Data communication I

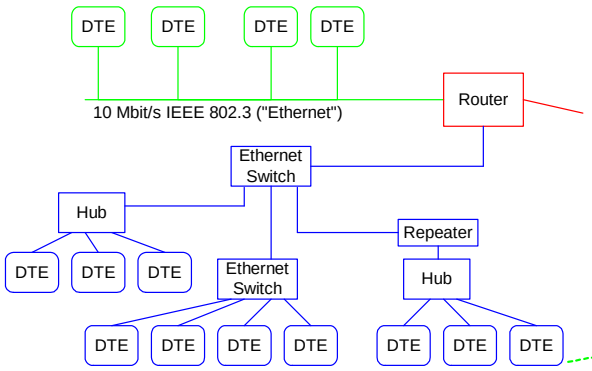
Lecture 8 – LANs

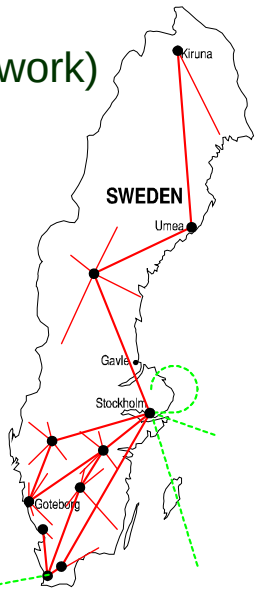
Local Area Networks (LANs)

- Topologies
- Transmission Media
- LAN protocol architecture
- LAN networking devices
- High speed LANs
  - Ethernet
  - Fibre Channel

WAN (Wide Area Network)

LAN (Local Area Network)





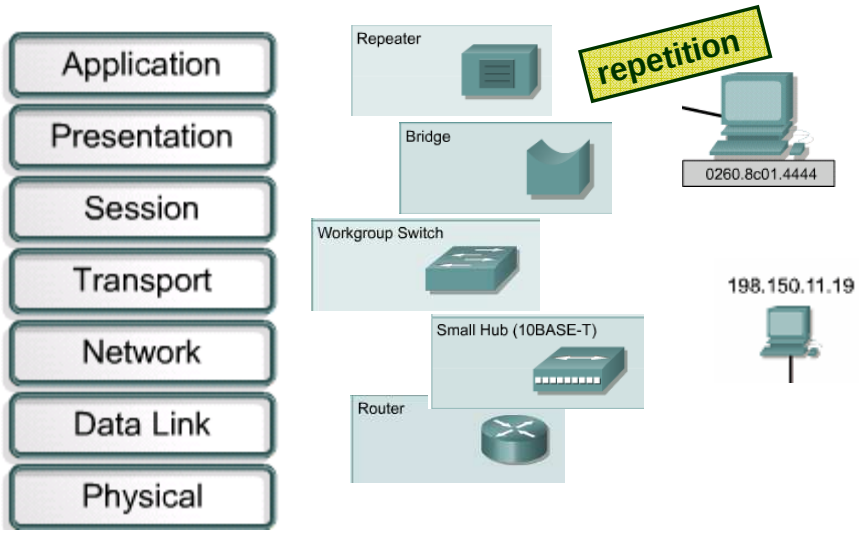
LANs…

- …are usually owned by the organization that uses the network
- …span a building, floor, room, campus etc.
- …include networking devices in layers 1 and 2
- …are connected to other LANs or a larger network (e.g. the Internet) through a router
- …are defined through their topologies, transmission media and mechanisms to share the common media (MAC methods)

