DOUBLE DEGREE PROGRAM IN INFORMATION AND COMMUNICATION TECHNOLOGIES ENGINEERING

GRADUATION PROJECT REPORT

NETWORK PLANNING TOOL

Advisers

Prof. Samir Gaber
Prof. Claudio Fornaro

Students

Milad Yossef
Peter Zaki
Ayman Abd El-Khalek
Ahmed Hagag

Academic year 2011/12

Acknowledgement

Many Thanks go to those who made this project possible:

Prof. Dr. Samir Gaber
Communication and Information Department Coordinator

We would like to express our deep gratitude and thanks for his continuous supervision, Wise advice and support, encouraging us to do our best, and above all making us proud of being engineers.

Eng. Ahmed Magdy

We would like to say thank you for your support and aid in finishing our project.

Prof. Dr. Claudio Fornaro

We would like to thank Prof. Dr. Claudio Fornaro for his kind patience and for his encouragement which made things easy yet valuable.

Prof. Dr. Dario Assante
Assistant Professor of Electrical Engineering

And finally we would like to express our sincere gratitude to Prof. Dr. Dario Assante for his clear vision which made the road remarkable and delightful.

We really feel so lucky that we are a part of this experience which symbolizes glory, peace, and love between Egypt and Italy.

Thank you

INTRODUCTION

Computer network plays a crucial role in our life because it touches many components of the infrastructure: end users, servers, middleware, and applications.

It provides sharing of expensive devices, software programs and information, work dividing and working in synchronization, also exchange files and documents.

With grown and the complexities of networks, it becomes complex and difficult to scale and manage, **So** it is necessary to use architectures and methodologies in network design to support business goals and the need to save time and efforts in planning and designing then save money and that what our project provides.

Also the desire to make additive effect in computer network field, and after research we find there is no software tool for computer network designing ,That is what make us decide to choose this project.

The Program Description:

The project is a Software tool which considers how to design a network including how to distribute network devices (switches, routers and ….. so on) within a given area and estimate the overall network cost in easy manner.

The tool input is the site description (i.e. the area dimensions: it's length and width , the number of buildings inside this area , location of them with respect to the area and detailed description about each building will be used in the design of the network such as number of floors in this building , number of rooms in each floor, location of them with respect to

the floor and finally the number of nodes or PCs in each room) , then the tool according to specific algorithm will calculate and draw the overall design of the computer network required for this building, it also estimates the network cost.

What does the Tool Provide?

Our program tool provides many benefits such as: flexibility, ease, quick in designing networks (including LANs & WANS), Suggestion of network's devices and tools (switches, routers, cables…), Estimation the cost of network, saving time, efforts and then money.

Business Vision:

Companies, offices and engineers which work in designing computer network can use this program easily.

The project's stages:

The project consists of 3 stages; where the first is The Input layer, flowing through The Business (Core) layer, going to The Data Base Layer and finally ended to The Output Layer. These stages are shown in the following figure:

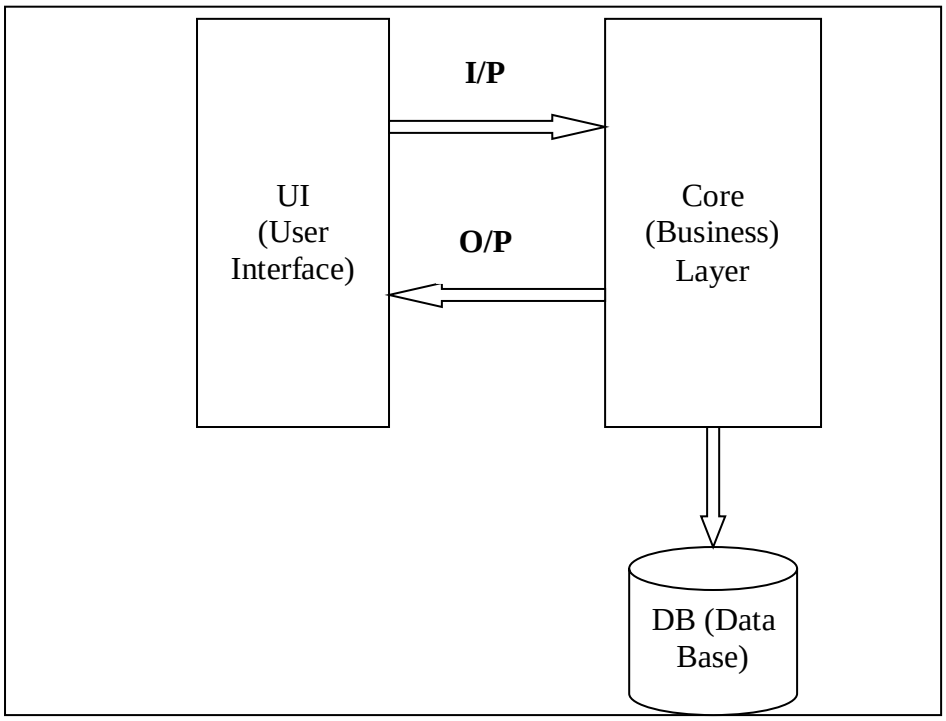


Fig.1. Project's Stages

The project stages are detailed for the following:

1- The Graphical User Interface(GUI):

In this Interface, user can draw the site (area, buildings, floors and rooms inside it), user also can edit any of the drawings he has been drawn to simulate the actual shape of the site.

This input entered to the next stage as data (numbers) not as drawings to be processed to obtain the output.

To learn more about this stage see the appendix in the end of the book.

2- Business (Core) layer :

This is the stage which calculates the main algorithm, which takes the input data from the previous stage, process it, and then produce output to pass it to the user interface layer to be drawn to the user another time.
The main algorithm is illustrated later.

3-Data Base Layer:

This layer is the layer which contains tables of data bases of switches and cables for number of companies.
This layer is called from the core layer and it respond to it with the required output.

Chapter 1

Introduction to Computer Network

Introduction to Computer Networks

This chapter gives a light-hearted perspective about networks, how they were originally created, and why networks work the way they do.

Computer Network

A network is basically all of the components (hardware and software) involved in connecting computers across small and large distances. Networks are used to provide easy access to information, thus increasing productivity for users.

Importance of Networks

Describes why and how computer networks support successful work.
Information and communication are two of the most important strategic issues for the success of every enterprise. While today nearly every organization uses a substantial number of computers and communication tools (telephones, fax, and personal handheld devices), they are often still isolated. While managers today are able to use the newest applications, many departments still do not communicate and much needed information cannot be readily accessed.

To overcome these obstacles in an effective usage of information technology, computer networks are necessary. They are a new kind (one might call it paradigm) of organization of computer systems produced by

the need to merge computers and communications. At the same time they are the means to converge the two areas; the unnecessary distinction between tools to process and store information and tools to collect and transport information can disappear. Computer networks can manage to put down the barriers between information held on several (not only computer) systems. Only with the help of computer networks can a borderless communication and information environment be built.

Computer networks allow the user to access remote programs and remote databases either of the same organization or from other enterprises or public sources. Computer networks provide communication possibilities faster than other facilities.

Because of these optimal information and communication possibilities, computer networks may increase the organizational learning rate, which many authors declare as the only fundamental advantage in competition.

Besides this major reason why any organization should not fail to have a computer network, there are other reasons as well: cost reduction by sharing hard- and software resources, high reliability by having multiple sources of supply, cost reduction by downsizing to microcomputer-based networks instead of using mainframes and greater flexibility because of possibility to connect devices from various vendors

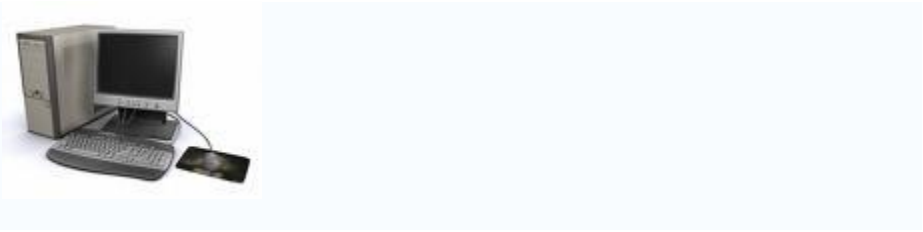
Because of the importance of this technology, decisions of purchase, structure, and operation of computer networks cannot be left to technical staff. Management as well has a critical need for understanding the technology of computer networks.

Network components

Three main network components:

1- Computers (servers and hosts)

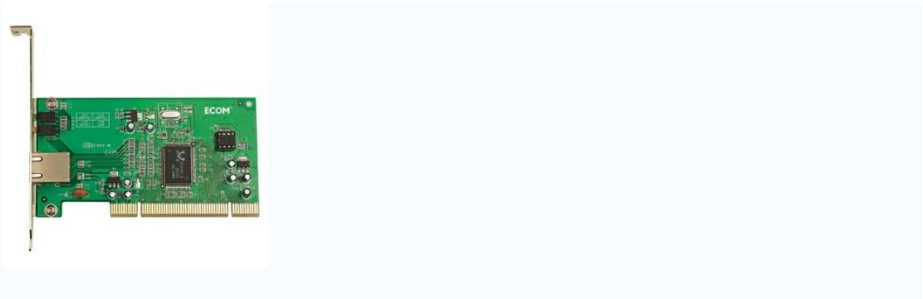
Considered as the big source of applications (network software applications);
Ex: HTTP (Hyper Text Transmission Protocol), FTP (File Transfer Protocol), SNMP (Simple Network Management Protocol) and Telnet.



