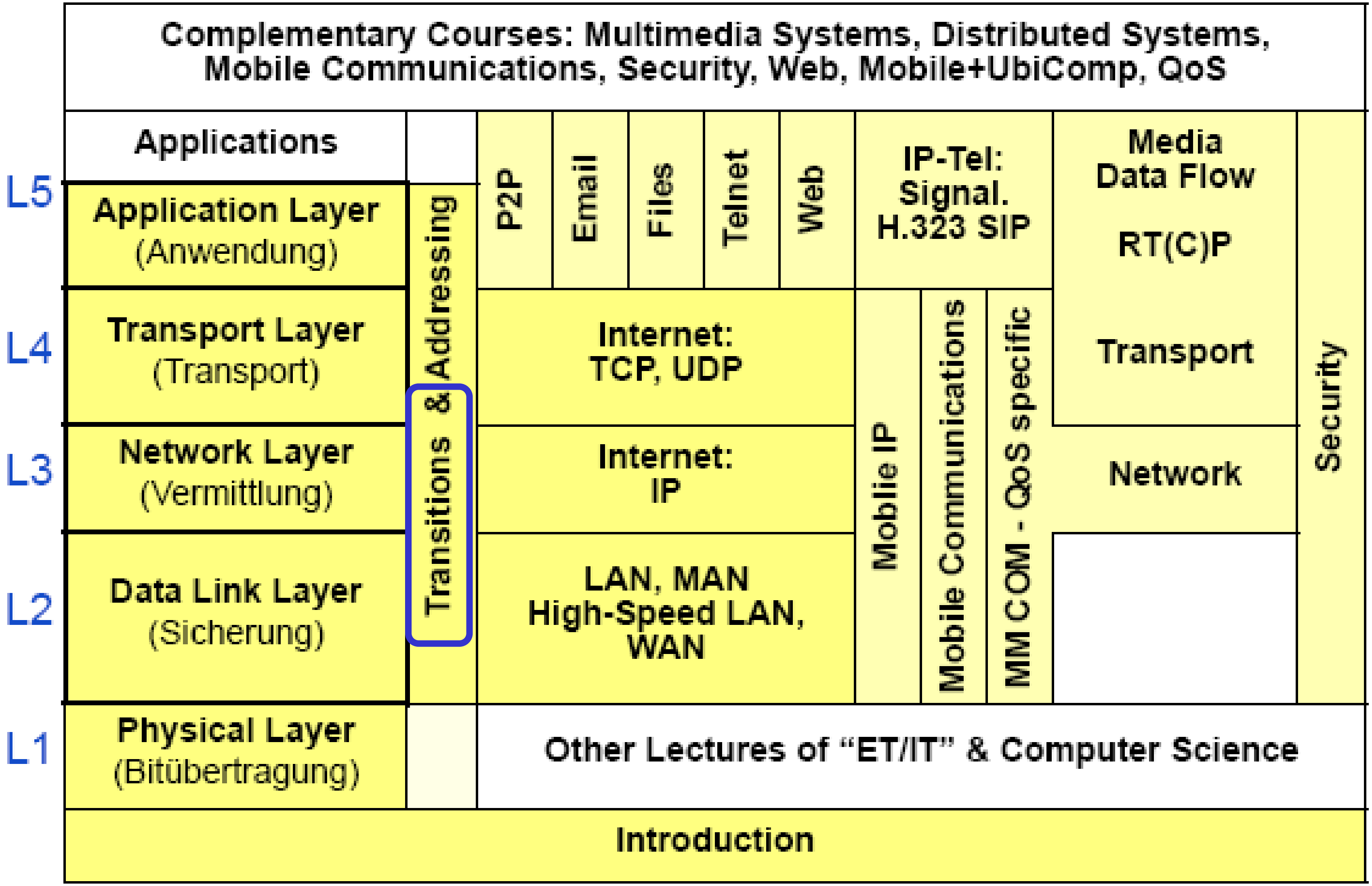
Computer Networks I

Internetworking

Prof. Dr.-Ing. **Lars Wolf**

IBR, TU Braunschweig
Mühlenpfordtstr. 23, D-38106 Braunschweig, Germany,
Email: wolf@ibr.cs.tu-bs.de

Scope



Complementary Courses: Multimedia Systems, Distributed Systems, Mobile Communications, Security, Web, Mobile+UbiComp, QoS
Applications
L5
Application Layer (Anwendung)
L4
Transport Layer (Transport)
L3
Network Layer (Vermittlung)
L2
Data Link Layer (Sicherung)
L1
Physical Layer (Bitübertragung)
Transitions & Addressing
P2P
Email
Files
Telnet
Web
IP-Tel: Signal. H.323 SIP
Media Data Flow
RT(C)P
Transport
Network
Internet: TCP, UDP
Internet: IP
LAN, MAN High-Speed LAN, WAN
Mobile IP
Mobile Communications
MM COM - QoS specific
Security
Other Lectures of "ET/IT" & Computer Science
Introduction

Overview

1 Motivation

Many heterogeneous networks
- past, nowadays, in future

Heterogeneous network technologies (data link):
- WAN: telephone networks, ISDN, ATM, ...
  mobile comm.: GSM, UMTS, DECT, Bluetooth, Zigbee, ...
- LAN: 802.3, 802.4, 802.5, 802.11, 802.16, ...
- MAN: FDDI, ...

Heterogeneous protocol architectures:
- former SNA (> 20 000 networks), DECNET (> 2000)
- OSI, ...
- Novell NCP/IPX, Appletalk
- TCP/IP