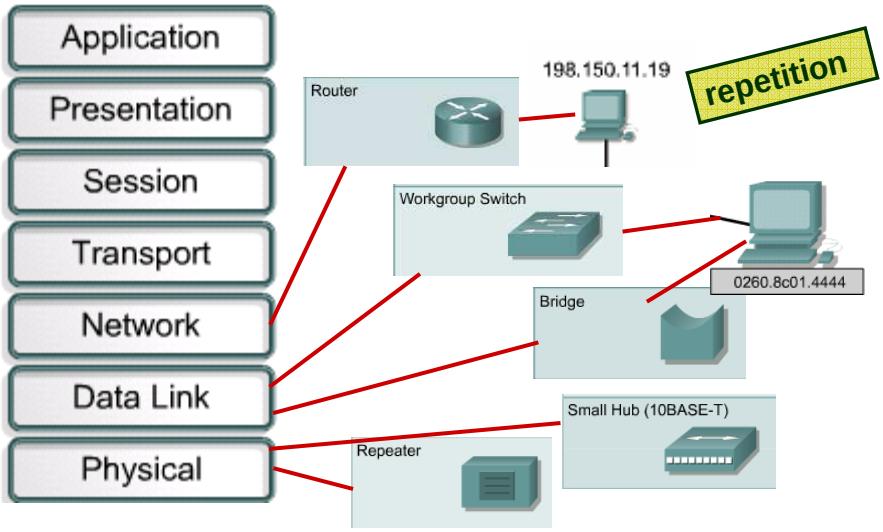
What are LANs used for?

- Used to interconnect equipment
  - Interconnect PCs
  - Connection to servers, computers with extra processing power to outsource computationally demanding tasks, etc.
  - Shared resources like printers
- Backend networks
  - To interconnect large systems like mass storage devices, supercomputers etc
  - Special demands on data rates and reliability
- Storage Area Networks (SAN)
  - Distributed storage of large amounts of data
  - Interconnection between SANs are needed
- High-speed LAN can be used to interconnect several low-speed LANS

The LAN and its networking devices



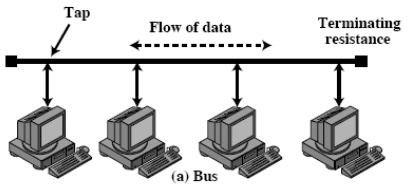
The LAN and its networking devices



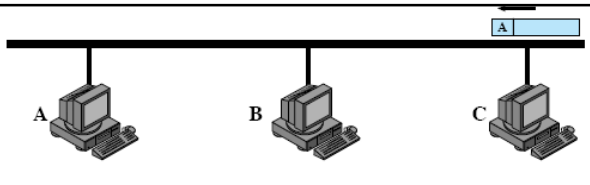
LAN topologies

- Topology = the way in that the nodes (stations) in a network are interconnected
- Different topologies used in LANs
  - Bus
  - Tree
  - Ring
  - Star
- Choice of topology depends on the demands on scalability, reliability, performance etc.

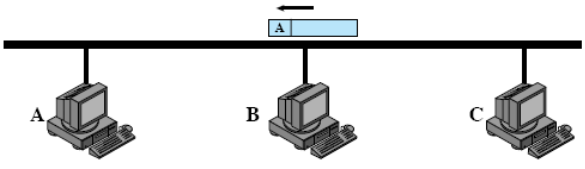
- Bus topology
  - Data from one node is spread to each other node on the bus, each node examines the MAC address (layer 2 address) and discards the frame if the address does not match
  - No networking devices needed
  - Link failure makes some nodes unreachable
  - Bus has to be shared by all nodes and a MAC method is crutial



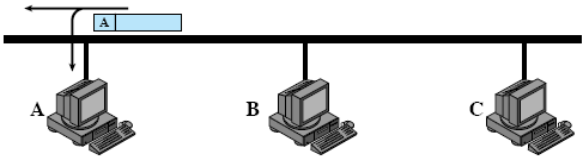
- Examining the frame's MAC address to determine if the frame should be received or not



C transmits frame addressed to A

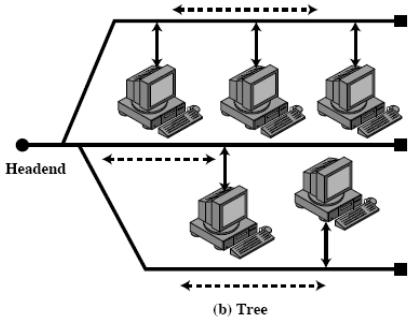


Frame is not addressed to B; B ignores it



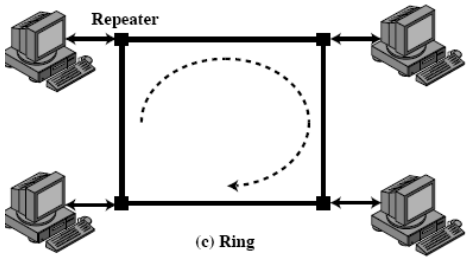
A copies frame as it goes by

- Tree topology (special case of bus)
  - Data from one node is spread to each other node on the tree, each node examines the MAC address (layer 2 address) and discards the frame if the address does not match
  - More complex topologies possible than with a bus
  - Networking devices might be used on connection points
  - Link failure makes some nodes unreachable
  - Tree has to be shared by all nodes and a MAC method is crutial



