UNIT 2 UNDERLYING LAN CONCEPTS

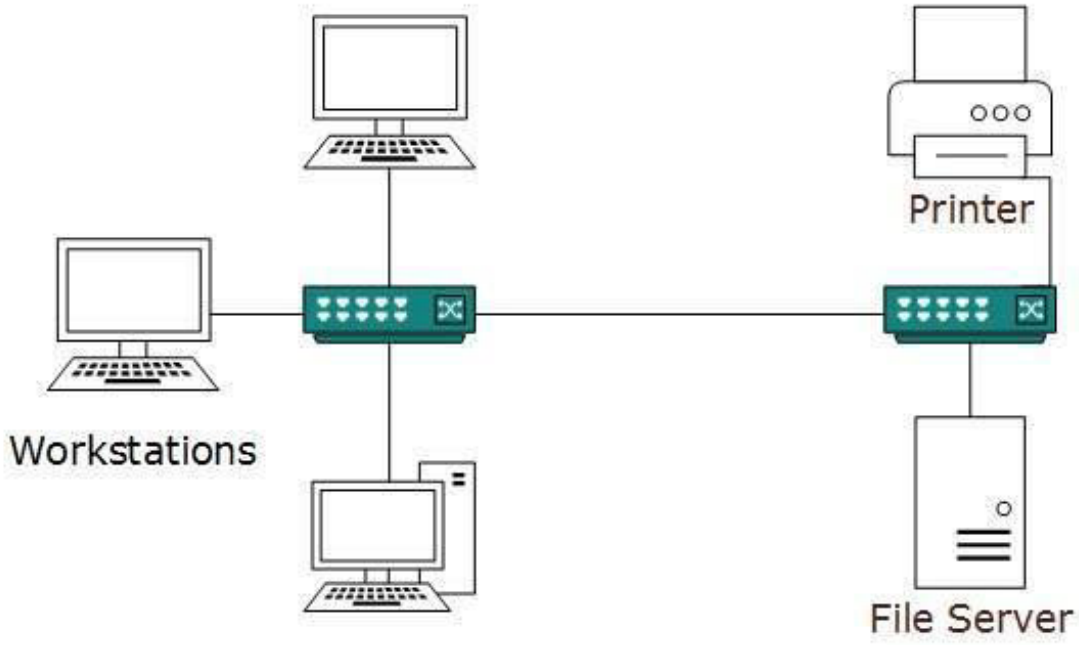
LAN connectivity for small businesses – Integration – Token-Ring – Ethernet – ATM LAN emulation – InterLAN Switching – LAN to Mainframe – Building network

LOCAL AREA NETWORKS (LANS)

A Local Area Network (LAN) is a private network that connects computers and devices within a limited area like a residence, an office, a building or a campus. On a small scale, LANs are used to connect personal computers to printers. However, LANs can also extend to a few kilometers when used by companies, where a large number of computers share a variety of resources like hardware (e.g. printers, scanners, audiovisual devices etc), software (e.g. application programs) and data.

The distinguishing features of LAN are

- Network size is limited to a small geographical area, presently to a few kilometers.
- Data transfer rate is generally high. They range from 100 Mbps to 1000 Mbps.
- In general, a LAN uses only one type of transmission medium, commonly category 5 coaxial cables.
- A LAN is distinguished from other networks by their topologies. The common topologies are bus, ring, mesh, and star.
- The number of computers connected to a LAN is usually restricted. In other words, LANs are limitedly scalable.
- IEEE 802.3 or Ethernet is the most common LAN. They use a wired medium in conjuncture with a switch or a hub. Originally, coaxial cables were used for communications. But now twisted pair cables and fiber optic cables are also used. Ethernet’s speed has increased from 2.9 Mbps to 400 Gbps.



LAN Connectivity Options for the Small Business:

SMALL BUSINESSES OF 2 TO 100 USERS are part of the fastest-growing segments of the networking market.

The most popular network topology among small businesses is Ethernet because it is relatively inexpensive, easy to set up and use, and very fast. There are currently three categories of Ethernet. Standard Ethernet operates at 10M bps, which is quick enough for most networking tasks. Fast Ethernet moves data 10 times faster at 100M bps, making it ideal for desktop video, multimedia, and other bandwidth-hungry applications. The latest category of Ethernet is Gigabit Ethernet, which moves data 100 times faster than standard Ethernet, making it suited for uplinks among high capacity hubs or switches as well as links among high-capacity servers. Although there are other types of LANs available, (e.g., token ring, fiber distributed data interface, and asynchronous transfer mode

As in any type of network, several elements merit consideration when building an Ethernet network, including cabling, media converters, network adapters, hubs, network operating systems, and routers for LAN-to-LAN communication over the wide area network (WAN).

Cable

Cable is the medium through which information usually moves from one network device to another. There are several types of cable which are commonly used with LANs. In some cases, a network will utilize only one type of cable, other networks will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol, and size.

Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network.

The following sections discuss the types of cables used in networks and other related topics.

- Unshielded Twisted Pair (UTP) Cable
- Shielded Twisted Pair (STP) Cable
- Coaxial Cable
- Fiber Optic Cable
- Cable Installation Guides
- Wireless LANs
- Unshielded Twisted Pair (UTP) Cable

Twisted pair cabling comes in two varieties: shielded and unshielded. Unshielded twisted pair (UTP) is the most popular and is generally the best option for school networks (See fig. 1).

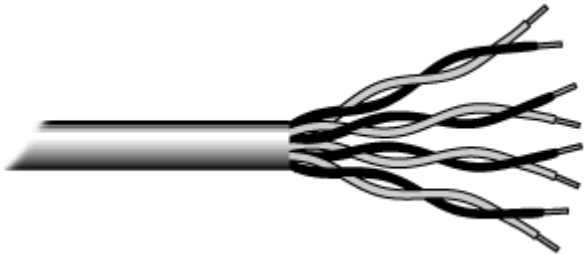


Fig.1. Unshielded twisted pair

The quality of UTP may vary from telephone-grade wire to extremely high-speed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot. The EIA/TIA (Electronic Industry Association/Telecommunication Industry Association) has established standards of UTP and rated six categories of wire (additional categories are emerging).

MEDIA CONVERTERS

All three types of media — twisted pair, thin coax, and optical fiber — can be used exclusively or together, depending on the type of network. There are even media converters available that allow segments using different media to be linked together. For example, some media converters link 10Base-T to 10Base-

2 and 10Base-T to 10Base-FL (single or multimode). There are also media converters that link 100Base-T to 100Base-FX (single or multimode). Because media conversion is a physical layer process, it does not introduce significant delays on the network.

Network Adapter

Network adapters are one of the many pieces that connect us to the internet. They're usually an antenna or card built into your device, but can also be plug-in USB dongles or antennae that allow purely wired devices to receive data wirelessly.

Network adapters allow computers and other devices to interface with a local area network (LAN) or another type of network in order to access the internet. They can work with wireless connections like Wi-Fi or wired ones like Ethernet.

Network Interface Card (NIC)

One of the most common network adapters available today is the Network Interface Card (NIC), also called the network interface controller. They're usually built into the motherboards of today's internet-capable devices and allow both wired and wireless connection to the internet.

NICs all usually use the 802.11 standard for Wi-Fi connectivity, so the one that comes with your laptop can work with any router using that standard to get online. Since it's the standard for most wireless internet connections, it's pretty easy for most devices to interface with.

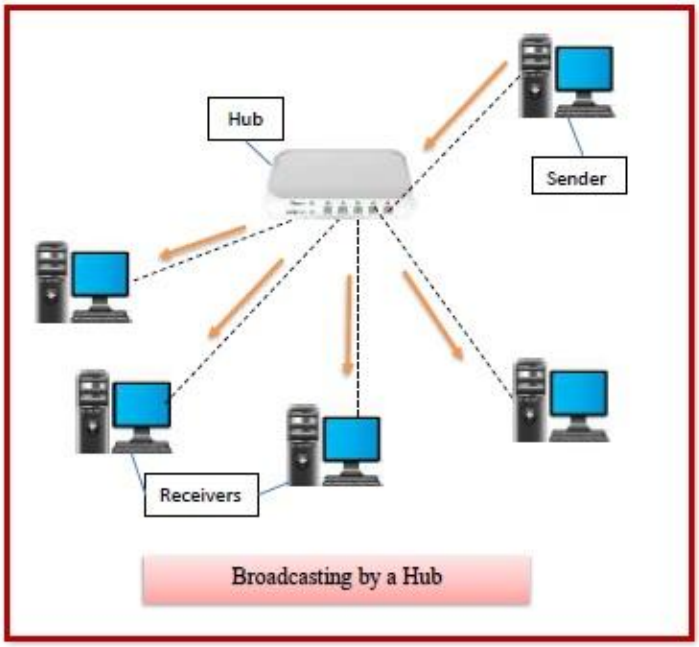
USB Adapters

This type of adapter is typically a USB dongle that plugs into a wired computer. It will have an antenna attached to receive the signal from a wireless network, and transmit the data it receives through the USB connection to the computer.

These adapters are a good option for enabling older computers with a wireless connection because they don't require physically opening the computer's case to install an internal network adapter. A popular choice is the TP-Link N150.

Hubs are networking devices operating at a physical layer of the OSI model that are used to connect multiple devices in a network. They are generally used to connect computers in a LAN.

A hub has many ports in it. A computer which intends to be connected to the network is plugged in to one of these ports. When a data frame arrives at a port, it is broadcast to every other port, without considering whether it is destined for a particular destination device or not.



Features of Hubs

- A hub operates in the physical layer of the OSI model.
- A hub cannot filter data. It is a non-intelligent network device that sends message to all ports.
- It primarily broadcasts messages. So, the collision domain of all nodes connected through the hub stays one.
- Transmission mode is half duplex.
- Collisions may occurs during setup of transmission when more than one computers place data simultaneously in the corresponding ports.
- Since they lack intelligence to compute best path for transmission of data packets, inefficiencies and wastage occur.
- They are passive devices, they don’t have any software associated with it.
- They generally have fewer ports of 4/12.

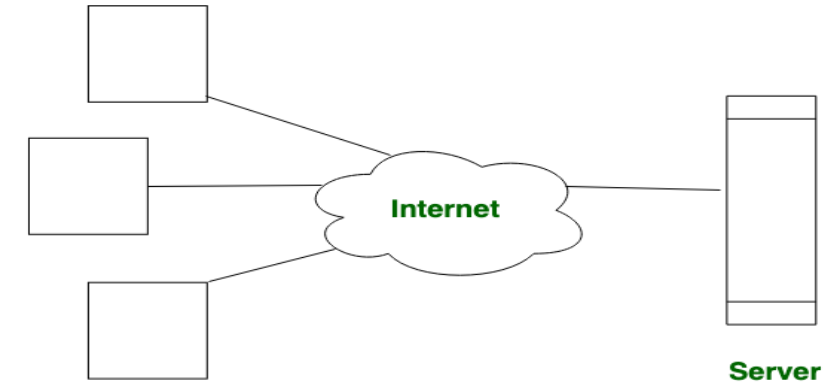
NETWORK OPERATING SYSTEM

Every computer that is attached to a network must be equipped with a network operating system (NOS) to monitor and control the flow of information between users. NOSs are of two types: peer-to-peer or client/server. Examples

of peer-to-peer NOSs that are commonly used by small businesses are Windows 95, Artisoft LANtastic, and Novell Inc.'s

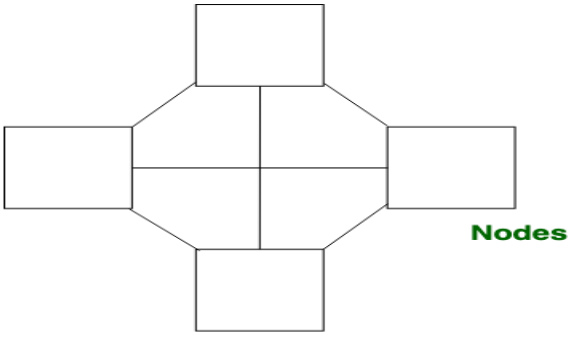
NetWare Lite. These NOSs are useful for sharing applications, data, printers, and other resources across PCs that are interconnected by a hub. Examples of client server NOSs are Windows NT and NetWare, which are used by large organizations whose users require fast network access to a variety of business applications.

Client-Server Network:
This model are broadly used network model. In Client-Server Network, Clients and server are differentiated, Specific server and clients are present. In Client-Server Network, Centralized server is used to store the data because its management is centralized.In Client-Server Network, Server respond the services which is request by Client.



Client-Server Network Model

Peer-to-Peer Network:
This model does not differentiate the clients and the servers, In this each and every node is itself client and server. In Peer-to-Peer Network, Each and every node can do both request and respond for the services.