2- Network Devices

Devices that interconnect different computers together; Ex: Repeaters, hub, bridge, switch, router, NIC and modems.

- **NIC:**



- **Switch:**

- **Router:**

- **Hub:**

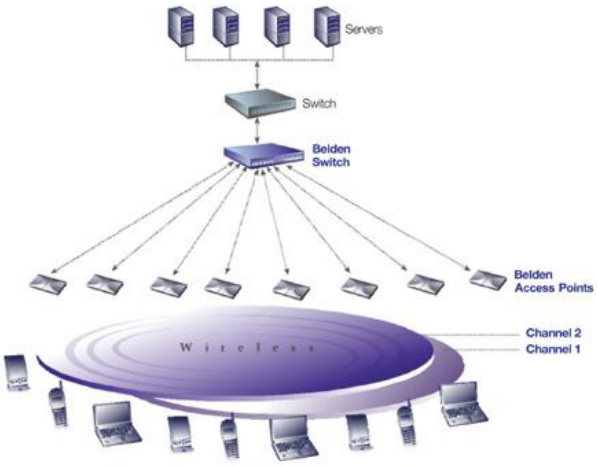
3-Connectivity

Media that physically connect the computers and network devices; Ex: Wireless and cables.

Network Types

There are three types of Networks :
LAN (Local Area Network), MAN (Metropolitan Area Network) and WAN (Wide Area Network).

1-Local area network (LAN)



A local area network is a network that spans a relatively small space and provides services to a small number of people. Depending on the number of people that use a Local Area Network, a peer-to-peer or client-server method of networking may be used. A peer-to-peer network is where each client shares their resources with

Other workstations in the network. Examples of peer-to-peer networks are: Small office networks where resource use is minimal and a home network. A client-server network is where every client is connected to the server and each other. Client-server networks use servers in different capacities. These can be classified into two types: Single-service servers, where the server performs one task such as file server, print server, etc.; while other servers can not only perform in the capacity of file servers and print servers, but they also conduct calculations and use these to provide information to clients (Web/Intranet Server). Computers are linked via Ethernet Cable, can be joined either directly (one computer to another), or via a network hub that allows multiple connections.

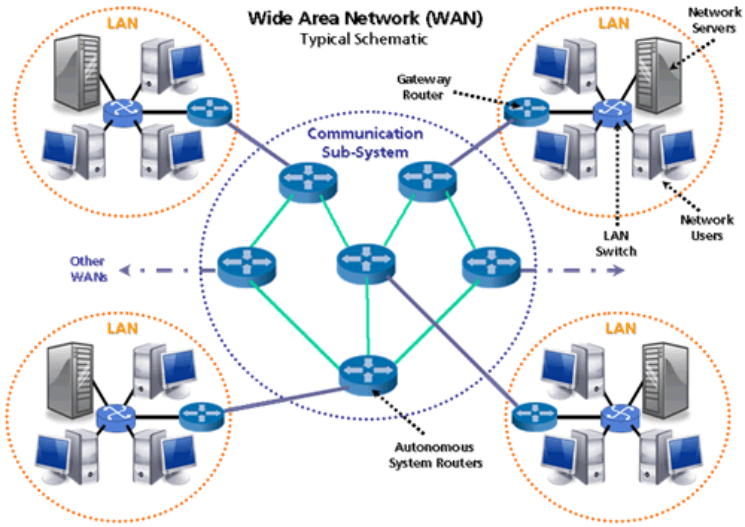
Historically, LANs have featured much higher speeds than WANs. This is not necessarily the case when the WAN technology appears as metro Ethernet, implemented over optical transmission systems.

2-Metropolitan area network (MAN)

A MAN is optimized for a larger geographical area than is a LAN, ranging from several blocks of buildings to entire cities. MANs can also depend on communications channels of moderate-to-high data rates. A MAN might be owned and operated by a single organization, but it usually will be used by many individuals and organizations.

MANs might also be owned and operated as public utilities. They will often provide means for internetworking of local networks. Metropolitan area networks can span up to 50km, devices used are modem and wire/cable.

3-Wide area network (WAN)



A wide area network is a network where a wide variety of resources are deployed across a large domestic area or internationally. An example of this is a multinational business that uses a WAN to interconnect their offices in different countries.

The largest and best example of a WAN is the Internet, which is a network comprised of many smaller networks.

The Internet is considered the largest network in the world. The PSTN (Public Switched Telephone Network) also is an extremely large network that is converging to use Internet technologies, although not necessarily through the public Internet.

A Wide Area Network involves communication through the use of a wide range of different technologies. These technologies include Point-to-Point WANs such as Point-to-Point Protocol (PPP) and High-Level Data Link Control (HDLC), Frame Relay, ATM (Asynchronous Transfer Mode) and Sonet (Synchronous Optical Network). The difference between the WAN technologies is based on the switching capabilities they perform and the speed at which sending and receiving bits of information (data) occur.

Different Network Topologies

The network topology defines the way in which computers, printers, and other devices are connected, physically and logically. A network topology describes the layout of the wire and devices as well as the paths used by data transmissions.

Physical Topology:

It describes how devices are physically cabled.

Logical Topology:

It describes how devices communicate across physical topology; Ex. unicast, broadcast, multicast.

Commonly used physical topologies include many types like:

Point to Point, Bus,Star (extended star), Tree (hierarchical), Linear, Ring, Mesh, Partially connected and Fully connected (sometimes known as fully redundant).

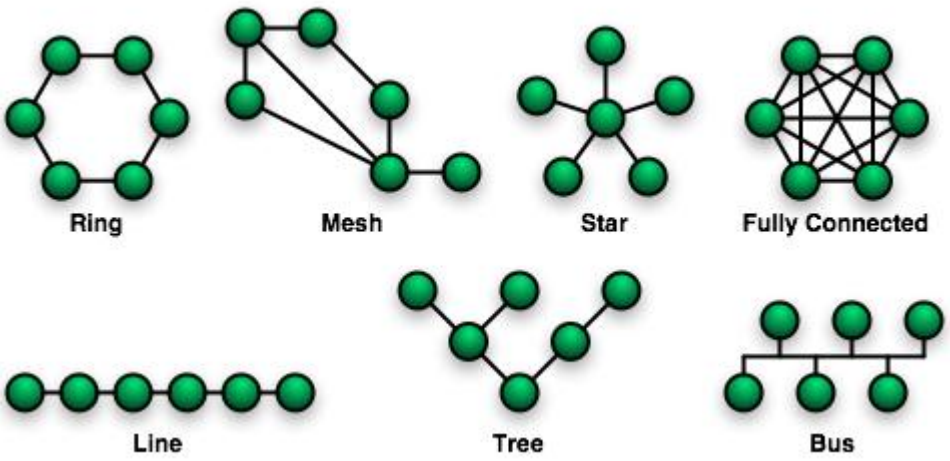


Fig shows different network topologies

Point-to-point:

The simplest topology is a permanent link between two endpoints. Switched point-to-point topologies are the basic model of conventional telephony. The value of a permanent point-to-point network is the value of guaranteed, or nearly so, communications between the two endpoints. The value of an on-demand point-to-point connection is proportional to the number of potential pairs of subscribers.

Permanent (dedicated):

Easiest to understand, of the variations of point-to-point topology, is a point-to-point communications channel that appears, to the user, to be permanently associated with the two endpoints.
With a microphone to a single public address speaker is an example.
Within many switched telecommunications systems, it is possible to establish a permanent circuit. One example might be a telephone in the lobby of a public building, which is programmed to ring only the number of a telephone dispatcher. a switched connection saves the cost of running a physical circuit between the two points. The resources in such a connection can be released when no longer needed, as, for example, a television circuit from a parade route back to the studio.

Switched:

Using circuit-switching or packet-switching technologies, a point-to-point circuit can be set up dynamically, and dropped when no longer needed. This is the basic mode of conventional telephony.

Bus:
Linear bus:

The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has exactly two endpoints (this is the 'bus', which is also commonly referred to as the backbone, or trunk) – all data that is transmitted between nodes in the network is transmitted over this common transmission medium and is able to be received by all nodes in the network virtually simultaneously (disregarding propagation delays)

Note: The two endpoints of the common transmission medium are normally terminated with a device called a terminator that exhibits the characteristic impedance of the transmission medium and which dissipates or absorbs the energy that remains in the signal to prevent the signal from being reflected or propagated back onto the transmission medium in the opposite direction, which would cause interference with and degradation of the signals on the transmission medium.

Distributed bus:

The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has more than two endpoints that are created by adding branches to the main section of the transmission medium – the physical distributed bus topology functions in exactly the same fashion as the physical linear bus topology (i.e., all nodes share a common transmission medium).

Notes:

i. All of the endpoints of the common transmission medium are normally terminated with a device called a 'terminator'.

ii. The physical linear bus topology is sometimes considered to be a special case of the physical distributed bus topology – i.e., a distributed bus with no branching segments.

iii. The physical distributed bus topology is sometimes incorrectly referred to as a physical tree topology – however, although the physical distributed bus topology resembles the physical tree topology, it differs from the physical tree topology in that there is no central node to which any other nodes are connected, since this hierarchical functionality is replaced by the common bus.

