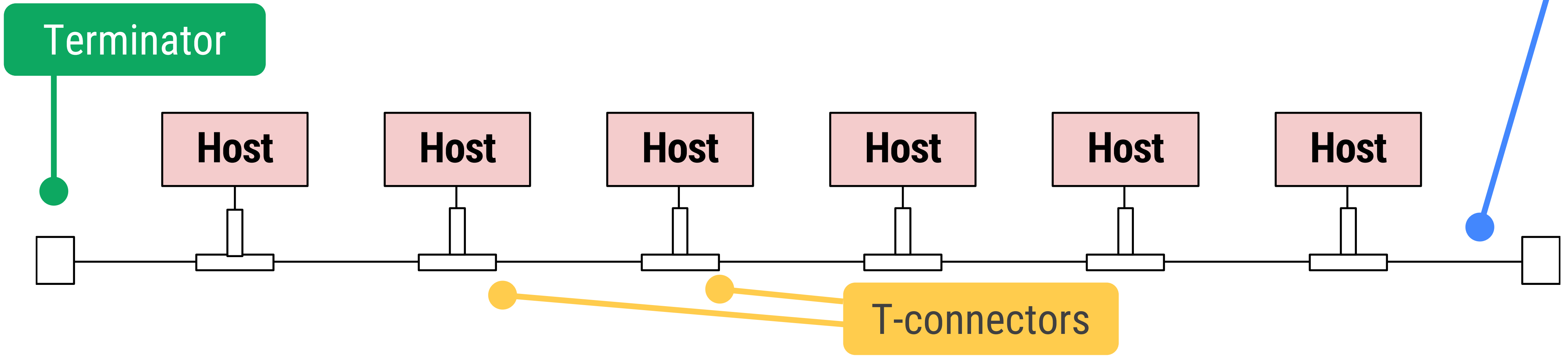
Source: http://goo.gl/OWHBpe



Source: http://goo.gl/KOxYzu

- Started with coaxial cables
- Designed for shared medium: Terminators, T-connectors
- Limited length due to loss of signal quality

RG-58 coaxial cable

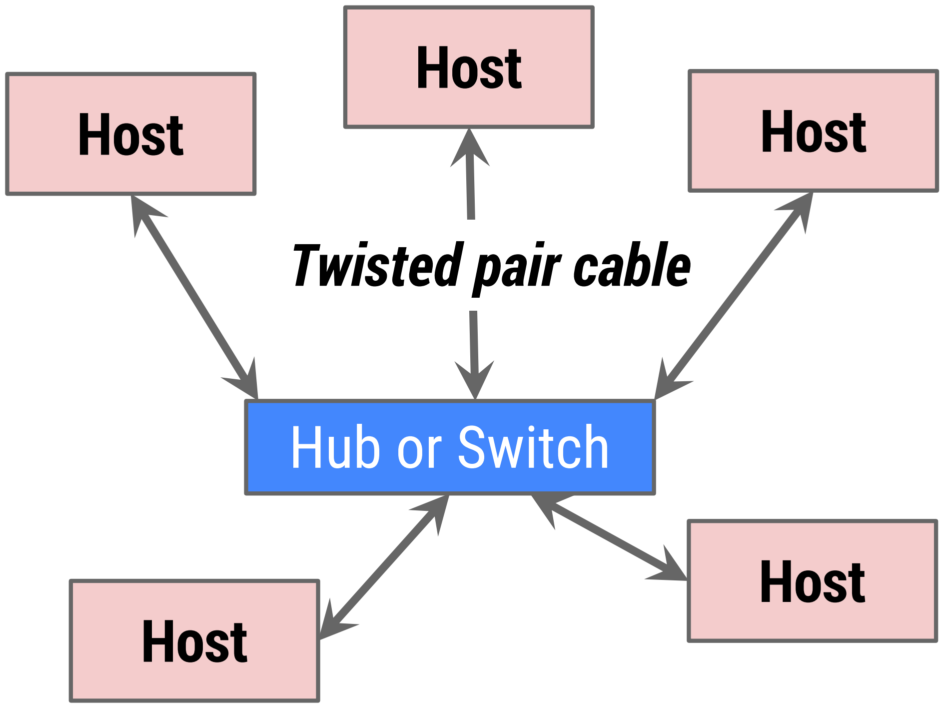


Ethernet – 10BASE-T

„Ethernet over Twisted pair cables“

Source: http://goo.gl/uyila7

- Coaxial cables replaced by nowadays used cables
- Star-shaped technology
  - More reliable approach than bus
- Upgrade from hub to switch easily possible
  - One hardware port for each node
- 10BASE-T introduced full duplex mode