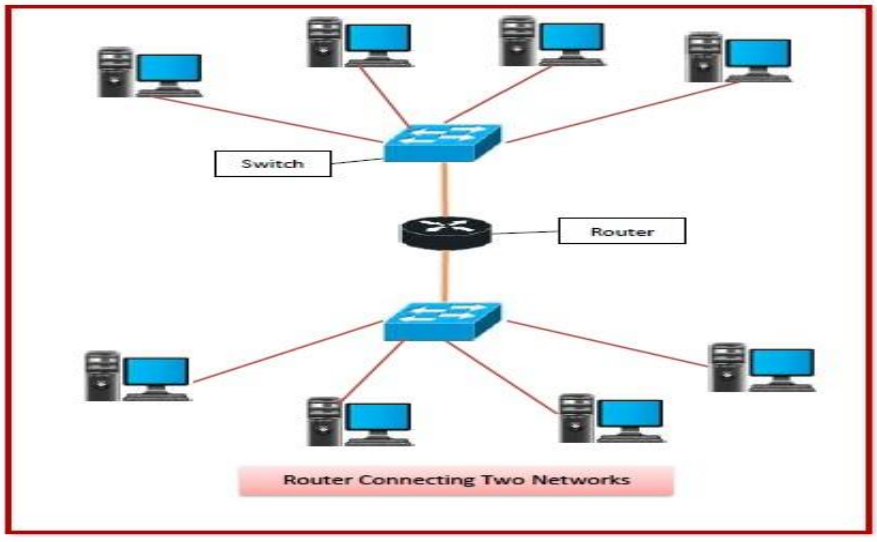


Peer-to-Peer Network Model

Peer-to-peer networks have several advantages over client/server. They are easy and inexpensive to set up and maintain, and there is no requirement for a dedicated network administrator. Many vendors offer documentation that is geared for the novice, and they offer telephone support when the occasional problem is encountered.

ROUTERS

For LAN-to-LAN communication between remote sites, a router is needed. A router can be a stand-alone device or it can come in the form of a module that plugs in to a managed hub. Routers operate at layer 3 of the OSI reference model (the network layer). Basically, they convert LAN protocols into wide-area packet network protocols such as Transmission Control Protocol/Internet Protocol (TCP/IP), and perform the process in reverse at the remote location



Features of Routers

- A router is a layer 3 or network layer device.
- It connects different networks together and sends data packets from one network to another.

- A router can be used both in LANs (Local Area Networks) and WANs (Wide Area Networks).
- It transfers data in the form of IP packets. In order to transmit data, it uses IP address mentioned in the destination field of the IP packet.
- Routers have a routing table in it that is refreshed periodically according to the changes in the network. In order to transmit data packets, it consults the table and uses a routing protocol.
- In order to prepare or refresh the routing table, routers share information among each other.
- Routers provide protection against broadcast storms.
- Routers are more expensive than other networking devices like hubs,bridges and switches.
- Routers are manufactured by some popular companies like −
    - Cisco
    - D-Link
    - HP
    - 3Com
    - Juniper
    - Nortel

ypes of Routers

A variety of routers are available depending upon their usages. The main types of routers are −

- **Wireless Router** − They provide WiFi connection WiFi devices like laptops, smartphones etc. They can also provide standard Ethernet routing. For indoor connections, the range is 150 feet while its 300 feet for outdoor connections.
- **Broadband Routers** − They are used to connect to the Internet through telephone and to use voice over Internet Protocol (VoIP) technology for providing high-speed Internet access. They are configured and provided by the Internet Service Provider (ISP).
- **Core Routers** − They can route data packets within a given network, but cannot route the packets between the networks. They helps to link all devices within a network thus forming the backbone of network. It is used by ISP and communication interfaces.
- **Edge Routers** − They are low-capacity routers placed at the periphery of the networks. They connect the internal network to the external networks, and are suitable for transferring data packets across networks. They use Border Gateway Protocol (BGP) for

connectivity. There are two types of edge routers, subscriber edge routers and label edge routers.

- **Brouters** − Brouters are specialised routers that can provide the functionalities of bridges as well. Like a bridge, brouters help to transfer data between networks. And like a router, they route the data within the devices of a network.

Integration

Organizations should consider running their voice traffic over the LAN infrastructure for several reasons:

• Single infrastructure. VoiceLAN eliminates the need for a cabling plant dedicated to voice only. Converged voice/data traffic running over a single wire reduces the upfront cost of equipment procurement (e.g., cable, patch panels, racks, installation), cable plant management (i.e., dealing with moves, adds, and changes), and maintenance. 0-8493-0859-3/00/$0.00+$.50 © 2000 by CRC Press LLC 14 UNDERSTANDING LANs

• Single organization. VoiceLAN allows enterprises to consolidate and streamline separate support organizations for data and voice networks. This convergence produces a more efficient, less costly management structure that spends less time “coordinating” and more time delivering network services and applications to users.

• Breaking PBX lock-in. For the most part, PBXs are proprietary, singlevendor systems, which usually means they are inflexible and expensive to maintain. VoiceLAN deployment paves the way for an open client/server model to be applied to telephony, creating a less rigid vendor-client relationship.

• New level of CTI. Current CTI systems allow data and voice application environments to “talk” to each other by means of computer-toPBX links. CTI is included implicitly in the voiceLAN model. VoiceLAN also distinguishes itself from CTI because data and voice applications actually share the same set of standards and software interfaces. ThusvoiceLAN leverages both media far beyond what is possible under present CTI systems, and has the potential to give organizations a distinct competitive advantage in the marketplace.

MIGRATING THE LAN INFRASTRUCTURE

Migration to voiceLAN is likely to encompass a number of smaller elements or activities. Migration cannot happen overnight, but is an evolutionary process that includes beneficial steps along the way. Over time, organizations can focus on improving elements of their network infrastructure, their desktop workstations, and their organizations in addition to their telephone systems. A first step in deploying voiceLAN is to upgrade the present LAN infrastructure to support the demands of voice traffic without affecting the flow of existing data traffic. Infrastructure refers to the cabling plant and the local networking equipment used to carry traffic from end station to end station (i.e., hub, bridge, router, switches, and network adapters). The PBX is not considered part of the infrastructure in a voiceLAN environment; rather, the PBX will evolve into a call server that can be considered another type of end station on the LAN. Solutions for Delay-Sensitive Applications Voice bandwidth is not usually of much concern when using LANs for transmission. An uncompressed high-quality voice conversation needs only 64 Kbps, and compression or packetization reduces bandwidth requirements further. This represents only a small fraction of a dedicated 10 Mbps Ethernet LAN segment. More important, voice is a delay-sensitive application that demands minimal latency (or minimal variations in latency, otherwise known as “jitter”) in 15 Integrating Voice and LAN Infrastructures and Applications communications. The vast majority of LANs today are based on shared-bandwidth media. With Ethernet LANs, all users contend for bandwidth on a first-come, first-served basis. Token ring LANs are somewhat more deterministic since each end station transmits only when that end station holds the token, which passes from end station to end station at more or less regular time intervals

Desktop Switching

It is Part of the solution to this problem is to provide dedicated bandwidth to each user end station through desktop LAN switching. In a fully switched network, end stations do not contend (as in Ethernet) or wait (as in token ring) for bandwidth with other users; instead, each user workstation gets its own dedicated LAN segment for connectivity into the network. Migrating to a fully switched network (i.e., a single workstation or server per dedicated switch port) entails replacing existing shared-media LAN hubs with LAN switches.

Minimize Routing

LAN switching only addresses bandwidth contention to the desktop. Links between desktop switches, or from desktop switches to building/campus switches, must also provide predictable, minimal delays for voice communications. In most enterprise networks, routers are used to calculate

paths and forward packets between LAN segments at Layer 3 of the OSI model. These routing algorithms introduce significant delay and usually add noticeable latency to voice communications. By contrast, switching involves a much simpler and faster process. Segmenting the network at OSI Layer 2 through switching, rather than at Layer 3 through routing, increases the capacity of the network to support delay-sensitive applications such as voice

Controlling LAN Backbone Traffic

Migrating the network from shared-access LANs and routing to switching is a prerequisite to voiceLAN implementation. However, a major challenge remains in ensuring that voice can be properly supported on the backbone links (e.g., trunk) between LAN switches. Supporting both data and voice over a common backbone LAN infrastructure is essentially a bandwidth-contention issue — determining how to make sure that delay-sensitive voice traffic is not preempted by other data traffic traversing the same links.

RSVP

Among the most promising solutions to Ethernet's lack of prioritization or guaranteed latency is to handle the problem at Layer 3 via the RSVP. RSVP, which was developed by the IETF and leading network product vendors, operates by reserving bandwidth and router/switch buffer space for certain high-priority IP packets such as those carrying voice traffic.

ATM-Based Backbone Solutions. An alternative solution for delivering voiceLAN over a common data infrastructure is ATM. ATM was designed specifically to support both voice and data traffic over a common infrastructure and provides multiple QoS levels.

ATM to the desktop is more problematic, however. The most common standard for ATM LANs operates at 155 Mbps over Category 5 UTC cable or optical fiber

An organization can choose from among several potential access solutions, including ATM25, Ethernet using IP/RSVP, or Ethernet/CIF. ATM25 Access. ATM25, as its name implies, is a 25 Mbps version of ATM designed specifically for desktop connectivity to a 155 Mbps ATM backbone. ATM25 provides all of the QoS benefits of higher-speed ATM and can be used to build end-to-end ATM networks. ATM25 can also operate over Category 3 UTC cable, whereas 155 Mbps ATM and Fast Ethernet require organizations to upgrade their UTP cabling to Category 5 UTP cable.

Ethernet RSVP/IP Access. The most popular desktop connectivity option for data networking continues to be Ethernet, and the addition of desktop switching and Fast Ethernet technology only continues this trend. The challenge is combining IP over Ethernet network access links with ATM in the backbone in such a way that voiceLAN performance requirements can be satisfied.

One solution requires Ethernet-to-ATM desktop switches to include routing and RSVP support. The desktop end station sends voice in IP packets (further encapsulated inside Ethernet frames) to the switch, using RSVP to request bandwidth to be reserved for the voice conversation. The desktop switch then terminates the IP connection and converts the voice payload to ATM cells for transmission across the backbone (or the desktop switch may forward these IP datagrams across the ATM backbone without terminating the IP connection).

Ethernet CIF Access.

CIF allows a desktop application to place voice traffic in ATM cells that are subsequently inserted into Ethernet frames by the network adapter driver for transport over the link from the adapter to switch. At the Ethernet switch, cells are extracted from the frames and sent across the ATM backbone. CIF's primary advantage is that high-priority traffic, such as voice, can be given the necessary QoS from the desktop across the ATM network without having to actually install ATM end-to-end in the network

MIGRATING THE DESKTOP

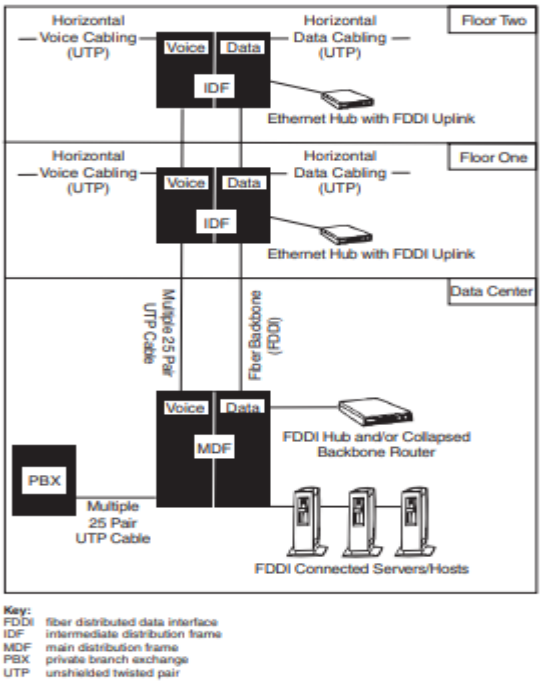
The deployment of voiceLAN also entails a migration of the desktop PC to become telephony-enabled. Exhibit 2-3 illustrates the voiceLAN-enabled desktop environment. This migration has two components: hardware and software.

Hardware Upgrades

In a pure voiceLAN architecture, all voice calls are received via a PC and its LAN adapter card rather than via a desktop telephone wired to a PBX or voice switch. There are two alternative human interfaces for people to interact with the PC to receive voice communications: the PC itself and the traditional desktop telephone

By using the PC as the interface, voice traffic is processed by a PC sound card and the user employs a PC-attached microphone and headset. This solution is appropriate for users who are already using a microphone and headset to keep their hands free for typing (e.g., telemarketers, travel agents, help desk operators).

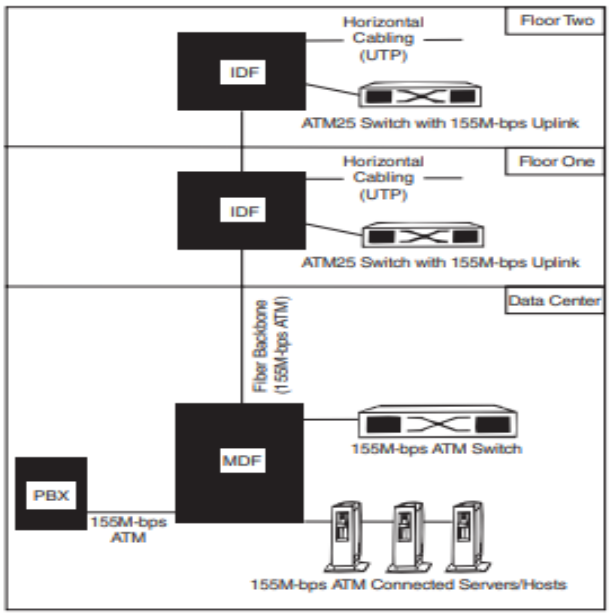
For most users the desktop telephone is still appropriate as their voice communications interface. However, in a voiceLAN solution, this phone set must be able to connect directly to the PC so that voice traffic can be received directly from the network adapter card without having to passthrough the CPU. Today this can be accomplished through a third-party plug-in card.