Star

The type of network topology in which each of the nodes of the network is connected to a central node with a point-to-point link in a 'hub' and 'spoke' fashion, the central node being the 'hub' and the nodes that are attached to the central node being the 'spokes' (e.g., a collection of point-to-point links from the peripheral nodes that converge at a central node) – all data that is transmitted between nodes in the network is transmitted to this central node, which is usually some type of device that then retransmits the data to some or all of the other nodes in the network, although the central node may also be a simple common connection point (such as a 'punch-down' block) without any active device to repeat the signals.

Notes:

i. A point-to-point link is sometimes categorized as a special instance of the physical star topology – therefore, the simplest type of network that is based upon the physical star topology would consist of one node with a single point-to-point link to a second node, the choice of which node is the 'hub' and which node is the 'spoke' being arbitrary.

ii. after the special case of the point-to-point link, as in note 1.) above, the next simplest type of network that is based upon the physical star topology would consist of one central node – the 'hub' – with two separate point-to-point links to two peripheral nodes – the 'spokes'.

iii. Although most networks that are based upon the physical star topology are commonly implemented using a special device such as a hub or switch as the central node (i.e., the 'hub' of the star), it is also possible to implement a network that is based upon the physical star topology using a computer or even a simple common connection point

as the 'hub' or central node – however, since many illustrations of the physical star network topology depict the central node as one of these special devices, some confusion is possible, since this practice may lead to the misconception that a physical star network requires the central node to be one of these special devices, which is not true because a simple network consisting of three computers connected as in note 2.) Above also has the topology of the physical star.

iv. Star networks may also be described as either broadcast multi-access or non broadcast multi-access (NBMA), depending on whether the technology of the network either automatically propagates a signal at the hub to all spokes, or only addresses individual spokes with each communication.

Extended star

A type of network topology in which a network that is based upon the physical star topology has one or more repeaters between the central node (the 'hub' of the star) and the peripheral or 'spoke' nodes, the repeaters being used to extend the maximum transmission distance of the point-to-point links between the central node and the peripheral nodes beyond that which is supported by the transmitter power of the central node or beyond that which is supported by the standard upon which the physical layer of the physical star network is based.

Note: If the repeaters in a network that is based upon the physical extended star topology are replaced with hubs or switches, then a hybrid network topology is created that is referred to as a physical hierarchical star topology, although some texts make no distinction between the two topologies.

Distributed Star

A type of network topology that is composed of individual networks that are based upon the physical star topology connected together in a linear fashion – i.e., 'daisy-chained' – with no central or top level connection point (e.g., two or more 'stacked' hubs, along with their associated star connected nodes or 'spokes').

Ring

The type of network topology in which each of the nodes of the network is connected to two other nodes in the network and with the first and last nodes being connected to each other, forming a ring – all data that is transmitted between nodes in the network travels from one node to the next node in a circular manner and the data generally flows in a single direction only.

Dual-ring

The type of network topology in which each of the nodes of the network is connected to two other nodes in the network, with two connections to each of these nodes, and with the first and last nodes being connected to each other with two connections, forming a double ring – the data flows in opposite directions around the two rings, although, generally, only one of the rings carries data during normal operation, and the two rings are independent unless there is a failure or break in one of the rings, at which time the two rings are joined (by the stations on either side of the fault) to enable the flow of data to continue using a segment of the second ring to bypass the fault in the primary ring.

Mesh

The value of fully meshed networks is proportional to the exponent of the number of subscribers, assuming that communicating groups of any two endpoints, up to and including all the endpoints.

Full (Fully connected)

The type of network topology in which each of the nodes of the network is connected to each of the other nodes in the network with a point-to-point link – this makes it possible for data to be simultaneously transmitted from any single node to all of the other nodes.
Note: The physical fully connected mesh topology is generally too costly and complex for practical networks, although the topology is used when there are only a small number of nodes to be interconnected.

Partial (Partially connected)

The type of network topology in which some of the nodes of the network are connected to more than one other node in the network with a point-to-point link – this makes it possible to take advantage of some of the redundancy that is provided by a physical fully connected mesh topology without the expense and complexity required for a connection between every node in the network.
Note: In most practical networks that are based upon the physical partially connected mesh topology, all of the data that is transmitted between nodes in the network takes the shortest path (or an approximation of the shortest path) between nodes, except in the case of a

failure or break in one of the links, in which case the data takes an alternate path to the destination. This requires that the nodes of the network possess some type of logical 'routing' algorithm to determine the correct path to use at any particular time.

Tree (also known as hierarchical):

The type of network topology in which a central 'root' node (the top level of the hierarchy) is connected to one or more other nodes that are one level lower in the hierarchy (i.e., the second level) with a point-to-point link between each of the second level nodes and the top level central 'root' node, while each of the second level nodes that are connected to the top level central 'root' node will also have one or more other nodes that are one level lower in the hierarchy (i.e., the third level) connected to it, also with a point-to-point link, the top level central 'root' node being the only node that has no other node above it in the hierarchy – the hierarchy of the tree is symmetrical, each node in the network having a specific fixed number, f, of nodes connected to it at the next lower level in the hierarchy, the number, f, being referred to as the 'branching factor' of the hierarchical tree.

Notes:

i. A network that is based upon the physical hierarchical topology must have at least three levels in the hierarchy of the tree, since a network with a central 'root' node and only one hierarchical level below it would exhibit the physical topology of a star.

ii. A network that is based upon the physical hierarchical topology and with a branching factor of 1 would be classified as a physical linear topology.

iii. The branching factor, f, is independent of the total number of nodes in the network and, therefore, if the nodes in the network require ports for connection to other nodes the total number of ports per node may be kept low even though the total number of nodes is large – this makes the effect of the cost of adding ports to each node totally dependent upon the branching factor and may therefore be kept as low as required without any effect upon the total number of nodes that are possible.

iv. The total number of point-to-point links in a network that is based upon the physical hierarchical topology will be one less than the total number of nodes in the network.

v. If the nodes in a network that is based upon the physical hierarchical topology are required to perform any processing upon the data that is transmitted between nodes in the network, the nodes that are at higher levels in the hierarchy will be required to perform more processing operations on behalf of other nodes than the nodes that are lower in the hierarchy.

Hybrid network topologies

The hybrid topology is a type of network topology that is composed of one or more interconnections of two or more networks that are based upon different physical topologies or a type of network topology that is

composed of one or more interconnections of two or more networks that are based upon the same physical topology, but where the physical topology of the network resulting from such an interconnection does not meet the definition of the original physical topology of the interconnected networks (e.g., the physical topology of a network that would result from an interconnection of two or more networks that are based upon the physical star topology might create a hybrid topology which resembles a mixture of the physical star and physical bus topologies or a mixture of the physical star and the physical tree topologies, depending upon how the individual networks are interconnected, while the physical topology of a network that would result from an interconnection of two or more networks that are based upon the physical distributed bus network retains the topology of a physical distributed bus network).

Star-bus

A type of network topology in which the central nodes of one or more individual networks that are based upon the physical star topology are connected together using a common 'bus' network whose physical topology is based upon the physical linear bus topology, the endpoints of the common 'bus' being terminated with the characteristic impedance of the transmission medium where required – e.g., two or more hubs connected to a common backbone with drop cables through the port on the hub that is provided for that purpose (e.g., a properly configured 'uplink' port) would comprise the physical bus portion of the physical star-bus topology, while each of the individual hubs, combined with the individual nodes which are connected to them, would comprise the physical star portion of the physical star-bus topology.

Star-of-stars (Hierarchical star)

A type of network topology that is composed of an interconnection of individual networks that are based upon the physical star topology connected together in a hierarchical fashion to form a more complex network – e.g., a top level central node which is the 'hub' of the top level physical star topology and to which other second level central nodes are attached as the 'spoke' nodes, each of which, in turn, may also become the central nodes of a third level physical star topology.

Notes:

1.) The physical hierarchical star topology is not a combination of the physical linear bus and the physical star topologies, as cited in some texts, as there is no common linear bus within the topology, although the top level 'hub' which is the beginning of the physical hierarchical star topology may be connected to the backbone of another network, such as a common carrier, which is, topologically, not considered to be a part of the local network – if the top level central node is connected to a backbone that is considered to be a part of the local network, then the resulting network topology would be considered to be a hybrid topology that is a mixture of the topology of the backbone network and the physical hierarchical star topology.

2.) The physical hierarchical star topology is also sometimes incorrectly referred to as a physical tree topology, since its physical topology is hierarchical, however, the physical hierarchical star topology does not have a structure that is determined by a branching factor, as is the case with the physical tree topology and, therefore, nodes may be added to, or removed from, any node that is the 'hub' of one of the individual physical star topology networks within a network that is based upon the physical hierarchical star topology.

3.) The physical hierarchical star topology is commonly used in 'outside plant' (OSP) cabling to connect various buildings to a central connection facility, which may also house the 'demarcation point' for the connection to the data transmission facilities of a common carrier, and in 'inside plant' (ISP) cabling to connect multiple wiring closets within a building to a common wiring closet within the same building, which is also generally where the main backbone or trunk that connects to a larger network, if any, enters the building.