Full Duplex vs. Half Duplex Mode

Half-duplex

- Sending and receiving **not** at the same time

- Quite obvious for a shared medium (hubs, repeaters)

Full-duplex

- Sending and receiving at the same time
  - 1Gbit LAN in full-duplex = 2Gbit at the same time (1Gbit sending, 1Gbit receiving)

- Leads to collision with shared medium
  - However: With full-duplex mode, no more collision handling needed!

- How to get full-duplex?

Hubs or Repeaters

Source: http://goo.gl/zCYRo0

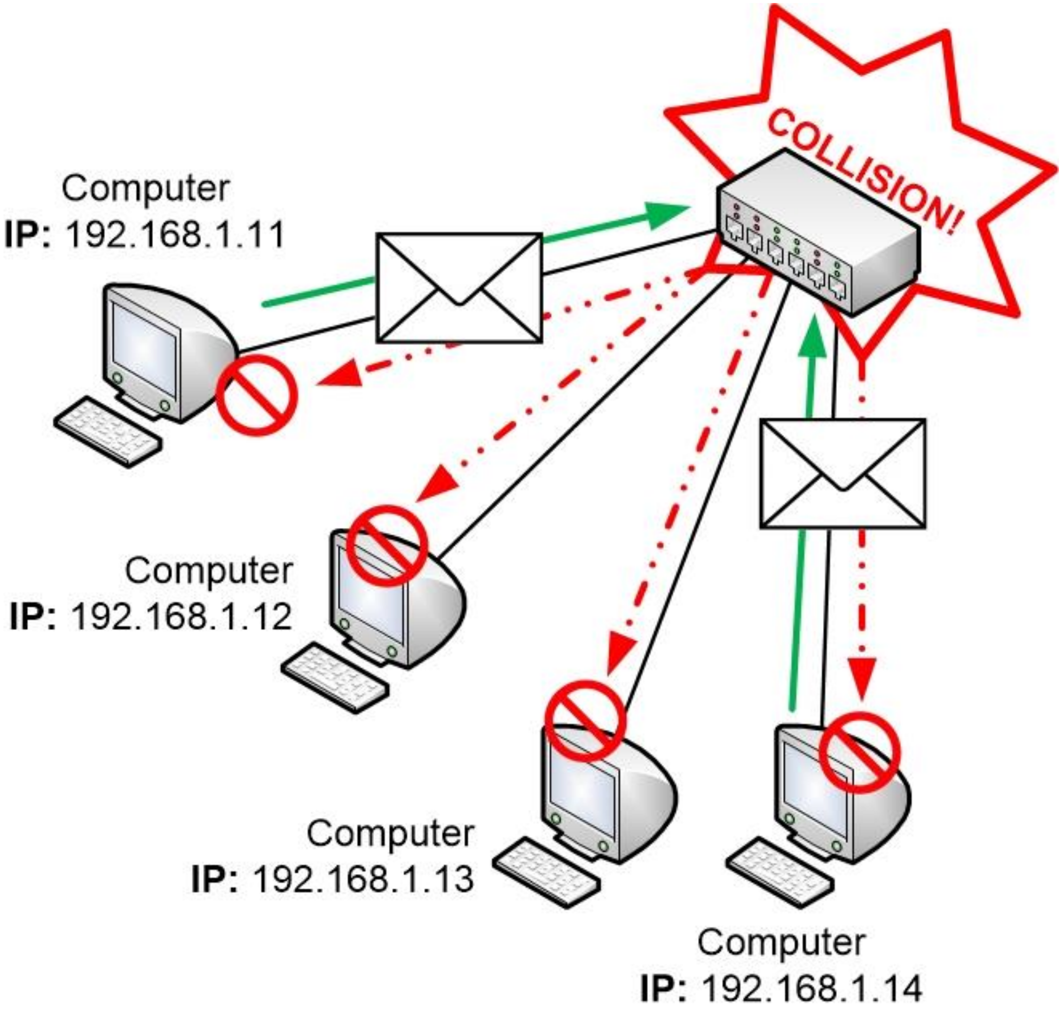
- Extend range of Ethernet
  - Make multiple devices act as single network segment
- Multiple ports, reads signal on port, reconstructs it, sends it to every other port
  - Not very sophisticated, obviously…
- Only half-duplex mode and no intermediate packet storage
  - Either packet is transmitted when received or collision occurs