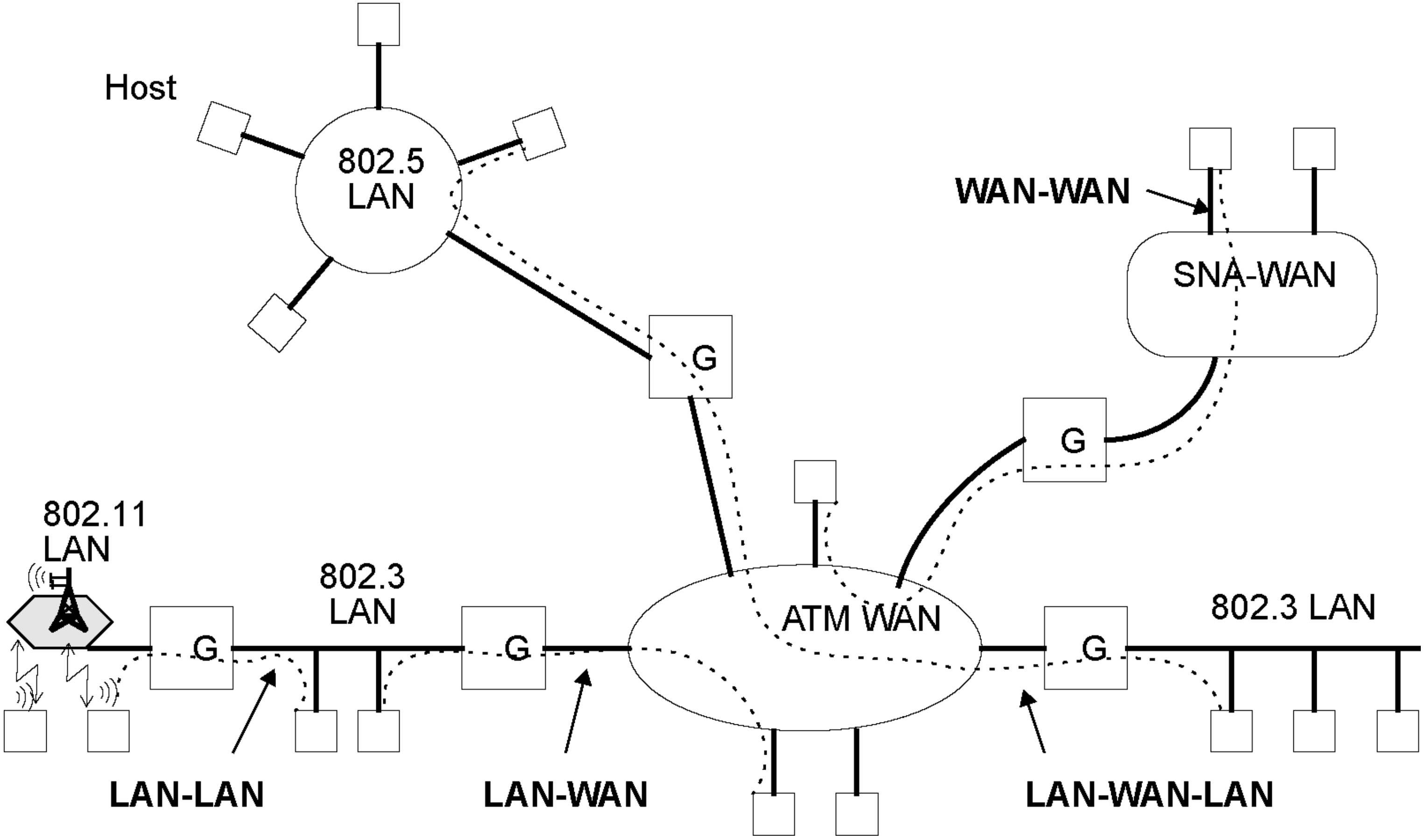
Heterogeneous application architectures (with same overall purpose):
- Email, Peer-to-Peer protocols
- Information access (WWW, WAP)

Changes in the near future ??
- high investments, migration becomes difficult
- decentralized investment decisions
  - departments install different networks
- constantly new technologies

Networks can differ

Item	Some Possibilities
Service offered	Connection oriented vs. connectionless
Protocols	IP, IPX, SNA, ATM, MPLS, AppleTalk, etc.
Addressing	Flat (802) vs hierarchical (IP)
Multicasting	Present or absent (same for broadcasting)
Packet size	Maximum different among nearly any two networks
Quality of service	Present or absent; many different flavors
Error handling	Reliable, ordered, unreliable, or unordered delivery
Flow control	Sliding window, rate control, other, or none
Congestion control	Leaky bucket, token bucket, RED, choke packets
Security, Trust	Privacy rules, encryption, etc.
Parameters	Different timeouts, flow specifications, etc.
Accounting	By connect time, by packet, by byte, or not at all

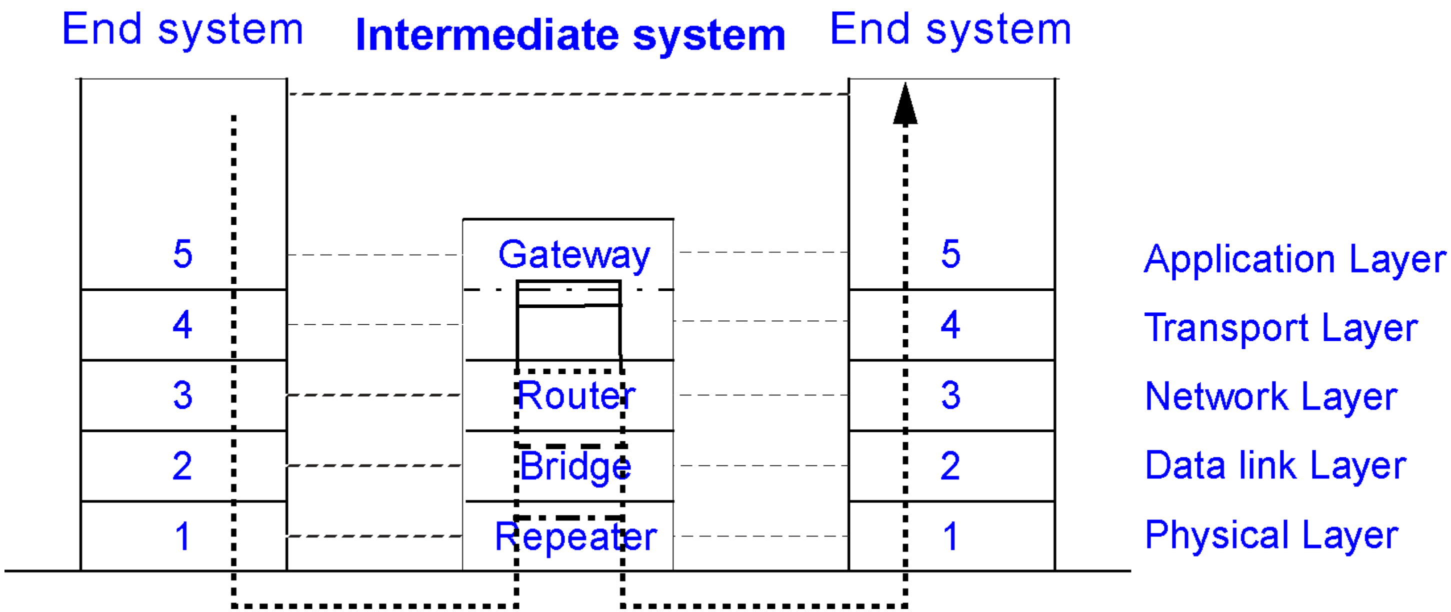
Interconnecting Different Networks



Why is it desirable to connect (heterogeneous) networks?

- resource sharing (CPU, data bases, programs, mailboxes, ...)
- increased availability
- ...

