LAN / WAN Technologies

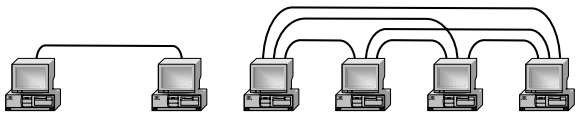
By
Edward Cheung
email: icec@polyu.edu.hk
15 July, 2003.

Agenda

- Direct Point-to-Point Communication vs Shared Communication Channels
- LAN Topologies
  - Star (e.g. switched Ethernet, ATM)
  - Ring (e.g. token ring, FDDI)
  - Bus (e.g. Ethernet)
  - Fiber Optic Extensions
  - Repeaters / Bridges / Switches
- WAN Technologies
  - Difference between LAN and WAN
  - Routing in a WAN
  - Examples – APPANET , ATM

Direct Point-to-Point Communication (1)

Each communication channel connected exactly two computers, and was available to those computers exclusively, known as a ***point-to-point network***.



The independent point-to-point connections required for (a) two, and (b) four computers.

Direct Point-to-Point Communication (2)

- exclusive access to individual network link enable connected computers to maximize individual link performance.
  - For example, different modem or interface to different machine, different protocol, frame format, etc.
- Two computers have access to a channel / link only. It is relatively easy to enforce security and privacy. No other computers handle data, and no other computers can obtain access.
- Disadvantage of fully connected network is non- scalable.

Direct Point-to-Point Communication (3)

The Disadvantage of point-to-point network:

In a point-to-point scheme that provides a separate communication channel for each pair of computers, the number of connections grows rapidly as the number of computers increases.

Mathematically, the number of connections needed for N computers is proportional to the square of N:

$$\textit{direct connections required} = \frac{(N^2 - N)}{2}$$

Shared Communication Channels (1)

In the networks, multiple computer communicate through one shared communication channel.

A shared networks used for local communication.

Typically used for Local Area Networks (LANs) due to the propagation delay limitations.

Each LAN consists of a single shared medium, usually a cable, to which many computers attach.

The computers take turns using the medium to send packets.

Shared Communication Channels (2)

Advantage:

- Saving of resources like the communication channel Reduces cost

Disadvantage:

- Shared networks with long delays are inefficient.
- High bandwidth communication channel over long distances.
- Collisions may cause delays and waste of bandwidth.
- An arbitration protocol required.

LAN Topologies (1)

Local area network topologies can be described using either a physical or a logical perspective.

A ***physical topology*** describes the geometric arrangement of components that comprise the LAN.

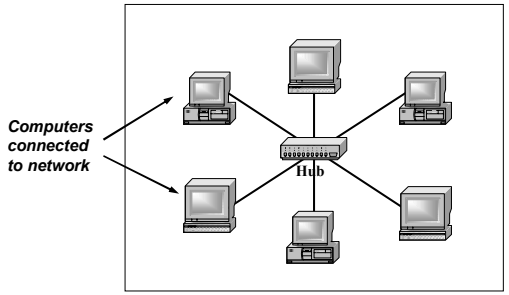
A ***logical topology*** describes the possible connections between pairs of networked endpoints communicate.

Network can be classified into three basic physical topologies:

- Bus
- Ring
- Star

Star Topology (1)

A network uses a *star topology* if all computers attach to a central point.



Star Topology (2)

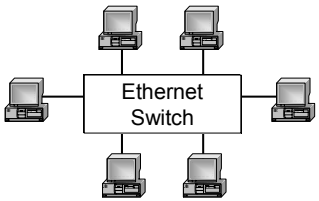
A star-shaped network resembles the spokes of a wheel, the center of a star network is often called a ***hub.***

A typical hub is an electronic network device that accepts data from a sending computer and delivers it to the appropriate destination.

In practice, star networks seldom have a symmetric shape in which the hub is located at an equal distance from all computers.

Example - Star Network (1)

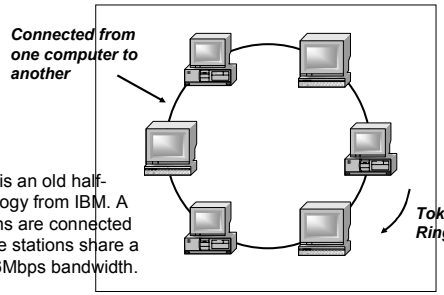
Six computers connected to an Ethernet switch and form a LAN.



Ring Topology (1)

A network that uses a ***ring topology*** arranges for computers to be connected in a closed loop.

- Each computer connects directly to two others.



Token Ring is an old half-duplex topology from IBM. A set of stations are connected in a ring. The stations share a 4Mbps or 16Mbps bandwidth.

