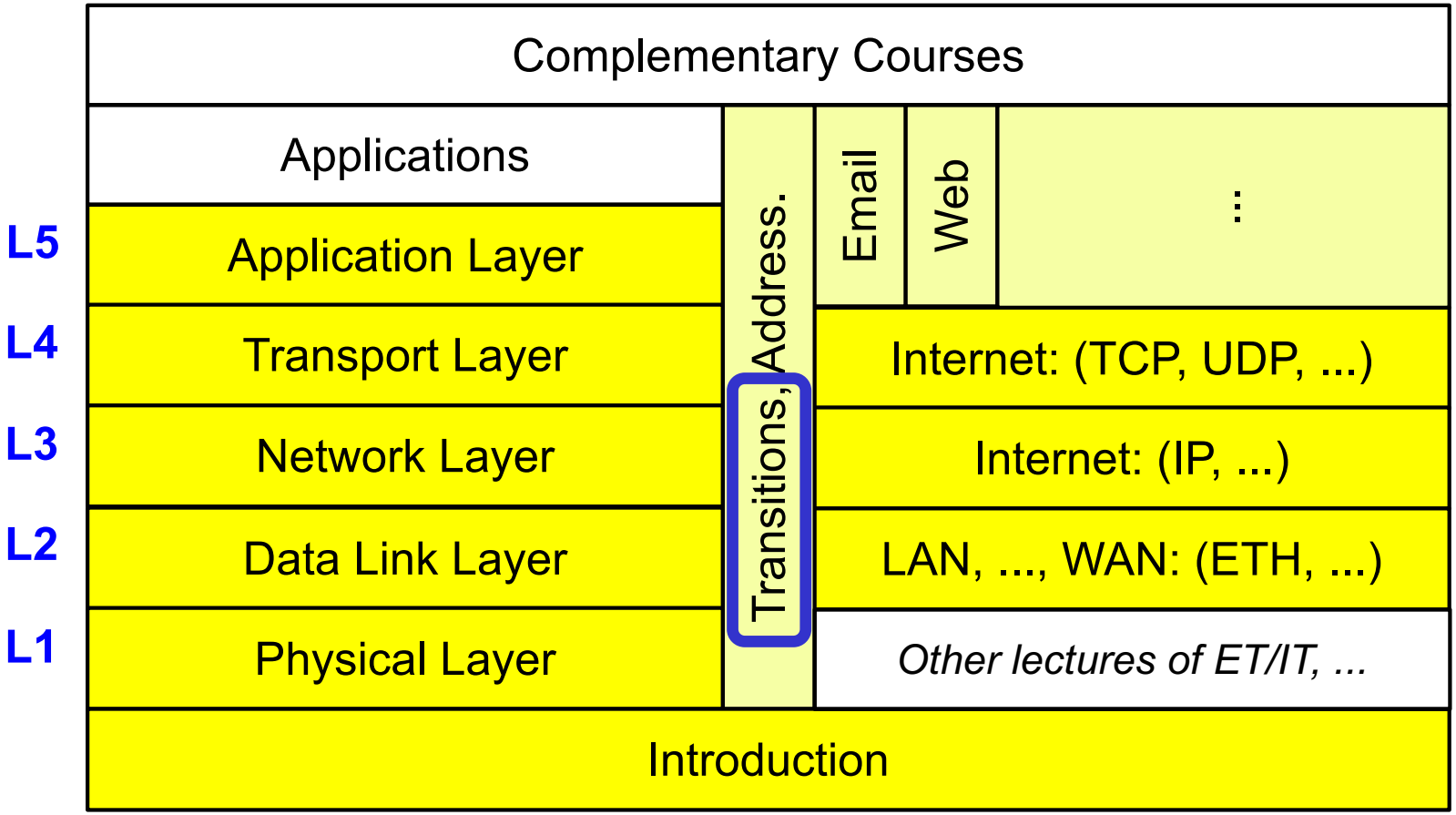
Computer Networks I

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
Applications
Email
Web
...
L5
Application Layer
L4
Transport Layer
Internet: (TCP, UDP, ...)
L3
Network Layer
Internet: (IP, ...)
L2
Data Link Layer
LAN, ..., WAN: (ETH, ...)
L1
Physical Layer
Other lectures of ET/IT, ...
Transitions, Address.
Introduction

Overview

In Computer Networks 2:

1 Motivation

Many heterogeneous networks
- past, nowadays, in future

Heterogeneous network technologies (data link):
- WAN: telephone networks, ISDN, ATM, ...
  mobile: GSM, UMTS, LTE, 5G, DECT, Bluetooth, Zigbee, ...
- LAN: 802.3, 802.5, 802.11, 802.16, ...