→ Two main problems:

- Large collision domain
- Decreased performance
  - Although: Good hubs disconnect ports with excessive collisions

Collisions

- The more data in a collision domain, the more collisions!
- **Consequence**: It is getting inefficient…



Q: How to get away from collisions?
A: By replacing hubs with switches!

Source: http://goo.gl/bRI07Q

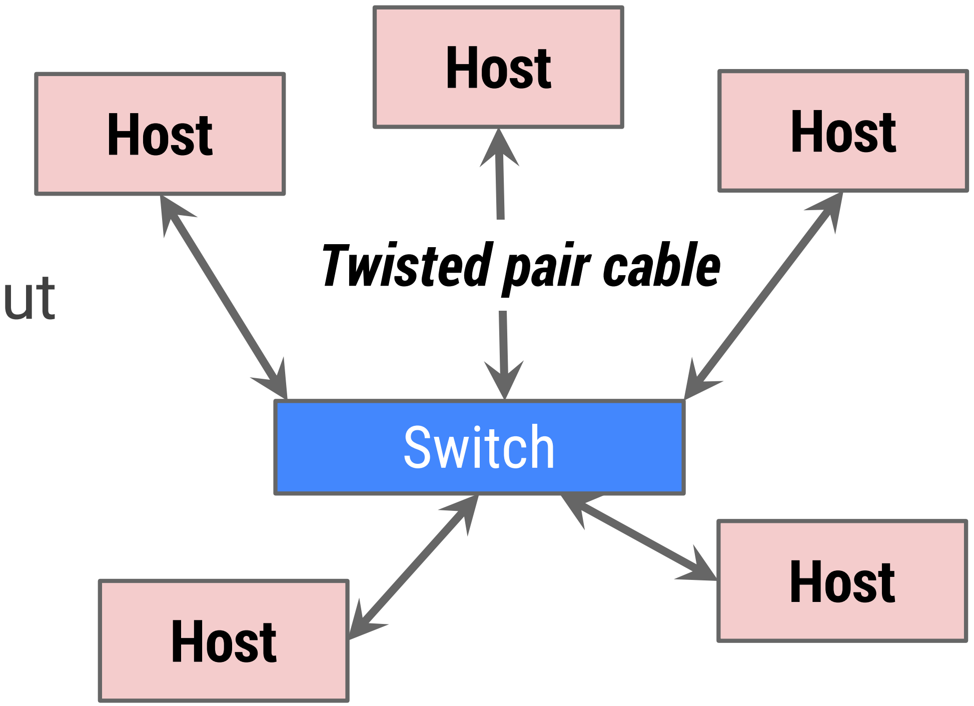
Switches

Source: https://goo.gl/najCrn

- Star topology like hub
  - But more intelligent :-)

- Analyze information from LLC layer (MAC addresses) and forward frames selectively

- Large collision domain (hub) now split into smaller ones → no collisions increase throughput



Note: **Switches** operate on OSI Layer 2

Routers forward IP packets (OSI layer 3)