2 Connecting Networks by “Relays”



Layer 1: Repeater / Hub

- copies bits between cable segments
- works solely as a repeater (does not modify the information)
- does not influence the traffic between networks
- example: connecting 802.3 cable segments (larger range)

Layer 2: Bridge / Switch

- relays frames between LANs (MAC level)
- minor frame modifications, increases the number of stations
- example: 802.x to 802.y

Connecting Networks by “Relays”

Layer 3: Router (or Layer 3 Gateway)

- relays packets between different networks
- (modifies packets)
- (converts different addressing concepts)
- (example: X.25 to SNA)

Layer 4 - 5: Gateway (or Protocol Converter)

- converts one protocol into another
  - (usually no1-to-1 mapping of functions)
- examples:
  - TCP in ISO Transport Protocol
  - OSI Mail (MOTIS) in ARPA Internet Mail (RFC 822)
  - change of media encoding (transcoding)
  - SIP to H.232 signaling for IP Telephony

Note:

- names (in products) are often intermixed
  - e. g. bridge and switch

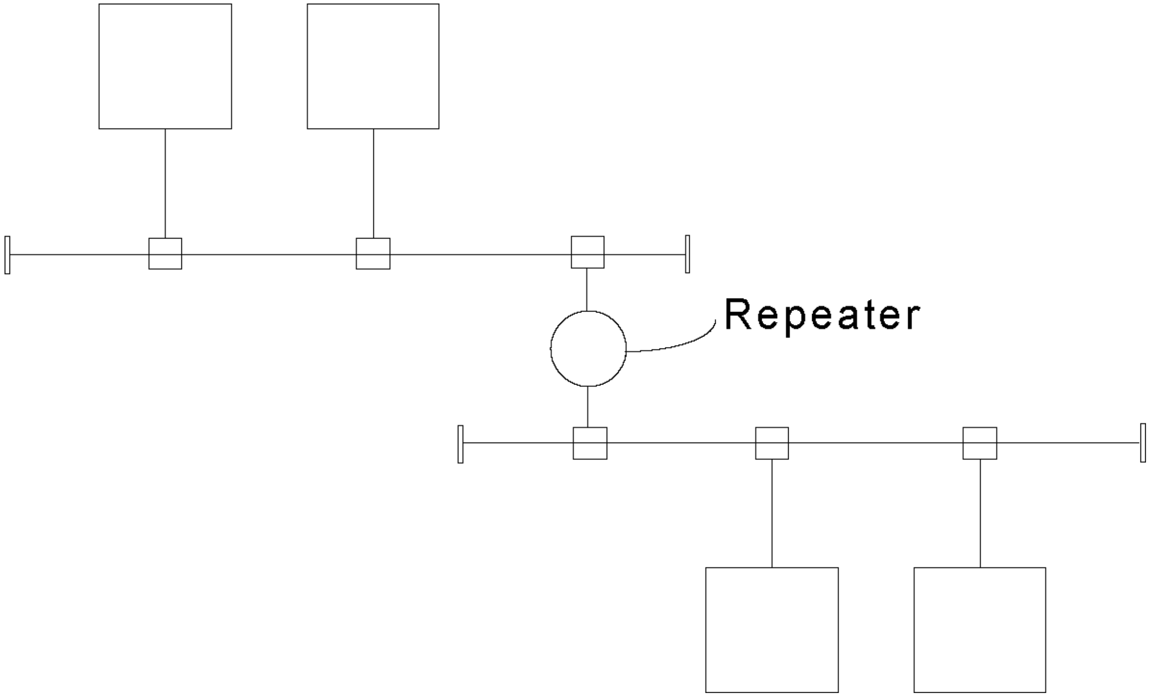
Basic components

- 2 or more network connections
- connection entitty
- control entity

2 Paths:

- control path and data path

2.1 Repeater (Physical Layer)

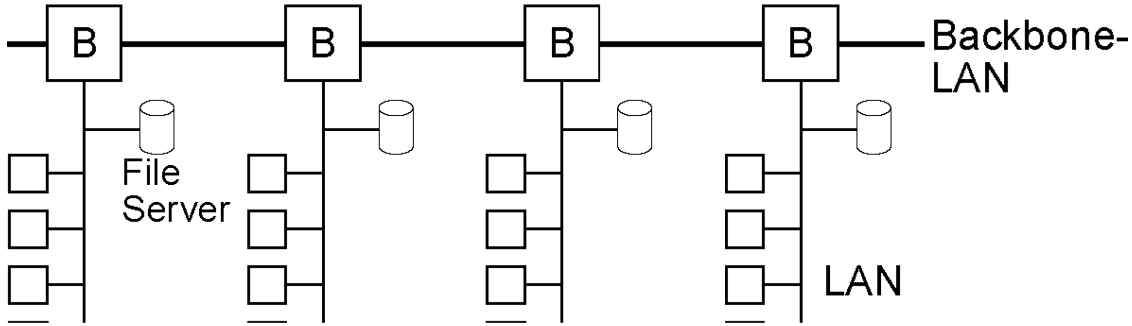


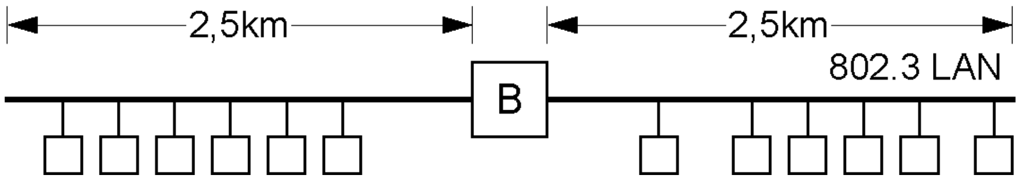
example: IEEE 802.3 configuration

Function

- to amplify the electrical signals
- to increase the range

2.2 Bridge (Data Link Layer)



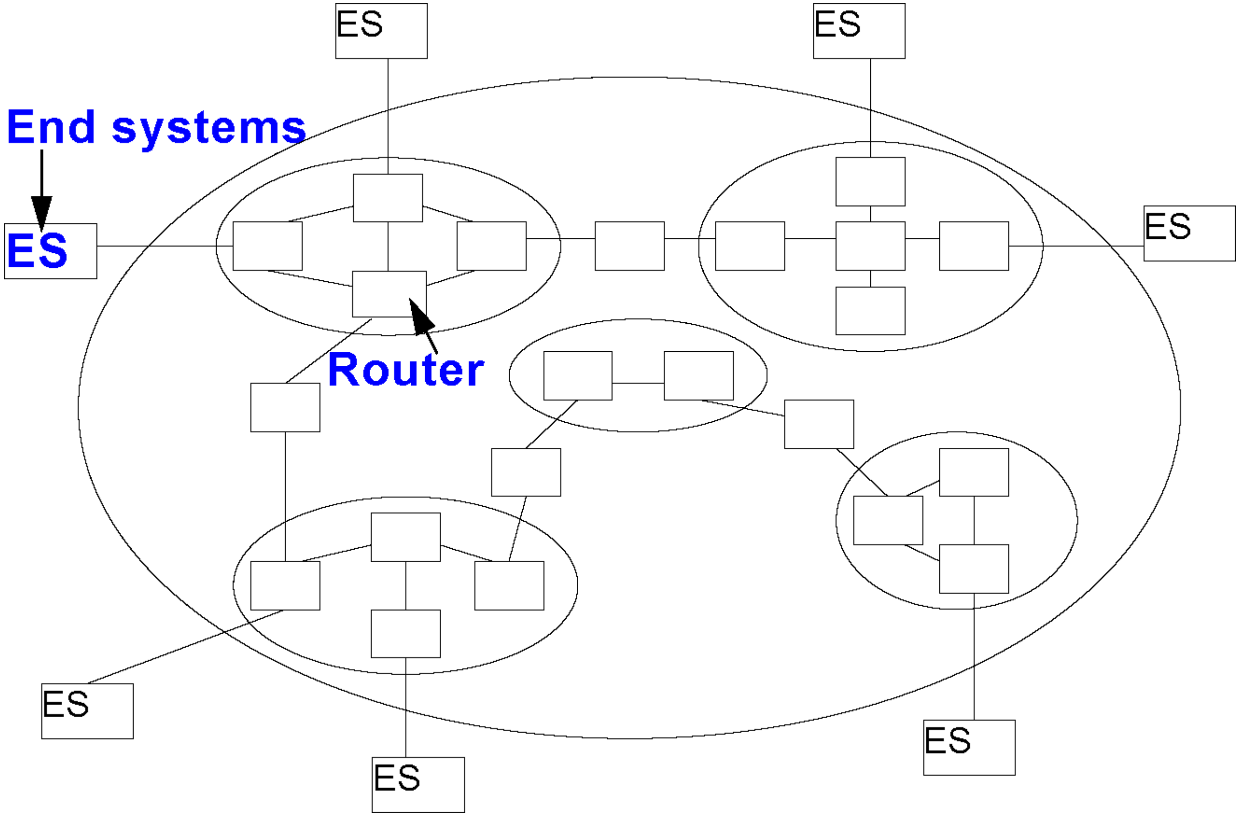


Tasks:

- to couple different LANs
- to provide scalability of networks
- to increase capacity
- to cover larger distances