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

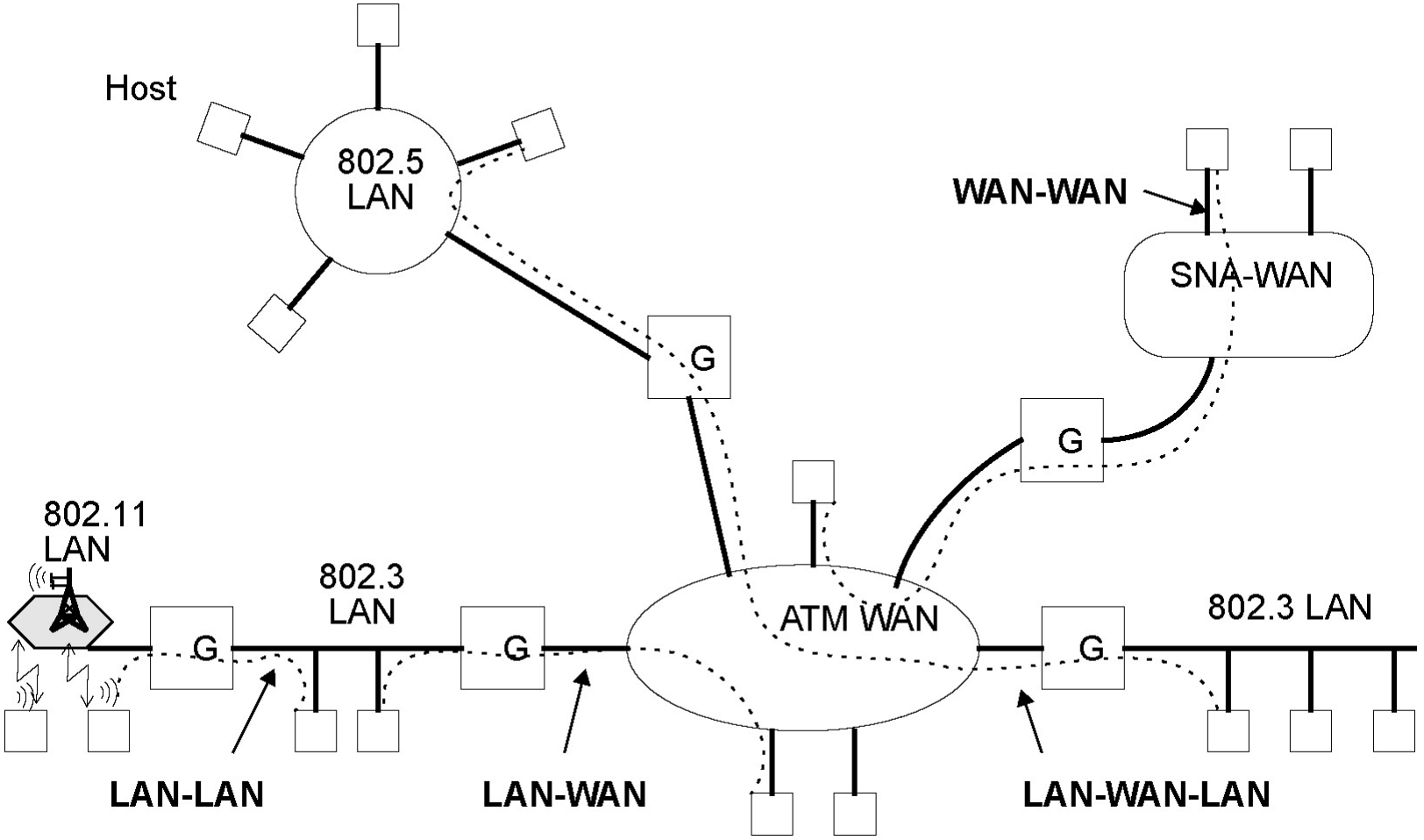
Heterogeneous application architectures (with same overall purpose):
- Email, Peer-to-Peer protocols
- Information access (WWW, WAP)