Key:
FDDI fiber distributed data interface
IDF intermediate distribution frame
MDF main distribution frame
PBX private branch exchange
UTP unshielded twisted pair

Exhibit 2-1. Legacy voice and data cabling infrastructures.

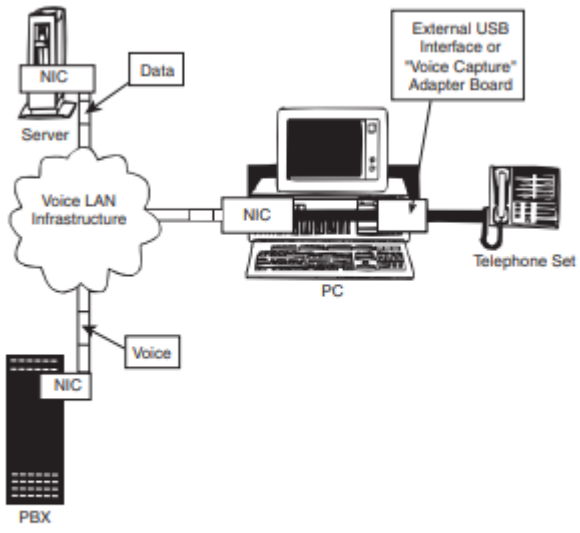
Universal Serial Bus. A more elegant solution for accomplishing a direct connection is the USB interface, originally developed by Intel. The motherboards of most new PCs included USB interfaces as standard features.The USB supports 12 Mbps of throughput and allows USB-compatible telephone sets to connect directly to the PC without the need for an additional plug-in card. This alternative greatly reduces the cost of deploying voiceLAN. Several vendors have released or will soon release telephones conforming to the USB standard.



Key:
FDDI fiber distributed data interface
IDF intermediate distribution frame
MDF main distribution frame
PBX private branch exchange
UTP unshielded twisted pair

Exhibit 2-2. Consolidated cabling infrastructure.

Firewire Bus. An alternative standard called Firewire — originally developed by Apple Corp., but currently being promoted by Sony and other consumer electronics companies — is also being introduced in new products.



Key:
NIC network interface card
PBX private branch exchange
USB universal serial bus

Exhibit 2-3. The VoiceLAN-enabled desktop.

Software Upgrades

To take maximum advantage of voiceLAN technology, PC-resident applications need to communicate with the PBX and PC-attached desktop phone sets. For this, a standardized software interface is required. Most PBXs today

support several such software APIs, though many of these interfaces provide translation of commands between the PBX andmainframe hosts for use in CTI applications such as call center applications. For Windows applications, most PBXs support Microsoft's TAPI. TAPI is available for Windows 95

MIGRATING THE PBX

Legacy Telephony

PBX and telephony systems are analogous to the host and dumb terminal model of the mainframe era. PBXs are relatively inflexible, proprietary, and expensive to maintain and upgrade in the same way mainframes are. Phone sets are still the most ubiquitous desktop instrument for telephony communications, but the PC offers the most intuitive interface to advanced features. Moving from the traditional PBX model to a serverbased telephony model represents the final stage in the migration to a fully integrated voice and data network.

Linking Distributed PBX Components

For organizations with large campus environments, an intermediate step between the legacy PBX and server-based telephony may be an architecture featuring multiple PBX components distributed throughout the campus. This type of architecture has traditionally required a dedicated fiber backbone to connect multiple units. Under a voiceLAN solution, these units, outfitted with network adapter cards, can be connected over a LAN backbone infrastructure. This infrastructure is already in place in most larger campus network environments. In this case, the horizontal connection between the PBXs and the telephone sets at the desktop can continue to use the traditional voice network infrastructure.

There are two advantages to this architecture:

1. Distributed PBXs scale more cost-effectively than a single, large PBX.

2. The necessity for installing and maintaining dual backbones, one for voice and one for data, is eliminated.

Server-Based Telephony

A server-based telephony architecture allows for the traditional functions of the PBX to be broken down into its components and distributed on the voiceLAN network. The switching function of the PBX can be handled by the frame or cell switches of the data network, whereas the call control function can be moved to a server. Specific telephony applications can also be moved to

distributed application servers and integrated with other networked data applications.

Desktop Telephony Applications.

Following are some examples of desktop telephony applications that should be considered for implementation in this initial phase. In these examples, the applications are enhanced by voiceLAN in that they are melded with real-time voice communications:

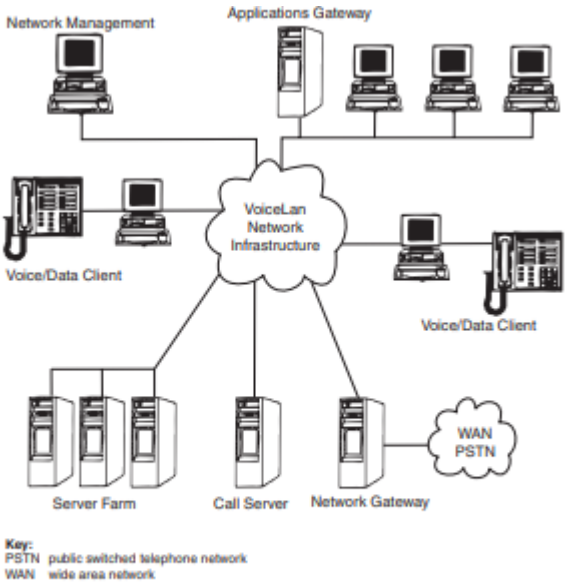


Exhibit 2-4. VoiceLAN architecture.

GUI phone. At its basic level, this application running on the desktop provides a phone handset interface on the PC. The GUI phone prompts users to take more advantage of advanced call features that they are reluctant to utilize today simply because of the nonintuitive interface of existing phone handsets.

• **Integration with PIM software.** Integrating the GUI phone with PIM software provides a seamless link between the user's PIM application (e.g., an advanced electronic Rolodex) and the user's actual communications interface (e.g., the GUI phone). This application offers functionality similar to call center applications to general users right at their desktops.

• **GUI voice mail.** Voice mail can easily benefit from a graphic representation. At the click of a mouse, users scroll through a list of voice mail messages — saving, deleting, or forwarding messages. With this type of application, voice messages are treated as objects that can be manipulated in the same way data files are. For users, this method is potentially far more user-friendly and time-efficient than using the keypad of a phone handset.

• **Integrated messaging**. When voice mail is decoupled from the PBX architecture, full integration with other types of messaging applications (i.e., e-mail) can more easily take place. VoiceLAN simplifies the process of combining message media and potentially reduces the cost of integrated messaging.

MIGRATING USERS

As the voiceLAN network is tested for its reliability as a dedicated voice network, the organization can begin to migrate the general population of users. Individual users or entire workgroups can be moved on a line-by-line basis by installing a USB PC and USB handset at the desktop, eventually eliminating the legacy phone set connected via the dedicated voice network. The order in which users/workgroups are moved depends on each user/workgroup's ability and willingness to take advantage of integrated voice/data applications.

While the general population of users is being migrated, the organization should also begin to deploy more advanced applications in the original testbed workgroups. These applications can be tightly integrated with networked data applications (as opposed to desktop applications). The client/server applications that can be deployed in this final stage include:

• Collaborative applications. A server-based telephony architecture facilitates the integration of voice communications to collaborative software that allows multiple people to work on the same document while communicating.

• Voice/database applications. At present, computer telephony integration permits a certain level of integration between PBXs and databases; however, deploying such applications is expensive and generally reserved for telemarketing or customer service applications. A server-based telephony architecture allows high-end CTI functionality to be deployed on a much wider scale and to be made accessible to the general user population.

Token-Ring

A token ring is a data link for a local area network (LAN) in which all devices are connected in a ring or star topology and pass one or more tokens from host to host. A token is a frame of data transmitted between network points. Only a host that holds a token can send data, and tokens are released

when receipt of the data is confirmed. IBM developed token ring technology in the 1980s as an alternative to Ethernet.

Also known as IEEE (Institute of Electrical and Electronics Engineers) 802.5, a token ring network connects all devices, including computers, in a circular or closed-loop manner. In this scenario, the word token describes a segment of data sent through the network.

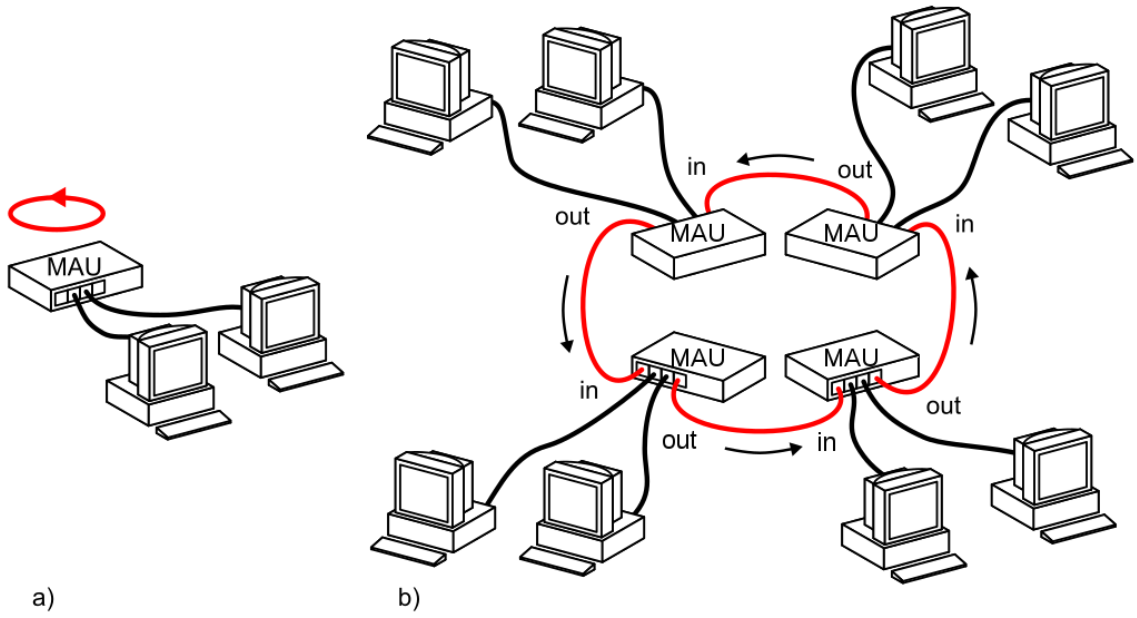
Token ring networks prevent data packets from colliding on a network segment because only a token holder can send data, and the number of tokens available is also controlled. When a device on the network successfully decodes that token, it receives the encoded data.

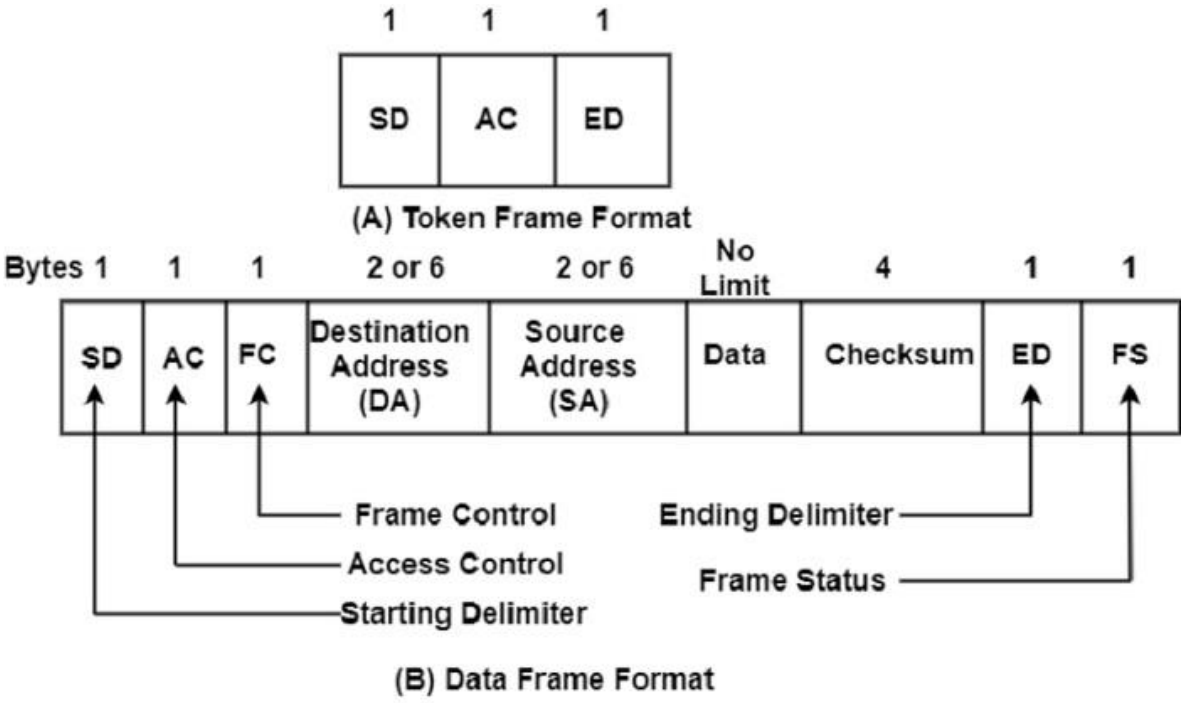
It uses a special three-byte frame called a *token* that is passed around a logical *ring* of workstations or servers. This token passing is a channel access method providing fair access for all stations, and eliminating the collisions of contention-based access methods.