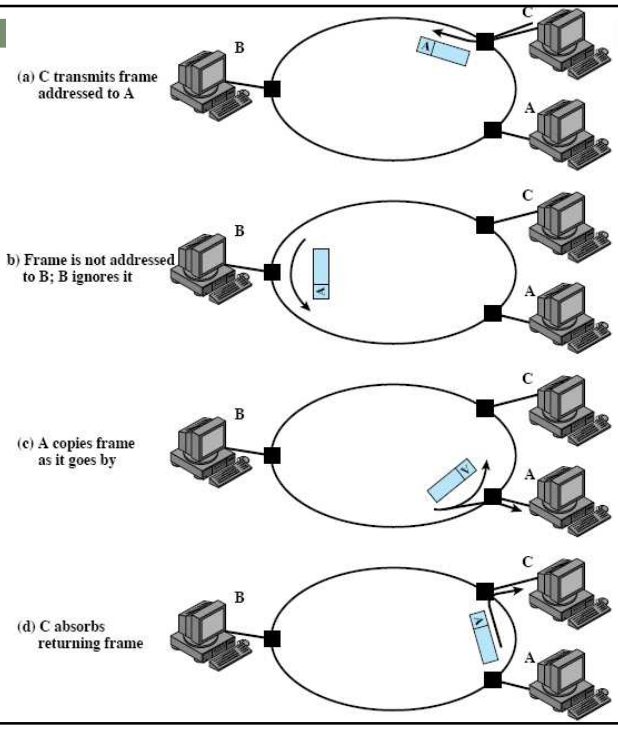
(b) Tree

- Ring topology
  - Closed loop of repeaters
  - Link failure does
    - not make nodes unreachable if communication in both directions possible
    - Make nodes unreachable if uni-directional communication
  - Frames are removed after one round
  - Bus has to be shared by all nodes and a MAC method is crutial

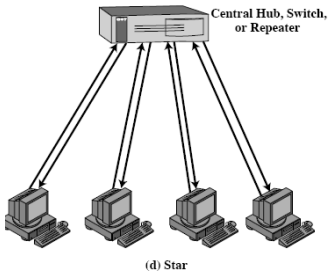


(c) Ring

- Frame transmission on a ring topology



- Star topology
  - Direct connection to a central common node
    - Hub: data goes to all connected nodes
    - Switch: data goes only to the node(s) with the right MAC address
  - Link failure does only cut off one single node
  - A link might be shared by several nodes (extended star), which would make a MAC protocol necessary



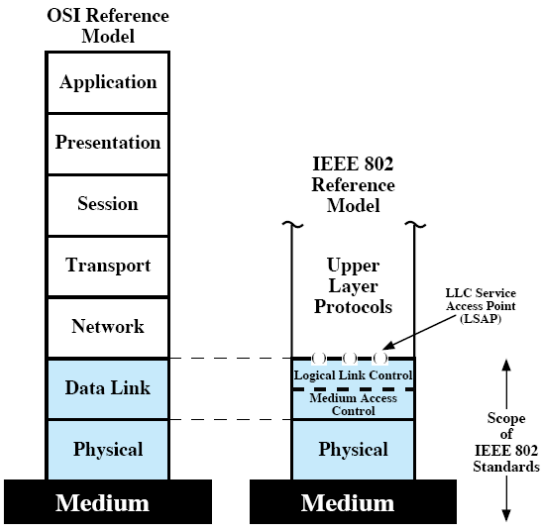
Choice of transmission medium in a LAN

- Coaxial cables for bus networks
- Star networks often with twisted pair cables or optical fibres

- Trend towards…
  - … high-performance UTP (unshielded twisted pair) cables due to their low cost
  - … optical fibres due to their characteristics (low interference, high speed), despite their high cost