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

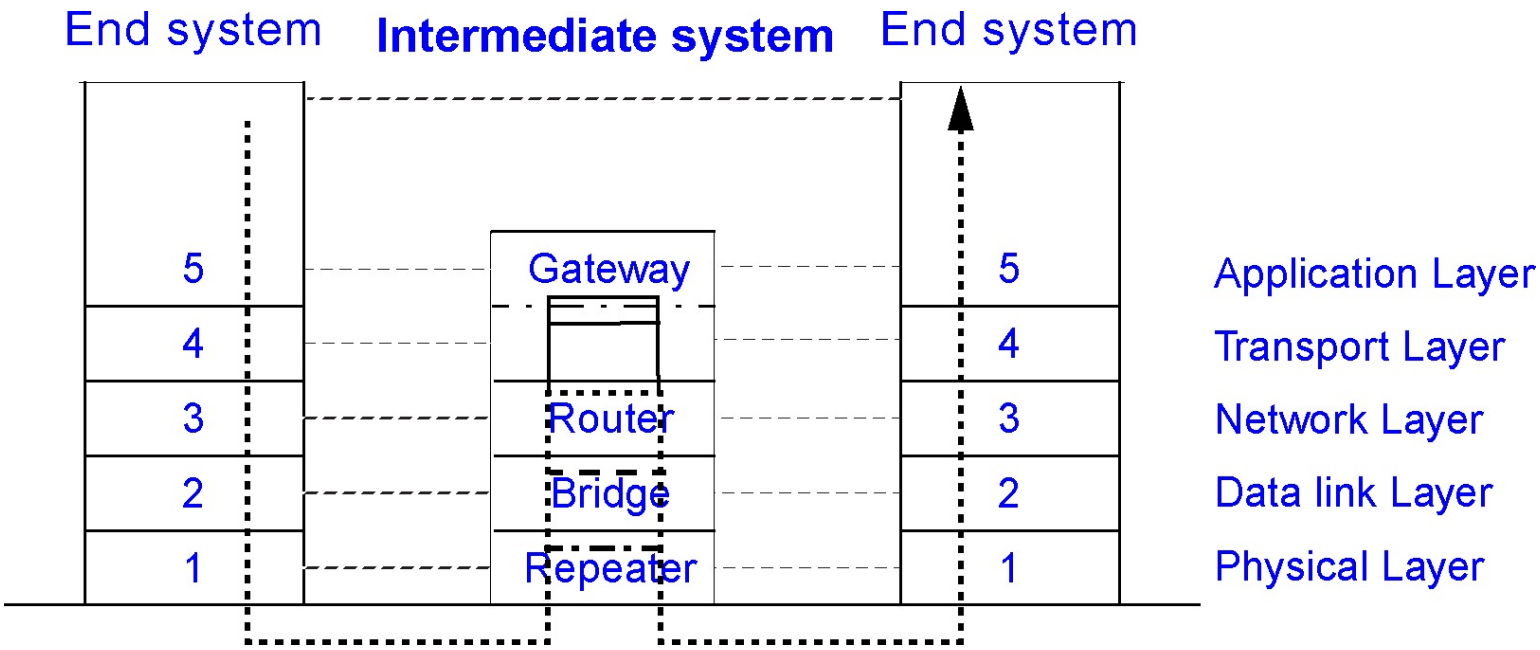
Interconnecting Different Networks



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)

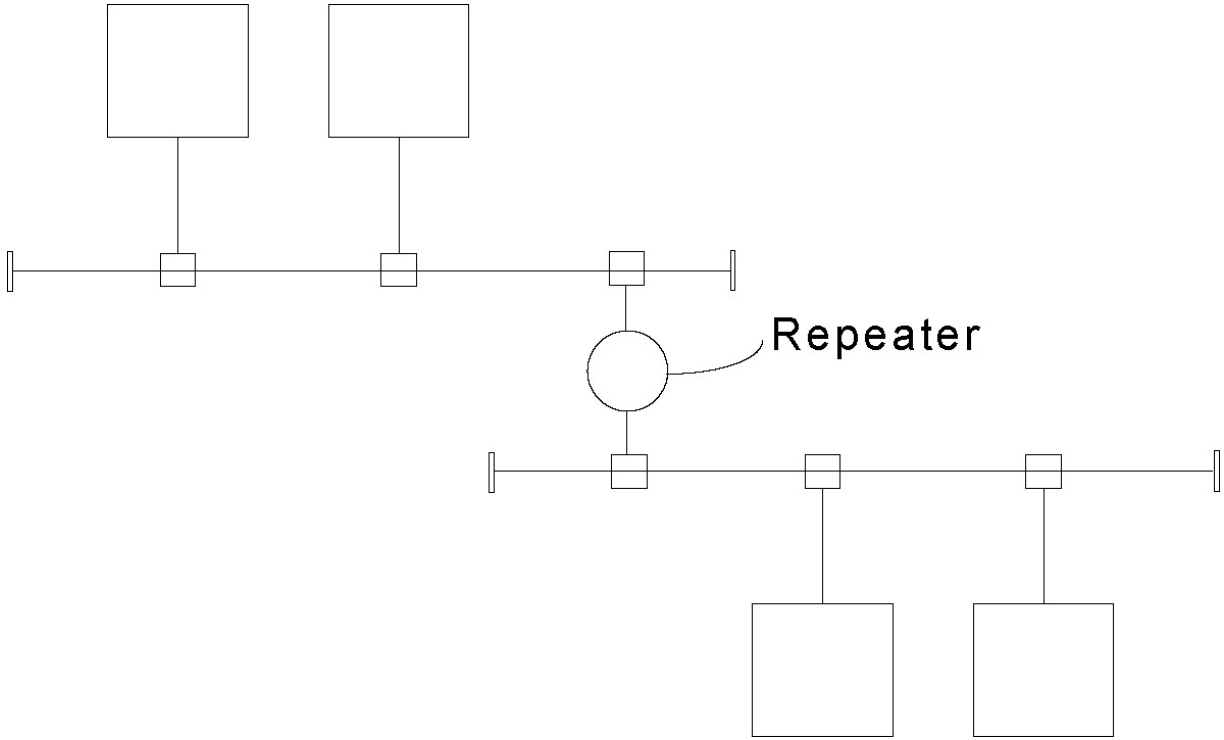
Layer 4 - 5: Gateway (or Protocol Converter)
- converts one protocol into another
  - (usually no1-to-1 mapping of functions)
- examples:
  - TCP in ISO Transport Protocol
  - OSI Mail (MOTIS) in ARPA Internet Mail (RFC 822)
  - change of media encoding (transcoding)
  - SIP to H.232 signaling for IP Telephony

