NETWORKING COMPONENTS

1) OBJECTIVES

The objectives of this chapter are to familiarize with the following: -

i) The LAN components

ii) Repeater

iii) Hub

iv) Bridge

v) Router

vi) Gateway

2) INTRODUCTION

Information does not exist in a vacuum. Just as the need to share in formation between desktop computers in an office has forced the proliferation of LANs, the need to share information beyond a single workgroup is forcing the adoption of LAN-to-LAN links, host gateways, asynchronous communication servers, and other methods of communicating with other systems.

3) LAN COMPONENTS

Local Area Network is a high speed, low error data network covering a relatively small geographic area. LAN connects workstations, peripherals, terminal and other devices in a single building or other geographically limited area. LAN standard specifies cabling and signaling at the physical and data link layers of the OSI model. Ethernet, FDDI and Token ring are widely used LAN technology. In LAN technology to solve the congestion problem and increase the networking performance single Ethernet segment is to divide into multiple network segments. This is achieved through various network components. Physical segmentation, network switching technology, using full duplex Ethernet devices, fast Ethernet and FDDI available bandwidth may be maximized.

4) REPEATERS

Repeaters are devices that amplify and reshape the signals on one LAN& pass them to another. A repeater forwards all traffic from one LAN to the other. Repeaters are usually used to extend LAN cable distances or connect different media type.

Repeaters connect LANs together at the lowest layer, the Physical layer, of the OSI model. This means that repeaters can only connect identical LANs, such as Ethernet/802.3 to Ethernet/802.3 or Token Ring to Token Ring.

OSI MODEL
LAN INTERCONNECTION DEVICE

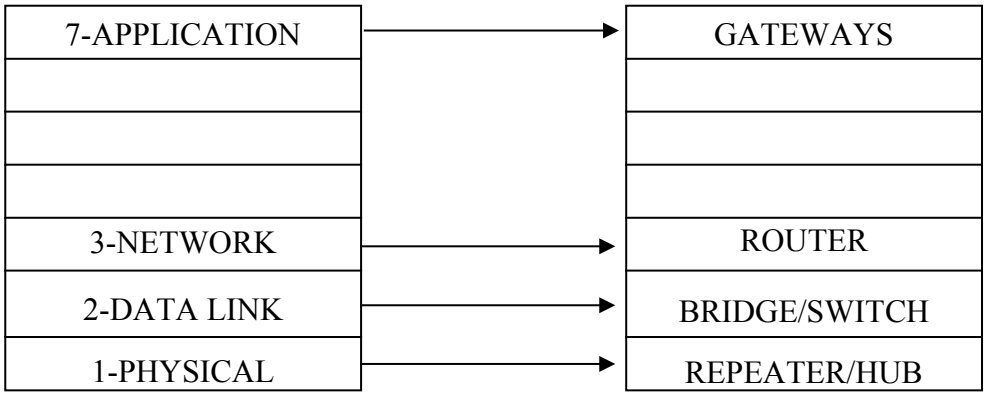


Fig. 1.1

Two physical LANs connected by a repeater become one physical LAN. Because of this, the proper use and placement of repeaters is specified as part of LAN architecture's cabling parameters.

5) HUB

As its name implies, a hub is a center of activity. In more specific network terms, a hub, or concentrator, is a common wiring point for networks that are based around a star topology. Arcnet, 10base-T, and 10base-F, as well as many other proprietary network topologies, all rely on the use of hubs to connect different cable runs and to distribute data across the various segments of a network. Hubs basically act as a signal splitter. They take all of the signals they receive in through one port and redistribute it out through all ports. Some hubs actually regenerate weak signals before re-transmitting them. Other hubs retime the signal to provide true synchronous data communication between all ports. Hubs with multiple 10base-F connectors actually use mirrors to split the beam of light among the various ports.

5.1)PASSIVE HUBS

Passive hubs, as the name suggests, are rather quiescent creatures. They do not do very much to enhance the performance of your LAN, nor do they do anything to assist you in troubleshooting faulty hardware or finding performance bottlenecks. They simply take all of the packets they receive on a single port and rebroadcast them across all ports--the simplest thing that a hub can do.

Passive hubs commonly have one 10base-2 port in addition to the RJ-45 connectors that connect each LAN device. 10base-5 is 10Mbps Ethernet that is run over thick-coax. This 10base-2 connector can be used as network backbone. Other, more advanced passive hubs have AUI ports that can be connected to the transceiver to form a backbone that may be more advantageous.

Most passive hubs are excellent entry-level devices that can be used as starting points in the world of star topology Ethernet. Most eight-port passive hubs are cheaper.