Star-wired ring

A type of hybrid physical network topology that is a combination of the physical star topology and the physical ring topology, the physical star portion of the topology consisting of a network in which each of the nodes of which the network is composed are connected to a central node with a point-to-point link in a 'hub' and 'spoke' fashion, the central node being the 'hub' and the nodes that are attached to the central node being the 'spokes' (e.g., a collection of point-to-point links from the peripheral nodes that converge at a central node) in a fashion that is identical to the physical star topology, while the physical ring portion of the topology consists of circuitry within the central node which routes the signals on the network to each of the connected nodes sequentially, in a circular fashion.
Note: In an 802.5 Token Ring network the central node is called a Multistation Access Unit (MAU).

Hybrid mesh

A type of hybrid physical network topology that is a combination of the physical partially connected topology and one or more other physical topologies the mesh portion of the topology consisting of redundant or alternate connections between some of the nodes in the network – the physical hybrid mesh topology is commonly used in networks which require a high degree of availability..

The network topologies mentioned above are only a general representation of the kinds of topologies used in computer network and are considered basic topologies.

Intranets, Extranets, and Internets

Now that you have a basic understanding of various types of networks, let's discuss some other terms that are used to describe locality: intranet, extranet, and internet.

An intranet is basically a network that is local to a company. In other words, users from within this company can find all of their resources without having to go outside of the company.
An intranet can include LANs, private WANs and MANs.

An extranet is an extended intranet, where certain internal services are made available to known external users or external business partners at remote locations.

The connections between these external users and the internal resource are typically secured via a firewall.

An internet is used when unknown external users need to access internal resources in your network.
In other words, any company might have a web site that sells various products, and it wants any external user to be able to access this service.

There is a difference between the terms internet and Internet.
The lowercase internet refers to any type of network connection where external users access publicly available resources.
The Internet is the main public network that most companies and people use when accessing external resources.
Typically, a firewall is used to secure your internal resources from external users.

The TCP/IP and OSI Networking Models

The term networking model, or networking architecture, refers to an organized description of all the functions needed for useful communications to occur.
Individual protocols and hardware specifications then are used to implement the functions described in the networking model.
When multiple computers and other networking devices implement these protocols, which, in turn, implement the functions described by the networking model, the computers can successfully communicate.

You can think of a networking model like you think of a set of architectural plans for building a house.

Sure, you can build a house without the architectural plans, but it will work better if you follow the plans.

And because you probably have a lot of different people working on building your house, such as framers, electricians, bricklayers, painters, and so on, it helps if they can all reference the same plan.

Similarly, you could build your own network, write your own software, build your own networking cards, and create a network without using any existing networking model.

However, it is much easier to simply buy and use products that already conform to some well-known Networking model.

And because the products from different vendors conform to the same networking architectural model, the products should work well together.

Then the functions of the Networking model are:

describe data transfer standards, a framework (guideline) for network implementation, troubleshooting and divides complex functions in to simpler components.

- Reference model types:

- TCP/IP
- OSI

1-The TCP/IP Protocol Architecture

TCP/IP defines a large collection of protocols that allow computers to communicate.

By implementing the required protocols defined in TCP/IP a computer can be relatively confident that it can communicate with other computers that also implement TCP/IP.

An easy comparison can be made between telephones and computers that use TCP/IP. I can go to the store and buy a phone from one of a dozen different vendors. When I get home, I plug the phone in to the wall socket, and it works.

The phone vendors know the standards for phones in their country and build their phones to match those standards.

Similarly, a computer that implements the standard networking protocols defined by TCP/IP can communicate with other computers that also use the TCP/IP standards.

Like other networking architectures, TCP/IP classifies the various protocols into different categories.

Table 2-2 outlines the main categories in the TCP/IP architectural model.

Table 2-2 TCP/IP Architecture	**Layer**	**Example Protocols**
	Application	HTTP, POP3, SMTP
	Transport	TCP, UDP
	Internetwork	IP
	Network interface	Ethernet, Frame Relay

CPTCP/IP Architectural Model and Example Protocols

The TCP/IP model represented in column 1 of the table lists the four layers of TCP/IP, and column 2 of the table lists several of the most popular TCP/IP protocols.

If someone makes up a new application, the protocols used directly by the application would be considered to

Be application layer protocols.

When the World Wide Web (WWW) was first created, a new application layer protocol was created for the purpose of asking for web pages and receiving the contents of the web pages.

Similarly, the network interface layer includes protocols and standards such as Ethernet.

If someone makes up a new type of LAN, those protocols would be considered to be a part of the networking interface layer.

In the next several sections, we will learn the basics about each of these four layers in the TCP/IP architecture and how they work together.

TCP/IP application layer protocols provide services to the application software running on a computer.

The application layer does not define the application itself, but rather it defines services that applications need - like the ability to transfer a file in the case of HTTP.

In short, the application layer provides an interface between software running on a computer and the network itself.

2- OSI Reference Model

OSI is the Open System Interconnection reference model for communications.

The OSI reference model consists of seven layers. Each layer defines a set of typical

Networking functions.

The OSI model can be used as a standard of comparison to other networking models.

The upper layers of the OSI reference model (application, presentation, and session—Layers

7, 6, and 5) define functions focused on the application. The lower four layers (transport,

Network, data link, and physical—Layers 4, 3, 2, and 1) define functions focused on end-to end delivery of the data.

Application
Presentation
Session
Transport
Network
Data Link
Physical

OSI Reference Model Layer Definitions:

Layer 7: Layer 7 defines the interface between the communications software and any applications that need to communicate outside the computer on which the application resides.

For example, a web browser is an application on a computer.

The browser needs to get the contents of a web page; OSI Layer 7 defines the protocols used on behalf of the application to get the web page.

Layer 6: This layer's main purpose is to define data formats, such as ASCII text, EBCDIC text, binary, and BCD. Encryption also is defined by OSI as a presentation layer service.

For example, FTP enables you to choose binary or ASCII transfer.

If binary is selected, the sender and receiver do not modify the contents of the file.

If ASCII is chosen, the sender translates the text from the sender's character set to a standard ASCII and sends the data.

The receiver translates back from the standard ASCII to the character set used on the receiving computer.

Layer 5: The session layer defines how to start, control, and end conversations (called sessions).

This includes the control and management of multiple bidirectional messages so that the application can be notified if only some of a series of messages are completed.

This allows the presentation layer to have a seamless view of an incoming stream of data.

The presentation layer can be presented with data if all flows occur in some cases.

For example, an automated teller machine transaction in which you withdraw cash from your checking account should not debit your account and then fail before handing you the cash, recording the transaction even though you did not receive money.

The session layer creates ways to imply which flows are parts of the same session and which flows must complete before any are considered complete.

Layer 4: Layer 4 protocols provide a large number of services. Although Layers 5 through 7 focus on issues related to the application, Layer 4 focuses on issues related to data delivery to the other computer—for instance, error recovery, segmentation of large application data blocks into smaller ones for transmission, and reassembly of those blocks of data on the receiving computer.

Layer 3: This layer defines end-to-end delivery of packets. To accomplish this, the network layer defines logical addressing so that any endpoint can be identified.

It also defines how routing works and how routes are learned so that the packets can be delivered.

The network layer of OSI defines most of the details that a Cisco router considers when routing.

For example, IP running in a Cisco router is responsible for examining the destination IP address of a packet, comparing that address to the IP routing table, fragmenting the packet if the outgoing interface requires smaller packets, and queuing the packet to be sent out to the interface.

Layer 2: The data link layer (Layer 2) specifications deliver data across one particular link or medium.

These protocols are necessarily concerned with the type of media in question; for example, 802.3 and 802.2 define Ethernet for the IEEE, which are referenced by OSI as valid data link layer (Layer 2) protocols.

Other protocols, such as High-Level Data Link Control (HDLC) for a point-to-point WAN link, deal with the different details of a WAN link.

Layer 1: These physical layer (Layer 1) specifications, which are also typically standards from other organizations that are referred to by OSI, deal with the physical characteristics of the transmission medium.
Connectors, pins, use of pins, electrical currents, encoding, and light modulation are all part of different physical layer specifications.
Multiple specifications sometimes are used to complete all details of
The physical layer. For example, RJ-45 defines the shape of the connector and the number of wires or pins in the cable. Ethernet and 802.3 define the use of wires or pins 1, 2, 3, and 6. So, to use a Category 5 cable with an RJ-45 connector for an Ethernet connection, Ethernet and RJ-45 physical layer specifications are used.

Layer Name	Examples
Application (Layer 7)	Telnet, HTTP, FTP, WWW browsers, NFS, SMTP gateways (Eudora, CC:mail), SNMP
Presentation (Layer 6)	JPEG, ASCII, EBCDIC, TIFF, GIF, PICT, encryption, MPEG,

	MIDI
Session (Layer 5)	RPC, SQL, NFS, NetBIOS names, AppleTalk ASP, DECnet SCP
Transport (Layer 4)	TCP, UDP, SPX
Network (Layer 3)	IP, IPX, AppleTalk DDP
Data link (Layer 2)	EEE 802.3/802.2, HDLC, Frame Relay, PPP, FDDI, ATM, IEEE 802.5/802.2
Physical (Layer 1)	EIA/TIA-232, V.35, EIA/TIA-449, RJ-45, Ethernet, 802.3, 802.5, B8ZS

Tab. OSI Reference Model—Example Protocols

The following list summarizes the benefits of layered protocol specifications:

_ Easier to learn—Humans can more easily discuss and learn about the many details of a protocol specification.

