5. LAN SYSTEMS
Copyrights on Figures

- Figures presented in these notes with the following captions are extracted from the textbook and copyrighted by the publisher as indicated:

- DISCLAIMER
  - Whilst every attempt is made to maintain the accuracy and correctness of these notes, the author, Dr. Roberto Togneri, makes no warranty or guarantee or promise express or implied concerning the content.
Local Area Networks: Why have them?

- Sample Scenario
  - Organisation resources:
    - 16 database servers
    - 32 database client workstations
    - 2 high-end scanners
    - 2 high-end colour printers
    - 4 laser printers
    - 6 high availability disk and backup servers (RAID, UPS, DLT, etc.)
  - Organisation needs:
    - Database servers must have access to disk servers
    - Clients must have access to printers, scanners, and all servers
    - Database servers must be able to communicate with each other
    - Disk servers must be able to communicate with each other

- Sample solution
  - WAN technology no good:
    - Too many point-to-point connections
  - LAN technology to the rescue:
    - Connect database and backup servers directly to a high-speed backbone LAN
    - Group clients, scanners and printers in a shared LAN and use a bridge/router to connect group to high-speed backbone LAN
Local Area Networks: Why have them?

Diagram:
- High-Speed Backbone
- LAN A
  - Bridge
  - Database Server
  - Backup Server
  - Clients (Office)
- LAN B
  - Bridge
  - Clients (Engineering)
Local Area Networks: Architecture

• What characterises a LAN?
  – Host/Peripheral/Server (Station)
    • Computer (PC, UNIX workstation), networked peripheral (printer) or server (workstation driving a printer, supporting a high-capacity disk stack, or connected to backup tape device)
  – Network Interface Card (NIC) / Medium Attachment Unit (MAU)
    • Hardware card in a host/peripheral/server which allows communication between device and network medium
    • Operates by buffering incoming and outgoing data to/from host and network and providing a compatible interface for both ends (network protocol on one side and computer bus protocol on the other)
    • Generates and transmits frames according to specified MAC protocol, monitors all network traffic and passes only **unicast** frames destined for host and **broadcast** frames to host network operating system software.
  – Hubs / Cabling / Topology
    • **Hub:** or concentrator into which multiple hosts are connected and communicate through. Necessary for STAR topologies but can also support/emulate BUS and RING topologies
    • **Cabling/Wiring:** that connects hosts and hubs together. Also includes the enclosing building infrastructure (e.g. as is the case for power, plumbing, telephones, etc.). Not needed for wireless LANs.
    • **Topology:** How stations are wired or interconnected together
Local Area Networks: Architecture

- **Shared access / Broadcasting**
  - All hosts share the same network medium and hence data sent from one host to another host can be “heard” by all hosts → trusted hosts only listen to data destined for them
  - *Promiscuous mode* of operation → NIC passes all frames to network operating system (used for network analysis and debugging but also for other “devious” purposes)
  - Allows data to be broadcast to all hosts → can implement special network services (time management, announcements, queries, etc.)

- **Sub-networks (Virtual LANs or VLANs)**
  - A group of connected hosts which physically share the same broadcast network medium
  - *Shared sub-networks*: all hosts “hear” all other hosts
  - *Switched sub-networks*: not all hosts may hear other hosts (like point-to-point) but all hosts hear one another when making a “broadcast”
  - *VLANs*: Logically group a collection of hosts to be within a defined broadcast domain, not necessarily identical to the physical grouping of hosts

- **Bridge**
  - Can be used to isolate/segment sub-networks. Hosts on one side of the bridge cannot listen to host source and destinations traffic on the other side.
  - Retransmits received frames on one end of the bridge if destination host is on the other side of the bridge (requires filtering of frames).
  - Improves network performance by reducing the amount of shared traffic (e.g. one bridge can halve the amount of shared traffic)
Local Area Networks: Architecture

– Router
  • Interconnects different sub-networks together to allow point-to-point communication across sub-networks (but not broadcast, maybe multicast).
  • Operates at the network layer, usually requiring processing and re-encapsulation of packets.
  • Can interconnect different types of sub-network technologies (i.e. X.25 to IP)