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

Basic components
- 2 or more network connections
- connection entity
- control entity

2 Paths:
- control path and data path

2.1 Repeater (Physical Layer)

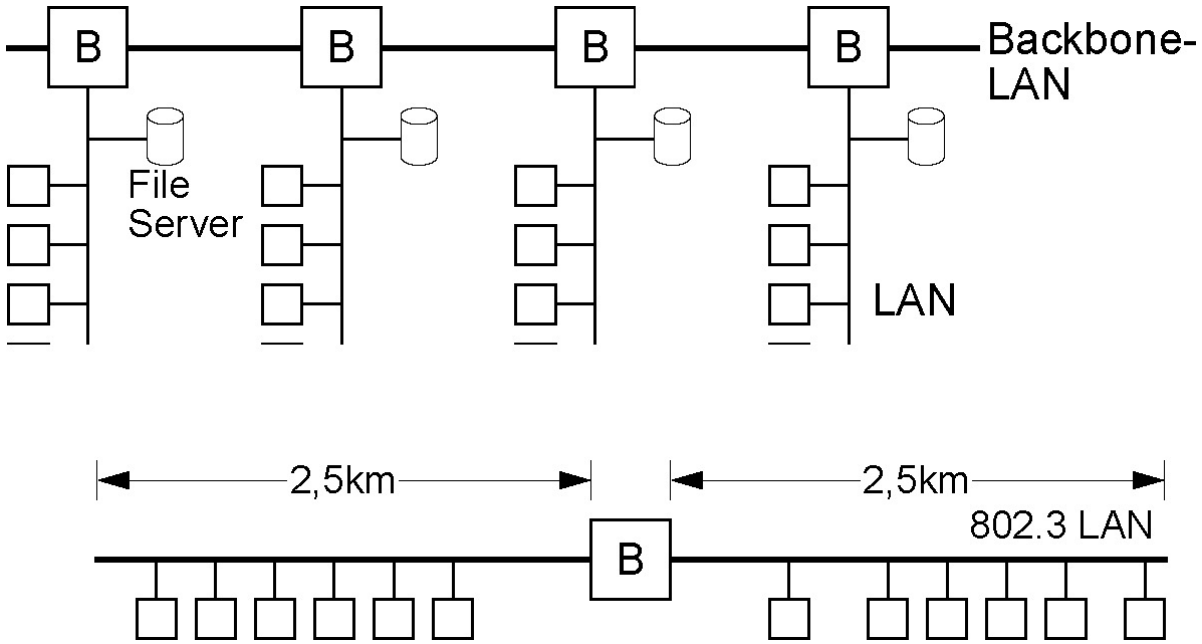


example: (classical) IEEE 802.3 configuration

Function

- amplify the electrical signals
- increase the range

2.2 Bridge (Data Link Layer)

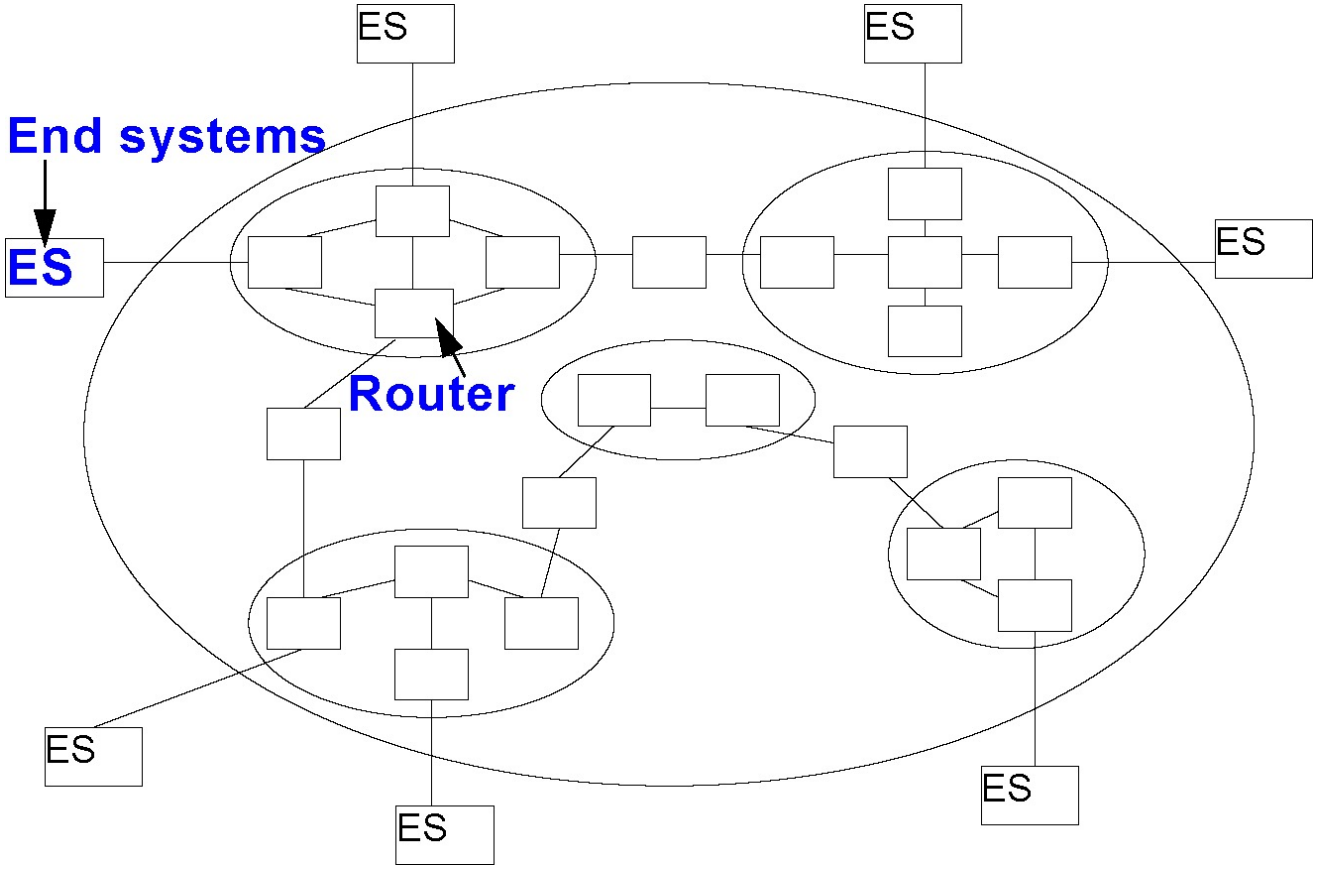


Tasks:

- couple different LANs
- provide scalability of networks
- increase capacity