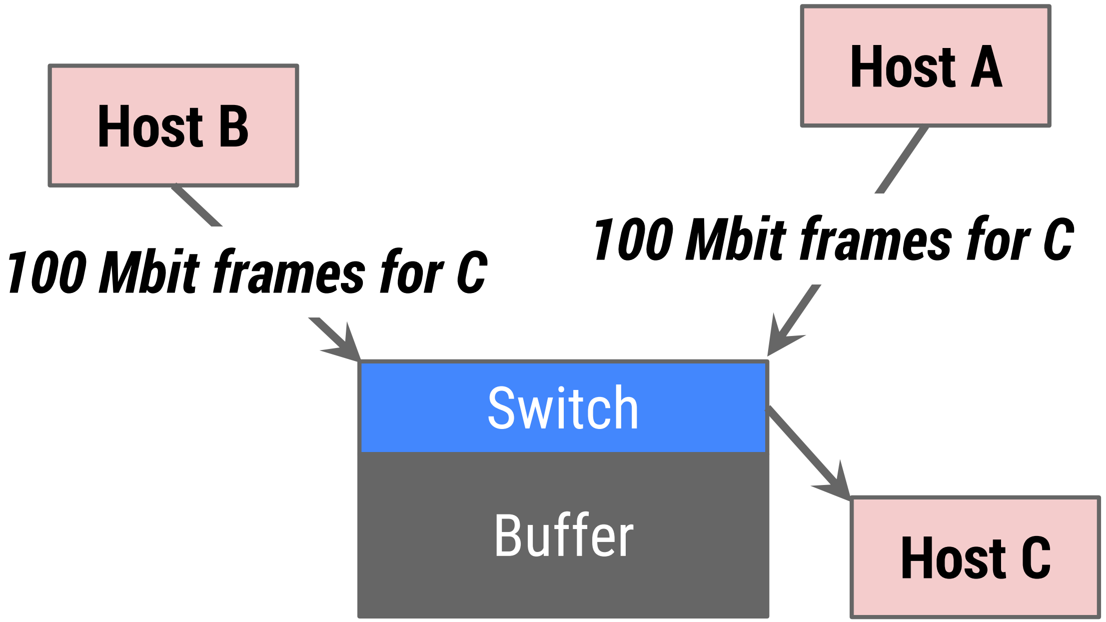
= Switch on OSI Layer 3

Switches

Characteristics

- Transparent to nodes
  - Nodes just use MAC address of each other, send data, receive it
  - Nodes do **not** address the switch!

- The rate a switch receives frames might exceed its output capacity
  - Switches need buffers



Q: How does a switch know where the frame recipients are?