– Firewall/Gateway
  • Enhanced router which connects organisation to the “rest of the world” (Gateway)
  • Can implement network filtering to control access to and from the outside to the inside of the organisation (Firewall)

– Backbone
  • High-speed sub-network which mainly connects to other sub-networks and supports the main sub-network to sub-network traffic
  • Also connects to standalone hosts and the gateway/firewall

– Communication Room/Closet
  • For hub-based networks (e.g STAR topologies, Unshielded Twisted Pair (UTP) networks, etc.)
  • Used where network cabling is part of building → all hubs and cables converge here
  • Single-point of failure for organisational networking
  • Easy upgradeability and maintenance of all networking by keeping everything in one place
  • Provides enhanced security and control of organisational network
LAN connectivity

• Repeaters
  – Physical layer 2-port device that receives, amplifies and forwards any signal received on one port to the other port
    • increases cable length of LAN by avoiding signal loss through signal attenuation
    • does not solve problem of increasing propagation delay with larger LANS (CSMA/CD slot time defines the maximum propagation delay allowed)
    • frames are only forwarded, not retransmitted and not processed

• Bridges
  – Physical / MAC layer 2-port device that receives, amplifies and retransmits frames received on one port to the other port only if MAC destination is there
    • increases cable length of LAN by avoiding signal loss through signal attenuation and segmenting the maximum propagation delay
    • improves security, reliability and performance by reducing network traffic
    • frames are processed to extract the source and destination MAC addresses, buffered and retransmitted according to the specified MAC protocol

• Hubs
  – Multi-port device used to interconnect individual client stations configured in a star or tree LAN topology

• Routers / Firewalls / Gateways
  – Network layer multi-port device that receives, filters, repacks, and routes packets received on one interface to the appropriate interface
Bridges

- Basic Operation for Bridge connecting LAN A and LAN B segments
  - Reads all frames transmitted on A and accepts only those addressed to stations on B
  - Checks the integrity of accepted frames (via the FCS), and rejects bad frames
  - Using the MAC for B, retransmits accepted frames onto B
  - Does the same for B-to-A traffic
  - Broadcast MAC frames are always accepted and retransmitted

Figure 14.2 (dcc5e)
Bridges: Advantages

• Independent LANs
  – Organisations have different departments each with their own LAN arrangement
  – Organisations have to communicate → LANs have to be connected

• Performance
  – Bridging a LAN splits the shared access and reduces load
  – Bridging a LAN reduces the bandwidth requirement for each segment

• Remote Connectivity
  – Geographical separation
  – Use remote bridges to connect the different areas together

• Reliability
  – Filtering operation of bridge isolates the LAN
    • Rogue station flooding network with packets will only effect the local segment

• Security
  – Stations can retrieve or snoop data not meant for that station
    (since medium is shared)
    • Stations on one side of the bridge cannot snoop data from stations on the other side of the bridge
Bridges: Disadvantages

- **Processing Latency**
  - A bridge operates in store-and-forward mode
    - Frames travelling across the bridge experience a delay
  - A bridge has to “learn” where destination stations are
    - Frames are only forwarded to LAN B if bridge knows destination is on LAN B

- **Buffer Overflow**
  - If traffic load is too high buffers may overflow
    - Bridge operates at the MAC layer and there is no flow control!
    - Frames will need to be retransmitted by a higher network layer

- **Unreliability**
  - If bridge fails, part of the network becomes unavailable
    - Additional network single-point of failure to servers and routers

- **Poor scaleability**
  - Does not filter broadcast frames → can create broadcast “storms”

- **Cost**
  - Purchasing, running and maintenance costs
Remote Bridges

- LAN-bridge-WAN-bridge-LAN
  - LANs interconnect transparently over a WAN link
  - LAN MAC frame is “tunnelled” through X.25 network

![Diagram of Remote Bridges](dcc5e)

Figure 14.4 (dcc5e)
Multi-MAC Bridges

- Differences which complicate the 802.x to 802.y bridge operation
  - Different Frame Formats
    - Figure 4.36 (cne3e)
  - Different Maximum Frame Lengths and Data Rates
    - 802.3(1500 bytes @ 10, 100 Mbps)
    - 802.4(8191 bytes @ 1, 5, 10 Mbps)
    - 802.5(token time @ 4, 16 Mbps)
Transparent Bridges