- to increase reliability
- to improve security
- to offer independence from protocols (IP, OSI, ...)

important goal: to achieve TRANSPARENCY

2.3 Router (Network Layer)



Data transfer from end system to end system

- several hops, (heterogeneous) subnetworks
- compensate for differences between end systems during data transmission

2.4 Gateway (Application Layer)

Task

- data format adaptation
- control protocol adaptation

Example media

- audio database with CD audio encoding and MIDI output at the system
- different audio data formats are converted in real time

Example signaling

- telephone connection establishment
  - From ordinary telephone (POTS)
  - to audio conferencing system (computer)
- adaptation by functional transformation and stubs

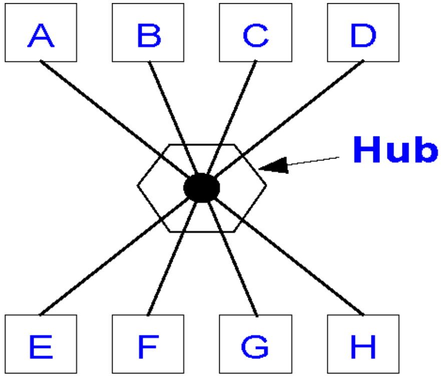
2.5 Repeaters, Hubs, Bridges, Switches

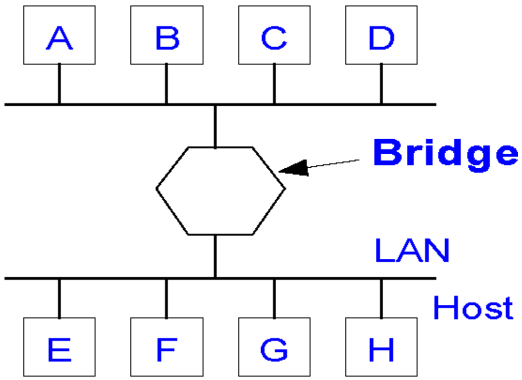
Repeaters & Hubs (L1):
- one collision domain

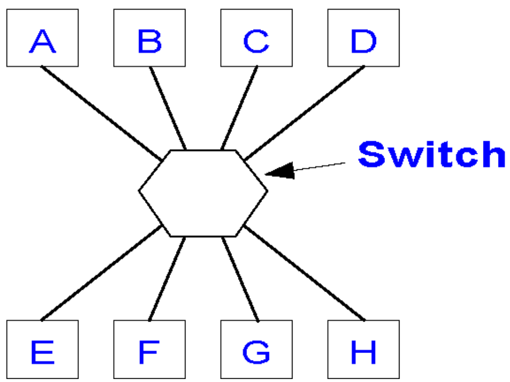
Bridges (L2):
- connects two or more LANs
  - (potentially of different types)
- each line is its own collision domain
- typically store-and-forward and (traditionally) CPU-based

Switches (L2)
- typically connects two or more computers
- each port / line is its own collision domain (no collisions)
- typically cut-through switching devices
  - begin forwarding as soon as possible
  - when destination header has been detected, before rest of frame arrived
- hardware-based

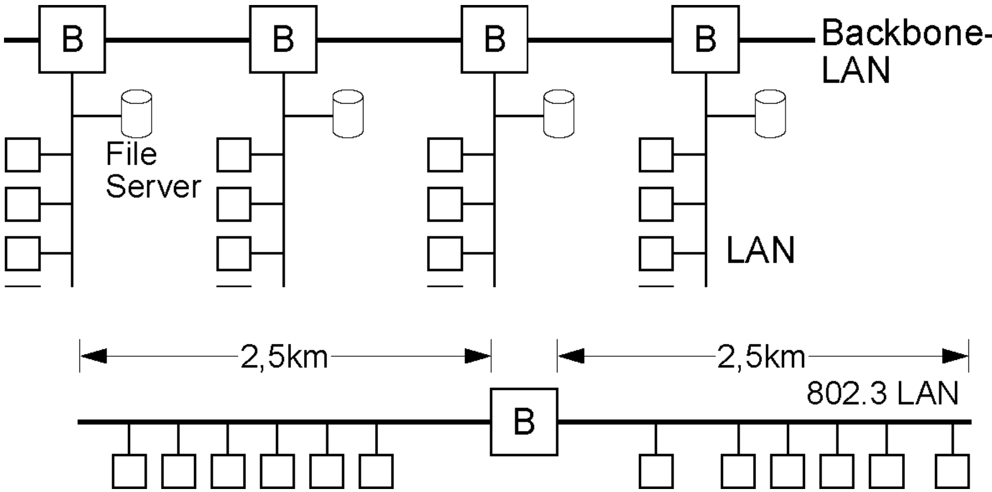
Bridges vs. Switches
- sometimes difference seems to be more a marketing issue than technical one