- cover larger distances
- increase reliability
- improve security
- 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

- different audio data formats are converted in real time

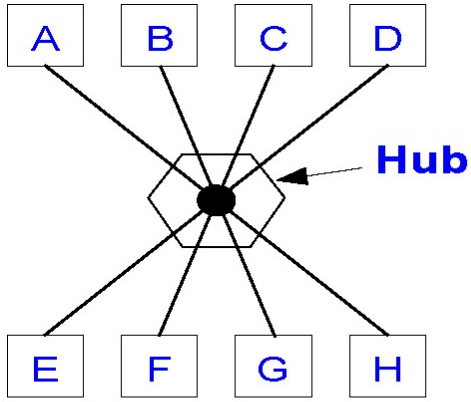
Example: signaling

- conference connection establishment
  - dial-in from classical telephone (POTS)
  - to audio / video conferencing system (computer)
- adaptation by functional transformation and stubs

2.5 Repeaters, Hubs, Bridges, Switches

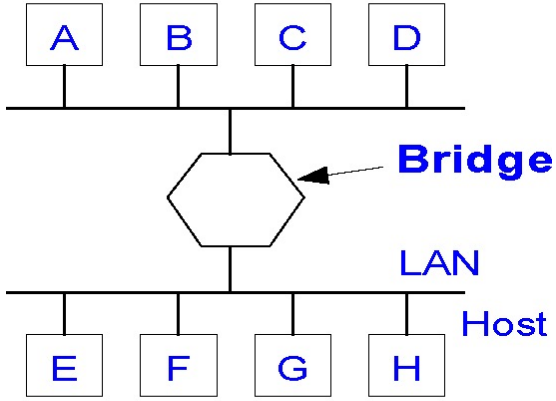
Repeaters & Hubs (L1):