The IEEE 802 protocol suite for LANs

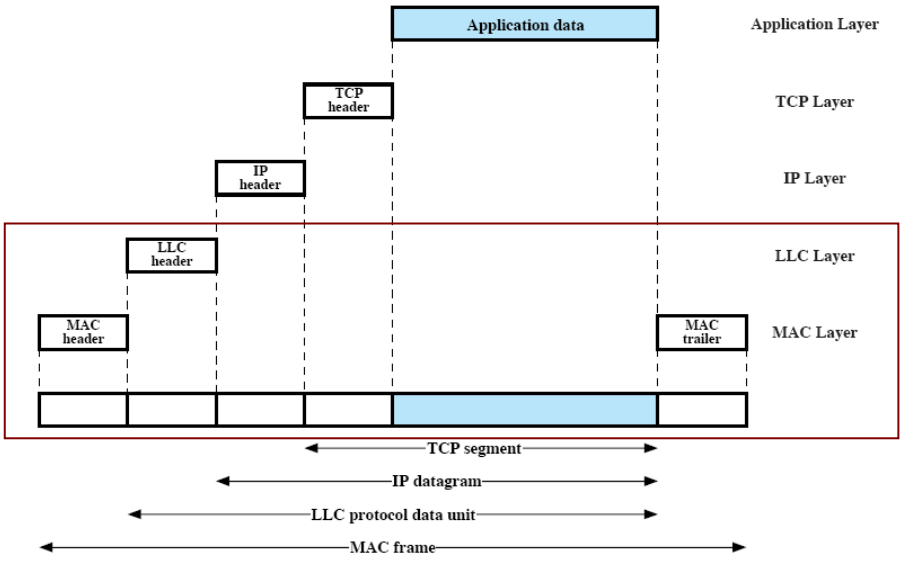
- A layered architecture defining protocols and technologies used for LANs
- defines…
  - …the communication medium
  - …protocols for the physical layer
  - …protocols for MAC
  - …protocols for logical link control (error and flow control)



Examples of commonly used protocols from the 802 LAN protocols suite:

- 802.3 Ethernet
- 802.5 Token Ring
- 802.11 Wireless LAN (WLAN)
- 802.15 for low-rate wireless personal area networks (WPANs)
  - 802.15.1 Bluetooth
  - 802.15.4 ”ZigBee” (often used for Wireless Sensor Networks)

Encapsulation in the 802 LAN protocol suite



LLC (Logical Link Control) in 802 LANs

- Similar to the functions of the data link layer in the OSI reference model (minus MAC protocols)
- Concerned with the direct point-to-point link between two nodes
- Different modes:
  - Connectionless without flow and error control (datagrams are sent without being acknowledges)
  - Connectionless with flow and error control (datagrams are acknowledged)
  - Connection-mode (connection is set up before data exchange and flow and error control are provided)

MAC (Medium Access Control) in 802 LANs

- Data traffic requirements of different applications over a LAN are unpredictable
  - Assigning a fixed amount of resources is therefore impractical and a waste of bandwidth
- MAC protocols needed that are flexible
  - Assign resources to a station when needed
  - Dynamically assign the amount of resources that is currently required

Repetition of MAC protocol types

- Just accept that collisions exist
  - **Random access** MAC protocols
    - try to reduce the probability of their occurence
    - Quickly recover from collision
- Make sure the multiple senders do not interfere with each other
  - **Channel partitioning** MAC protocols
    - divide channel into smaller “pieces” (time slots, frequency, code)
    - allocate piece to node for exclusive use
  - ”**Taking turns**” MAC protocols
    - nodes take turns, but nodes with more to send can take longer turns