Ring Topology (2)

The name ***ring*** arises because the computer apparently to be connected in a circular fashion.

The ring, like the star topology, refers to logical connections among computers, not physical orientation - the computers and connections in a ring network need not to be arranged in a circle. However, the ring must be a continuous loop. For example, the cable between a pair of computers in a ring network may follow the contour of hallways or rise vertically from one floor to another.

Disadvantages of the token ring networks:

- Because each computer attached to a ring must pass bits of a frame to the next computer, failure of a single machine can disable the entire network.

Example - Ring Network (1)

Fiber Distributed Data Interconnect (FDDI)

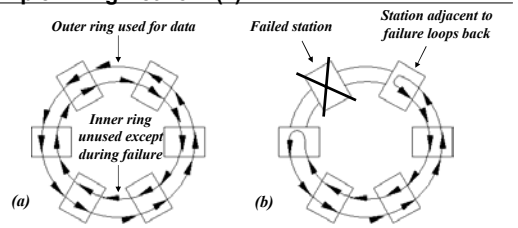
FDDI is a fiber-optic token ring LAN that offers a data rate of 100 Mbps, max. length 2km between stations, 100km max. ring circumference and 500 stations per ring.

FDDI is fault-tolerant topology and it uses dual ring redundancy to overcome failures.

An FDDI network contains two complete rotating rings – Dual counter-rotating ring

- The primary ring is used to send data when everything is working correctly.
- The secondary ring provides an alternative data path when a fault occurs in the primary ring.

Example - Ring Network (2)



FDDI network is called ***self-healing*** because the hardware can detect a catastrophic failure and recover automatically

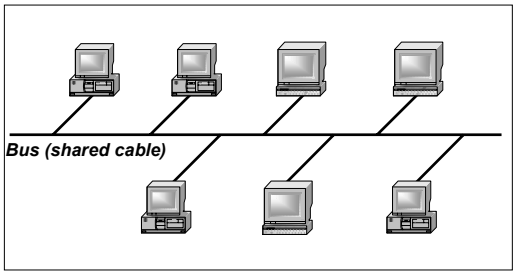
Hardware in the stations adjacent to a failure detect the disconnection and reconfigure so they loop incoming bits back along the reverse path.

A Note on Token Ring / FDDI

- Ring is actually a form of star topology.
- Basically, a token is passing around the stations and that station captured the token has the right to transmit. Others has to wait for its turn.
- Token ring conforms to IEEE 802.5
  - http://www.8025.org
- Copper Distributed Data Interface (CDDI) is the implementation of FDDI protocols over Cat.5 STP/UTP.
  - The distance from desktop to concentrator is reduced to 100m.
- The industry is not interested in Token Ring anymore. The last Token Ring standard is 802.5v-2001 for Gigabit speed. The working group is now inactive with no new development.

Bus Topology (1)

A network that uses a ***bus topology*** usually consists of a single, long cable to which computers attach.



Bus Topology (2)

Any computer attached to a bus can send a signal down the cable, and all computers receive the signal.

Because all computers attached to the cable can sense an electrical signal, any computer can send data to any other computer.

The computers attached to a bus network must coordinate to ensure that only one computer sends a signal at any time or signals will collide with each other.

Example - Bus Network (1)

Ethernet:
Ethernet is a well-known and widely used network technology that employs bus topology. IEEE802.3 working group controls the Ethernet standards.

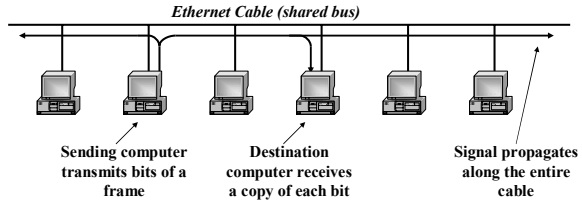
- The original Ethernet hardware operated at a rate of 10 Mbps
- A later version known as ***Fast Ethernet*** operates at 100 Mbps.
- The most recent version, which is known as ***Gigabit Ethernet*** operates at 1000 Mbps or 1 Gigabit per second (Gbps).
- 10Gbps on copper will soon be available
  - IEEE 10GBASE-T Study Group Meeting on Jan 9-10/2003

    http://www.ieee802.org/3/10GBT/public/jan03/index.html

Example Bus Network (2)

Ethernet uses a bus topology, Ethernet requires multiple computers to share access to a single medium.

Figure illustrates how data flows across an Ethernet.



While transmitting a frame, a computer has the exclusive use of the cable.

Example Bus Network (3)

A sender transmits a signal, which propagates from the sender toward both ends of the cable.