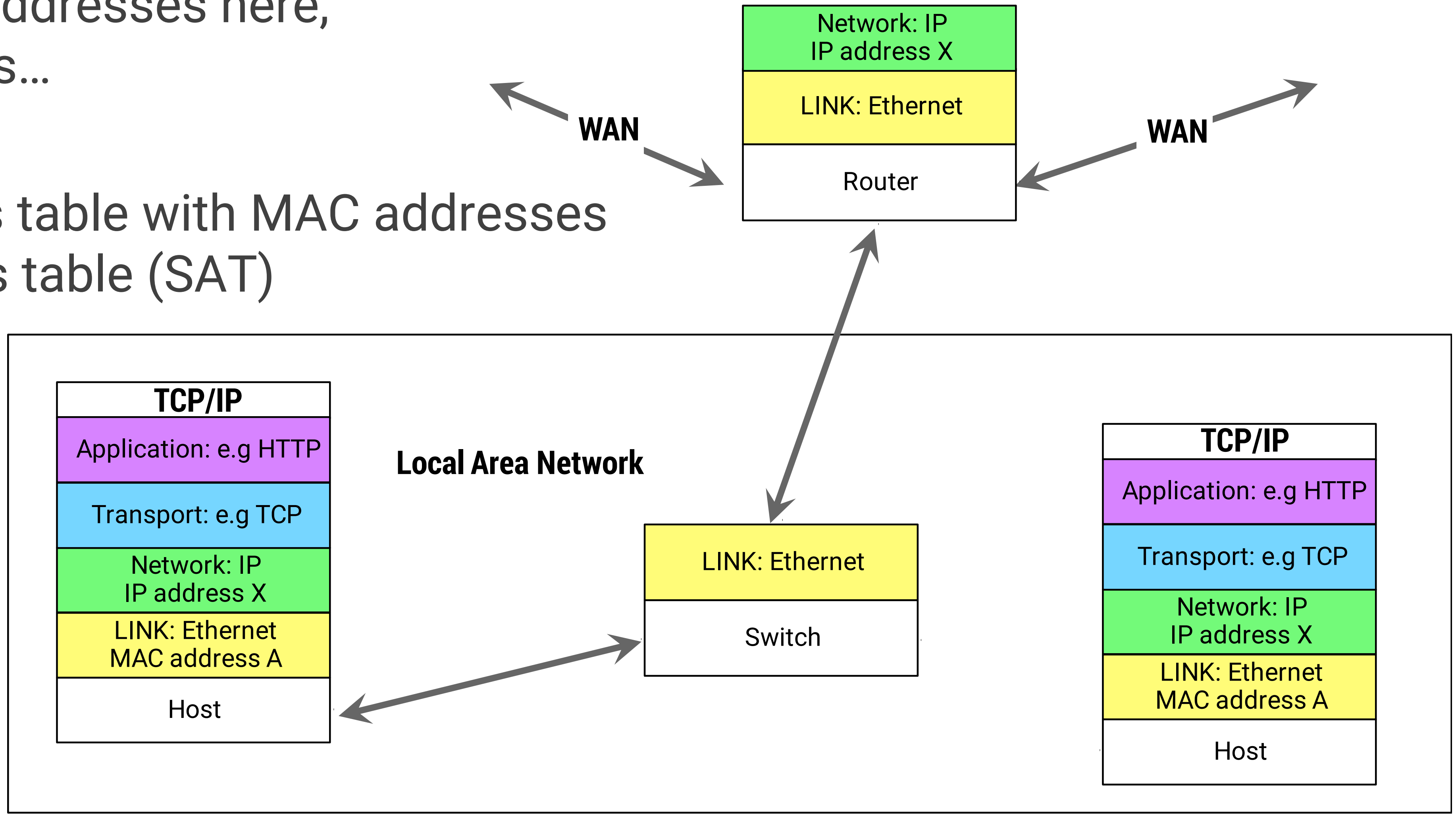
A: Forwarding and filtering

Switches – Forward / Filter

How does it work?

We do not have IP addresses here,
only MAC addresses…

→ Switch maintains table with MAC addresses
= Source address table (SAT)