- one collision domain



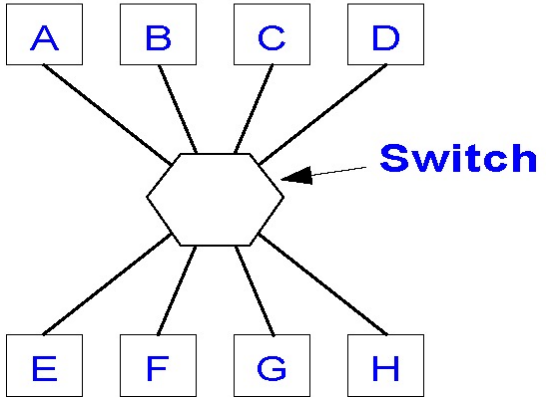
Bridges (L2):

- 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)

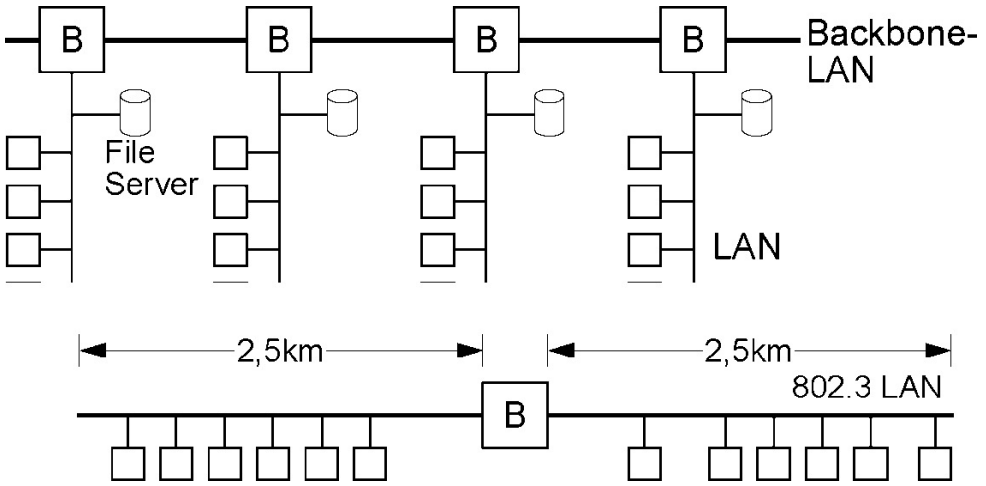
- typically connects two or more computers
- each port / line is its own collision domain (no collisions)
- (store-and-forward or) cut-through switching
  - begin forwarding as soon as possible
  - when destination header has been detected, before rest of frame arrived
- hardware-based (ASIC or FPGA)



3 Bridge / Switch (Data Link Layer)

Tasks:

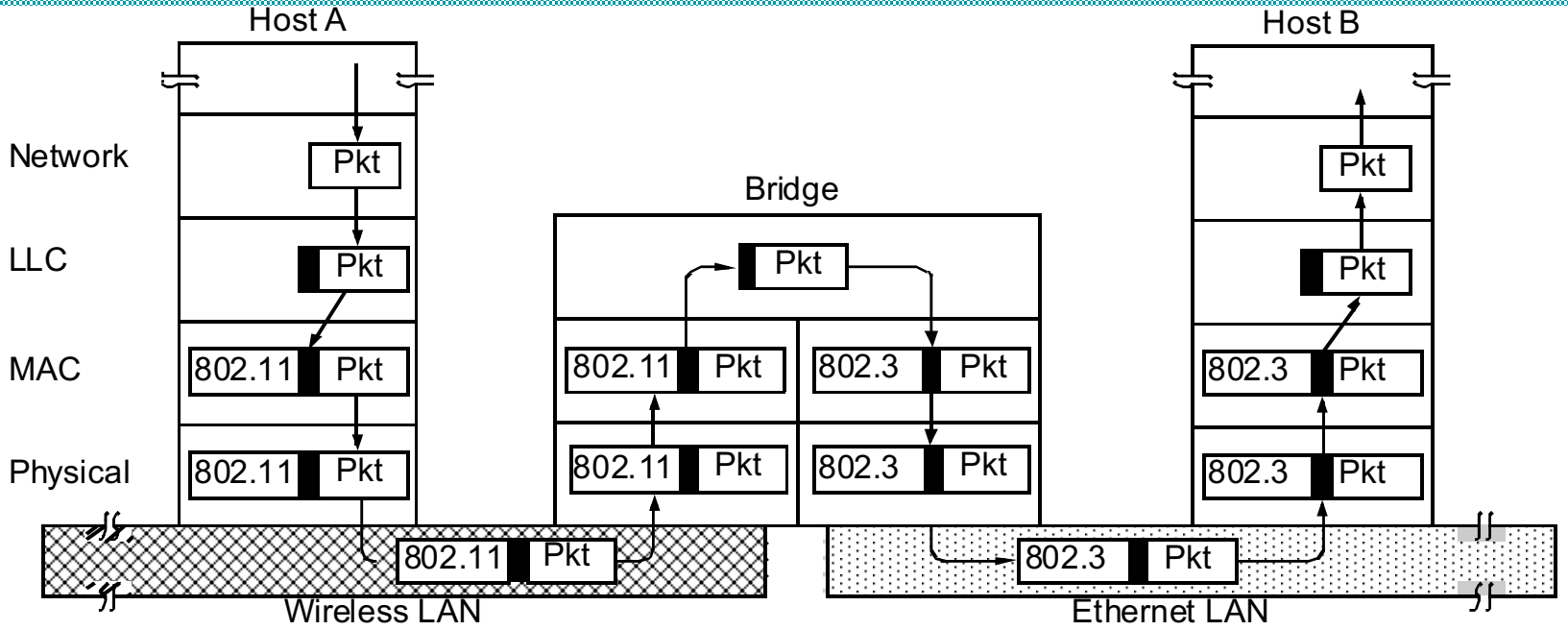
- coupling of different LANs
- better scalability of networks
  - increase capacity
  - cover larger distances
- increase reliability
  - bridge serves as "fire door"
- improve security
  - stations can work in a promiscuous mode, i.e., read all frames on the network
  - bridge placement limits the spreading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