Sharing in local area networks technologies does not mean that multiple frames from different computers are being sent at the same time. Instead, the sending computer has exclusive use of the entire cable during the transmission of a given frame – other computers must wait.

Only one computer can transmit at any time. After the computer finishes transmitting one frame, the shared cable becomes available for another computer to use.

Hence, we need a bus arbitration scheme.

CSMA (1)

All computers attached to an Ethernet participate in a distributed coordination scheme called ***Carrier Sense Multiple Access (CSMA).***

The scheme based on electrical signal activity on the cable to determine status.

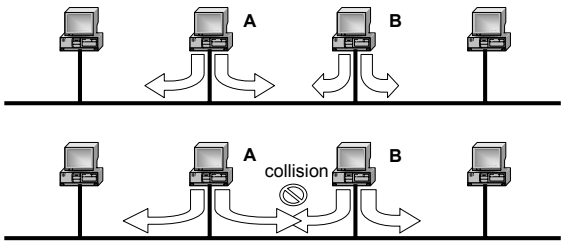
When no computer is sending a frame, the cable does not contain electrical signals. During frame transmission, a sender transmits electrical signals used to carry encode bits. We can determine whether the media is being used by detecting the presence of a carrier.

If no carrier is present, the computer can transmit a frame. If a carrier is present, the computer must wait for the sender to finish before proceeding.

CSMA (2)

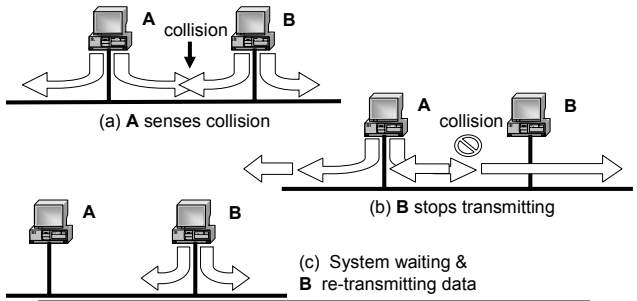
CSMA cannot prevent a computer from interrupting an ongoing transmission (conflicts).

If two computers at opposite ends of an idle cable both have a frame ready to send simultaneously, a ***collision*** occurs.



Collision Detection and CSMA/CD (1)

Carrier Sense Multiple Access with Collision Detect (CSMA) is the formal name for access method that can monitoring a cable during transmission to detect collisions.



Collision Detection and CSMA/CD (2)

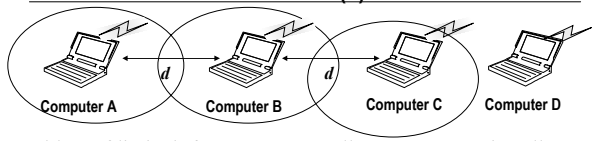
After a collision occurs, there will be a corrupted Ethernet frame and the computer must wait for the cable to become idle again before transmitting a frame. The sender will send a noise burst to all stations to abort transmission.

Ethernet requires each computer to delay for an arbitrary time ***t1*** (where $0 \le t1 \le d$) after a collision before attempting to retransmit.

If another collision occurs, the computer will wait for ***t2*** (where $0 \le t2 \le 2d$) and double range for successive collision. In general, the wait is between 0 and 2^r -1 where r is the number of collision. This is called Binary Exponential Backoff algorithm.

The computer will freeze the time interval after 10 attempts and stop trying after 15 attempts.

Wireless LANs and CSMA/CA (1)



Problem of limited rf coverage:- not all computers receive all transmissions hence cannot use CSMA/CD. In the above example, if the maximum transmission distance is d, computer A does not receive computer C's message.

When A transmits to B and C also transmits to B, the frames will collide at B – hidden terminal problem.

When C hears the transmission from B to A, C may falsely concluded that it cannot transmit to D – exposed terminal problem

Wireless LANs and CSMA/CA (2)

A set of wireless LAN technology are available that use a modified form of CSMA/CD known as ***Carrier Sense Multiple Access with Collision Avoidance (CSM/CA***); basis for IEEE 802.11 LAN.

The basic idea is that the sender simulates the receiver into outputting a short frame before transmitting data so that station nearby can detect this transmission and avoid transmitting for the duration of the upcoming (large) data frame.

Control messages are much shorter than data frames, the probability of a second collision is much lower than with conventional Ethernet. Collisions of control messages can still occur and they can be handled with backoff algorithm

Wireless LANs and CSMA/CA (3)

The operation is as follows:-

- B wants to send message to C
- B send a Request To Send (RTS); 30 bytes packet to C. This packet contains the length of the data frame that will eventually follow.
- C replies by sending a Clear To Send (CTS) also contain the length of the data. B is clear to send data after receiving the CTS.
- All stations know the length of the data and their relative position to the transmitter / receiver and they can act accordingly.