- Bridges learn location of stations by themselves
  - learning is transparent to stations
  - used by 802.3 and 802.4 LANs

- Bridge Forwarding
  - Frame arrives on port $x$ with DA = $z$
    - If (DA = $z$) is not in filtering database then frame is flooded on all outgoing ports (except $x$)
    - If (DA = $z$) is in filtering database as port $y$ then frame is repeated only on port $y$

- Bridge Learning
  - If frame arriving on port $y$ has an SA = $z$ not present in the bridge routing table then that entry is added (DA = $z$ is located on LAN connected to port $y$)
    - Entries in table are aged and eliminated after a certain time (e.g. 5 minutes)

Figure 14.8 (dcc5e)
Transparent Bridges

• **Bridge “Loop” Problem**
  – Bridge Forwarding and Learning is OK for tree topologies, but general topologies may have bridge loops which can cause problems

![Diagram of bridge loop problem](image)

**Problem 1:** Station B receives duplicate copies!
  – Station A on LAN X transmits frame to station B (SA=A and DA=B)
  – Bridges $\alpha$ and $\beta$ update their table to indicate station A is on LAN X and both forward the frame to LAN Y (station B is known to be on LAN Y)

**Problem 2:** Station A is unreachable!
  – Bridge $\alpha$ picks up the forwarded frame on LAN Y from bridge $\beta$ and seeing that SA=A updates its table to indicate station A is now on LAN Y
  – Bridge $\beta$ does the same thing

**Problem 3:** Bridges enter an infinite loop and kill off the network
  – If bridge $\alpha$ and $\beta$ do not know where station B is, the frame is flooded onto LAN Y. Bridge $\alpha$ picks up the flooded frame on LAN Y from bridge $\beta$ and seeing the unknown DA=B floods this frame on LAN X.
  – Bridge $\beta$ does the same thing, and of course bridge $\alpha$ now sees the flooded frame on LAN X from bridge $\beta$ and floods it on LAN Y and so on it goes
  – Station B does not have the opportunity to send a return reply and tell the bridges where it is really located since the network has probably collapsed by then
Transparent Bridges

• Bridge “Loop” Solution
  – Spanning Tree Algorithm is used to define a spanning tree of the bridge network
    • Bridges are assigned their own MAC address and are able to exchange special Bridge PDU’s (BPDU’s) to build the spanning tree
    • Bridges elect a root bridge and a root port to that bridge
      – Spanning tree is defined by a tree configuration starting at the root bridge and through the root ports of the remaining bridges
      – Bridges creating loops will effectively be removed (i.e. become non-operational) and end up as a leaf node

• Occurrence of Bridge “Loops”
  – Complex and large bridged LAN environments still subject to broadcast storms
    • Use a router to define and isolate sub-networks
      – Each sub-network is a single broadcast domain
    • Modify selected bridge operation to not repeat broadcast frames
      – May interfere with network operations (e.g. IP) which assume a sub-network is also a single broadcast domain
Source Routing Bridges

- Stations have to figure out and learn the route to the destination
  - Bridges are “dumber” (and cheaper) than with transparent bridges but stations have to be “smarter” (more costly).
    - And there are more stations than bridges
  - Stations may be able to learn a more optimal routing than strict spanning tree
  - Used by 802.5

- Basic Operation
  - Stations enter a route discovery and selection phase
    - *Option 1:* Source transmits an all-routes request so all possible routes to the destination are discovered (assuming the network survives the experience)
    - *Option 2:* Source sends a single-route (any route will do) and destination uses an all-routes response (which is really no better than option 1)
  - Broadcast “storm” operation saved by the fact that bridges only really connect small networks together
    - use routers and sub-networks for larger LANs as with transparent bridges
Transparent vs. Source Routing Bridges

- **Transparent Bridges**
  - **Advantages**
    - They are transparent!
    - No network management necessary as bridges do it all by themselves
    - Bridges quickly learn when a station or bridge is “down” as part of their operation
  - **Disadvantages**
    - Waiting for return reply from unknown destination to learn its location could take a long time
    - Bridges can be expensive
    - Routing is limited to (possibly sub-optimal) spanning tree and bridges not part of the tree remain idle (can’t be used to share load)