A Token Ring network can be modeled as a polling system where a single server provides service to queues in a cyclic order

There are three types of frame formats that are supported on a Token Ring network such as token, abort, and frame. The token format is the mechanism by which access to the ring is passed from one computer attached to the network to another device connected to the network.

Three bits are used as a priority indicator, three bits are used as a reservation indicator, while one bit is used for the token bit, and another bit position functions as the monitor bit.





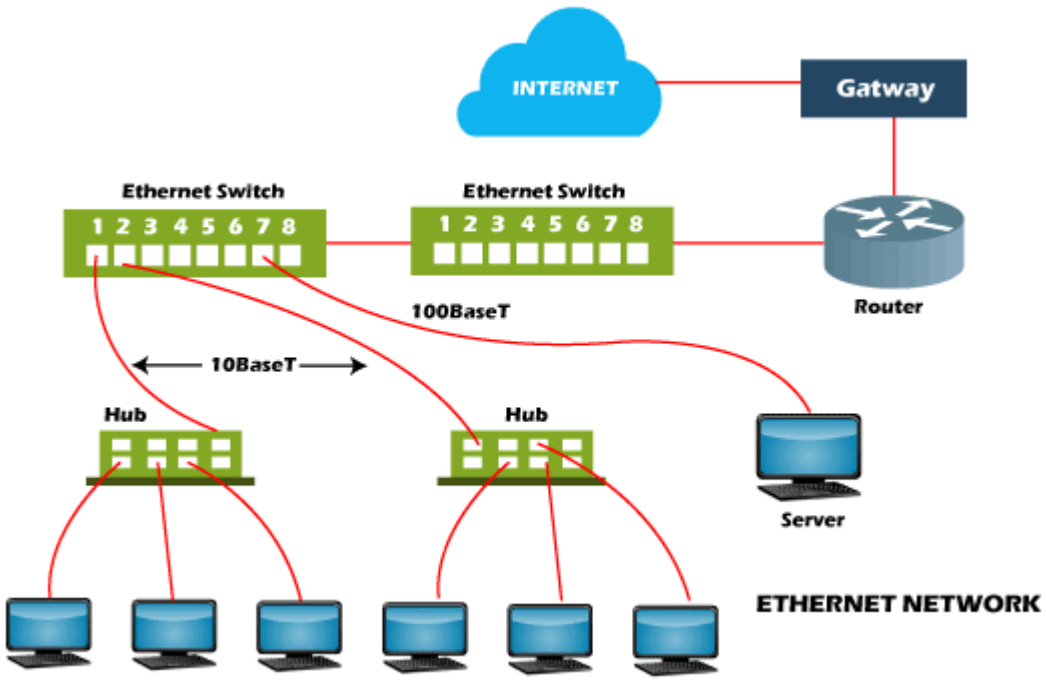
The components of the Token Ring Frame Format are as follows −

- **Start Delimiter (SD)** − The first field of the data/command frame, SD, is one byte long and is used to alert the receiving station to the arrival of a frame as well as to allow it to synchronize its retrieval timing.
- **Access Control (AC)** − The AC field is one byte long and includes four subfields. The first three bits are the priority field. The fourth bit is called the token bit.

- **Frame Control (FC)** −The FC field is one byte long and contains two fields. The first is a one-bit field used to indicate the type of information contained in the Protocol Data Unit (PDU).
- **Destination Address (DA)** −The two-to-six-byte DA field contains the physical address of the frame's next destination. If its ultimate destination is another network, the DA is the address of the router to the next LAN on its path.
- **Source Address (SA)** − The SA field is also two to six bytes long and contains the physical address of the sending station. If the ultimate destination of the packet is a station on the same network as the originating station, the SA is that of the originating station.
- **Data** −The sixth field, data, is allotted 4500 bytes and contains the PDU. A token ring frame does not include a PDU length or type field.
- **Checksum** −The checksum field is 4 bytes long. The checksum field is used to cross-check the data at the sending station. This field contains the total number of bytes in the frame. The number is checked at the receiver end after counting the bytes in the received frame.
- **End Delimiter (ED)** −The ED is a second flag field of one byte and indicates the end of the sender's data and control information.
- **Frame Status** −The last byte of the frame is the FS field. It can be set by the receiver to indicate that the frame has been read or by the monitor to indicate that the frame has already been around the ring.

Ethernet

Ethernet is a type of communication protocol that is created at Xerox PARC in 1973 by Robert Metcalfe and others, which connects computers on a network over a wired connection. It is a widely used LAN protocol, which is also known as Alto Aloha Network. It connects computers within the local area network and wide area network. Numerous devices like printers and laptops can be connected by LAN and WAN



The application layer is the topmost layer that makes capable of users to download and access data from a mail client or a web browser. Users enter their queries with the help of the application; then, it is sent to the next layer, where the request is known as a "packet." The information about the sender and the destination web address is contained by the packet. Until the packet is reached the bottom layer, called the Ethernet frame, the packet is transmitted from the application layer. The layer closest to your device is the first or bottom layer.

Types of Ethernet Networks

An Ethernet device with CAT5/CAT6 copper cables is connected to a fiber optic cable through fiber optic media converters. The distance covered by the network is significantly increased by this extension for fiber optic cable. There are some kinds of Ethernet networks, which are discussed below:

- Fast Ethernet: This type of Ethernet is usually supported by a twisted pair or CAT5 cable, which has the potential to transfer or receive data at around100 Mbps. They function at 100Base and 10/100Base Ethernet on the fiber side of the link if any device such as a camera, laptop, or other is connected to a network. The fiber optic cable and twisted pair cable are used by fast Ethernet to create communication. The 100BASE-TX,

100BASE-FX, and 100BASE-T4 are the three categories of Fast Ethernet.

- Gigabit Ethernet: This type of Ethernet network is an upgrade from Fast Ethernet, which uses fiber optic cable and twisted pair cable to create communication. It can transfer data at a rate of 1000 Mbps or 1Gbps. In modern times, gigabit Ethernet is more common. This network type also uses CAT5e or other advanced cables, which can transfer data at a rate of 10 Gbps.
- 10-Gigabit Ethernet: This type of network can transmit data at a rate of 10 Gigabit/second, considered a more advanced and high-speed network. It makes use of CAT6a or CAT7 twisted-pair cables and fiber optic cables as well. This network can be expended up to nearly 10,000 meters with the help of using a fiber optic cable.
- Switch Ethernet: This type of network involves adding switches or hubs, which helps to improve network throughput as each workstation in this network can have its own dedicated 10 Mbps connection instead of sharing the medium. Instead of using a crossover cable, a regular network cable is used when a switch is used in a network. For the latest Ethernet, it supports 1000Mbps to 10 Gbps and 10Mbps to 100Mbps for fast Ethernet.

Baseband uses digital signals, while broadband uses analog signals. Baseband is further divided into five standard names as follows −

- 10 Base 5
- 10 Base 2
- 10 Base T
- 1 Base 5
- 100 Base T

The first numbers used in all standards, i.e., 10, 1, 100, indicate the data rate in Mbps, while the last numbers 2, 5, and letter T indicate the maximum cable length or type of cable. Only one specification is defined for broadband, and that is 10 Broad 36. 10 Base 5 means a data rate of 10 Mbps and cable length restriction of 500 meters.

The network uses Carrier-sense multiple access with collision detection (CSMA/CD) technique. When multiple users access a single line, there is always a chance of overlapping and destroying data called collisions. Thus, if traffic increases on a single line, there are always chances of collision.

The carrier senses several access with collision Detection (ICMP/CD) is a technique that can help detect a collision, quits the current transmission and retransmission of data and takes place after waiting for some predetermined time to get the line cleared.

Electrical Signification for Ethernet

There are various electrical significations for Ethernet, which are as follows:

Signaling

Baseband system uses Manchester digital encoding while the broadband system uses differential PSK.

Data Rate

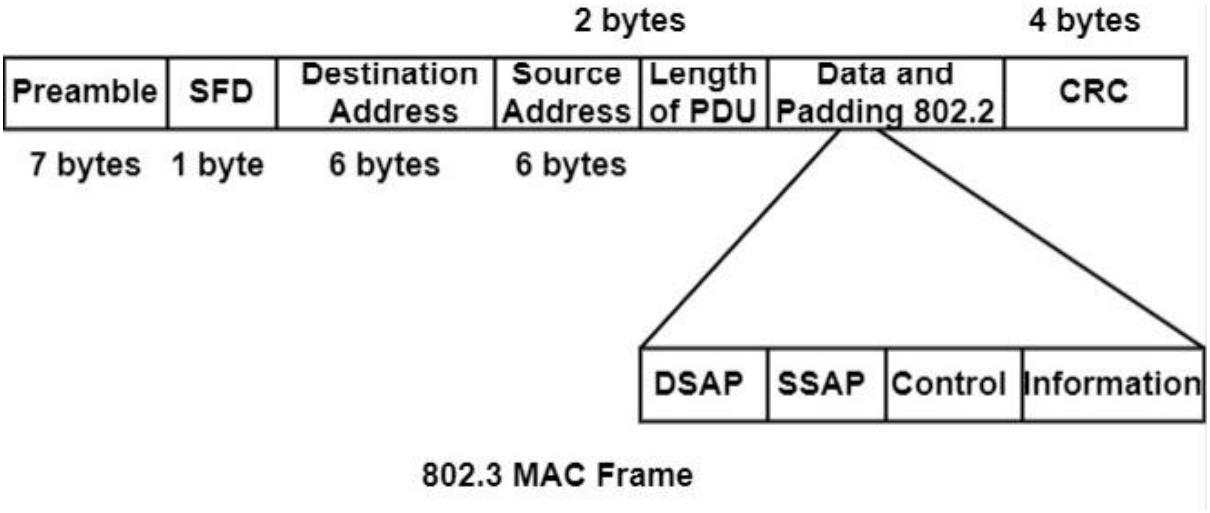
The Ethernet LANs supports a data rate between 1 Mbps to 100 Mbps. Baseband defines 1, 10, and 100 Mbps data rates, while broadband defines a data rate of 10 Mbps.

Frame Format

IEEE 802.3 specifies only one type of frame format that includes seven fields. These fields are as follows−

- **Preamble** − It contains seven bytes (56 bits) and is used for synchronization.
- **Start frame delimiter (SFD)** − It is a one-byte field and is used to signal the frame's beginning.
- Destination Address and Source Address fields are six bytes' fields containing sender and receiver address as declared by the Network Interface Card.
- The next field **length/type** is a two-byte field and indicates the number of PDU bits and its type. It provides a base for other protocols.
- The **PDU** or 802.2 frames contain the entire 802.2 frames as a modular removable unit. It can start from the 46th byte and can continue up to the 1500th byte. It is generated by the LLC sublayer depending on the size and type of the PDU, and then it is linked to an 802.3 frame.
- The last field is **CRC**, which contains error detection information.

The frame format is demonstrated in the figure



ATM

Asynchronous Transfer Mode (**ATM**) is a telecommunications standard defined by ANSI and ITU-T (formerly CCITT) for digital transmission of multiple types of traffic.

ATM is a form of data transmission that allows voice ,video and data to be sent along the same network in the form Time Division Multiplexing(TDM).ATM has its similarities with the frame relay,particularly in the term of data unit size ,frame replay used a variable length data unit called frame.ATM used fixed data unit named as "cell", we can say ATM as Cell-Relay in analog to frame relay.ATM is a high speed data communication technology which can run in any medium.

ATM Features:

- ATM provides functionality that uses features of circuit switching and packet switching networks by using asynchronous time-division multiplexing
- ATM is a packet network like X.25,frame relay.
- ATM integrates all different types of traffic into one network
- ATM supports multiplexing of multiple logical connections over single physical channel.
- ATM does not provide flow control and error control at data link layer.

- ATM can serve as a LAN or WAN backbone without requiring any network replacement.
- ATM can be used in existing physical channels and networks. It is also compatible with wireless and satellite communications.

ATM Cell:

In ATM these frames are of a fixed length (53 octets or bytes) and specifically called *cells*.

ATM transfers data in fixed-size units are known as cells. Each cell includes 53 octets or bytes, as shown in the figure. The first 5 bytes contain cell-header data, and the remaining 48 include the payload (user information).