5.2) ACTIVE HUBS

Active hubs actually do something other than simply re-broadcasting data. Generally, they have all of the features of passive hubs, with the added bonus of actually watching the data being sent out. Active hubs take a larger role in Ethernet communications by implementing a technology called store & forward where the hubs actually look at the data they are transmitting before sending it. This is not to say that the hub prioritizes certain packets of data; it does, however, repair certain "damaged" packets and will retime the distribution of other packets.

If a signal received by an active hub is weak but still readable, the active hub restores the signal to a stronger state before re-broadcasting it. This feature allows certain devices that are not operating within optimal parameters to still be used on your network. If a device is not broadcasting a signal strong enough to be seen by other devices on a network that uses passive hubs, the signal amplification provided by an active hub may allow that device to continue to function on your LAN. Additionally, some active hubs will report devices on your network that are not fully functional. In this way, active hubs also provide certain diagnostic capabilities for your network.

Active hubs will also retime and resynchronize certain packets when they are being transmitted. Certain cable runs may experience electromagnetic (EM) disturbances that prevent packets from reaching the hub or the device at the end of the cable run in timely fashion. In other situations, the packets may not reach the destination at all. Active hubs can compensate for packet loss by re-transmitting packets on individual ports as they are called for and re-timing packet delivery for slower, more error-prone connections. Of course, re-timing packet delivery slows down overall network performance for all devices connected to that particular hub, but sometimes that is preferable to data loss--especially since the re-timing can actually lower the number of collisions seen on LAN. If data does not have to be broadcast over and over again, the LAN is available for use for new requests more frequently. Again, it is important to point out that active hubs can help you diagnose bad cable runs by showing which port on your hub warrants the retransmission or re-timing.

5.3) INTELLIGENT HUBS

Intelligent hubs offer many advantages over passive and active hubs. Organizations looking to expand their networking capabilities so users can share resources more efficiently and function more quickly can benefit greatly from intelligent hubs. The technology behind intelligent hubs has only become available in recent years and many organizations may not have had the chance to benefit from them; nevertheless intelligent hubs are a proven technology that can deliver unparalleled performance for LAN.

In addition to all of the features found in active hubs, incorporating intelligent hubs into your network infrastructure gives you the ability to manage your network from one central location. If a problem develops with any device on a network connected to an intelligent hub, it can easily identify, diagnose, and remedy the problem using the management information provided by each intelligent hub. This is a significant improvement over standard active hubs. Troubleshooting a large

enterprise-scale network without a centralized management tool that can help you visualize your network infrastructure usually leaves you running from wiring closet to wiring closet trying to find poorly functioning devices.

6) BRIDGES

Bridges connect LANs together at the Data Link layer of the OSI model. Specifically bridges connect at the Media Access Control (MAC) sub-layer of the Data Link layer, and are often referred to as MAC-layer bridges. In the past, Novel incorrectly referred to Net Ware routers as bridges.

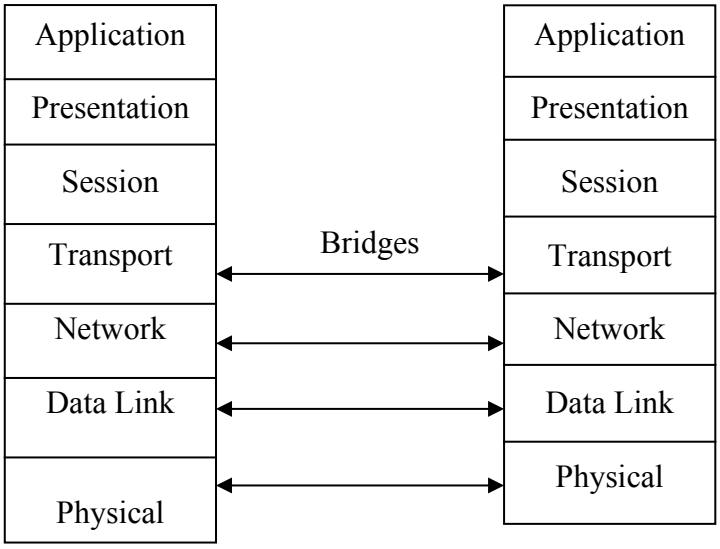


Fig 1.2

This diagram shows a typical multi-protocol remote bridge application.

Bridges connect similar or identical LANs. Bridges can be used to connect Ethernet/ 802.3 to Ethernet/ 802.3, 10-Mbps Ethernet/802.3 to 1-Mbps Star LAN, 4-Mbps Token Ring to 4-Mbps Token Ring, or 4-Mbps Token Ring to 16-Mbps Token Ring. Like repeaters, bridges can be used to connect LANs using different media (10BASE-T to 10BASE5, for example).

Bridges are transparent to the network-layer protocols (such as IPX and IP) being used on the network. Two networks connected via a bridge are physically separate network, but logically a single network. This means that a network's cabling rules apply to each individual network, not both collectively, but Network-layer protocols will address the bridged network as if they were one.