3 Bridge (Data Link Layer)

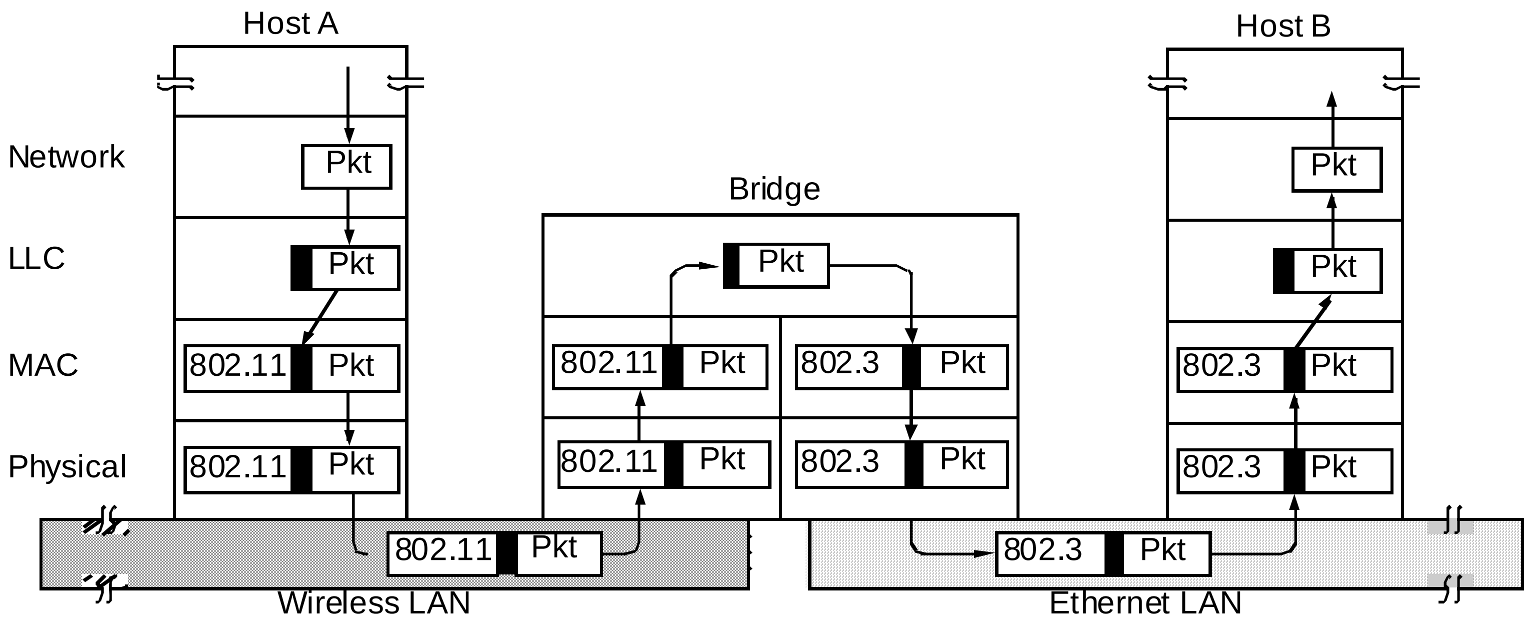


Tasks:

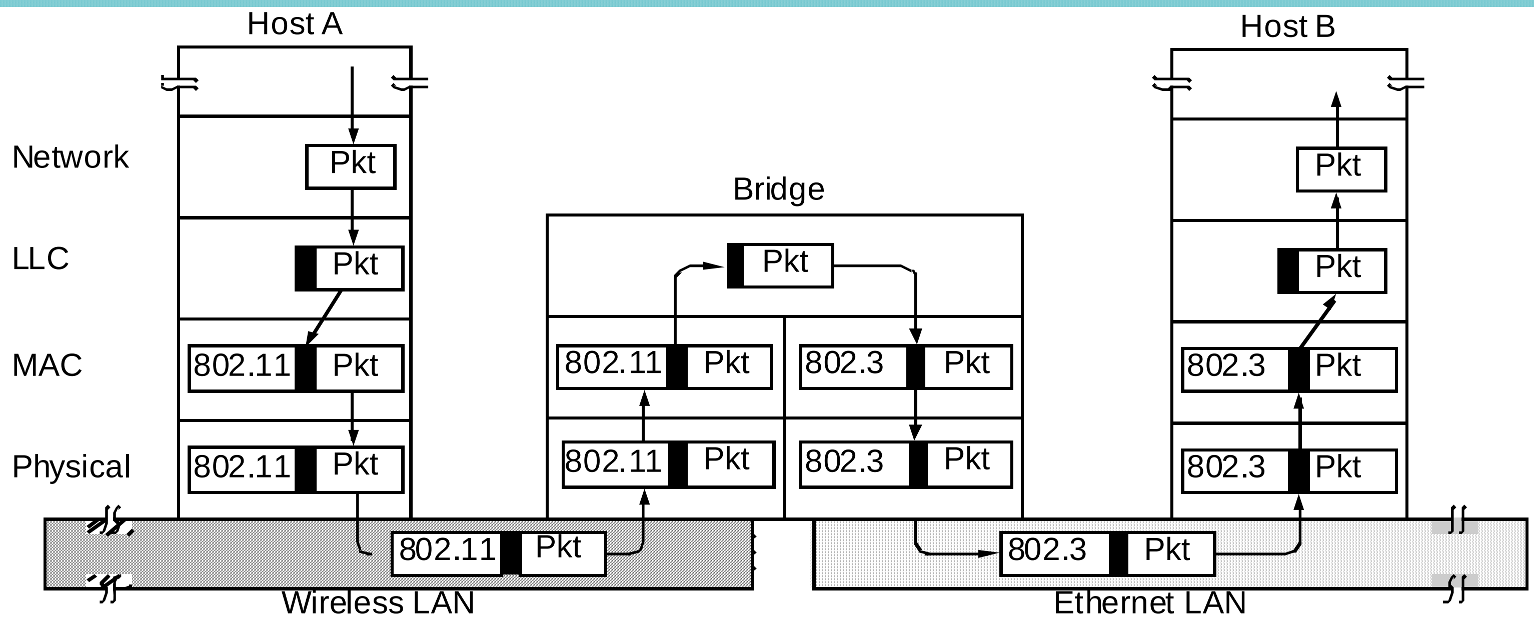
- coupling of different LANs
- scalability of networks
- to increase capacity
- to cover larger distances
- to increase reliability
  - bridge serves as "fire door"
- to improve security
  - stations can work in a promiscuous mode, i.e., read all frames on the network
  - bridge placement limits the spreading of information
- to offer independence from protocols (IP, …)
  - in opposite to routers

Important goal: to achieve TRANSPARENCY

- change attachment point without changes to HW, SW, configuration tables
- machines on any two segments should be able to communicate without regard to types of LANs used (directly or indirectly)


Host A
Host B
Network
LLC
MAC
Physical
Bridge
Pkt
802.11
802.3
Wireless LAN
Ethernet LAN