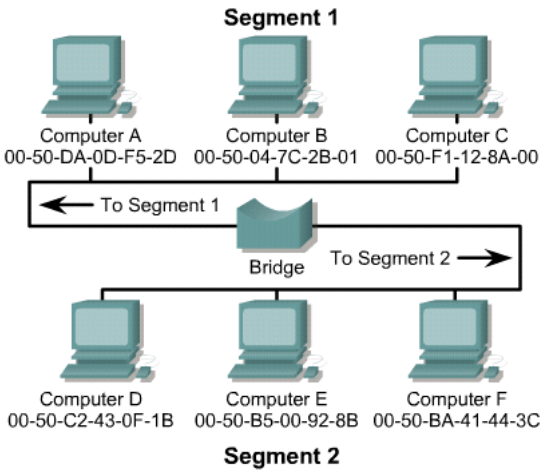
MAC protocols in LANs

- Channel partitioning protocols (called reservation protocols in the course book) are often not suitable
  - E.g. TDMA or FDMA
- Random access protocols (called contention protocols in the course book) are often used
  - E.g. CSMA/CD
- ”Taking turns” protocols are common
  - E.g. ”token passing” (called ”round robin” in the course book)

Bridge

Layer 2

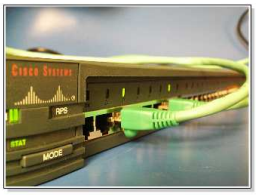
- A bridge makes decisions based on the MAC address (physical address) and keeps data from entering parts of the network where it is not needed



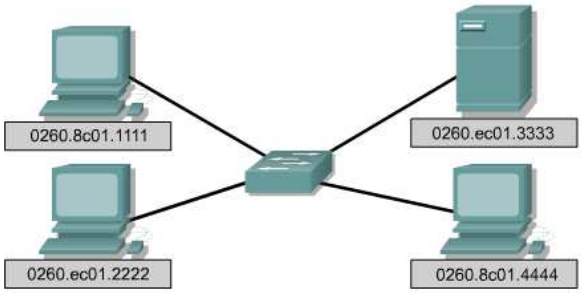
Switch

Layer 2

- A switch is a multi-port bridge.



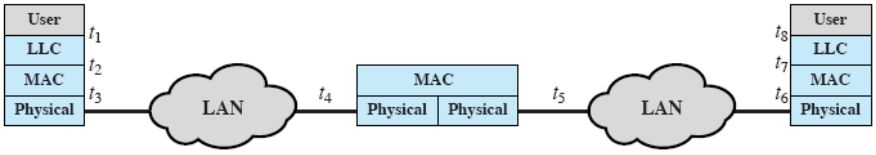
Interface	MAC Address
E0	0260.8c01.1111
E1	0260.ec01.2222
E2	0260.ec01.3333
E3	0260.8c01.4444



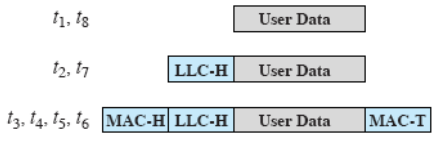
Switch and bridges

- Two types
  - Store and forward
    - Has to receive the entire frame before sending it on
    - Includes error control
    - Adds delay for long frames
  - Cut through
    - Sufficient to receive the header (so that the destination MAC address can be read) before the frame is sent on
    - No error control possible
- *Don't get confused if you hear/read about "Layer 3 switches"*
  - *Does basically the same as a router (path decisions based on layer 3 network addresses)*
  - *Does "switching" in hardware (which is much faster), not in software as a router and is therefore called layer 3 "switch"*

Bridge or switch operation in a LAN

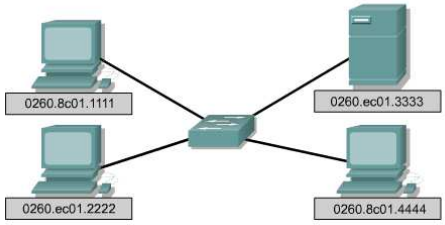


(a) Architecture



Bridge or switch operation in a LAN

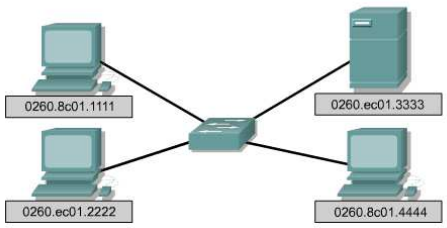
Interface	MAC Address
E0	0260.8c01.1111
E1	0260.ec01.2222
E2	0260.ec01.3333
E3	0260.8c01.4444