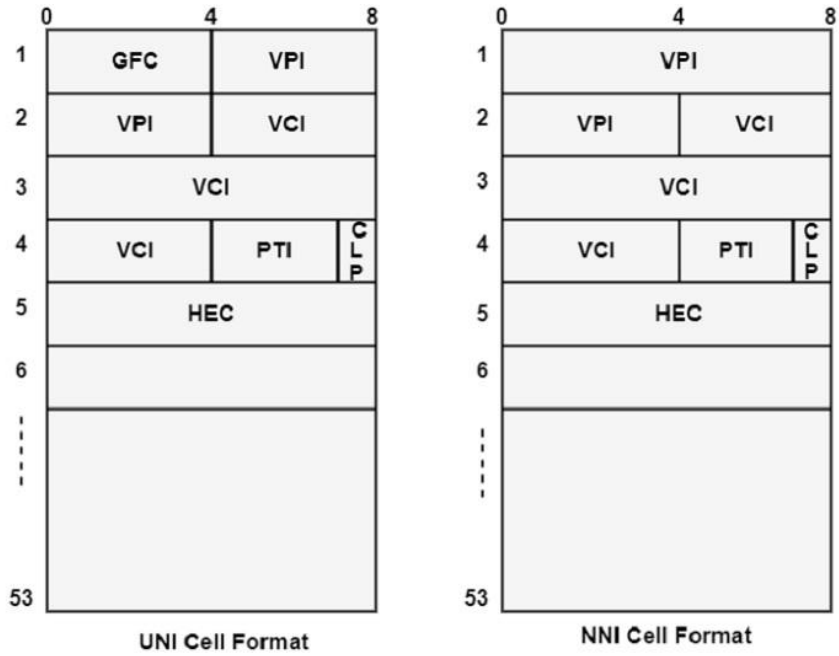
Small, fixed-length cells are well appropriated to transfer voice and video traffic due to such traffic is biased to delays that result from having to wait for a huge data packet to download, among other things.

Header	Payload
5 Bytes	48 Bytes

ATM Cell Format

An ATM cell header can be two formats, such as User Network Interface (UNI) or Network to Network Interface (NNI). The UNI header can be used for communication between ATM endpoints and ATM switches in private ATM networks. The NNI header can be used for communication between ATM switches.

The figure shows the ATM UNI cell header format and the ATM NNI cell header format. Unlike the UNI, the NNI header does not contain the Generic Flow Control (GFC) field. The NNI header has a Virtual Path Identifier (VPI) field that appears in the first 12 bits. It is allowing for high trunks between public ATM switches.



ATM Cell Formats

ATM Cell Header Fields

The following definitions summarise the ATM cell header fields as shown in the figure above −

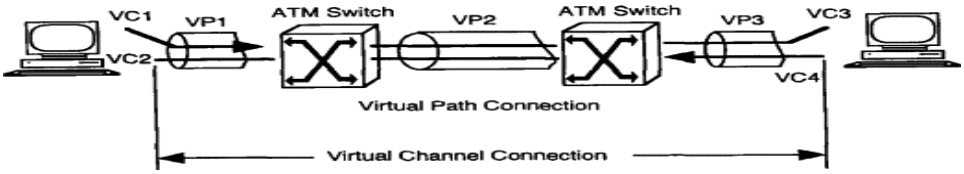
- **Generic Flow Control (GFC)** − It supports local functions, such as recognizing multiple stations that send a single ATM interface. This field is generally not used and is set to its default value of 0 (binary 0000).
- **Virtual Path Identifier (VPI)** − In conjunction with the Virtual Channel Identifier (VCI), it recognises the next destination of a cell as it transfers through a series of ATM switches on the way to its destination.
- **Virtual Channel Identifier (VCI)** − In conjunction with the VPI, it recognizes the next destination of a cell as it transfers through a series of ATM switches on the way to its destination.
- **Payload Type (PT)** − It denotes in the first bit whether the cell includes user data or control data. If the cell includes user data, the bit is set to 0. If it includes control data, it is set to 1. The second bit denotes congestion (0 = no congestion, 1 = congestion), and the third bit denotes whether the cell is the last in a sequence of cells that define a single AAL5 frame (1 = last cell for the frame).
- **Cell Loss Priority (CLP)** − It denotes whether the cell should be removed if it encounters extreme congestion as it transfers through the network. Suppose the CLP bit similar is to 1, and the cell should be discarded in preference to cells with the CLP bit equal to 0.

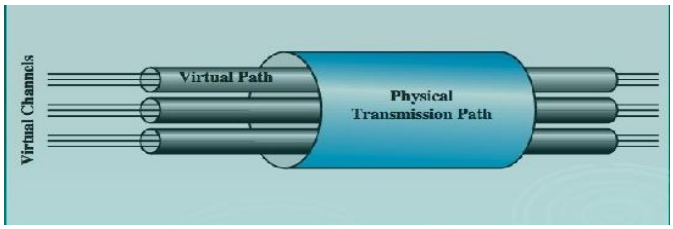
- **Header Error Control (HEC)** − It evaluates checksum only on the first 4 bytes of the header. It can be valid a single bit error in these bytes, thereby preserving the cell instead of discarding it.

Working of ATM:

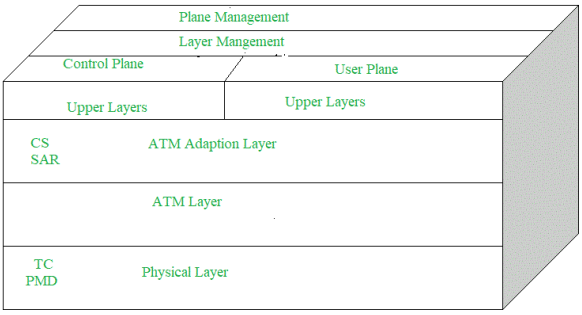
ATM standard uses two types of connections. i.e., Virtual path connections (VPCs) which consist of Virtual channel connections (VCCs) bundled together which is a basic unit carrying a single stream of cells from user to user. A virtual path can be created end-to-end across an ATM network, as it does not rout the cells to a particular virtual circuit. In case of major failure, all cells belonging to a particular virtual path are routed the same way through the ATM network, thus helping in faster recovery.

Switches connected to subscribers use both VPIs and VCIs to switch the cells which are Virtual Path and Virtual Connection switches that can have different virtual channel connections between them, serving the purpose of creating a *virtual trunk* between the switches which can be handled as a single entity. Its basic operation is straightforward by looking up the connection value in the local translation table determining the outgoing port of the connection and the new VPI/VCI value of connection on that link.





ATM Layers:



Physical Layer –
It manages the medium-dependent transmission and is divided into two parts physical medium-dependent sublayer and transmission convergence sublayer. The main functions are as follows:

- It converts cells into a bit stream.
- It controls the transmission and receipt of bits in the physical medium.
- It can track the ATM cell boundaries.
- Look for the packaging of cells into the appropriate type of frames.

ATM Layer –
It handles transmission, switching, congestion control, cell header processing, sequential delivery, etc., and is responsible for simultaneously sharing the virtual circuits over the physical link known as cell multiplexing and passing cells through an ATM network known as cell relay making use of the VPI and VCI information in the cell header.
It accepts the 48 byte segments from the upper layer, adds a 5 byte header to each segment and converts into 53 byte cells. This layer is responsible for routing of each cell, traffic management, multiplexing and switching.

ATM Adaption Layer (AAL) –
It is meant for isolating higher-layer protocols from details of ATM processes and prepares for conversion of user data into cells and segments it into 48-byte cell payloads. AAL protocol excepts transmission from upper-layer services and helps them in mapping applications, e.g., voice, data to ATM cells. It accepts the data and converts them into fixed sized segments. The transmissions can be of fixed or variable data rate. This layer has two sub layers − Convergence sub layer and Segmentation and Reassembly sub layer.

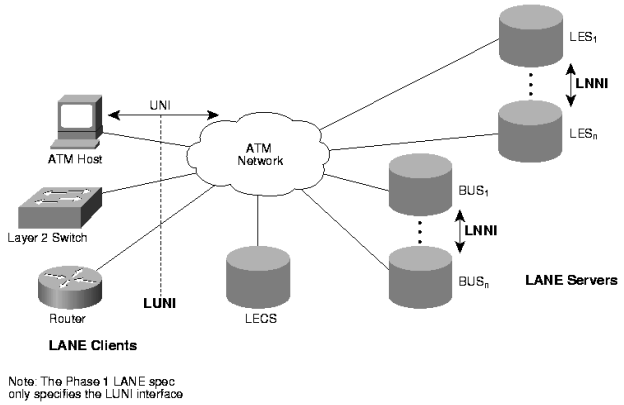
The functionalities of all the ATM protocol layers are categorized into control plane, user plane and managementplane.

➡**User plane** layers handle user information transfer and required associated controls e.g. error control and flow control.

➡**Control plane** takes care of call and connection related control signals.
➡**Management plane** is divided into plane and layer management. Plane management manages whole system functionality. Layer management takes care of management of all resources and parameters of the protocol entities.

ATM LAN EMULATION:

LAN Emulation ,also Known as LANE, ia an Asynchronous Transfer Mode(ATM) technology that enables local area network(LAN) traffic such as Ethernet frames to be carried over an ATM network. ATM as a backbone for connecting LANs



Ethernet and ATM technologies are difficult to connect because ATM is a connection oriented technology and Ethernet is a broadcast-based connectionless technology,Also Ethernet frames and ATM cells are different in format and addressing

For an ATM network to act as a backbone for connecting Ethernet LAN,it must support MAC-to-ATM address mapping.LANE converts variable-length Ethernet frames into fixed-length ATM cells for transmission over the ATM backbone.LANE services run on one or more network servers and map ATM.

When a user on an ATM network wants to access a resource on the Ethernet LAN, the client sends an address resolution message(ARM) to the LANE server ,which forwards the message to a bridge or router connected to the Ethernet network If the bridge or router knows the destination MAC address ,it acts as a proxy and forwards the message to the destination client ; if it doesn't know the destination MAC address it relays the message to the broadcast unknown server(BUS),a LANE service that broadcasts the message to all stations on the Ethernet LAN.

LANE operation:

- Workstationsuses ATM adapter card

- Frames converted to cells by segmentation and reassembly(SAR)
- Maps Ethernet addresses to ATM addresses
- SAR converts ATM cells to Ethernet frames

LANE Components:

LANE is made up of four components:

1. LAN Emulation Client(LEC)
2. LAN Emulation Server(LES)
3. Broadcast and Unknown Server(BUS)
4. LAN Emulation and Configuration Server(LECS)

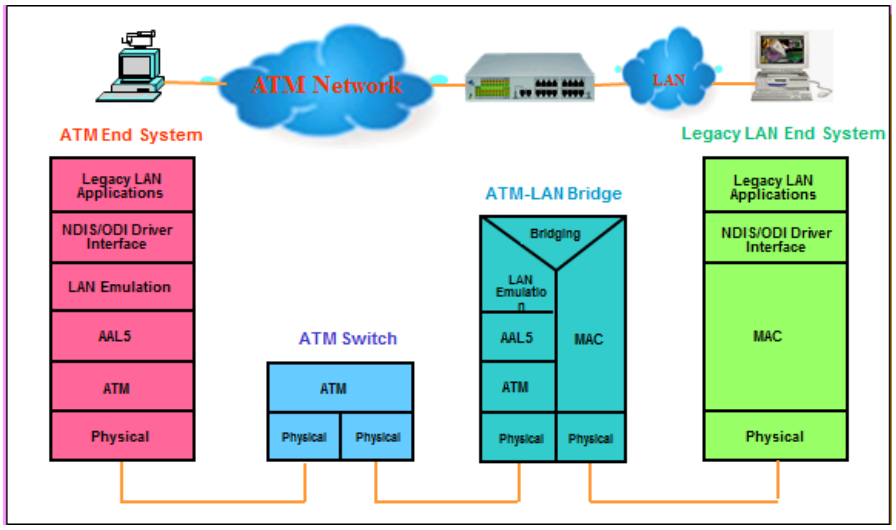


Fig:ATM LAN Emulation

1.LAN Emulation Client (LEC)

- An end system (host, bridge, or router) on an emulated LAN
- Represents one or more end users, identified by their MAC addresses
- The LAN emulation software (LAN emulation layer) provides a MAC level emulated 802.3 or 802.5 interface to higher level protocols, such as IP, or IPX

- Performs address translation (between MAC addresses and ATM addresses), address resolution, data forwarding, and other control functions

2. **LAN Emulation Server (LES)**

   - A component of the LANE service, implements control and coordination functions for the ELAN
   - Controls the joining of LECs to its ELAN
   - Provides registration service to LECs
   - An LEC registers its MAC and ATM addresses with the LES
   - Responsible for address resolution from MAC address to ATM address
   - Has unidirectional point-to-point VCs for ARP data coming from LECs and unidirectional point-to-multipoint VCs for ARP data going to LECs
   - Each ELAN has one LES

3. **Broadcast and Unknown Server (BUS)**

   - A component of the LANE service, used by an LEC to forward frames to broadcast/multicast addresses
   - Also used by an LEC to send unicast frames to all clients before the destination is known
   - All broadcast, multicast, and unknown traffic to and from an LEC passes through this single entity
   - The multicast server function provided in the BUS is required as part of LANE to provide the connectionless data delivery characteristics of a shared-media network to LECs
   - Has unidirectional point-to-point VCs for data coming from LECs
   - Has unidirectional point-to-multipoint VCs for data going to LECs
   - Each ELAN has one BUS