3.1 Connecting 2 different Networks: IEEE 802.x - Bridges



Example: 802.11 (Wireless LAN) and 802.3 (Ethernet)

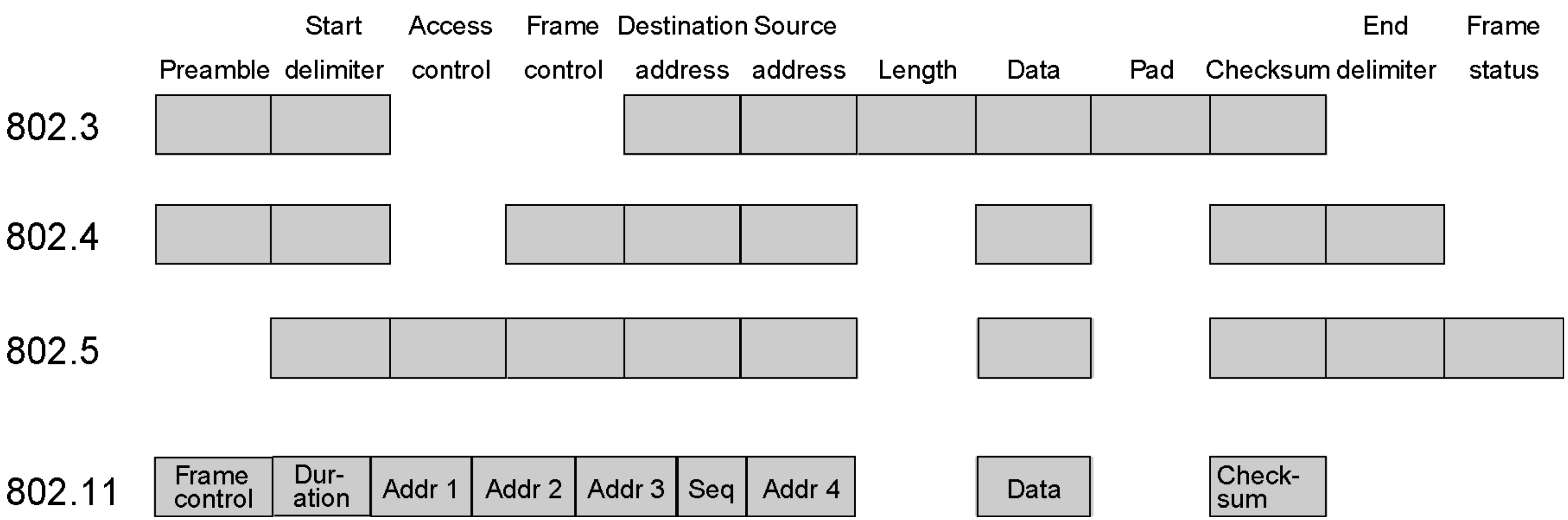
Approach

- LLC as common layer
- frames are routed to the respective MAC
- bridge contains
  - its own implementation for each different MAC
  - for each physical layer the corresponding implementation

802.x <-> 802.y: Tasks

Some different 802.x frame formats:

- there are even more different frame formats ...
- some fields are technically necessary in one case but useless in another
  - e.g. DURATION of 802.11



802.x <-> 802.y: Tasks

Different transmission rates (4/10/11/16/100/1000/... Mbps)

- bridge between fast LAN and slow LAN (or several LANs to one)
  - link can be overloaded
- buffering frames which cannot be transmitted immediately
- potentially many frames must be buffered within bridge
- (end-to-end) retransmission timer (at higher level) tries n*retransmissions
  - but then reports that end system is not available

Different frame lengths

- 802.3: 1518 bytes, 802.4: 8191 bytes, 802.5: unlimited, 802.11: 2346 bytes
- 802 does not support segmentation
  - not the task of this layer (at least typically seen this way)

➔ frames that are too long are dropped

- loss of transparency

802.x <-> 802.y: Tasks

Different checksum calculations

- means conversion, delay, buffering

Security

- 802.11 provides some data link layer encryption
- 802.3 does not

Quality of Service / Priorities

- supported (in various forms) by both 802.4 and 802.5
- NOT supported by 802.3
- 'kind of' in 802.11 (PCF / DCF and esp. 802.11e)

Acknowledgements

- supported by 802.4 (temporary token handoff)
- supported by 802.5 (C+A bits)
- not supported by 802.3

802.x <-> 802.y: Tasks

Example: 802.5 Token Ring to 802.3 CSMA/CD

- frame size Ra:
  if Ra(Token Ring) > Ra(CSMA/CD)
  - no overall solution
  - L2 does not offer segmentation
  - network considers a frame as an atomic unit only

- Priorities
  - Token Ring priorities are lost

- Acknowledgement
  - bridge has to confirm Token Ring frame,
    - even though it was not delivered to the CSMA/CD receiver

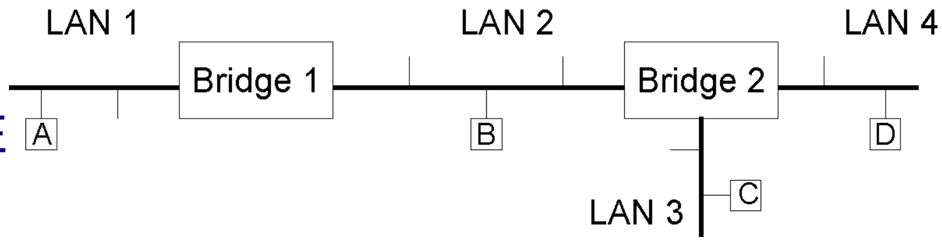
3.2 Connecting Several Networks: Transparent Bridges

Transparency:

- bridges not visible as such for the other components of the network

➔ simplifies other components

Principle: transparent bridge



- bridge works in PROMISCUOUS MODE
  - receives every frame of each connected LAN
- bridge manages table: station → LAN (output line)

Bridge1: A → LAN 1 B → LAN 2 C → LAN 2 D → LAN 2

Decision procedure

1. source and destination LANs identical
   ➔ frame dropped
2. source and destination LANs differ
   ➔ frame rerouted to destination LAN
3. destination unknown
   ➔ flooding

Transparent Bridges

Bridge table initially empty

- use flooding for unknown destination

Learning process: backward learning

- bridge works in promiscuous mode:
  - receives any frame on any of its LANs
- bridge receives frames with source address Q on LAN L

  ➔ Q can be reached over L

  ➔ create table entry accordingly

Adaptation to changes in topology

- entry associated with timestamp (frame arrival time)
- timestamp of an entry (Z, LAN, TS) is updated when frame received from Z
- table scanned periodically and old entries purged
  - if no update for some time, usually several minutes
    - e.g., because system moved and reinserted at different position
    - flooding is used if machine was quiet for some minutes