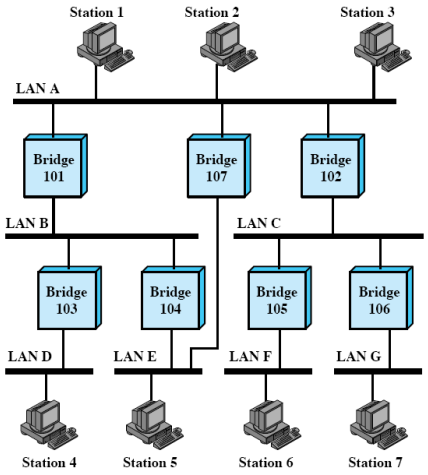
- Bridgeing/switching table
  - Works like a routing table, just with MAC addresses and interfaces instead of network addresses and next-hop routers
  - Fixed tables can be used for fixed topologies
  - Dynamically adapting tables
    - E.g. spanning tree algorithm
  - Course book calls these ”routing tables” → don’t get confused…

- Spanning Tree Algoritm
  - To dynamically update the bridging/switching tables
  - Mechanism:
    - Frame is coming in through interface E1
    - Bridge/switch examines source MAC address and adds it to the table under interface 1
    - All frames with this MAC address as their destination are now sent through interface E1
    - A timer is set and when it expires, the entry is discarded from the table again

Interface	MAC Address
E0	0260.8c01.1111
E1	0260.ec01.2222
E2	0260.ec01.3333
E3	0260.8c01.4444

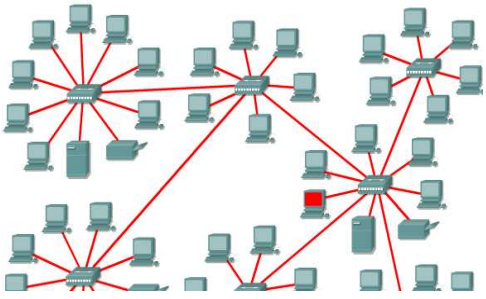


- A more complex topology with several alternative paths between a source-destination pair…
  - …makes **load balancing** possible
  - Provides **redundancy** (and thereby increased reliability)

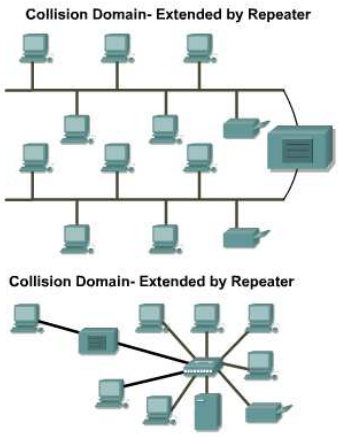


Breaking up a LAN into smaller parts

- Without bridges and switches the LAN is one single ”collision domain”

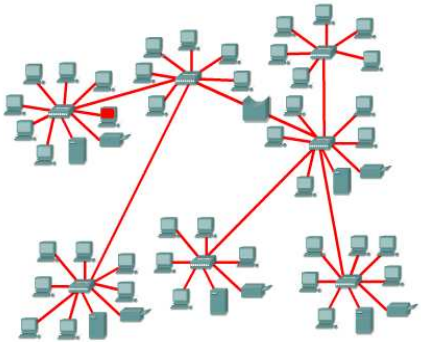


One single collision domain



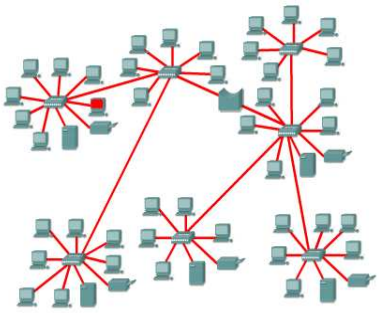
Breaking up a LAN into smaller parts

- Bridges and switches break up the LAN into several ”collision domains”.
- Data frames with a wrong destination MAC address are kept out of a collision domain by the bridge or switch

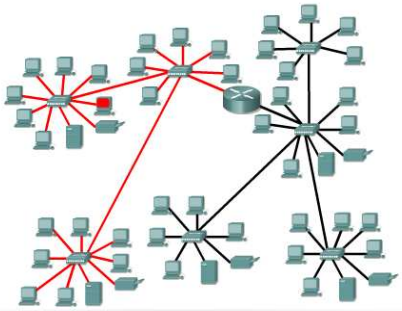


Breaking up a LAN into smaller parts

- Bridges and switches extend the LAN’s broadcast domain
- Only routers can break up the LAN into different broadcast domains (subnets)