_ Easier to develop—reduced complexity allows easier program changes and faster product evolution.

_ Multivendor interoperability—creating products to meet the same networking standards means that computers and networking gear from multiple vendors can work in the same network.

_ Modular engineering—One vendor can write software that implements higher layers— for example, a web browser—and another can write software that implements the lower layers— for example, Microsoft's built-in TCP/IP software in its operating systems.

Chapter 2

Transmission Media

What is Network Cables?

The term *cable* refers to a combination of plastics, metal wires, optical fibers, possibly rubber, and other materials molded into a cord of varying lengths.

Well, that's at least a formal definition.

People see cables every day. The power cords that go from the electrical wall socket to each of your electrically powered appliances and lamps at home are all cables.

There are cables protruding from the back of your PC. And for networking, the phone cord stretching from the wall outlet to your phone is actually a networking cable.

Most networking cables use either copper wires inside the cable to transfer an electrical signal, or glass fiber inside the cable to transfer optical light signals.

So, many people refer to cabling as *wiring* just because the vast majority of networking cables are actually copper wire cables.

The wire cables also sometimes are called *copper cabling*, just because the most popular metal to use in the cable is copper.

When sending an electrical signal over a cable, the signal introduces a magnetic field and also introduces radio frequency interference.

Translation: When the cable is in use, it emits radiation that can interfere with other signals in other wires or signals that pass through the air.

When one wire affects another in this manner, it is commonly referred to as *crosstalk*. So, the various national governments tend to regulate how much of these unwanted physics effects are allowed.

These metallic wire cables are designed to reduce the effects of the radiation and interference.

The wires can be affected by outside interference as well. Nearby cables can interfere with the transmission on the cable, actually changing the electrical signal and causing bit errors.

So, electrical cables create their own emissions and are susceptible to problems from the emissions from other sources, particularly nearby cables.

The most popular way today to reduce the effects of emissions is to transmit over a pair of wires and twist those two wires together.

By using an opposite current on each wire, each wire produces an identical magnetic field, but in an opposite direction. It's sort of like having two equal-power magnets of the same polarity, both trying to pull things toward them.

Essentially,

Twisted-pair wiring is used in today's most popular electrical (wire) networking cables.

The other popular way to reduce the emissions of copper cabling is to shield the wires.

That means that the wires have some material placed around them, using a material that blocks most of the electromagnetic radiation.

By shielding the cables, the cables emit less radiation.

Unfortunately, shielding the wires makes the cable more expensive and less flexible. The need to add more materials to a cable to shield the cable increases materials and manufacturing costs for the cables.

You need a lot of cables to build a typical enterprise network, so the extra cost does add up.

If the cable does not bend easily, you might not be able to run it in tight spaces behind walls, in ceilings, into where the wall plate sits behind the wall, and so on.

So, inflexible cabling could require you to open walls in the building to make a new space for the cables to run—costing time and money.
The following sections discuss

The types of cables used in networks are: Unshielded Twisted Pair (UTP) Cable, Shielded Twisted Pair (STP) Cable, Coaxial Cable **,** Fiber Optic Cable, Wireless LANs and Cable Installation Guides

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).

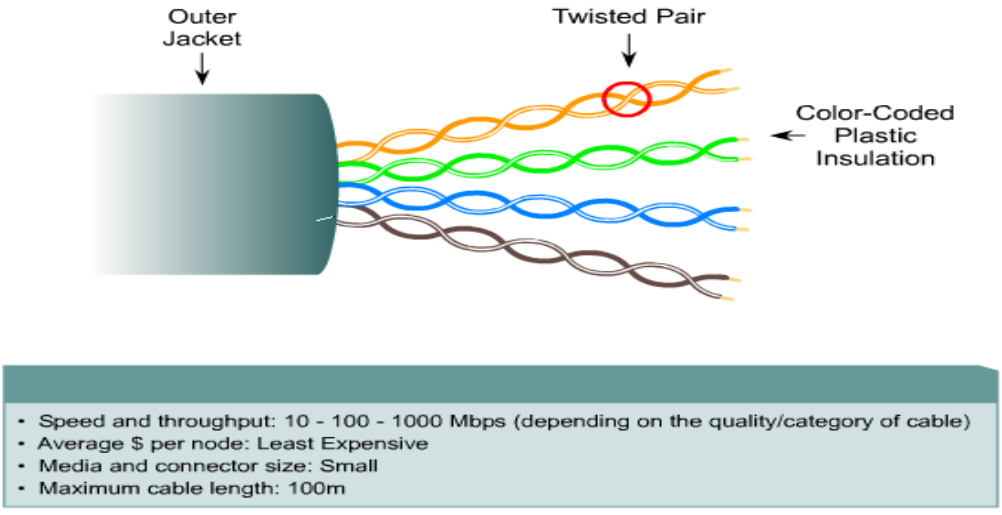


Fig.1. Unshielded twisted pair

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 is 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 five categories of wire.

UTP Category	Max Speed Rating	Description
1	—	Used for telephones but not for data.
2	4 Mbps	Originally intended to support Token Ring over UTP.
3	10 Mbps	Can be used for telephones as well. Popular option for Ethernet in years past, if CAT3 cabling for phones already was in place.
4	16 Mbps	Intended for the fast Token Ring speed option.
5	1 Gbps	Very popular for cabling to the desktop.
5e	1 Gbps	Lower emissions, more expensive than CAT5, but better for Gigabit Ethernet.
6	1 Gbps+	Intended as a replacement for CAT5e, with capabilities to support multigigabit speeds when standards are created.

Tab.1-Categories of Unshielded Twisted Pair

You can buy the best cable you can afford; most schools purchase Category 3 or Category 5. If you are designing a 10 Mbps Ethernet network and are considering the cost savings of buying Category 3 wire instead of Category 5, remember that the Category 5 cable will provide more "room to grow" as transmission technologies increase. Both Category 3 and Category 5 UTP have a maximum segment length of 100 meters. In Florida, Category 5 cable is required for retrofit grants. 10BaseT refers to the specifications for unshielded twisted pair cable (Category 3, 4, or 5) carrying Ethernet signals. Category 6 is relatively new and is used for gigabit connections.

Using UTP cable to connect devices:

There are three ways to connect devices by UTP by: Straight cable, Cross cable or Roll over cable.

Straight-Through or Crossover cables

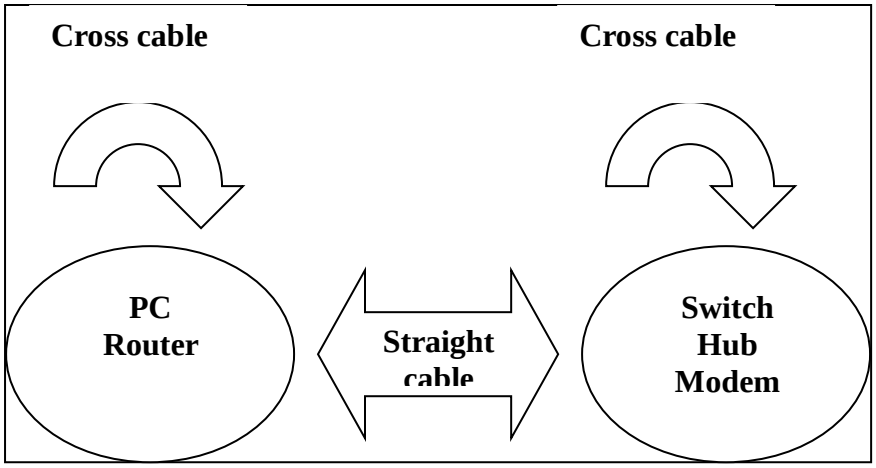


Fig.2.

Unshielded Twisted Pair Connector

The standard connector for unshielded twisted pair cabling is an RJ-45 connector. It is a plastic connector that looks like a large telephone-style connector (See fig. 2). A slot allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.

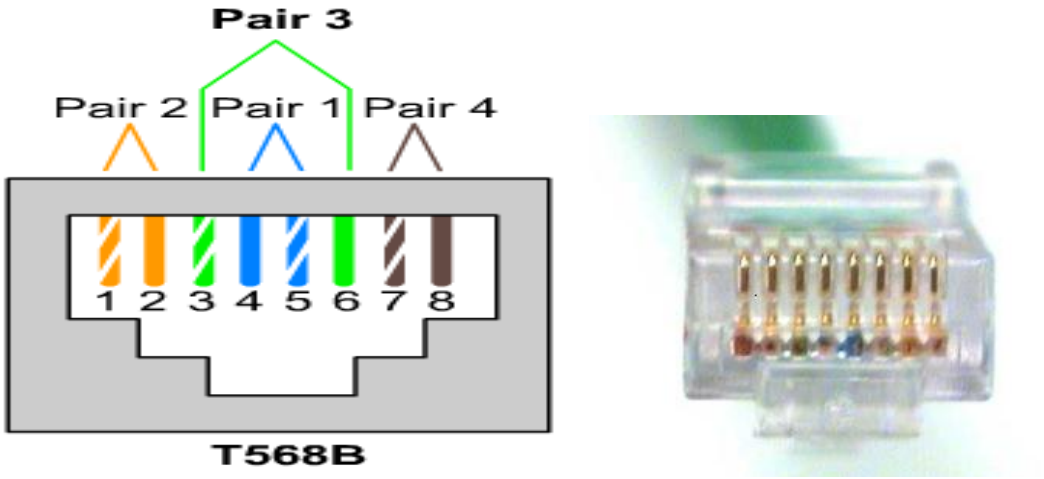


Fig. 2. RJ-45 connector

Shielded Twisted Pair (STP) Cable

A disadvantage of UTP is that it may be susceptible to radio and electrical frequency interference. Shielded twisted pair (STP) is suitable for environments with electrical interference; however, the extra shielding can make the cables quite bulky. Shielded twisted pair is often used on net works using Token Ring topology.