Type of Ethernet (1)

Ethernet has several different variations, each of which uses different cable types, topologies, and distance limitations.

The different types are:

- 10 Base-5 (Thick Ethernet)
- 10 Base-2 (Thin Ethernet)
- 10 Base-T (UTP Ethernet)
- 10 Base-FL
- 100 Base-T
- 100 Base-F
- Gigabit Ethernet
- 10-Gigabit Ethernet

10 Base-5 -- Thick Ethernet (1)

Thick Ethernet, officially known as 10 Base-5

10 Base-5 is laid out in a bus topology, with a single coaxial cable connecting all nodes together.

At each end of the coaxial cable is a terminator.

Each node on the network physically connects to the coaxial cable through a device called a transceiver and an AUI cable is connected between the node and the transceiver.

10 Base-5 -- Thick Ethernet (2)

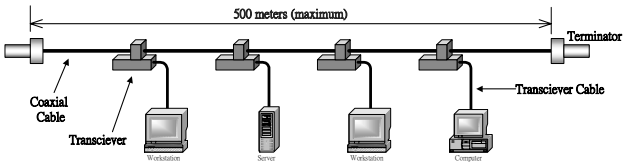


Figure: Thick Ethernet Physical Topology

A single 10 Base-5 segment may be up to 500 meters (1650 feet) in length and may have up to 255 nodes connected to it. Please note that each node must be at least 2.5 meters (8.25 feet) apart.

Advantage and Disadvantage of 10 Base-5 (1)

Advantage

Long Distances Possible

10 Base-5 allows distances up to 500 meters (1650 feet). This makes it very useful as a "backbone" technology for wiring together multiple locations within a building without the use of repeaters

Noise Immunity

Since 10 Base-5 uses a very heavily shielded cable, it can be used in electrically noisy environments which can cause other network types to fail.

Conceptually Simple

Since all devices on a 10 Base-5 network are simply chained together on a common coaxial cable, it is a simple matter to plan the routing of the cable.

Advantage and Disadvantage of 10 Base-5 (1)

Disadvantages

Inflexible

10 Base-5 networks do not lend themselves well to installations where the setup of the network will change much after the initial installation. It can be very difficult to add or move a node once it is connected to the coaxial cable.

Fault Intolerant

Since 10 Base-5 uses a common physical cable to interconnect all the nodes, the failure of any part of the coaxial cable or any node has the ability to cause the collapse of the entire network.

10 Base-5 -- Thick Ethernet (6)

Susceptible To Ground Loops

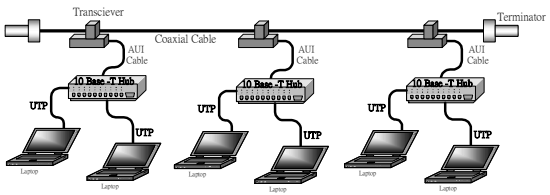
A ground loop occurs when a network cable is used to interconnect devices which are powered from different sources, and therefore a difference in voltage exists between two points on the network. The result is an electrical current flowing through the shields of the cable, which causes considerable noise to be introduced into the center conductor.

Very Difficult Troubleshooting

As mentioned above, a failure anywhere on a 10 Base-5 segment has the ability to drop the entire network. Troubleshooting such a failure can be extremely frustrating, as the only way to do it is to check each node and the cabling between them one at a time. This is very time consuming, and can be expensive if a company's entire business relies on the network to be up.

10 Base-5 -- Thick Ethernet (7)

The most common use for 10 Base-5 was using it as a "backbone" technology. For example, a backbone can be used to connect 10 Base-T hubs to create one large network.



10 Base-2 – Thin Ethernet (1)

Thin Ethernet, officially known as 10 Base-2. Sometimes also known as Thinnet or Cheapnet.

It is a less expensive version of 10 Base-5 technology. It uses a lighter and thinner coaxial cable and dispenses with the external transceivers used with 10 Base-5.

10 Base-2 uses an RG-58A/U coaxial cable and is wired in a bus topology. Each device on the network is connected to the bus through a BNC "T" adapter, and each end of the bus must have a 50 Ohm terminator attached. Each node on the bus must be separated by a minimum of 0.5 meters (1.5 feet) apart, and the overall length of the bus must be less than 185 meters (606 feet).

10 Base-2 – Thin Ethernet (2)

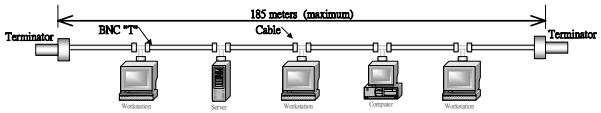


Figure: *Sample 10 Base-2 Network*

10 Base-2 network is connected in a simple daisy-chained format with inexpensive coax cable and "T" adapters. There are usually no hubs, transceivers, or other devices used. It was quite popular because its low cost and easy implementation.