- **Source Route Bridges**
  - **Advantages**
    - Optimal routing possible and all bridges can participate
    - Bridges are not expensive
  - **Disadvantages**
    - Network management needed when changing the LAN physical configuration
      - Stations have to be told where the bridges are
    - Stations do not notice when a bridge or station is down (limited response to changes)
    - Stations more complex
    - Route discovery procedure inefficient
Hubs

- Used in Ethernet STAR LANs (10BASE-T and 100BASE-TX)
  - Uses UTP wiring:
    - One twisted pair for receive, One twisted pair for transmit
  - Each station is connected to either a *shared hub* or *switched hub*
    - **Shared hub** acts like a multi-port repeater (cheap option)
      - Data arriving on a port is repeated on all other outgoing ports
      - If data arrives from two or more different ports Hub sends out a *Collision Presence (CP) or enforcement signal* on all outgoing ports (forces CSMA/CD MAC to detect collision)
    - **Switched hub** acts like a multi-port bridge (expensive option)
      - Data arriving on a port is only repeated on the outgoing port connected to the destination station (unicast) or on all outgoing ports for a broadcast destination address
      - Bridge intelligence is required to learn location of stations connected to ports
      - For a 10 Mbps switched N-port device a 10xN Mbps *backplane* is required
  - Hubs can be stacked
    - Special Hub port can be used to interconnect Hubs and increase LAN capacity
    - Stacked Hubs act as one large Hub (Two 12-port stacked hubs act as one 24-port Hub)
  - Hubs can be arranged in a tree topology
    - *Header hub* (HHUB) forms the root of the tree
    - *Intermediate hubs* (IHUB) form the nodes of the tree
    - Stations form the leaves of the tree
Shared and Switched Hubs

(a) Shared medium bus

(b) Shared medium hub

(c) Switching hub

Figure 5.4 (hsn1e)
Shared Hub Combinations

Figure 6.4 (Imn5e)
Switched Hubs

- Two types of switch technologies
  - Store-and-forward switch
    - Hub accepts a frame on an input line, buffers it briefly in order to check the frame integrity (using the FCS field), and then routes it to the appropriate output line
    - Forwarding delay due to buffering and checking operation, but the overall integrity of network data transmission is improved
  - Cut-through switch
    - Since DA field is in the frame header, the hub repeats the frame on the appropriate output line as soon as the hub recognises the destination address
    - Faster throughput with minimal delay, but there is some risk of propagating bad frames since frame integrity is not checked

- Two types of NIC operations
  - Half-duplex operation (standard Ethernet operation)
    - Normal NIC operation with bus and shared hubs
    - Receive pair are used to monitor medium for collisions
  - Full-duplex operation (non-standard Ethernet operation)
    - Only possible with switched hubs
    - Station no longer needs to worry about collision detection (no carrier sensing)
    - Station can simultaneously transmit and receive network data → doubles per station throughput (e.g. full-duplex 10 Mbps operation implies a 20 Mbps throughput)
Hub Features

- Features
  - Uses existing telephone wiring infrastructure independent of station location
    - Bus LANs require running a cable between each station across different rooms which is dependent on the location of the stations
    - Hub is located in a communication closet which can be secured and managed centrally
  - Hub can isolate a station from network if cable breaks or station is defective
    - All stations on a Bus LAN are affected if the cable breaks, cable is not properly terminated or a station is defective and interferes with MAC signalling
  - UTP has poor attenuation
    - *Category 3 UTP*: Stations must be within 100m of Hub
    - *Category 5 UTP*: Stations must be within 150-200m of Hub
  - Hub is added expense, but can include more “intelligence”
    - Acts as repeater and allows extended LAN configurations by stacking hubs
    - More expensive switched hubs can greatly improve network utilisation by handling collisions directly within hub → no need to replace infrastructure to improve network performance, just buy a better hub.
    - Managed hubs allow network monitoring, debugging and analysis
  - Different Hub arrangements can be made for optimal performance
    - Client stations can be grouped by a shared 10Mbps hub
    - High capacity servers can be grouped by a switched 100Mbps hub
    - A dual hub can be used to interconnect the client 10Mbps LANs with the 100 Mbps server LAN
Gigabit Ethernet