Important goal: **TRANSPARENCY**

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

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



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

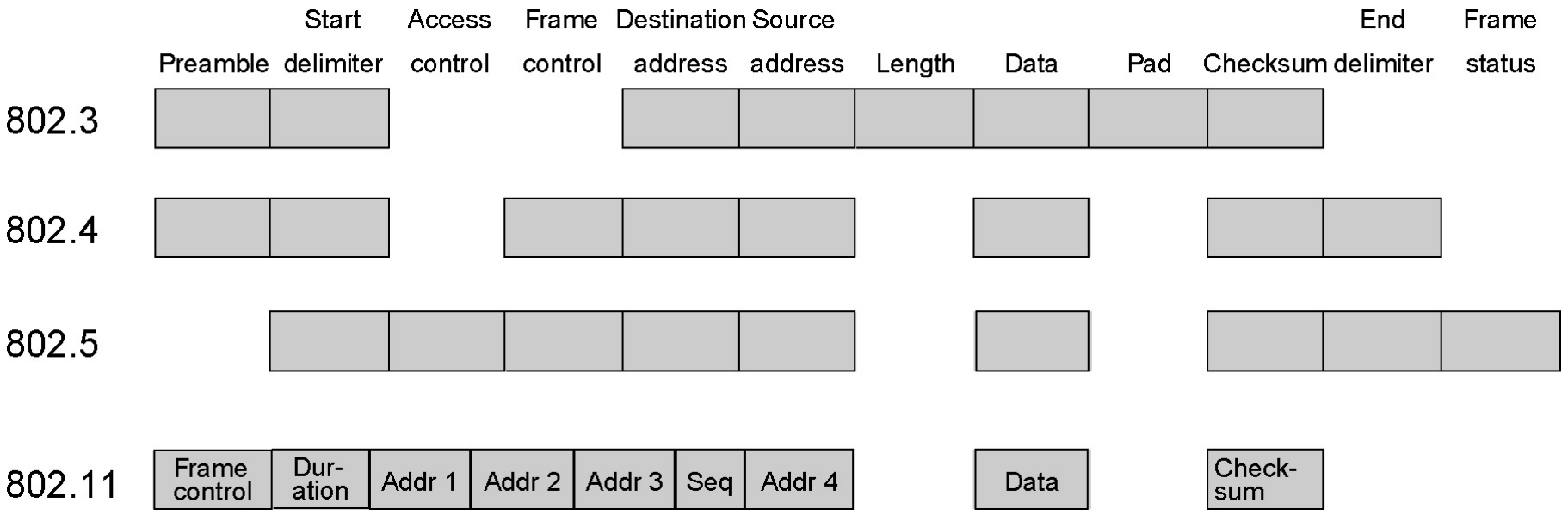
Approach

- 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

Several differences exist,
e.g. 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

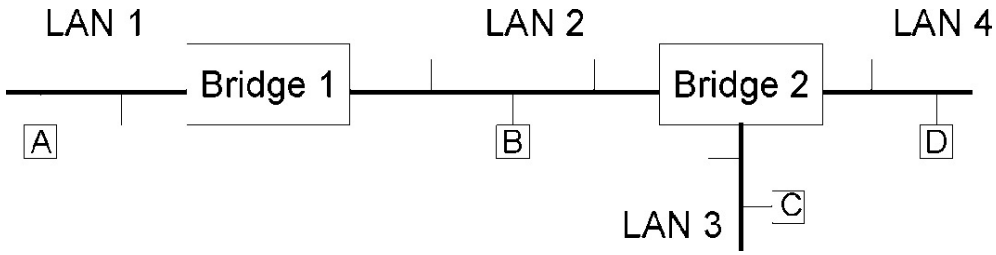


3.2 Connecting Networks: Transparent Bridges

Transparency:

- Bridges / switches not visible to other network components

➔ 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 S on LAN L
  ➔ S 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 (D, LAN, TS) is updated when frame received from D
- table is scanned periodically and old entries are 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

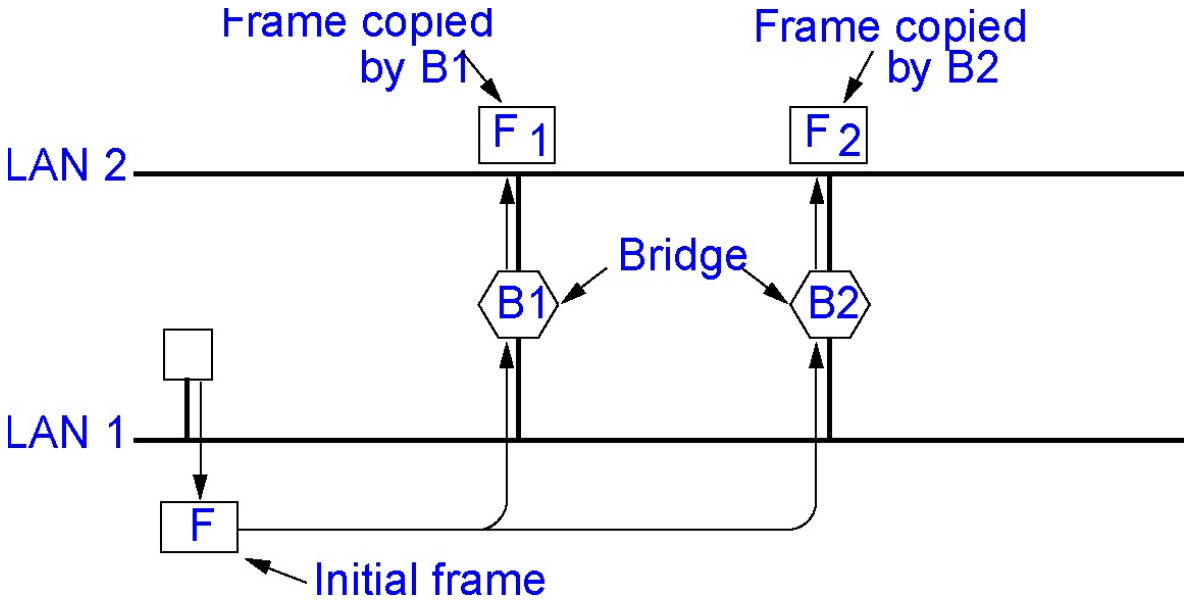
Transparent Bridges: Spanning Tree

Increase reliability:

- connect LANs via various bridges in parallel

Problem

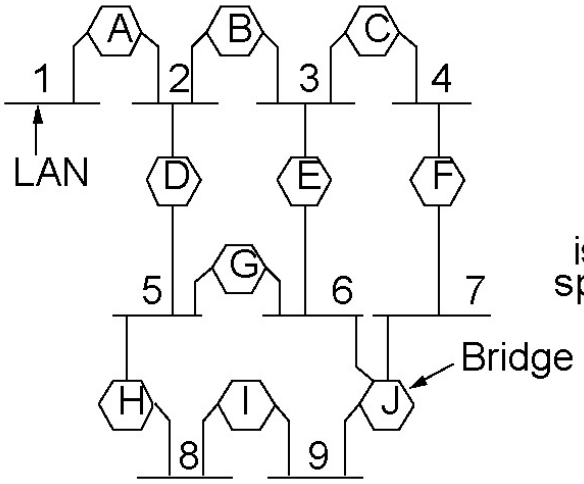
- this creates a loop in the topology
- frames with unknown destination are flooded
  - frame is copied again and again



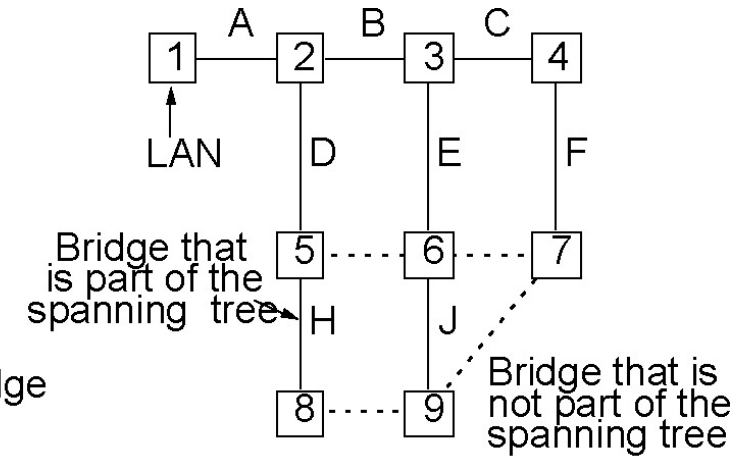
Solution:

- 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