10 Base-2 – Thin Ethernet (3)

Fault Intolerant Problem

10 Base-2 technology is generally well suited to small networks which will not change much after the initial installation is complete. Reconfiguring a 10 Base-2 network is difficult because any change to the network will result in at least some "down time," as the bus must be broken.

If any device or cable section attached to the network fails, it will most likely make the entire network go down. Therefore, it is not suitable for large network. 10 Base-2 networks are very difficult to troubleshoot. There is no easy way to determine what node or cable section is causing a problem, and the network must be troubleshot by a "process of elimination." This can be very time consuming.

10 Base-T – Unshielded Twisted Pair

10 Base-T utilizes Category 3 (or higher) Unshielded Twisted Pair (UTP) cable in a star topology. Each node on the network has its own cable run back to a common hub, and each of these cable runs may be up to 100 meters (330 feet) in length.

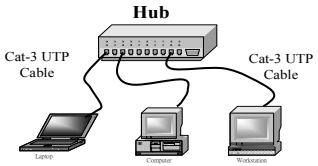


Figure: *10 Base-T network*

10 Base-T

Cabling Considerations

10 Base-T uses two pairs of wires: one pair for transmission and the second pair for receive.

The physical connector used is an 8 position modular plug, commonly referred to as an RJ-45.

All cables must be rated at a minimum of Category 3, and must be wired such that pins 1 & 2 are on one twisted pair and pins 3 & 6 are on a second pair.

Common wiring standards which meet this requirement are EIA/TIA T568A and T568B.

10 Base-F (1)

10 Base-F is basically a version of Ethernet which runs over fiber optic cable. In physical topology, it is very similar to 10 Base-T

10 Base-F runs over 62.5/125 micron multimode fiber optic cable. It supports distances up to 2000 meters (6600 feet).

10 Base-F is wired in a star topology with all of the fiber optic runs originating from a central hub. It is also acceptable to connect a pair of 10 Base-F devices directly together with a point to point link.

10 Base-FL is very useful for use in interconnecting buildings in a campus environment where distances could be very long.

Pros and Cons of 10 Base-T over UTP (1)

Fault Tolerant

Since each node on a 10 Base-T network has its own cable connecting it to a central hub, it is far less likely that any node can cause the entire network to fail. The hub also has a "partitioning" function built into it which allows it to detect a problem on any of its ports. If a problem is found, the node is disconnected from the rest of the network. This isolates the problem until the node can be troubleshot and repaired.

Inexpensive, Easy Moves & Changes

Disconnecting a node from the network has no effect whatsoever on the rest of the network. Therefore, moving an attached device is simply a matter of unplugging it from the hub and reconnecting it somewhere else. UTP is inexpensive, lightweight, easy to pull and easy to terminate.

Pros and Cons of 10 Base-T over UTP (2)

Easy Troubleshooting

Because of the partitioning function built in to the hubs and the star-wired topology, it is generally easy to troubleshoot a 10 Base-T network. In a worst-case scenario, one can be troubleshot by simply disconnecting nodes from the hub one at a time until the network recovers. Usually, the hub will give an indication as to which node is causing a problem, allowing the technician to troubleshoot that node as opposed to spending many hours finding where the problem is.

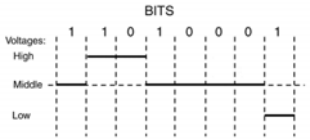
The real problem is the short segment length

10 Base-T only allows distances from the hub to the node of 100 meters (330 feet). In some installations, this is a problem if nodes need to be located far away.

100BaseT

- Known as Fast Ethernet
- Normally use Cat.5 cable
- Use 4B5B encoding; every group of 5 clock period is used to send 4 bits. Hence the efficiency is 80%.
- For transmitting 100Mbps, the bandwidth need on the twisted pair will be 125Mbps.
- 4B5B encoding provide enough transitions to allow easy clock synchronization and create unique patterns for frame delimiting; e.g. “11111” means idle line.
- (Multilevel Transmit) MLT-3 coding is used to minimize EMI effect.
- In MLT-3, a transition occur for every binary 1 in 3 voltage levels.