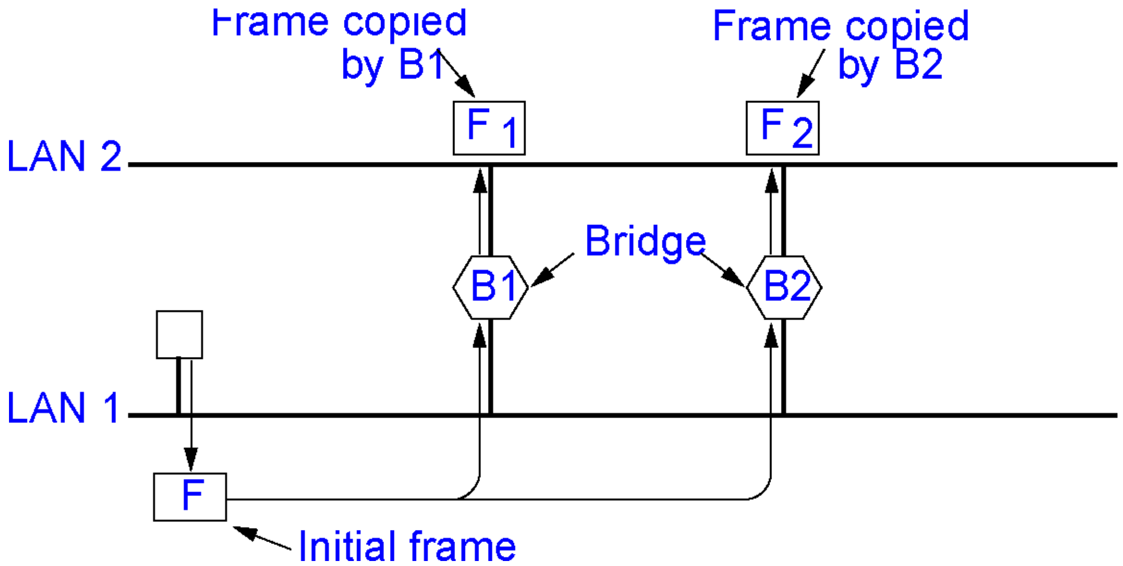
Transparent Bridges: Spanning Tree

Increase reliability:

- connect LANs via various bridges in parallel

Problem

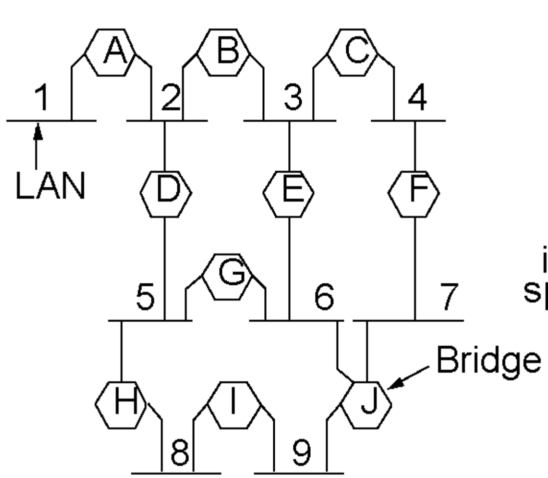
- this creates a loop in the topology
- frames with unknown destination are flooded
  - frame is copied again and again



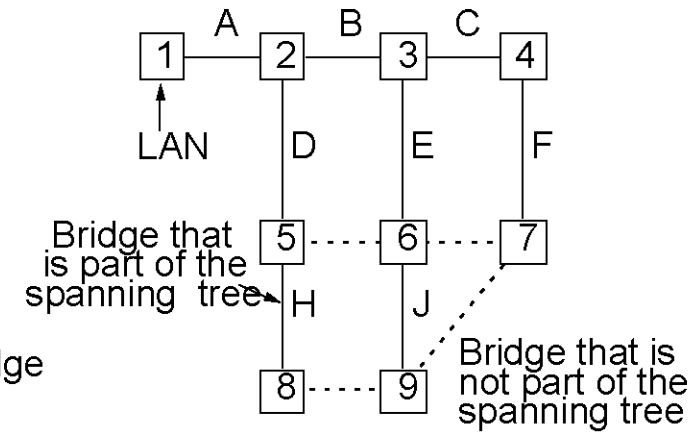
Solution:

- Communication among bridges
- Overlay actual topology by spanning tree reaching every LAN
  - exactly one path from any LAN to every other LAN

Transparent Bridges: Spanning Tree



Bridges between LANs



A Spanning Tree

Example

Algorithm

- root of tree selection
  - Bridge identified by unique identifies
    - e.g. serial number
    - e.g. MAC address and a priority
  - all bridges broadcast their unique id,
    lowest chosen as root for all other bridges
- generation of spanning tree (from the root to every bridge and LAN)
  - configured with bridges representing the nodes within the tree
  - thereby avoiding loops
- adaptation if configuration is changed (bridge or LAN)

Drawback:

- ignores some potential connections between LANs
  i.e., not all bridges are necessarily present in the tree

3.3 Source Routing Bridges

Has been proposed (and used) as alternative to transparent bridges

Principle

- the frame's sender defines path
- bridge routes the frame

Prerequisite

- LAN has a unique address (12 bit)
- bridge at the respective LAN is also unique (4 bit)

then

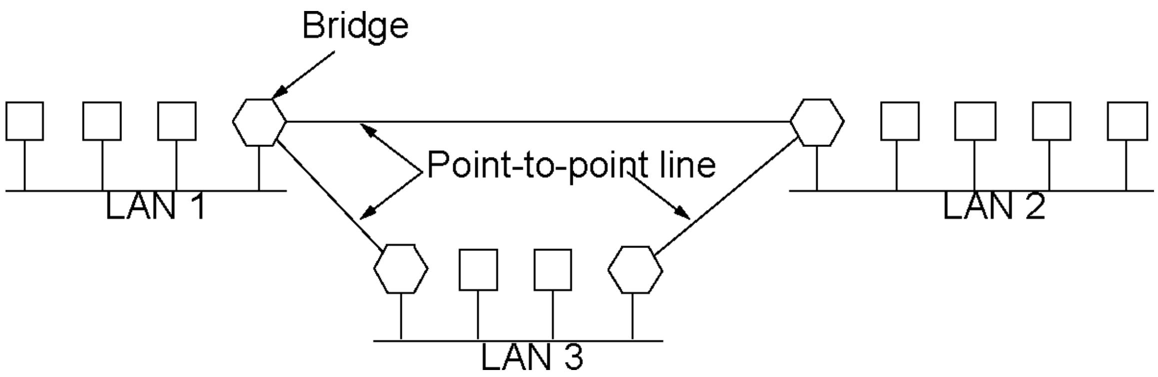
- sender flags the frame (top bit of its own address = 1), if destination address is not reachable in LAN
- bridge routes only frames that have been flagged in such a way