Forward / Filter

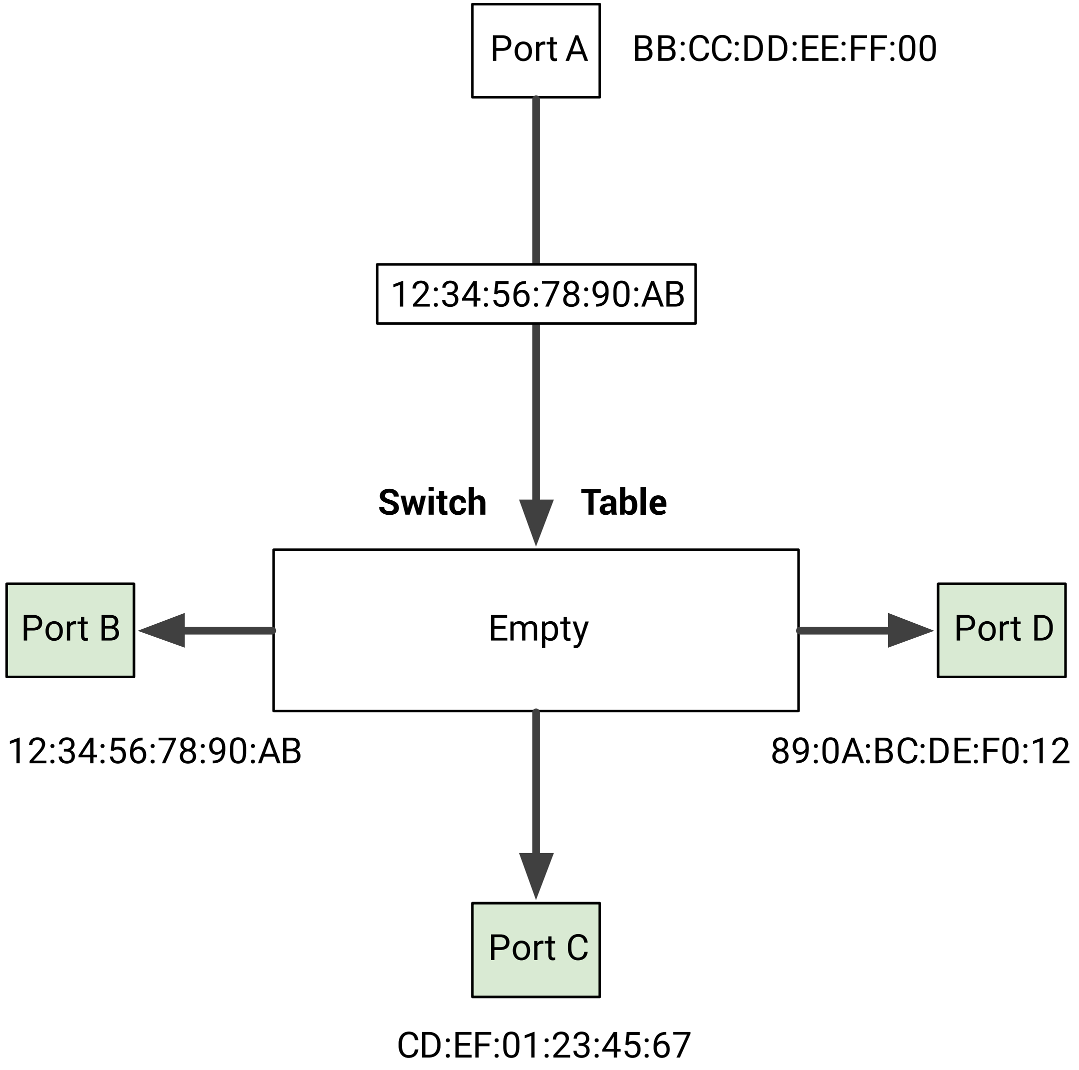
Assumptions

- Source MAC address **not** in table
- Destination MAC address **not** in table

Process

- Switch broadcasts frame to all ports
- **Add** source MAC address and timestamp to table