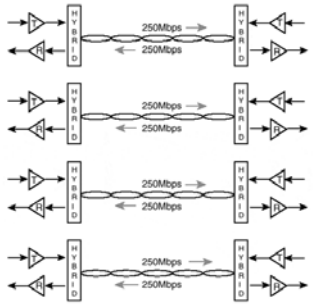
MLT-3 5B4B Encoding in 100BASE-Tx



Hex	4B	5B
0	0000	11110
1	0001	01001
2	0010	10100
3	0011	10101
4	0100	01010
5	0101	01011
6	0110	01110
7	0111	01111
8	1000	10010
9	1001	10011
A	1010	10110
B	1011	10111
C	1100	11010
D	1101	11011
E	1110	11100

1000BaseT

- IEEE802.3ab
- Gigabit Ethernet over Category 5 UTP
- Uses Four-dimensional five-level pulse amplitude modulation (4D-PAM5) encoding scheme and keep the symbol rate below 125Mbps per cable pair.
- For server to switch link



High Speed Ethernet Coverage

Name	Media	Cable	Distance
100Base-T4	4-Twisted Pair Copper	Cat. 3 UTP	100m
100Base-TX	2-Twisted Pair Copper	Cat. 5 UTP	100m
1000BASE-T	4-Twisted Pair Copper	Cat. 5 UTP	100m
1000BASE-CX	2-Twisted Pair Copper	Twinaxial STP	25m
1000BASE-SX	2 x MMF Fiber (850nm)	MMF (62.5µm)	220m-275m
1000BASE-LX	2 x MMF Fiber (1300nm)	MMF (62.5µm)	550m
1000BASE-ZX	2 x SMF Fiber (1550nm)	SMF (9µm)	550m

Extending LANs

- LAN technology is designed for a specific combination of speed, distance, and cost.
- Different LAN technologies specifies maximum distances that the LAN can span. Typically, LANs are designed to span a few hundred meters.
- The coverage for LAN can be extended by interconnecting different LANs using equipment such as:- Fiber Modems, Repeaters, Bridges, Switches, etc.

Fiber Optic Extensions (1)

Coverage of LAN segment can be extended by inserting optical fibers and a pair of fiber ***modems*** between a computer and a transceiver.

Fiber has low delay and high bandwidth.

Provides connection to remote LAN without changing the original LAN or the computer.

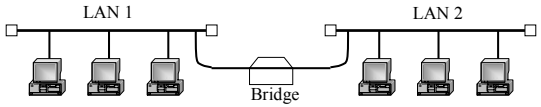


Figure illustrates fiber modems used to extend an Ethernet connection.

Fiber Optic Extensions (2)

To provide a connection to a remote LAN without changing the original LAN or the computer.

Since delays across fiber are low and bandwidth is high, the mechanism will operate correctly across distances of several kilometers.

The most common use involves connecting a computer in one building to a LAN in another building.

Repeaters & Hubs (1)

Repeater works at level 1 and no buffering or logical isolation of segments.

A repeater is usually an analog electronic device that continuously monitors electrical signals on each cable.

The repeater transmits an amplified copy signal on one cable to the other cable.

A repeater connects two Ethernet ***segments***, each of which must has the usual termination.

Hub is a twisted-pair repeater, shared / collision medium.

Repeaters & Hubs (2)

A repeater connecting two Ethernets, it can double the effective size of an Ethernet network.

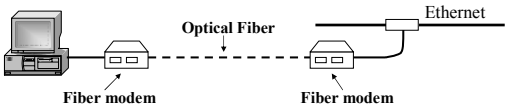
Repeaters do not understand the frame format, nor do they have physical addresses.

The maximum size of an Ethernet segment is 500 meters.

When using repeaters, the source and destination computers cannot determine whether they are connect to the same segment or to different segments.

Bridges and Switches (1)

- Working at layer 2, modern bridges are switches.
- Connect LAN segments using store and forward strategy.
- Bridges can examines the Media Access Control (MAC) address of the datagram that flow through it to build a table of known destinations.
- Can be used to link between different technology. For example, joining 100BaseT to 10Base2. Joining 802.x to 802.y; for example, Ethernet to Token Ring is difficult because of incompatibility at framing level, use router instead of bridge.



Bridges and Switches (2)

Transparent Bridges

- No configuration is needed, plug and work.
- Computers on the network will not know if a bridge has been added.
- Transparent bridge operates in promiscuous mode. That is accepting every frame transmitted on all of the LAN attached.
- Backward learning algorithm; looking at the source address of the packet and update its filter table.
- better than repeaters; help isolate problems
- Bridge will discard broken frame and will not forward a bad frame from one segment to another. Thus, the bridge keeps problems on one segment from affecting the other.