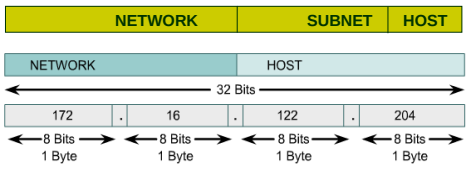
A broadcast is picked up by all stations. A broadcast is also forwarded across all bridges whether the receiving host is on the other side of the bridge or not. This eliminates the benefits of having a bridged network.

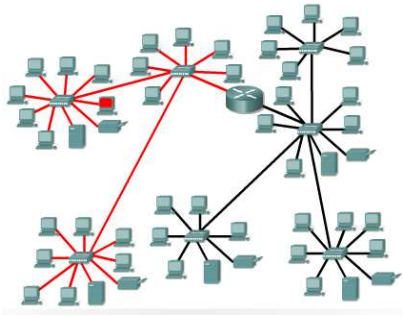


By using a router in place of a bridging device a layer two broadcast is contained. Layer three devices are the only devices that contain broadcasts.

Breaking up a LAN into smaller parts

- Subnets
  - A network (with a specific network address) can be divided into subnets
  - Some bits of the host part of the IP-address are then used to identify the subnet





Why divide the LAN into several collision domains or subnets?

- Reliability
  - Faults on the network
- Performance
  - The total amount of data in the network is reduced
  - More convenient (shorter) wiring
- Security
  - harmful data is contained in one part of the network
- Often logical to separate a large network into networks of different purposes (e.g. staff and student network) or different geographical location (e.g. one subnet per floor in an office building)

High-speed LANs

- Ethernet (IEEE 802.3)
  - Fast Ethernet and Gigabit Ethernet
  - 10 Mbps – 10 Gbps
- Fibre Channel
- High-speed WLAN

	Fast Ethernet	Gigabit Ethernet	Fibre Channel	Wireless LAN
Data Rate	100 Mbps	1 Gbps, 10 Gbps	100 Mbps - 3.2 Gbps	1 Mbps - 54 Mbps
Transmission Media	UTP, STP, optical Fiber	UTP, shielded cable, optical fiber	Optical fiber, coaxial cable, STP	2.4-GHz, 5-GHz microwave
Access Method	CSMA/CD	Switched	Switched	CSMA/Polling
Supporting Standard	IEEE 802.3	IEEE 802.3	Fibre Channel Association	IEEE 802.11

Ethernet

- The most widely used high-speed LANs today are based on Ethernet
- Protocol standards developed by the IEEE 802.3 standards committee
- MAC for a shared Ethernet bus:
  - CSMA/CD as random access MAC method
- Switched Ethernet

Ethernet standards for the physical layer

Table 16.3 IEEE 802.3 100BASE-T Physical Layer Medium Alternatives

	100BASE-TX		100BASE-FX	100BASE-T4
Transmission medium	2 pair, STP	2 pair, Category 5 UTP	2 optical fibers	4 pair, Category 3, 4, or 5 UTP
Signaling technique	MLT-3	MLT-3	4B5B, NRZI	8B6T, NRZ
Data rate	100 Mbps	100 Mbps	100 Mbps	100 Mbps
Maximum segment length	100 m	100 m	100 m	100 m
Network span	200 m	200 m	400 m	200 m

Key terms

- LAN
- IEEE 802 standards
- Ethernet (802.3)
- Token Ring (802.5)
- WLAN (802.11)
- WPAN (802.15)
- High-speed LAN
- Fibre Channel
- Switched Ethernet
- LAN topologies
- LAN transmission media
- MAC layer
- LLC layer
- Store-and-forward vs cut-through switches/bridges
- ”layer 3 switch”
- Switching/bridging table
- Spanning tree algorithm
- Load balancing
- Redundancy
- Collision domain
- Broadcast domain
- Subnetting
- Fast and Gigabit Ethernet