Determining Path

- sender sends discovery frames as broadcast
- each bridge reroutes these (reaches every LAN)
- during return (route)
  - the complete path is copied and
  - transmitted to sender
- problem: high traffic

Conclusion: usually transparent bridges are used

3.4 Connecting 2 Equal Networks: Encapsulation



Example: remote bridge
Interconnect different sites of one organization

Principle
1. incoming data unit is packaged as payload,
2. transmitted and
3. then fed into the destination network

Properties
- certain protocol on connecting route
  - e.g. PPP
  - i.e. e.g. MAC frame in PPP
- only station at the destination network can be reached
  - but for example not the network being bridged
- simple

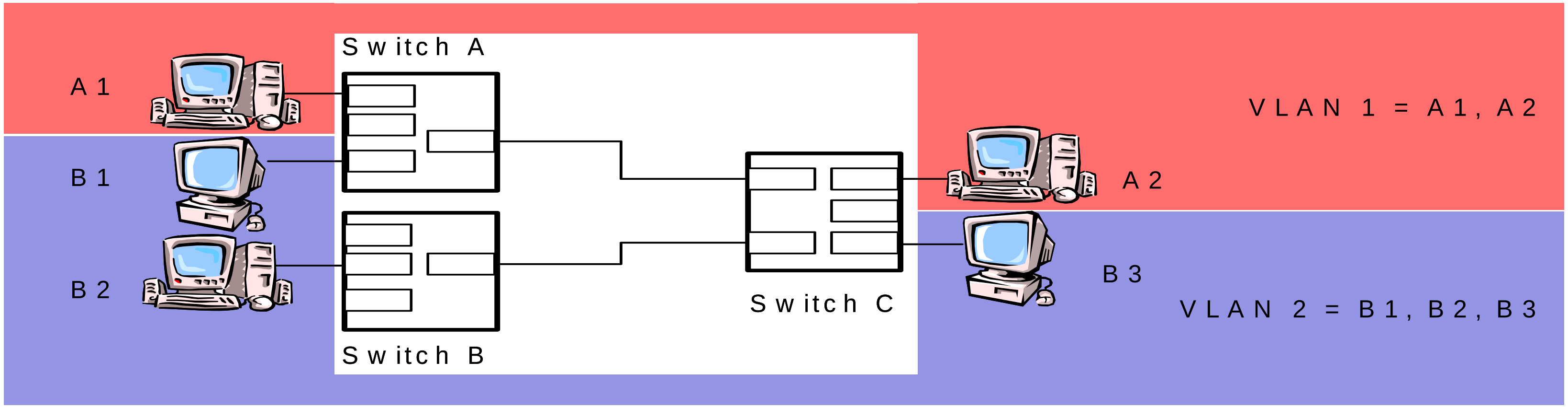
4 Virtual LAN (VLAN)

Problem:

- Switches cannot partition large networks in logical networks

Virtual LANs: A broadcast domain defined by specific criteria

- Separation of physical and logical network structure
    - Data packets (e.g., broadcasts) are only distributed in the respective VLAN
    - VLAN members can be (spatially) distributed, e.g. members of a workgroup located in different buildings



e.g. frames from A1 are never forwarded to B3, also not for broadcast frames

Virtual LAN (VLAN): Advantages & Technologies

Advantages

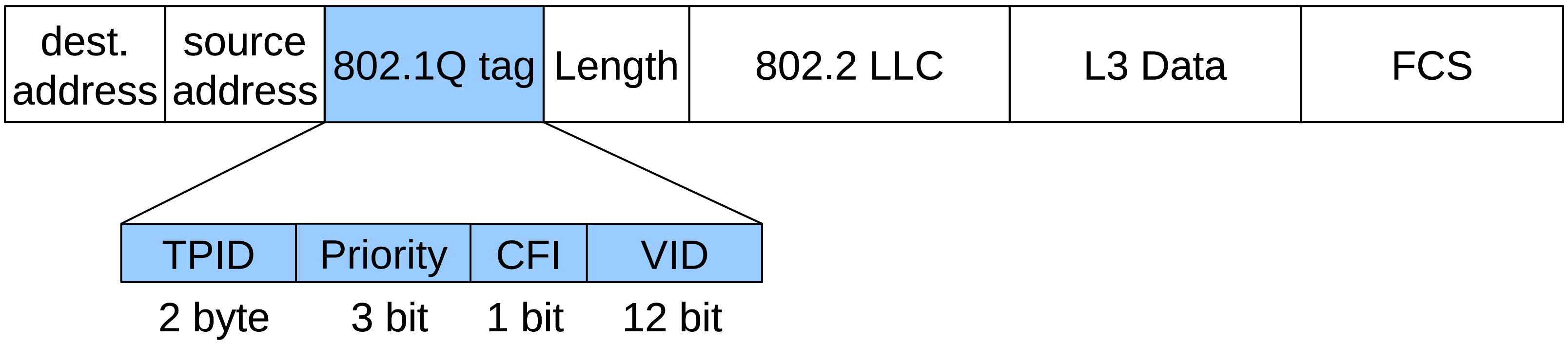
- Restriction of the broadcast/multicast domain
  - Better utilization of available bandwidth
- Efficient management and reduced configuration
  - E.g., after modifications of the network topology (due to a relocation)
  - i.e., logical topology can be changed without changing addresses or wiring
- Improved security
  - New station has to authenticate itself at the VLAN
  - Strict separation of data traffic in different LANs

Important Technologies

- Port-based VLAN (L1): based on physical switch ports
- MAC VLAN (L2): membership based on MAC addresses
- L3 VLAN: based on IP addresses of the stations, but requires L3 switches
- Rule-based LANs: combine L2/L3 information to form the VLAN

VLAN based on IEEE 802.1Q

- IEEE 802.1Q uses VLAN tagging 802.1Q Tag Header
- Extends L2 frame by a tag assigning the L2 frame to a VLAN ID
- Example: Ethernet frame



- TPID: Defines Ethertype; must be 0x8100 to indicate 802.1Q frame
- Priority: defines the user priority according to IEEE 802.1P
- CFI: Canonical Format Indicator (for compatibility), is set to 0 for Ethernet
- VID: VLAN Identifier

IEEE 802.1P: Layer 2 QoS/CoS Protocol for Traffic Prioritization

- IEEE 802.1P enables L2 switches to prioritize traffic and perform dynamic multicast filtering
- Supported by VLANs (IEEE 802.1Q) in 3 bit user priority field
- User Priority groups packets into 8 traffic classes (ordered by importance of the user priorities):
  - 1: background traffic (games, bulk transfers)
  - 2: spare traffic (no further definition)
  - 0: best effort („ordinary LAN priority“)
  - 3: excellent effort („best effort for important users“)
  - 4: controlled load („some important application“)
  - 5: video (< 100 ms delay)
  - 6: voice (< 10 ms delay)
  - 7: network control (high requirement to get through)

- Must be supported by end systems and switches
- Does not make bandwidth reservation