→ Every node that sends a frame is added to the table



Receives frame

Does not receive frame

Switch table afterwards

BB:CC:DD:EE:FF:00	A	09:34

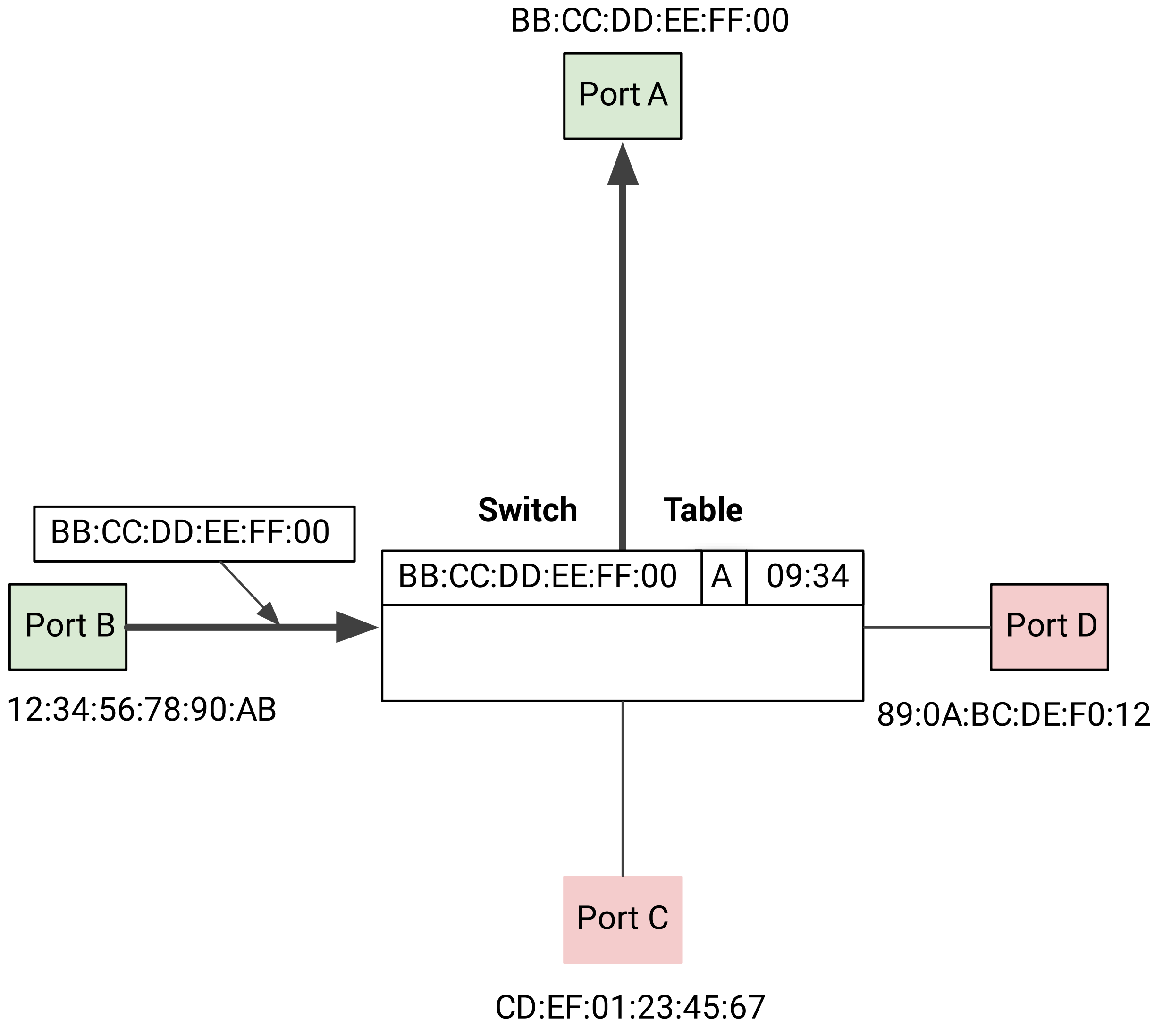
Forward / Filter

Assumptions

- Source MAC address **not** in table
- Destination MAC address **is** in table

Process

- Forward frame to stored Port A
- **Add** source MAC address and timestamp to table