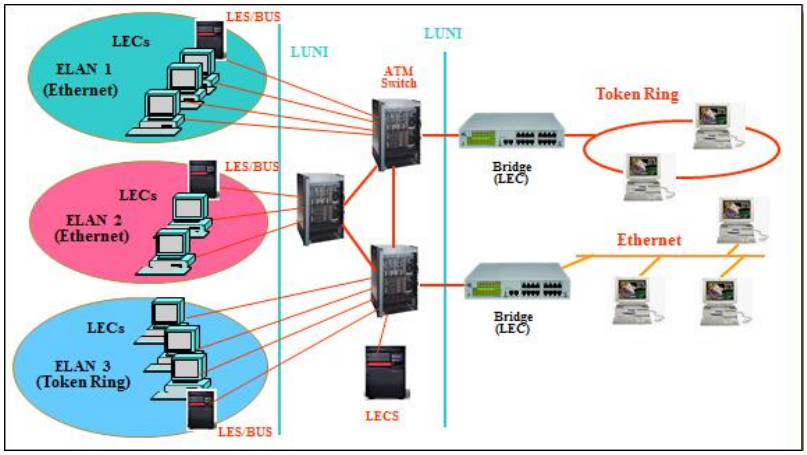
- Must always exist in the ELAN
- All LECs must join its distribution group

4. **LAN Emulation Configuration Server (LECS)**
    - A component of the LANE service, responsible for initial configuration of LECs
    - Provides configuration information to LECs prior to joining the emulated LAN
    - Responsible for the assignment of individual LECs to different ELANs based on administrative policies
    - Provides the LES's ATM address to LEC
    - One LECS serves one network that consists of many ELANs

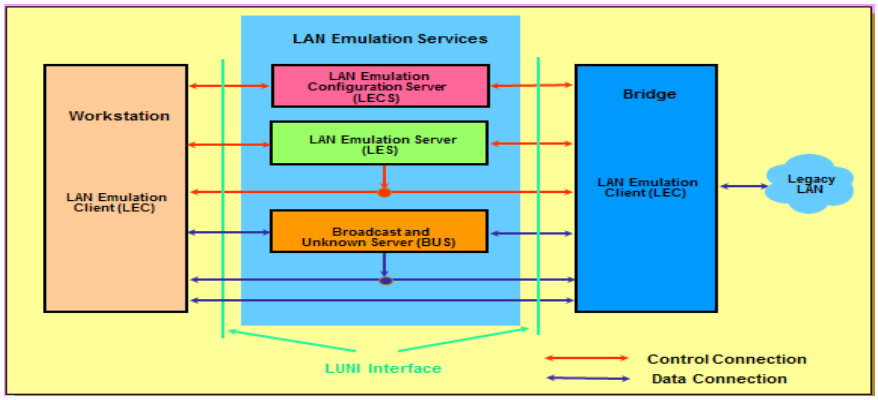
Bridge

- To connect legacy LANs (802.3 and 802.5) to the emulated LAN
- To implement features required in the LUNI interface to support both transparent and source routing bridging

LAN Emulation Conceptual Configuration



Emulated LAN Connections



The following are the functions of LANE operation

- **Initialization**
- **Joining and Registration**
- **Address Resolution**
- **Data Transfer**

Initialization

- The main goal of the initialization procedure is to reduce the required manual configuration of LEC when it first joins an ELAN
- Ideally, all configuration and initialization is done automatically without human interaction (plug-and-play)
- This is achieved by using LECS
- The LECS contains all the information required by an LEC such as
    - 0 The ATM address of its LES
    - 0 LAN type (Ethernet or Token Ring) to be emulated
    - 0 Maximum data frame size (1516, 4544, 9234, or 18190)
    - 0 Name of the emulated LAN (Engineering/Marketing)
- Prior to joining the emulated LAN, an LEC (after power-up) uses the following order to locate the LECS
    - 0 Get the LECS address via ATM Forum defined Interim Local Management Interface (ILMI) procedure which takes place between the LEC and the ILMI software in the switch

- 0 If the ILMI procedure fails, use the well known LECS address defined by the ATM Forum's LANE standards
- 0 If the well known address fails, use the ATM Forum defined LECS PVC (VPI = 0, VCI = 17)

- LECS connection
  - = Once the location of LECS is known, the LEC establishes a configuration Direct VCC to the LECS

- Configuration
  - = Once a connection is established between the LEC and the LECS, the LEC is configured automatically with the information provided by the LECS

Joining and registration

- To join an ELAN, LEC establishes a bi-directional point-to-point Control Direct VCC to its LES
- Transmits join request with ATM address, MAC address, proxy indication (workstation or bridge) to LES
- If the LEC is a proxy for a number of end systems on a legacy LAN (a bridge), it sends a list of all MAC addresses on the legacy LAN
- This information will be used by the LES to perform address resolution functions.
- If accepted, LES responds with a join response indicating acceptance
  - 0 Then a Control Distribute point-to-multipoint VCC is established from LES to LEC used for address resolution functions
  - 0 LES provides LEC with the ATM address of the BUS
  - 0 LEC creates a bidirectional multicast send VCC to BUS

- LEC accepts a unidirectional multicast forward VCC from BUS
- At this point, the LEC is registered and ready to transfer data

Data Transfer

- Once a client is registered, it is able to send and receive MAC frames
- There are three cases to consider:
  - Unicast MAC frame, ATM address known
  - Unicast MAC frame, ATM address unknown
  - Multicast or broadcast MAC frame
- If the client knows the ATM address of the unicast frame (in its internal cache), it checks whether it has a virtual data connection already established to the destination client
- If so, it sends the frame over that connection (as a series of ATM cells)
- Otherwise, it uses the ATM signaling to set up a connection and then sends the frame
- If the destination ATM address is unknown, the LEC asks LES for address resolution
- While waiting, the LEC transmits frame(s) via BUS
- When an LES response is received, the LEC establishes a direct connection with the destination
- Connections are timed out on inactivity
- If the MAC frame is a multicast or broadcast frame, the LEC sends the frame to the BUS
- The BUS replicates that frame and sends it over the virtual data connections to all clients on the ELAN

Address Resolution

- In ELAN, the destination stations are usually known by their MAC addresses
- Only ATM addresses can be used for connection set up in the ATM network
- LES allows LECs to request the resolution of a target MAC address into ATM address to to be used to establish a direct VCC to the target end system
- For MAC group address, a single ATM address is returned as the root of a point-to-multipoint VCC for the support of multicast service.

LANE features include:

- **Flexibilit**y: All existing and legacy LAN applications operate over ATM networks without applying substantial changes. All Ethernet components are connected to an ATM network that is only used as needed. Additionally, ATM backbones may be directly connected to a logical LAN.
- **Data transmission**: LANE uses different protocols to establish connectivity. Multiple stages required for data transmission include initialization, configuration and joining.
- **Emulation architecture**: Four LANE components work as a single backbone. The LANE Client (LEC) is an end-system that uses LANE applications to communicate with other clients. The LANE Configuration Server (LECS) is used to configure the LEC and LANE Server (LES). Each LANE network has one LES, which defines all network clients. Finally, because ATM does not support broadcast communication, a Broadcast Server bus is used to broadcast, unicast and multicast LEC traffic.
- **Fault tolerance**: The best LANE feature. If a LEC is disconnected from a network, LANE efficiently recovers the client status from the fault point. If the LES fails and restarts, the LEC is automatically self-configured.

InterLAN Switching

A variety of LAN topologies are available to fit any network:

- ***Ethernet* technology** is most widely used because of its efficiency and its cost. Ethernet technology is constantly evolving to maintain its status and to stay ahead of the network demands. Ethernet is fairly easy to install because of the wide variety of equipment on the market and the standards that accompany it. Ethernet speed ranges from 10Mbps to 10,000Mbps, for a wide variety of networks.

- ***Token Ring*** is the second most widely used technology in today's networks. Token Ring uses a ring topology and a Token-passing method to access the physical medium, which consist of a virtual ring.

- ***ATM*** is great for high-speed technologies, such as video and voice. Most companies, however, do not pass large amounts of video or sound, sending mainly straight data. Because of ATM's large overhead, these companies don't need to pay the extra money for ATM simply because they won't fully utilize its capabilities.

- ***Wireless LANs*** are very convenient and will likely be highly considered for short-distance WANs and LANs. Wireless LANs will almost always be connected to a wired network. Although wireless technology boast speeds as high as 11Mbps, they are probably running at a speed of 5Mbps to 7Mbps in reality.

Local Area Networking

A local area network (LAN) is a group of computers and peripheral devices that share a common communications line or wireless link to a server within a distinct geographic area. A local area network may serve as few as two or three users in a home office or thousands of users in a corporation's central office. Homeowners and information technology (IT) administrators set up LANs so that network nodes can communicate and share resources such as printers or network storage.

LAN networking requires Ethernet cables and Layer 2 switches along with devices that can connect and communicate using Ethernet. Larger LANs often include Layer 3 switches or routers to streamline traffic flows.

Setting up a basic local area network

Operating systems (OSes), such as Microsoft Windows, Linux, Apple OS X, Android and iOS, have Internet Protocol Version 4 (IPv4) and IPv6 networking capabilities incorporated into them. Additionally, personal computer (PC), tablet and smartphone hardware all come with an Ethernet port, Wi-Fi chip or both. This means that, as long as the network administrator has a relatively up-to-date laptop or desktop PC, it's fairly straightforward to network machines together onto a wired or wireless LAN.

Setup of a simple wired LAN requires an administrator to connect the end device to a LAN switch using a twisted-pair Ethernet cable. Once connected, the devices can communicate with each other on the same physical LAN or VLAN.

To set up a wireless network, the administrator needs a wireless access point (WAP). The WAP can be configured to broadcast a network service set identifier (SSID) and require devices to authenticate to the network using one of several Wi-Fi authentication techniques. Popular authentication options include Wi-Fi Protected Access 2 pre-shared key and WPA2 Enterprise.

VLAN

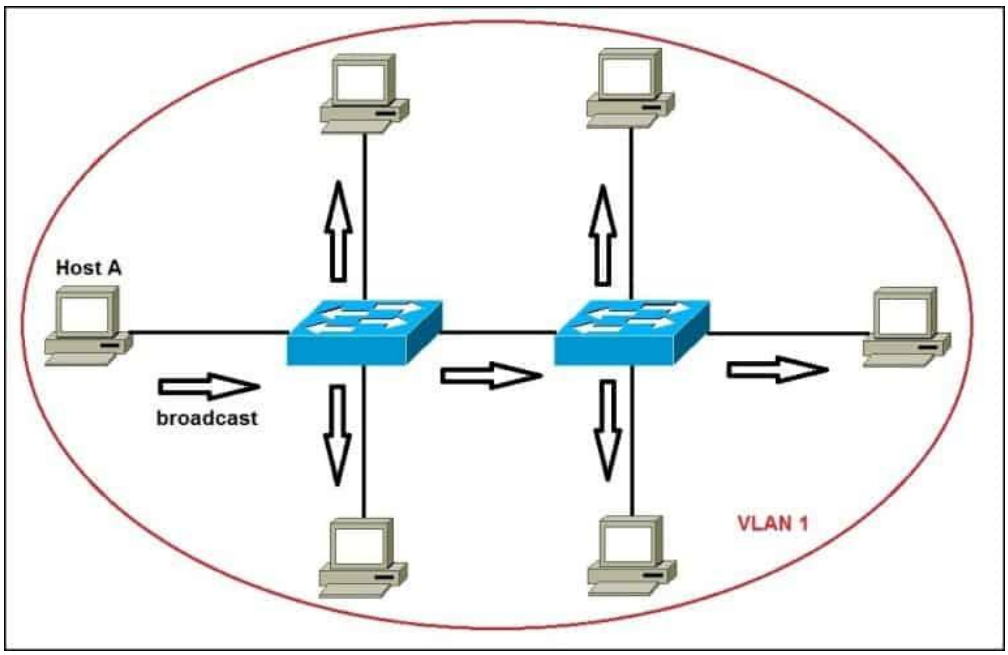
VLANs (Virtual LANs) are logical grouping of devices in the same broadcast domain. VLANs are usually configured on switches by placing some interfaces into one broadcast domain and some interfaces into another. Each VLAN acts as a subgroup of the switch ports in an Ethernet LAN.

VLANs can spread across multiple switches, with each VLAN being treated as its own subnet or broadcast domain. This means that frames broadcasted onto the network will be switched only between the ports within the same VLAN.