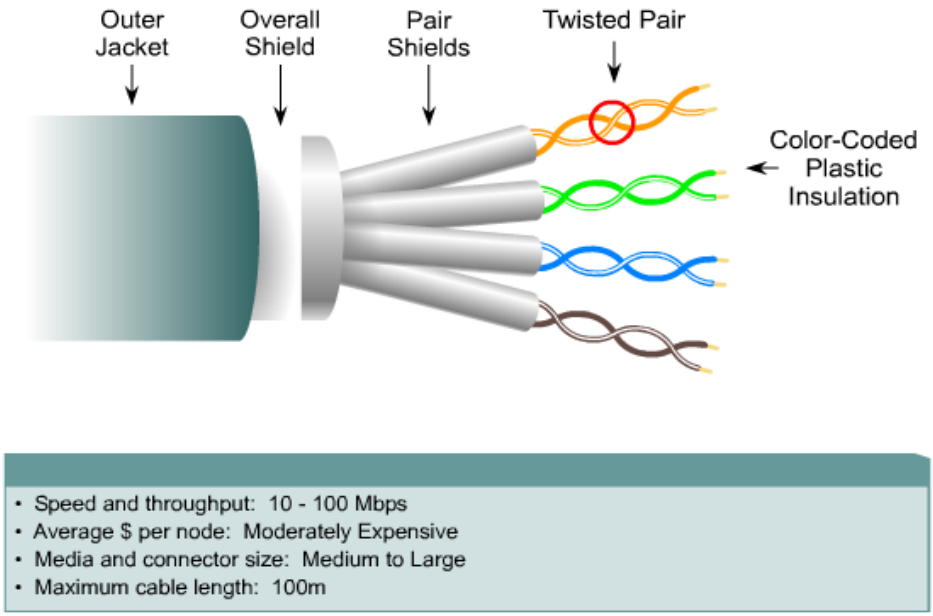


Fig.2.Sshielded twisted pair

Coaxial Cable

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield (See fig. 3). The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.

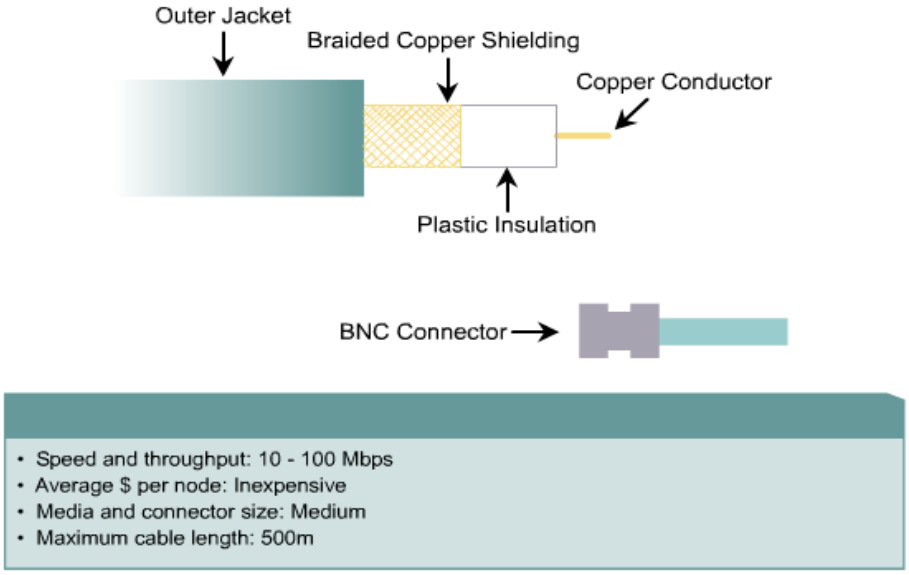


Fig. 3. Coaxial cable

Although coaxial cabling is difficult to install, it is highly resistant to signal interference. In addition, it can support greater cable lengths between network devices than twisted pair cable. The two types of coaxial cabling are thick coaxial and thin coaxial.

Thin coaxial cable is also referred to as thinnet. 10Base2 refers to the specifications for thin coaxial cable carrying Ethernet signals. The 2 refers to the approximate maximum segment length being 200 meters. In

actual fact the maximum segment length is 185 meters. Thin coaxial cable is popular in school networks, especially linear bus networks.

Thick coaxial cable is also referred to as thicknet. 10Base5 refers to the specifications for thick coaxial cable carrying Ethernet signals. The 5 refers to the maximum segment length being 500 meters. Thick coaxial cable has an extra protective plastic cover that helps keep moisture away from the center conductor. This makes thick coaxial a great choice when running longer lengths in a linear bus network. One disadvantage of thick coaxial is that it does not bend easily and is difficult to install.

Coaxial Cable Connectors

The most common type of connector used with coaxial cables is the Bayone-Neill-Concelman (BNC) connector (See fig. 4). Different types of adapters are available for BNC connectors, including a T-connector, barrel connector, and terminator. Connectors on the cable are the weakest points in any network. To help avoid problems with your network, always use the BNC connectors that crimp, rather than screw, onto the cable.

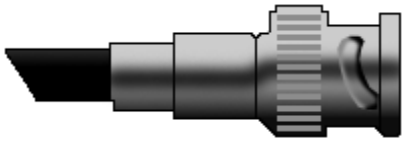


Fig. 4. BNC connector

Fiber Optic Cable

Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials (See fig. 5). It transmits light rather than electronic signals eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of

electrical interference. It has also made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.

Fiber optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pair. It also has the capability to carry information at vastly greater speeds. This capacity broadens communication possibilities to include services such as video conferencing and interactive services. The cost of fiber optic cabling is comparable to copper cabling; however, it is more difficult to install and modify. 10BaseF refers to the specifications for fiber optic cable carrying Ethernet signals.

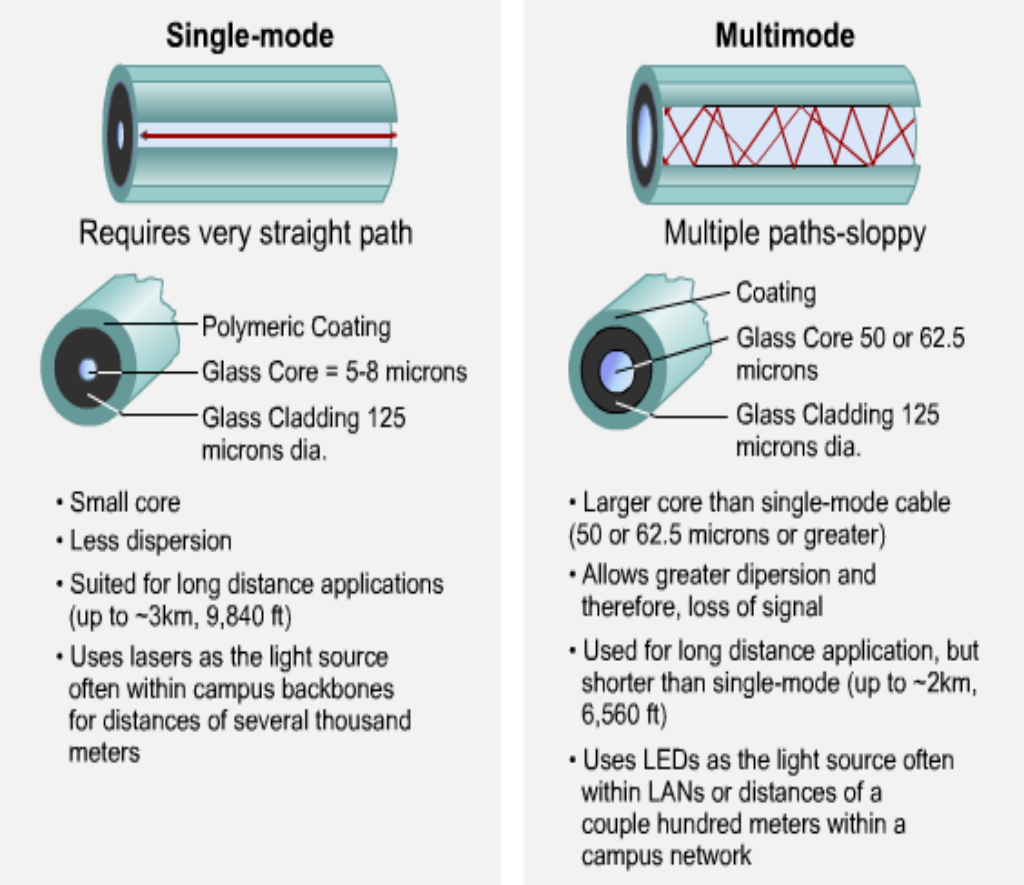


Fig. 5. Fiber optic cable

Some Facts about fiber optic cables are that the Outer insulating jacket is made of Teflon or PVC;

The Kevlar fiber helps to strengthen the cable and prevent breakage.