- IEEE 802.3z standard
  - 1 Gbps data rate implications
    - Category 5 UTP no longer good enough (for now); use optic fibre wiring
    - Requires modification to CSMA/CD MAC
    - End stations cannot cope with sustained Gigabit speeds
      - 33 MHz synchronous PCI burst transfer of 32-bit data is exactly 1 Gbps
      - Operating system copying (kernel buffers → user space buffers) will reduce this
      - CPU and Bus context switching does not allow sustained data transfers and processing
    - Best used as inter-switch / inter-hub high-speed backbone links
  - Modified CSMA/CD MAC
    - 64-byte minimum frame size is too small
      - Ethernet maximum contention interval of 51.2 µsec → 5 km network span (2τ = 10 km)
      - Fast Ethernet max. contention interval of 5.12 µsec → 500 m network span (OK)
      - Gigabit Ethernet max. contention interval of 512 nsec → 50 m network span (Not OK!)
    - True network span is usually 0.25 of the theoretical due to attenuation within the transmission medium and delays at repeaters, bridges and hubs.
    - Solutions for 50 m network span
      - Carrier extension: short frames are padded to 512-bytes to permit collision detection
        - No data throughput on network during carrier extension → inefficient utilisation
      - Frame bursting: short frames are collected into 512-byte burst segments
        - Requires modified network driver software operation
Hub Mixed Configurations

- **Auto-Negotiation**
  - Extension to Ethernet protocol to allow different NIC and hub links to know about one another’s capabilities
    - 10/100 Mbps full-duplex NIC uses auto-negotiation to operate as a 10Mbps half-duplex when connected to a 10Mbps shared hub
  - Allows mixed configurations to be matched and inter-operate automatically
  - Auto-Negotiation operates at power-up / initialisation of devices
    - May fail if devices are re-connected while powered-up or if improperly initialised

- **Common Strategy**
  - Connect client and low-end stations into 10 Mbps hubs
    - Shared hub is most common with switched hubs for high-performance groups
  - Connect server and router/gateway/firewall stations into 100 Mbps hubs
    - Aggregate 10 Mbps client traffic to server can be accommodated
  - Each 10 Mbps hub has one switched 100 Mbps port
    - Allows 10 Mbps groups to access servers from same hub
  - Actual configuration depends on hub technology
  - Use Gigabit switched hubs for high-performance organisation level server access
100-Mbps Ethernet Backbone Strategy

Figure 5.7 (hsn1e)
Gigabit Ethernet Configuration

Figure 5.8 (hsn1e)

18-Jan-99

IND426, Roberto Togneri, E&E Eng, Univ. of Western Australia
ATM LAN Emulation (LANE)

- ATM performs MAC level emulation
  - ATM network performs a “bridge” function
    - ATM is transparent to network protocols
    - Can be used to interface with any “legacy” LAN
  - LAN Emulation Protocol (LEP) layer above AAL 5
    - Supports traditional LAN MAC operation

Figure 14.13 (dcc5e)  
Figure 14.14 (dcc5e)
ATM LAN Emulation (LANE)

• Problems
  – “Legacy” LANs use MAC addresses and ATM connections require ATM addresses → How are address translations made?
  – ATM is connection-oriented but the LAN MAC is basically connectionless and higher layer networks can use datagrams → How can ATM support datagrams?
  – ATM is connection-oriented but the LAN MAC allows multicast and broadcast addressing → How can ATM do broadcasting?

• Solution: use special servers
  – Terminology
    • LEC (LAN Emulation Client)
      – The LAN bridge to the ATM network
      – The LAN host connected to the ATM network
    • LECS (LAN Emulation Configuration Server)
      – Tells the LEC where the LES and BUS are located
    • LES (LAN Emulation Server)
      – Performs the MAC to ATM address translation
    • BUS (Broadcast and Unknown Server)
      – Performs Multicast/Broadcast communication
      – Uses broadcasting for locating unknown addresses
ATM LAN Emulation (LANE)

Figure 10.15 (dccn4)