Receives frame

Does not receive frame

Switch table afterwards

BB:CC:DD:EE:FF:00	A	09:34
12:34:56:78:90:AB	B	09:35

Forward / Filter

Assumptions

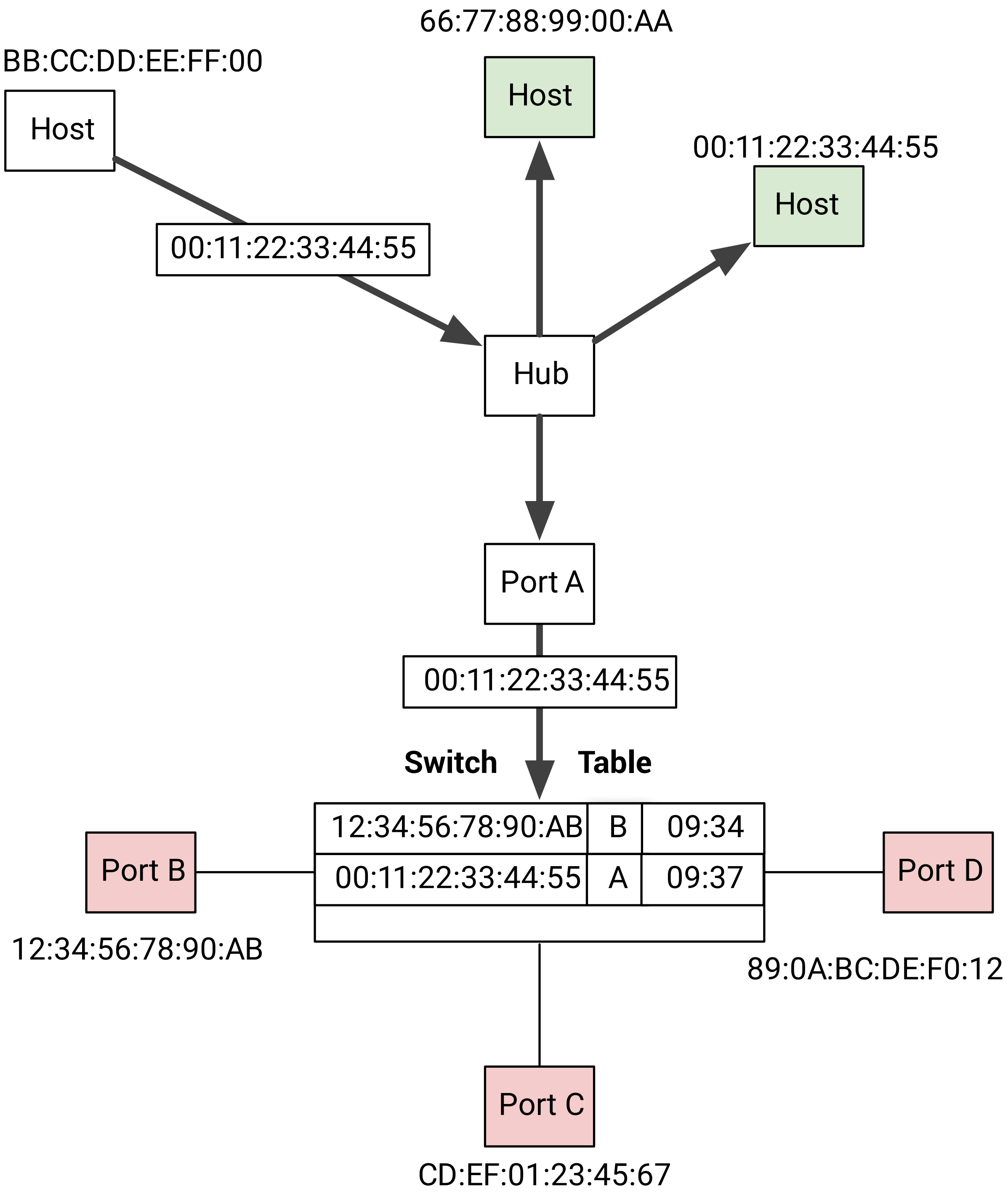
- Destination MAC address of sender is within incoming segment port

Sender: `BB:CC:DD:EE:FF:00`

Destination: `00:11:22:33:44:55`

Process

- Filter (= drop) frame



Receives frame
Does not receive frame

Switch – Properties

- Old entries are deleted from table
  - Compare saved timestamp to max. age threshold value
- Full duplex connections
  - No collisions! No collision handling needed…
  - Send and receive at the same time
- Different duplex mode and speed (10/100/1000 Mbit/s) per port
- Build trees of multiple switches
  - Spanning Tree Protocol (STP)

Switches – VLANs

„Virtual Local Area Network“

- Behave like real separated LANs on one switch
  - No traffic broadcast from one VLAN into other
  - Efficient use of switches
    - E.g. 100 port switch: VLAN A with 90 nodes, VLAN B with 10 nodes

Advantages

- Easy management
  - Modify switch ports and user is in other VLAN (e.g. with different firewall rules)
- Performance aspects
  - Broadcasts target smaller network segments
  - „Traffic Shaping“, e.g. prioritize VoIP traffic in certain VLAN

Cables, Hubs, Switches – Summary

Source: http://goo.gl/uyila7

- Cables
  - Coaxial
  - Twisted pair: Current standard
- Full-duplex, half-duplex connection
- Hubs
- Switches
  - Basics
  - VLANs

Outlook

- 27.11.2019
  - Between Link and Network Layer: ARP
  - Network layer: IPv4, Addresssing, Fragmentation, NAT

- 04.12.2019
  - Network layer: IPv6
    - Addressing, Differences to IPv4, NDP, ICMPv6
  - Transport layer: TCP / UDP
    - Flow and Congestion control

Bachelor@**IAIK Topics** + Student **Research Awards**

Friday **29 Nov** 2019, **12:00–13:00**

IAIK Foyer, Inffeldgasse 16a, Ground floor

www.iaik.tugraz.at/bachelor