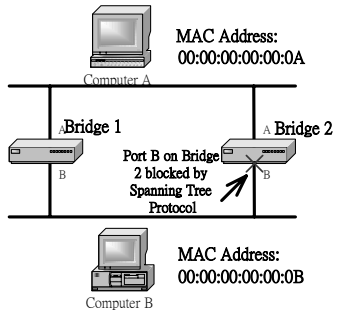
Operation of a Bridge

- If the bridge receives a datagram with destination address on the same segment as the source of the datagram, it drops the datagram. If the bridge knows that the destination is on another segment, it transmits the datagram on that segment only.
- If the bridge does not know the destination segment, the bridge transmits the datagram on all segments except the source segment (a technique known as flooding).
- The primary benefit of bridging is that it limits traffic to certain network segments.
- Additional benefit is that the bridge will verifies that the integrity of an incoming frame before forwarding a copy to other segment.

Spanning Tree Bridges (1)

- Problem exists when loops are created when connecting bridges.
- Some frames may circulate in bridges forever.
- The solution is to organize interconnected LANs into a spanning tree.
- To build the spanning tree, first choose one bridge to be the root of the tree. The bridge with the lowest MAC address will be elected. Next, a tree of shortest path to each LAN will be constructed.
- A STP bridge will send out message known as Bridge Protocol Data Unit (BPDU) to determine network configuration for every 2 seconds by default on Cisco switches and update the tree.
- Spanning Tree Protocol is IEEE802.1d

Spanning Tree Bridges (2)



Issues in Bridges and Switches (1)

They are ***store-and-forward*** devices, meaning that they introduce an intrinsic delay between interconnected LANs: characterized in terms of the number of frames forwarded per second.

Cisco supports 3 switching methods:

Store and forward
- Forward on receiving the entire frame, check CRC, etc., conventional, most reliable, high latency

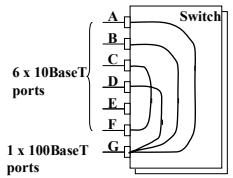
Cut-through
- Start forwarding after receiving the first 6 bytes, fast, high end switch, assume good LAN with low corrupt frame

Fragment Free
- Start forwarding after receiving the first 64bytes known as the collision window.

Issues in Bridges and Switches (2)

- The advantage with switching is that collisions can be avoided entirely.
- However, there is no ***flow control*** at the MAC layer so it is possible for a bridge to receive frames faster than they can be buffered and re-transmitted.

Such frames must be discarded, leading to increased traffic as higher layer protocols attempt to resend lost data frames. Hence backplane bus speed and the capacity of buffer are important specifications for a switch.



Virtual LAN

- A virtual LAN (VLAN) is a group of hosts or network devices, such as routers (running transparent bridging) and bridges, that forms a single bridging domain. Layer 2 bridging protocols, such as IEEE 802.10 and Inter-Switch Link (ISL), allow a VLAN to exist across a variety of equipment, including LAN switches.
- the goal is to group users into VLANs so that most of their traffic stays within the VLAN
- Traditionally, we have 80/20 rule means that 80% of traffic is in the LAN and 20% is connecting to outside. Depending on different application, now may reversed.

Benefits of VLAN

Broadcast control

- isolate collision domains

Security

- users outside of that VLAN cannot communicate with the users in the VLAN and vice versa without a gateway inside VLAN

Network management

- easy to assign users to different VLANs without cabling for administration and manage bandwidth to tune for better performance

Difference between LAN and WAN

LAN:

LAN technologies is used at a single site, techniques can extend the distance spanned to within a building or campus.

A satellite bridge / modem can connect two segments of a LAN over an arbitrary distance. VSAT – Very Small Aparture Terminal

Bandwidth limitations prevent a bridged LAN from serving arbitrarily many computers at arbitrarily many sites.

Difference between LAN and WAN

WAN:

WAN technologies from LAN technologies is scalability.

WAN must be able to grow as needed to connect any sites spread across cities in large geographical distances. Sometimes, it is also known as long-haul network.

A technology is a WAN technology if it is scalable and can deliver reasonable performance to cover a large geographical area, large network and manageable. In today's development, many technologies exist in both LAN and WAN application. e.g. Ethernet, ATM.

Packet Switch

A packet switch is the basic building block of WANs. A WAN is formed by interconnecting a set of packet switches, and then connecting computers.

The packet switches used in WAN operates at high-speed connections to other packets switches. In today's network, fiber technology is a common technology in WAN switching.

A packet switch does not keep complete information on how to reach all possible destinations. It only has next hop information. A switch usually has multiple I/O connectors, making it possible to form many different topologies and to connect multiple computers – multiple interface. Ethernet, Frame Relay or ATM is common packet technologies to link up packet switches or routers.