A plastic coating is used to cushion the fiber center And a Center (core) is made of glass or plastic fibers.

Fiber Optic Connector

The most common connector used with fiber optic cable is an ST connector. It is barrel shaped, similar to a BNC connector. A newer connector, the SC, is becoming more popular. It has a squared face and is easier to connect in a confined space.

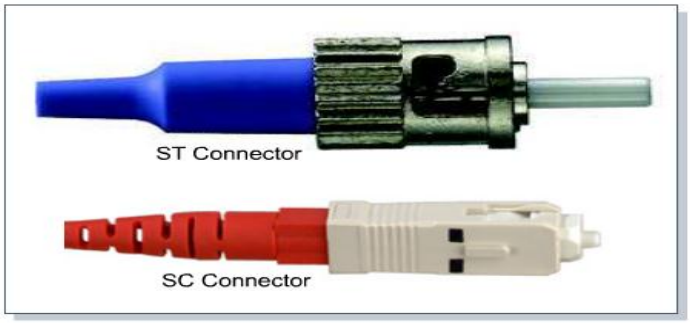


Fig. 6. Fiber optic connectors

Ethernet Cable Summary:

Specification	Cable Type	Maximum length
10BaseT	Unshielded Twisted Pair	100 meters
10Base2	Thin Coaxial	185 meters
10Base5	Thick Coaxial	500 meters
10BaseF	Fiber Optic	2000 meters
100BaseT	Unshielded Twisted Pair	100 meters
100BaseTX	Unshielded Twisted Pair	220 meters

Tab. 2-Ethernet Cable Summary

Wireless LANs

Not all networks are connected with cabling; some networks are wireless. Wireless LANs use high frequency radio signals, infrared light beams, or lasers to communicate between the workstations and the file server or hubs. Each workstation and file server on a wireless network has some sort of transceiver/antenna to send and receive the data. Information is relayed between transceivers as if they were physically connected. For longer distance, wireless communications can also take place through cellular telephone technology, microwave transmission, or by satellite.

Wireless networks are great for allowing laptop computers or remote computers to connect to the LAN. Wireless networks are also beneficial in older buildings where it may be difficult or impossible to install cables.

The two most common types of infrared communications used in schools are line-of-sight and scattered broadcast. Line-of-sight communication means that there must be an unblocked direct line between the workstation and the transceiver. If a person walks within the line-of-sight while there is a transmission, the information would need to be sent again. This kind of obstruction can slow down the wireless network.

Scattered infrared communication is a broadcast of infrared transmissions sent out in multiple directions that bounces off walls and ceilings until it

eventually hits the receiver. Networking communications with laser are virtually the same as line-of-sight infrared networks.

Wireless LANs have several disadvantages. They provide poor security, and are susceptible to interference from lights and electronic devices. They are also slower than LANs using cabling.

Installing Cable - Some Guidelines

When running cable, it is best to follow a few simple rules:

- Always use more cable than you need. Leave plenty of slack.
- Test every part of a network as you install it. Even if it is brand new, it may have problems that will be difficult to isolate later.
- Stay at least 3 feet away from fluorescent light boxes and other sources of electrical interference.
- If it is necessary to run cable across the floor, cover the cable with cable protectors.
- Label both ends of each cable.
- Use cable ties (not tape) to keep cables in the same location together.

Chapter 3

Local Area Network

The objectives covered in this chapter are as follows:

This chapter covers the following hardware technologies as they can be applied to LAN design:

- Repeaters
- Hubs
- Bridges
- Switches
- Routers
- Layer 3 switches
- Combining hubs, switches, and routers

Repeaters

Repeaters are the basic unit used in networks to connect separate segments.

Repeaters take incoming frames, regenerate the preamble, amplify the signals, and send the frame out all other interfaces.

Repeaters operate in the physical layer of the OSI model. Because repeaters are not

Aware of packets or frame formats, they do not control broadcasts or collision domains.

Repeaters are said to be protocol transparent because they are not aware of upper-layer protocols such as IP, IPX, and so on.

Repeaters introduce a small amount of latency, or delay, when propagating the frames.

A transmitting device must be able to detect a collision with another device within the specified time after the delay introduced by the cable segments and repeaters is factored in.

The 512 bit-time specification also governs segment lengths.

Hubs

With the increasing density of LANs in the late 80s and early 90s, hubs were introduced to concentrate Thinnest and 10BaseT networks in the wiring closet. Traditional hubs operate on the physical layer of the OSI model and perform the same functions as basic repeaters.

Bridges

Bridges are used to connect separate segments of a network.
They differ from repeaters in that bridges are intelligent devices that operate in the data link layer of the OSI model.
Bridges control the collision domains on the network.
Bridges also learn the MAC layer addresses of each node on each segment and on which interface they are located.
For any incoming frame, bridges forward the frame only if the destination MAC address is on another port or if the bridge is not aware of its location.
The latter is called flooding.

Bridges filter any incoming frames with destination MAC addresses that are on the same segment from where the frame arrives; they do not forward the frame on.
Bridges are store and forward devices. They store the entire frame and verify the CRC before forwarding.
If a CRC error is detected, the frame is discarded. Bridges are protocol transparent; they are not aware of the upper-layer protocols like IP, IPX, and AppleTalk. Bridges are designed to flood all unknown and broadcast traffic.

Bridges implement the Spanning-Tree Protocol to build a loop free network topology. Bridges communicate with each other, exchanging information such as priority and bridge interface MAC addresses.
They select a root bridge and then implement the Spanning-Tree Protocol.
Some interfaces are placed in a hold state, while other bridges will have interfaces in forwarding mode.

Switches

Switches are the evolution of bridges. Switches use fast integrated circuits that reduce the latency that bridges introduce to the network.
Switches also enable the capability to run in cut-through mode.
In cut-through mode, the switch does not wait for the entire frame to enter its buffer; instead, it forwards the frame after it has read the destination MAC address field of the frame.
Cut-through operation increases the probability that error frames are propagated on the network, which increases CRC and runt frames on the network.
Because of these problems, most switches today perform store-and-forward operation with CRC check as bridges do.
Note that it controls collision domains but not broadcast domains.
Switches have characteristics similar to bridges; however, they have more ports and run faster.
Switches keep a table of MAC addresses per port, and they implement Spanning-Tree Protocol.
Switches also operate in the data link layer and are protocol transparent.
Each port on a switch is a separate collision domain but part of the same broadcast domain. Switches do not control broadcasts on the network.

Routers

Routers make forwarding decisions based on network layer addresses. In addition to controlling collision domains, routers control broadcast domains.
Each interface of a router is a separate broadcast domain defined by a subnet and a mask.
Routers are protocol aware, which means they are capable of forwarding packets of routed protocols such as IP, IPX, Decnet, and AppleTalk.
Each interface is a broadcast and a collision domain.
Routers exchange information about destination networks by using one of several routing protocols.
The following are lists of routing protocols. The lists are divided by the protocols that can be routed.

For routing TCP/IP:

• Enhanced Interior Gateway Routing Protocol (EIGRP)
• Open Shortest Path First (OSPF)
• Routing Information Protocol (RIP)
• Intermediate System-to-Intermediate System (ISIS)
• Protocol Independent Multicast (PIM)

For routing Novell:

• Novell Routing Information Protocol (Novell RIP)

• NetWare Link Services Protocol (NLSP)
• Enhanced Interior Gateway Routing Protocol (EIGRP)

For routing AppleTalk:
• Routing Table Maintenance Protocol (RTMP)
• Enhanced Interior Gateway Routing Protocol (EIGRP)

Routers are the preferred method of forwarding packets between networks of differing media, such as Ethernet to Token Ring, Ethernet to FDDI, or Ethernet to Serial.
They also provide methods to filter traffic based on the network layer address, route redundancy, load balancing, hierarchical addressing, and multicast routing.

LAN switching

Is a form of packet switching used in Local Area Network. Switching technologies are crucial to network design, as they allow traffic to be sent only where it is needed in most cases, using fast and hardware-based methods.

Layer 2
switching

Layer 2 switching is hardware based which means it uses the media access control address (MAC address) from the host's network interface cards (NICs) to decide where to forward frames. Switches use application-specific integrated circuits (ASICs) to build and maintain

filter tables (also known as MAC address tables). One way to think of a layer 2 switch is as a multiport bridge.

Layer 2 switching provides the following

- Hardware-based bridging (MAC)
- Wire speed
- High speed
- Low latency
- Low cost

Layer 2 switching is highly efficient because there is no modification to the data packet, only to the frame encapsulation of the packet, and only when the data packet is passing through dissimilar media (such as from Ethernet to FDDI). Layer 2 switching is used for workgroup connectivity and network segmentation (breaking up collision domains). This allows a flatter network design with more network segments than traditional 10BaseT shared networks. Layer 2 switching has helped develop new components in the network infrastructure

- Server farms — Servers are no longer distributed to physical locations because virtual LANs can be created to create broadcast domains in a switched internetwork. This means that all servers can be placed in a central location, yet a certain server can still be part of a workgroup in a remote branch, for example.
- Intranets — Allows organization-wide client/server communications based on a Web technology.