Bridges segment traffic by only forwarding traffic that is addressed to stations on the opposite side of the bridge. This means that bridges do not forward local traffic. This can considerably reduce overall traffic in a multi-LAN inter-network.

6.1) TRANSPARENT BRIDGES

The type of bridges used for Ethernet/802.3 LANs is called a transparent bridge. This is because the existence of the bridge is transparent to workstations, file

servers and other network devices. The bridge performs all the functions necessary to route traffic between bridged networks.

Transparent bridges keep routing tables of physical addresses of network devices and forward traffic based on the locations of the particular network device to which packets are being sent. Early bridges required the system administrator to manually build the routing tables. Current bridges automatically learn station addresses and build the routing tables and are sometimes referred to as learning bridges.

6.2) SPANNING TREE ALGORITHM.

Transparent bridges to not allow redundant paths. By using a scheme called the Spanning Tree Algorithm, however, alternate paths are allowed. In simplest terms, the Spanning Tree Algorithm ensures that only one bridge path between any two networks is active at a time. If a bridge path fails, another bridge path (if it exists) will automatically be activated. Not all bridges support the Spanning Tree Algorithm, and although Spanning Tree Algorithm is now part of the IEEE 802 specifications, not all bridges that support the Spanning Tree Algorithm conform with the IEEE specifications.

6.3) SOURCE ROUTING BRIDGES

Although transparent bridging can be used with Token Ring Networks, IBM has promoted another bridging method called source routing. With source routing, the bridge does not keep track of the route by which packets are sent. Each network node that initiates communication with another node across one or more bridges must keep track of the route used. Unlike transparent bridges, source routing bridges allow redundant paths.

To establish a route, the station initiating communication broadcasts a discovery packet, which makes its way through the Network's source routing bridges. The discovery packet keeps track of the bridges it crosses on the way to the destination. Depending on the configuration of the bridges and the method used to send the discovery packet (the description of which is beyond the scope of this book), the discovery packet will arrive at the destination via one or more routes, meaning one or more copies of the discovery packet will be received at the destination.

The destination returns its response(s) using reverse addressing, meaning it uses each discovery packet's list of crossed bridges, in reverse order, to return its response(s). If the initiating station receives responses via more than one route, the first response received establishes the route to be used.

7) ROUTERS

Routers connect LANs at the Network layer of the OSI model Routers connect LANs that use the same Network-layer protocol, such as IPX-to-IPX and IP-to-IP. Because routers operate at the Network layer, they can be used to link dissimilar LANs, such as ARCNET, Ethernet, and Token Ring.

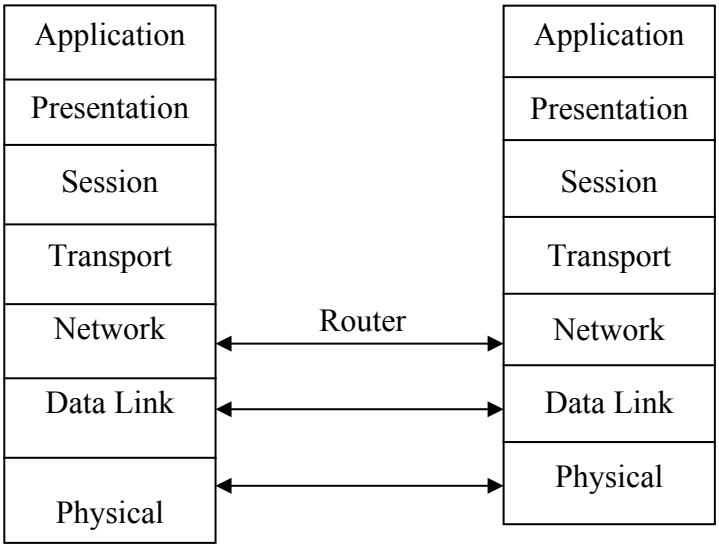
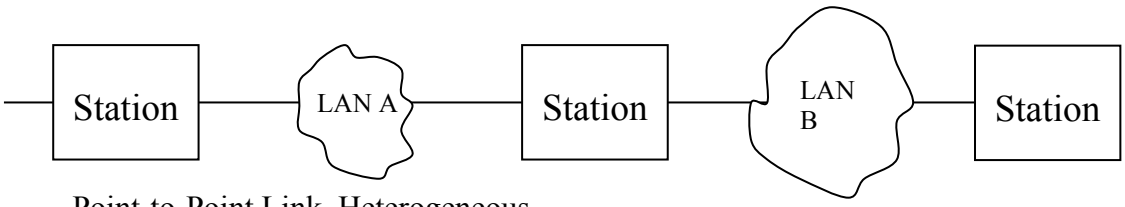