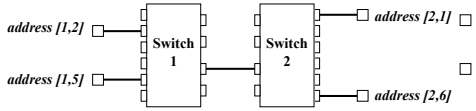
Physical Addressing in a WAN

WAN network operates similar to a LAN

- Data transmitted in packets (equivalent to frames)
- Each packet has format with header.
- Packet header includes source and destination's address

Two part hierarchical addressing scheme:

- One part of address identifies destination switch.
- Other of address identifies port on switch



Routing in a WAN

For a WAN to work correctly, both ***interior*** and ***exterior packet switches*** must have a routing table and both types must forward packets.

Values in the routing table must guarantee the following:

- **Universal routing.** The routing table in a switch must contain a next-hop route for each possible destination.
- **Optimal Routes**. In a switch, the next-hop value in the routing table for a given destination must point to the shortest path to the destination.Each computer connects directly to two others.

Routing in a WAN

Modeling a WAN

A graph representation of a network is useful. Because a graph represents packet switches without attached computers

Each ***node*** in the graph corresponds to a packet switch in the network. If the network contains a direct connection between a pair of packet switches, the graph contains an ***edge*** or link between the corresponding nodes.

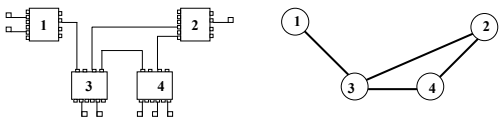


Figure: shows an example WAN and the corresponding graph.

Routing in a WAN

Route computation with a graph

A graph can be used to compute and understand next-hop routes.

destin-ation	next hop
1	--
2	(1, 3)
3	(1, 3)
4	(1, 3)

node 1

destin-ation	next hop
1	(2,3)
2	--
3	(2,3)
4	(2,4)

node 2

destin-ation	next hop
1	(3,1)
2	(3,2)
3	--
4	(3,4)

node 3

destin-ation	next hop
1	(4,3)
2	(4,2)
3	(4,3)
4	--

node 4

The routing table for each node in the graph of previous Figure. The next-hop field in an entry contains a pair (u,v) to denote the edge in the graph from node u to node v.

Example - WAN Technology

ARPANET:

ARPANET was one of the first packet switched WANs.

Packet switched WANs began in the late 1960s. Packet switch or routers are connected together which formed the early Internet

The *Ad*vanced *Research Projects Agency (ARPA)* research project developed a Wide Area Network to determine whether packet switching technology could be used in battlefield conditions.

History of ARPANET can be found at:

http://www.nic.funet.fi/index/FUNET/history/internet/en/arpanet.html

For today's Internet, check out:

http://www.startap.net

Example WAN Technology

ATM:

Asynchronous Transfer Mode (ATM), provides an example of a WAN technology.

ATM is a circuit switched communication procedure.

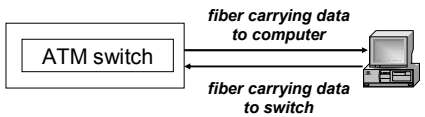
Goals:-

- To handle conventional telephone voice traffic as well as data traffic,
- To serve as a local area technology as well as a wide area technology.

Typical ATM Connection

Because ATM is designed to provide high throughput, a typical connection between a computer and an ATM switch operates at a speed of 155 Mbps or faster. For copper connections, the data rate is 25Mbps.

A connection between an ATM switch and a computer.



Each connection consists of a pair of optical fibers. One fiber carries data to the switch, and the other carries data to the computer.

ATM (2)

ATM is a packet switching technology but emulates circuit switching.

- A virtual connection must be established before user data is transferred- connection oriented; Virtual Circuit (VC).
- Virtual circuit means that the connection does not exists physically but rather exist in a routing table.

Two kinds of connections:-

- Permanent Virtual Circuit (PVC)
  - Set up and typically maintained for months and years
- Switched Virtual Circuit (SVC)
  - Set up dynamically as needed and torn down after use.

ATM (3)

- 2 Interface exists in ATM
  - User Network Interface (UNI)
    - Interface between subscriber switch and terminal equipment
  - Network Node Interface (NNI)
    - Interface between network switches
- ATM cells are the smallest standardized information units within the ATM network
- Fixed length packet 53 bytes (5 bytes header + 48 bytes payload)
- Header included 2 Identifier
  - Virtual Path Identifier (VPI)
    - 8 bits for UNI and 12 bits for NNI
  - Virtual Channel Identifier (VCI)
    - 16 bits

ATM (4)

- The cells find their way through the network using the VPI/VCI. The information only applies to a section of the connection. The VCI is assigned by the switching centre.
- Routing between switches is based on the VPI only.
- VCI is used for routing at the final hop in each direction, between the host and switch.
- Reduce the computation needed to route a packet by separates routing address. The VPI allows the collection of VCs.
- Transmission is transparent to ATM. TDM telephone system, SONET or (Synchronous Optical Network) can be used to transport the ATM cell.

Example of an ATM Network