A VLAN acts like a physical LAN, but it allows hosts to be grouped together in the same broadcast domain even if they are not connected to the same switch. Here are the main reasons why VLANs are used:

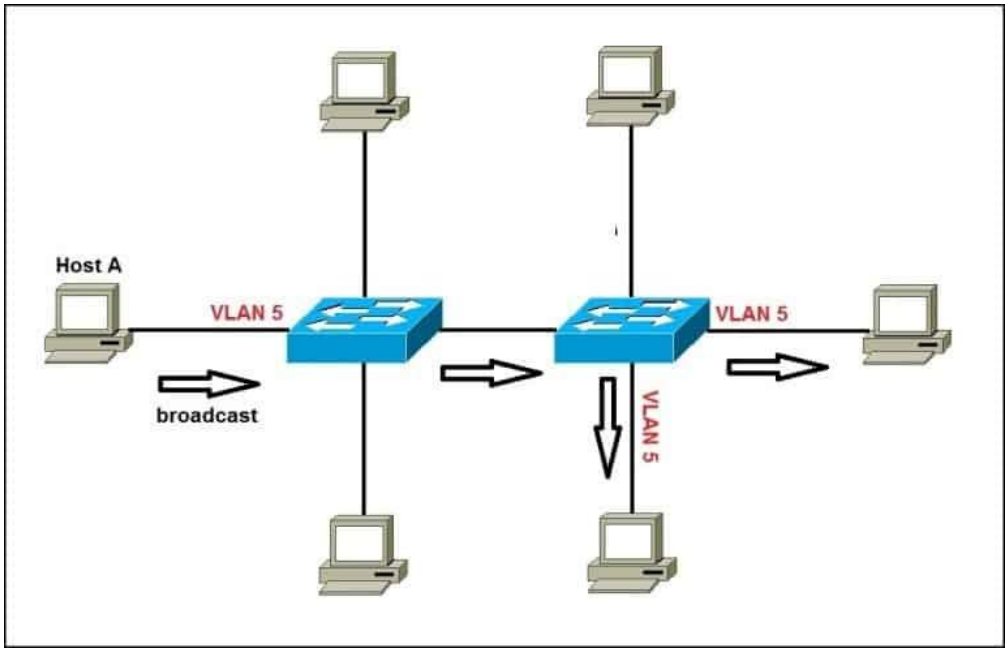
- VLANs increase the number of broadcast domains while decreasing their size.
- VLANs reduce security risks by reducing the number of hosts that receive copies of frames that the switches flood.
- you can keep hosts that hold sensitive data on a separate VLAN to improve security.
- you can create more flexible network designs that group users by department instead of by physical location.
- network changes are achieved with ease by just configuring a port into the appropriate VLAN.

The following topology shows a network with all hosts inside the same VLAN:



Without VLANs, a broadcast sent from host A would reach all devices on the network. Each device will receive and process broadcast frames, increasing the CPU overhead on each device and reducing the overall security of the network.

By placing interfaces on both switches into a separate VLAN, a broadcast from host A would reach only devices inside the same VLAN, since each VLAN is a separate broadcast domain. Hosts in other VLANs will not even be aware that the communication took place. This is shown in the picture below:



InterLAN Switching

LAN interconnection devices offers a number of options, including hubs, LAN switches, virtual LANs (VLANs), bridges, routers, and IP switches.

LAN Switches

- ✓ LAN switches are a very cost-effective solution to the need for increased bandwidth in workgroups.
- ✓ Each port on the switch delivers a dedicated channel to the device or devices attached to that port, thereby increasing the workgroup's total bandwidth and also the bandwidth available to individual users.
- ✓ Figure 6.8 shows a simple example of a switched Ethernet configuration.
- ✓ One workstation requires 100Mbps on its own, so it has the full services of a 100Mbps port on the switched Ethernet card.
- ✓ Five workstations, on the other hand, each need 20Mbps, so one 100Mbps port serves all five workstations.
- ✓ These five workstations connect to a hub, and that hub connects to the actual port. (Today such configurations are largely managed by the local switches.)
- ✓ Servers have extra bandwidth requirements ones in Figure 6.8 require 200Mbps so they are each served by bonding of several 100Mbps ports.

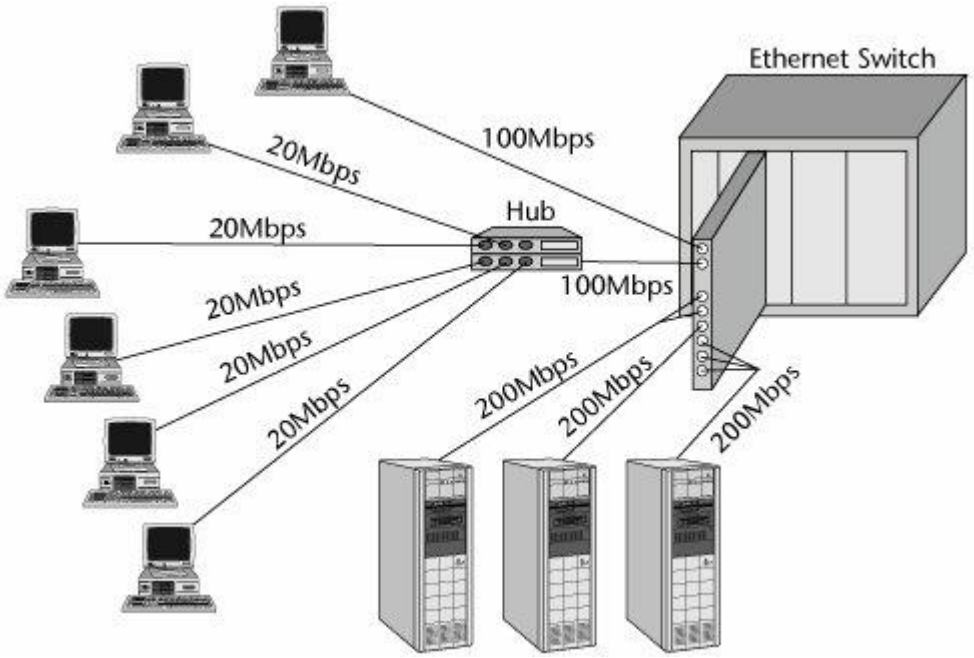


Figure 1. An example of a switched Ethernet configuration

- ✓ The key applications for LAN switches are to interconnect the elements of a distributed computing system, to provide high-speed connections to campus backbones and servers, and to provide high bandwidth to individual users who need it.
- ✓ Instead of sharing a 10Mbps or 100Mbps LAN among several terminals in a workgroup, a LAN switch can be used, and an individual workstation can get the entire 10Mbps or 100Mbps.
- ✓ LAN switches provide great scalability because they enable the network to increase in bandwidth with the fairly simple addition of more switched ports.
- ✓ In addition, switches operate in full-duplex mode and as such use dedicated outgoing and incoming channels to allow full-speed transmission in both directions at the same time.
- ✓ Thus, LAN switches have many benefits, including scalability in terms of bandwidth, flexibility, and high performance.
- ✓ Figure 1 shows how an Ethernet switch can be used to connect devices that are on the same segment, some of which are served by one shelf of the Ethernet switch and others which are served by connecting shelves.
- ✓ On the backplane, you can provide internetworking between the Ethernet segments, so you can provide internetworking on a campus-wide basis.

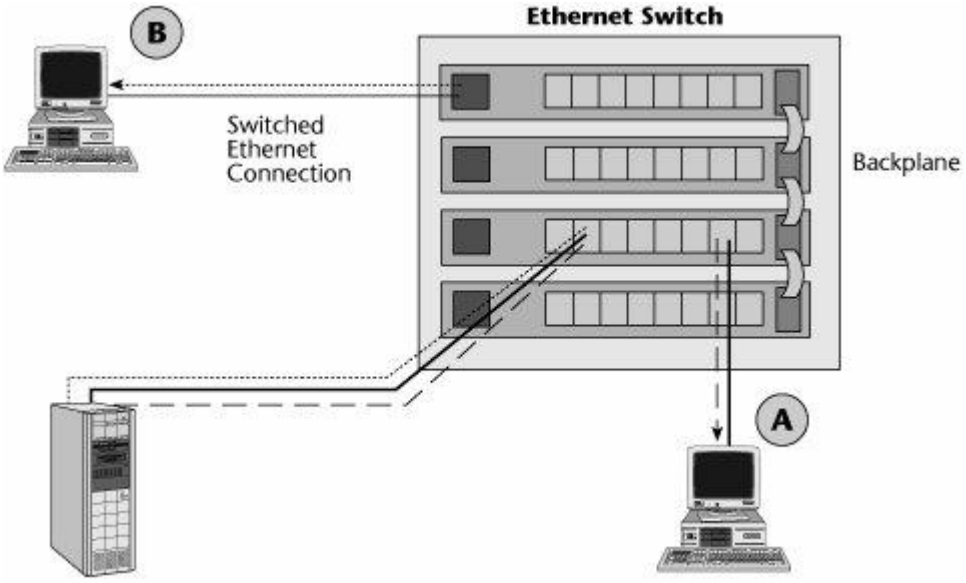
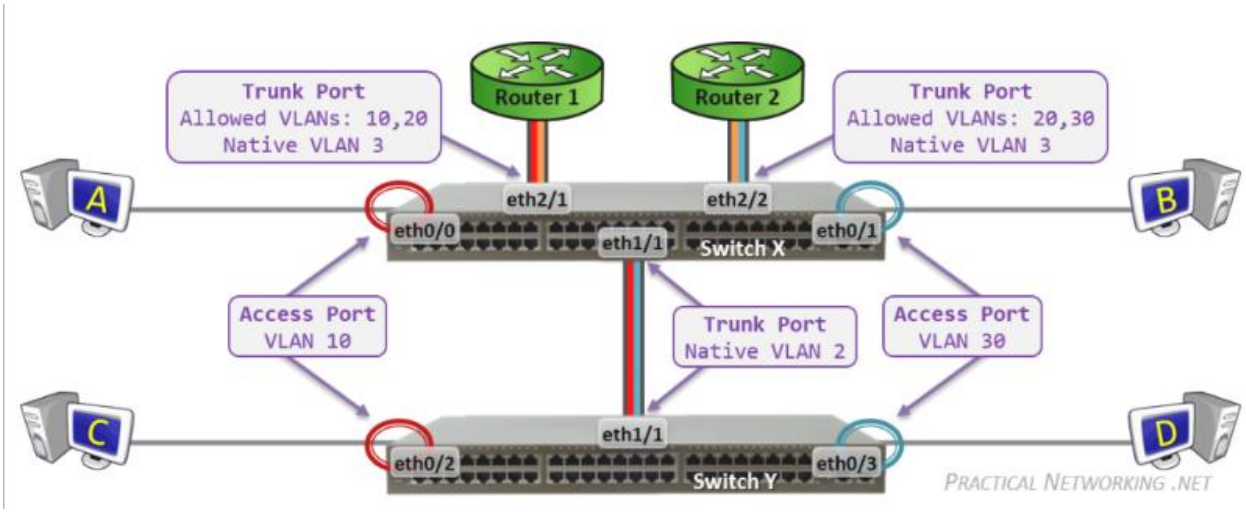


Figure .2 An Ethernet switch

- ✓ As the amount of traffic has grown in enterprises and as the nature of applications has become more sophisticated, we have been increasing the bandwidth associated with LANs.
- ✓ Today, it is common to see 10Mbps being delivered to an individual desktop and 100Mbps serving as the cluster capacity.
- ✓ To facilitate internetworking between these high-capacity desktops and Fast Ethernet clusters, Gigabit Ethernet is increasingly being used in the backbone.
- ✓ Gigabit Ethernet switches can connect underlying 100Mbps or 10Mbps LAN segments, and the 10Mbps or 100Mbps LAN switches can deliver 10Mbps to the desktop and 100Mbps to the segment.

InterVLAN Switching Diagram



LAN TO MAINFRAME

Mainframe computers are powerful computers that can handle vast quantities of data and offer highly stable transaction processing (a transaction is a discrete computer operation that must be completed in its entirety and cannot be sub divided into separate tasks). They find their greatest usage in corporate and governmental systems to facilitate the processing of large data flows.

A *network* is the hardware and software that enables computers to share files and resources and exchange data. Networks play a significant role in much of the world's transaction processing. A large corporation conducts daily operations over one or more networks that connect the business--locally or remotely--to partners, suppliers, and customers around the world.

- **Mainframes and Networks**

  To support the changing requirements of online transactions, enterprise networks can be designed, customized, operated, and supported using the combined features and functions of network protocols, such as SNA and TCP/IP.

- **Networklayers and protocols review**

  The first step in discussing network technology is to ensure that you understand the terms and acronyms. Starting from the physical layer, progressing to the data link layer (Ethernet), and moving up through the network layer (IP and routing) on to the transport layer (TCP and UDP), there are a large number of terms to be understood. These terms need to be clearly understood when z/OS systems programmers communicate with network administrators in an organization.
- **Hardware Connectivity on the Main Frame**

Network connections can be made in several different fashions. The mainframe originally relied upon the channel subsystem to offload I/O processing to channel programs. DASD is still accessed using ESCON channels, but for networking connectivity, OSA-Express cards offer better performance and availability.