Fig. 1.3

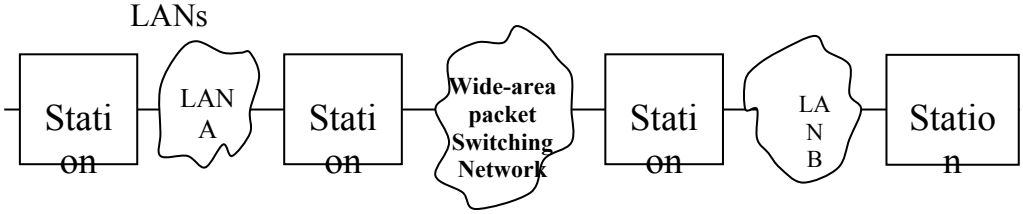
Two networks connected via a router are physically and logically separate networks. Network-layer protocols have their own addressing scheme separate from the addressing scheme of MAC-layer protocols. This addressing scheme may or may not include the MAC-layer addresses of the network cards. Each network attached to a router must be assigned a logical identifier, or network address, to designate it as unique from other physical networks.

For example, NetWare's IPX routers (NetWare file servers or external NetWare routers using ROUTER.EXE) use each LAN card's MAC-layer address and a logical address for each network assigned by the router installer.

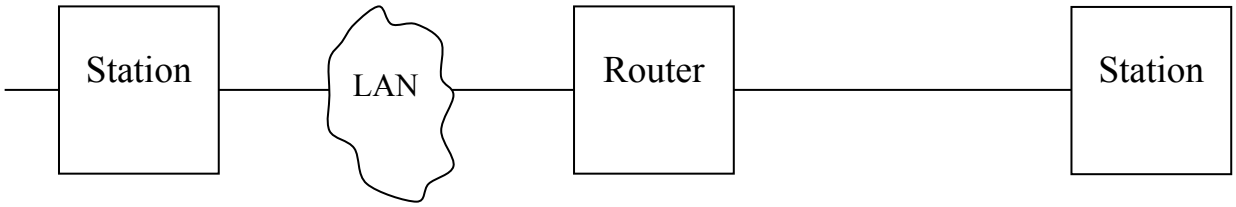
A router can support single or multiple Network-layer protocols. Net Ware 2.2 File servers and Net Ware external routers, for example, only support NetWare's IPX protocol. NetWare 3.11 file servers. Routers on the other hand, can route IPX, IP and Apple Talk, if the proper routing software is loaded into the file server. Dedicated routers from Proteon, Cisco, Welfleet, and others can route a number of different protocols.



Point-to-Point Link, Heterogeneous LANs



Wide-Area Network Link, Heterogeneous LANs



LAN to Host Link

Fig. 1.4

Like bridges, routers only forward traffic addressed to the other side. This means that local traffic on one LAN will not affect performance on another. Again, like bridges, routers can be proprietary devices, or can be software and hardware residing in a general purpose computer, such as a PC.

Like transparent bridges, routers maintain routing tables. A router's routing table, however, keeps track of network addresses and possible routes between networks, not individual node addresses. Using routers, redundant paths between networks can be established, and traffic will be routed between networks based on some algorithm to determine the best path. The simplest routers usually select the path with the fewest number of router hops as the best path. More intelligent routers consider other factors, such as the relative response times of various possible routes, when selecting the best path.

Because routers operate at the network layer, they can connect dissimilar types of LANs, such as ARCNET and Ethernet. LAN cards using different frame types, such as 802.3 and Ethernet II, can co-exist on the same LAN cable, but are actually separate logical networks. A router can connect two or more such logical networks.

Routing is more complex than bridging, and, all other things being equal, routers are somewhat slower than bridges. Routers usually do not provide the extensive filtering capabilities that some bridges do. Another downside to routers is that there are few standards, so different vendor's products may not inter operate. Routers do provide better network segmentation than bridges, however, so that things like broadcast packet storms will not affect an entire inter-network.

8) GATEWAYS

A gateway is a fundamentally different type of device than a repeater, bridge, router, or switch and can be used in conjunction with them. A gateway makes it possible for an application program, running on a system, confirming to network architecture, to communicate with an application program running on a system confirming to some other network architecture.

A gateway performs its function in the Applicatio0n layer of the OSI model. The function of a gateway is to convert one set of communication protocols to some other set of communication protocols. Protocol conversion may include the following:

- Message Format Conversion- Different networks may employ different message format, maximum message size, or character codes. The gateway must be able to convert messages to appropriate format, size and coding.
- Address translation- Different networks may employ different addressing mechanism and network address structures. The gateway must be able to interpret network address in one network and convert them into network address in other network.
- Protocol conversion- When a message is prepared for transmission, each layer adds control information, unique to the protocol used in that layer. The gateway must be able to convert control information used by each layer so that the receiving system receives the control information in the format it expects. Services affected may include message segmentation and reassembly, data flow control, and error detection and recovery.