- **Sample network configuration**

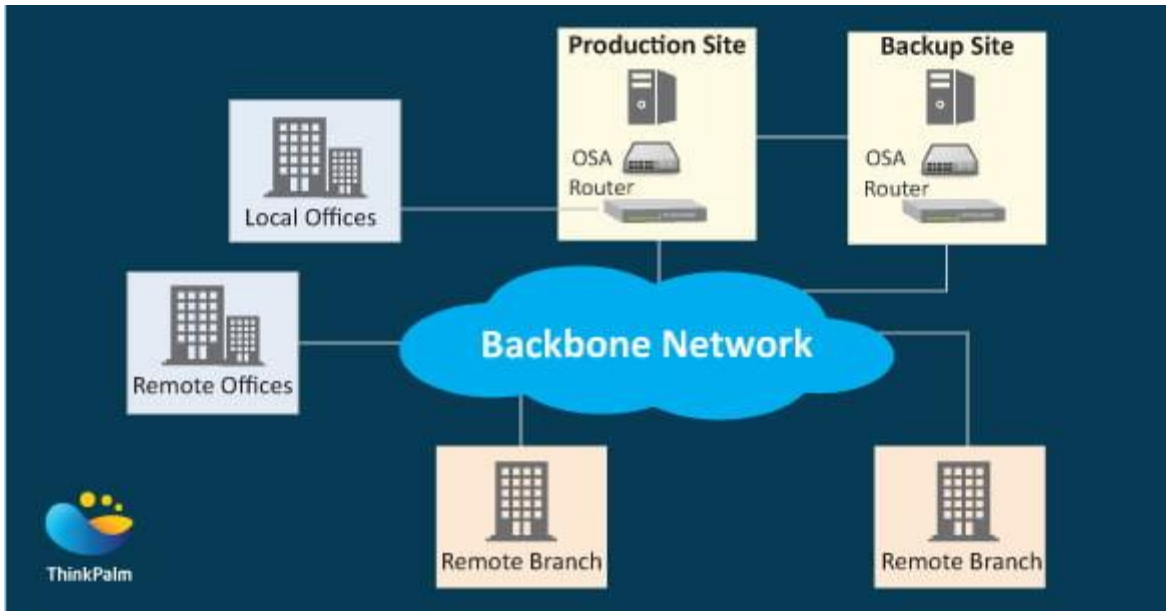
  Organizations run many of their mission-critical applications on the mainframe and system availability is a key factor in maintaining an organization's business. To meet this goal, organizations duplicate hardware and software components.

Mainframe Network Capabilities :

Mainframe architecture includes a variety of network capabilities. The following details use the mainframe operating system used at IBM, the z/OS operating system as an example. Some of these capabilities include:

- IP communication among large numbers of Linux and z/OS operating systems running as Virtual Machines

- IP communication among independent operating systems running in logical partitions on the same machine
- Communications via the TCP/IP suite of protocols, applications, and equipment
- System Network Architecture (SNA)
- SNA integration into IP networks using Enterprise Extender (EE) technology



Mainframe-Based Network

The above figure illustrates a simplified mainframe-based network architecture. The mainframe is connected to external devices using Open Systems Adapter-Express (OSA-Express) which is an integrated LAN Adapter. It is equivalent to a network interface card (NIC) used in Windows and UNIX systems. It supports various protocols and operational modes. OSA-Express card majorly uses the Ethernet protocol, running over copper wire or fiber optic cabling. The I/O systems of mainframe differ from UNIX/Intel systems because of which, OSA card implements advanced technologies required for networking.

For a particular organization, a redundant backbone switch or router is used to connect critical business servers to the primary network. The switch or router

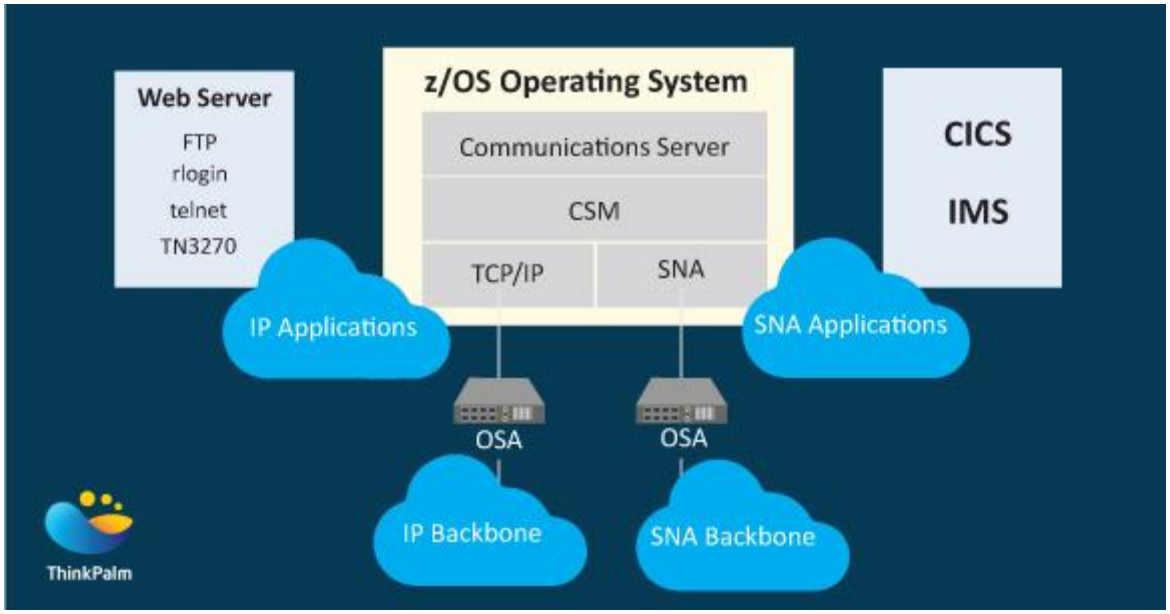
provides redundancy by providing more than one physical path to the backbone network. The backbone network is the organization’s high traffic density network.

As expected in every network the Backup site takes care of data processing for planned as well as unplanned outages in the production site. The backup site can provide a data processing site for a very long time. The level and the type of services provided by the backup site is determined by the cost of a backup compared to the cost of failure. Larger the organization, higher is the value placed on the backup site. The backup and the production sites are connected using high-speed connections, normally using fiber optics.

Offices used for computer personnel, administration and back-office services are usually located in the vicinity of the production computer site. These locations may be in the same building, the same campus, or a few blocks away. These sites would be connected using high-speed connections.

Remote sites, such as branch offices and remote offices, are connected to the backbone network. The backbone network normally uses carrier-supplied communication lines. A carrier-supplied network is a network that is provided on behalf of another organization. The speed, the protocol and the topology are designed and implemented by the networking department and the network users.

The z/OS operating system includes a software component called z/OS Communications Server. It implements the SNA and TCP/IP protocols.



Z/OS Communication Server

The above figure shows a z/OS Communications Server with three major components, which are:

- The TCP/IP protocol stack
- The SNA protocol stack
- The Communications Storage Manager (CSM), which provides a shared I/O buffer area for both TCP/IP and SNA data flow. The CSM function allows host applications to share data without physically moving the data.

It is to be noted that z/OS application programmers can exploit various advancements in communications in distinctly different operating systems since TCP/IP, as well as SNA protocols, are implemented in almost all existing platforms.

Security in a Network Provided by Mainframe

The mainframe software and hardware are ideally used for network transactions since they are capable of managing huge amounts of data, users and applications simultaneously, without external interference. In networks that

support thousands of end-users, the mainframe concepts of data integrity, security and reliability are extended to include the network.

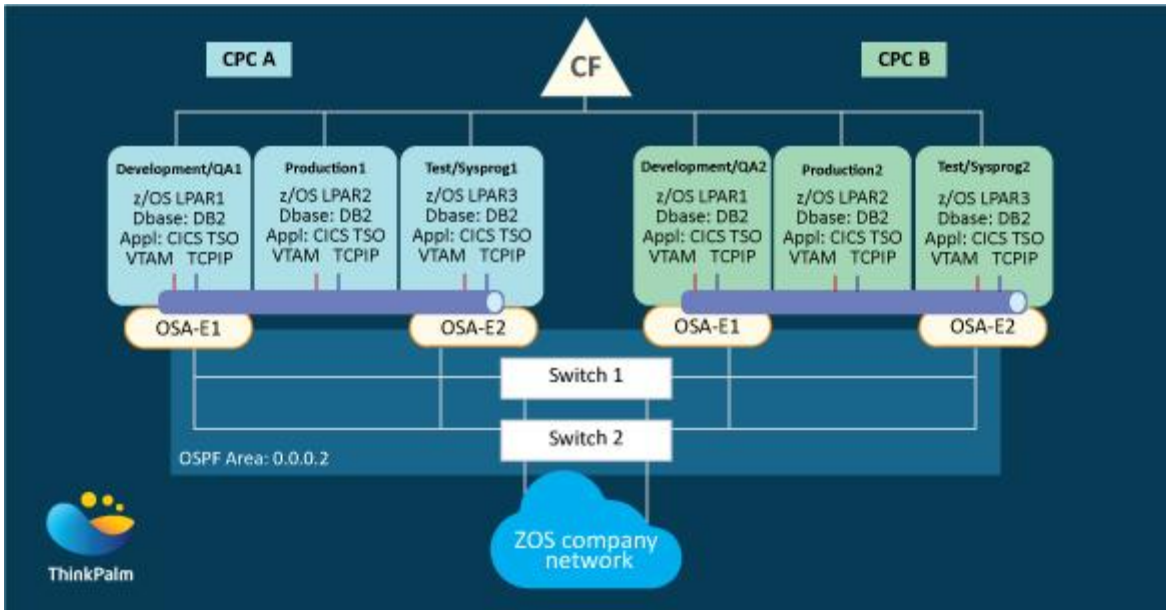
Most z/OS hosts will be located in secure physical locations with strict authorization requirements for employee access. Certain data on such a z/OS host is likely to be considered highly secure. If the data is to be transferred between two z/OS hosts within that secure physical location, the data transfer will most likely be classified as highly secure.

The System Authorization Facility (SAF) interface is a standardized function call available to all applications running on z/OS. The interface call is used to provide quick and controlled authorization, authentication, and logging services. The SAF call is forwarded to an external security manager such as the Resource Access Control Facility (RACF). SAF can collectively restrict end-user capabilities to any organization.

Requirements of a Mainframe Network

Businesses require their networks to be reliable, always available and fast. They invest a great amount of time and money creating an IT infrastructure that supports these goals – by duplicating hardware and software components, in addition to various other strategies. The extent to which an organization implements a solution depends on availability and performance goals, balanced against the cost of the solution.

The sample configuration below is designed to meet these goals, especially for availability. It illustrates a medium-to-large z/OS data center.



Sample Configuration

The process is divided physically by central processor complexes and logically by logical partitions.

- CPC-Central Processor Complex includes a physical collection of hardware that consists of main storage, more than one central processor, channels, and timers.
- A logical partition (LPAR) is a subset of a single physical system that contains resources (processors, memory, and input/output devices) and operates as an independent system.

Other components are

- CICS: Customer Information Control System. Provides transaction management functions and connectivity to application programs. Runs as an address space in z/OS.
- CF: Coupling Facility. Enables sharing of data between multiple LPARs using high-speed channels. Communicates LPAR status information.

- DB2 for z/OS: Relational database product used on most mainframe customer sites. Runs as an address space in z/OS.
- OSA: Open Systems Adapter. High speed integrated cards used for network communication.
- OSPF: Open Shortest Path First. The routing protocol used to communicate between router and mainframe TCP/IP OMPROUTE application.
- TSO: Time Sharing Option. An element of z/OS that enables users to create an interactive session with the z/OS system. TSO provides a unique user login capability and a basic command prompt interface to z/OS. This is similar to a normal PC command prompt window.
- VTAM: Virtual Telecommunications Access Method. The original SNA networking protocol for mainframes. Provides services to TCP/IP as well. Runs as an address space in z/OS.
- TCP/IP: TCP/IP server address spaces.

BUILDING HIGHLY RELIABLE COMPUTER NETWORKS

Good networks do not happen by accident. They are the result of hard work by network designers and technicians, who identify network requirements and select the best solutions to meet the needs of a business.

The steps required to design a good network are as follows:

Step 1. Verify the business goals and technical requirements.

Step 2. Determine the features and functions required to meet the needs identified in Step 1.

Step 3. Perform a network-readiness assessment.

Step 4. Create a solution and site acceptance test plan.

Step 5. Create a project plan**.**

After the network requirements have been identified, the steps to designing a good network are followed as the project implementation moves forward.

Network users generally do not think in terms of the complexity of the underlying network. They think of the network as a way to access the applications they need, when they need them.

Network Requirements

Most businesses actually have only a few requirements for their network:

■ The network should stay up all the time, even in the event of failed links, equipment failure, and overloaded conditions.

■ The network should reliably deliver applications and provide reasonable response times from any host to any host.

■ The network should be secure. It should protect the data that is transmitted over it and data stored on the devices that connect to it.

■ The network should be easy to modify to adapt to network growth and general business changes.

■ Because failures occasionally occur, troubleshooting should be easy. Finding and fixing a problem should not be too time-consuming.

Fundamental Design Goals

When examined carefully, these requirements translate into four fundamental network design goals:

■ **Scalability**: Scalable network designs can grow to include new user groups and remote sites and can support new applications without impacting the level of service delivered to existing users.

■ **Availability**: A network designed for availability is one that delivers consistent, reliable performance, 24 hours a day, 7 days a week. In addition, the failure of a single link or piece of equipment should not significantly impact network performance.

■ **Security**: Security is a feature that must be designed into the network, not added on after the network is complete. Planning the location of security devices, filters, and firewall features is critical to safeguarding network resources.

■ **Manageability**: No matter how good the initial network design is, the available network staff must be able to manage and support the network. A network that is too complex or difficult to maintain cannot function effectively and efficiently.