These new technologies are allowing more data to flow off of local subnets and onto a routed network, where a router's performance can become the bottleneck.

Limitations

Layer 2 switches have the same limitations as bridge networks. Remember that bridges are good if a network is designed by the 80/20 rule: users spend 80 percent of their time on their local segment.

Bridged networks break up collision domains, but the network remains one large broadcast domain. Similarly, layer 2 switches (bridges) cannot break up broadcast domains, which can cause performance issues and limits the size of your network. Broadcast and multicasts, along with the slow convergence of spanning tree, can cause major problems as the network grows. Because of these problems, layer 2 switches cannot completely replace routers in the internetwork.

Layer 3 switching

The only difference between a layer 3 switch and a router is the way the administrator creates the physical implementation. Also, traditional routers use microprocessors to make forwarding decisions, and the switch performs only hardware-based packet switching. However, some traditional routers can have other hardware functions as well in some of the higher-end models. Layer 3 switches can be placed anywhere in the network because they handle high-performance LAN traffic and can cost-effectively replace routers. Layer 3 switching is all hardware-based packet forwarding, and all packet forwarding is handled by hardware ASICs. Layer 3 switches really are no different functionally than a traditional router and perform the same functions, which are listed here

- Determine paths based on logical addressing

- Run layer 3 checksums (on header only)
- Use Time to Live (TTL)
- Process and responds to any option information
- Can update Simple Network Management Protocol (SNMP) managers with Management Information Base (MIB) information
- Provide Security

The benefits of layer 3 switching include the following

- Hardware-based packet forwarding
- High-performance packet switching
- High-speed scalability
- Low latency
- Lower per-port cost
- Flow accounting
- Security
- Quality of service (QoS)

Layer 4 switching

Layer 4 switching is considered a hardware-based layer 3 switching technology that can also consider the application used (for example, Telnet or FTP).

Layer 4 switching provides additional routing above layer 3 by using the port numbers found in the Transport layer header to make routing decisions.

These port numbers are found in Request for Comments (RFC) 1700 and reference the upper-layer protocol, program, or application.

Layer 4 information has been used to help make routing decisions for quite a while. For example, extended access lists can filter packets based on layer 4 port numbers. Another example is accounting information gathered by NetFlow switching in Cisco's higher-end routers.

The largest benefit of layer 4 switching is that the network administrator can configure a layer 4 switch to prioritize data traffic by application, which means a QoS can be defined for each user.

For example, a number of users can be defined as a Video group and be assigned more priority, or band-width, based on the need for video conferencing.

However, because users can be part of many groups and run many applications, the layer 4 switches must be able to provide a huge filter table or response time would suffer. This filter table must be much larger than any layer 2 or 3 switch. A layer 2 switch might have a filter table only as large as the number of users connected to the network and may be even less if some hubs are used within the switched fabric. However, a layer 4 switch might have five or six entries for each and every device connected to the network. If the layer 4 switch does not have a filter table that includes all the information, the switch will not be able to produce wire-speed results.

Multi-layer switching (MLS)

Multi-layer switching combines layer 2, 3, and 4 switching technologies and provides high-speed scalability with low latency. It accomplishes this high combination of high-speed scalability with low latency by using huge filter tables based on the criteria designed by the network administrator.

Multi-layer switching can move traffic at wire speed and also provide layer 3 routing, which can remove the bottleneck from the network routers. This technology is based on the idea of route once, switch many.

Multi-layer switching can make routing/switching decisions based on the following

- MAC source/destination address in a Data Link frame
- IP source/destination address in the Network layer header
- Protocol field in the Network layer header
- Port source/destination numbers in the Transport layer header

There is no performance difference between a layer 3 and a layer 4 switch because the routing/switching is all hardware based

Layer-1 hubs versus higher-layer switches

A network hub, or repeater, is a fairly unsophisticated cast device, and rapidly becoming obsolete. Hubs do not manage any of the traffic that comes through them. Any packet entering a port is broadcast out or "repeated" on every other port, save the port of entry. Since every packet is repeated on every other port, packet collisions result, which slows down the network.

Hubs have actually become hard to find, due to the widespread use of switches. There are specialized applications where a hub can be useful, such as copying traffic to multiple network sensors. High end switches have a feature which does the same thing called port mirroring. There is no longer any significant price difference between a hub and a low-end switch

Combining Hubs, Switches, and Routers

Available in Ethernet and Fast Ethernet, hubs are best used in small networks where there are few nodes on the segment.
Hubs do not control the broadcasts nor do they filter collision domains on the network.
If higher bandwidth is required, use 100 Mbps hubs. When the number of nodes on the network grows, move to switches.
With the cost of switch ports comparable to hubs, use switches as the basic network Connectivity devices on the network. Switches reduce collisions and resolve media contention on the network by providing a collision domain per port.

Replace hubs with switches if the utilization is over 40 percent on Ethernet networks or above 70 percent on Token Ring and FDDI networks.
Switches cannot resolve broadcast characteristics of protocols; use routing to resolve protocol-related problems.
The repeaters are pushed to the outer layer of the design, connecting to switches.
Switches control the collision domains.
Fast Layer 3 switches are used for routing between LAN segments, and the router provides access to the WAN.

Chapter 4

Computer Network Design

.

This chapter begins with an introduction to the lifecycle of a network and a network design methodology based on the lifecycle is presented. Each phase of the network design process is explored in detail, starting with how to identify customer requirements, including organizational and technical goals and constraints. As many customers build on an existing network and at existing sites.

.

This chapter also covers the steps of network design and contains an overview of all the major topics of network design

Customer Objectives

The design of network is based on the customer's objectives. In other words, you will

Need to find out what the customer wants to solve. You then must create a design that solves the networking problem or issue the customer is having.

The first step in network design is to obtain the customer's requirements. To obtain a complete

Picture of the customer's objectives, the engineer needs to document the client's business requirements, technical requirements, and any business and political constraints.

Business Requirement of the customer

For this aspect of determining the customer's objectives, think about the purpose of the project.

Project how the business will improve. Find out if the network is affecting the company's capability or effectiveness to develop, produce, and track products. Find out if any business applications are being affected.

Determine whether the company will be audited.

Scalability is a very important consideration, and it is wise for the network designer to build a network that can scale. You should figure out how much the company will grow in one year or in five years.

Business Drivers for a New Network Architecture

New business requirements, the growth of applications, and the evolution of IT combine to drive the need for new network architecture. In today's business environment, intense competition and time-to-market pressures are prompting enterprises to look for new IT solutions that can help them better respond to market and customer demands. Consumers are asking for new products and service offerings—and they want them fast. They are also demanding improved customer service, enhanced customization flexibility, and greater security, all at a lower cost.

Intelligence in the Network

Integrating intelligence into the network involves aligning network and business requirements. To accommodate today's and tomorrow's network requirements, the Cisco vision of the future includes the Intelligent Information Network (IIN), a strategy that addresses how the network is integrated with businesses and business priorities. This vision encompasses the following features:

- Integration of networked resources and information assets that have been largely unlinked.
- Intelligence across multiple products and infrastructure layers.
- Active participation of the network in the delivery of services and applications.

Technical Requirements for the Customer:

Think about the type of technical problems you are trying to solve. Consider the network's topology.

For example, it may be difficult to introduce Ethernet to a customer that religiously uses Token Ring.

Also consider the company's use of modern technologies. Find out whether the client is willing to experiment with the latest, bleeding-edge technologies.

Keep in mind scaling issues; decide whether switched Ethernet will provide the necessary bandwidth or

Whether Fast Ethernet is necessary to scale the network.

Technical requirements can be divided into the following areas

- Performance requirements
- Applications requirements
- Network management requirements
- Security requirements

Performance Requirements

Determine the following performance requirements:

- Identify any issues concerning network latency and response times.
- Find out if there is high utilization on LAN segments or WAN links.
- Determine how often the WAN links go down.

Application Requirements

Consider existing application integration. The network design will need to seamlessly accommodate the existing applications, investigate the current application flows, and incorporate those into the network design.

Determine the following application requirements:

- Find out what new applications have been introduced to the network.
- Determine the number of users using these applications.

• Find out the traffic flow for these applications.

• Identify what new protocols are being introduced to the network.

• Determine what applications are used during the daytime hours and what are used during the nighttime hours.

• Determine the time of day that represents the peak usage hours of applications.

Network Management Requirements

Determine the following network management requirements:

• Determine how the network is managed.

• Determine whether there is a network management station to view network performance and faults.

• Ascertain whether there are any accounting and security management requirements.

• Find out whether the staff is training on the network management applications.

• Find out whether there is a station for configuration management.

Requirements Security

Determine the following security requirements:

• Determine what type of security is required.

• Find out what external connections are present in the network and why they are there.

- Determine whether additional security is required on Internet connections.

Network Design Methodology

The network design methodology presented in this section is derived from the Cisco Prepare, Plan, Design, Implement, Operate, and Optimize (PPDIOO) methodology, which reflects a network's lifecycle. The following sections describe the PPDIOO phases and their relation to the network design methodology, and the benefits of the lifecycle approach to network design.

Design as an Integral Part of the PPDIOO Methodology

The PPDIOO network lifecycle, illustrated in Figure 2-5, reflects the phases of a standard
network's lifecycle. As shown in this figure, the PPDIOO lifecycle phases are separate, yet closely
related.

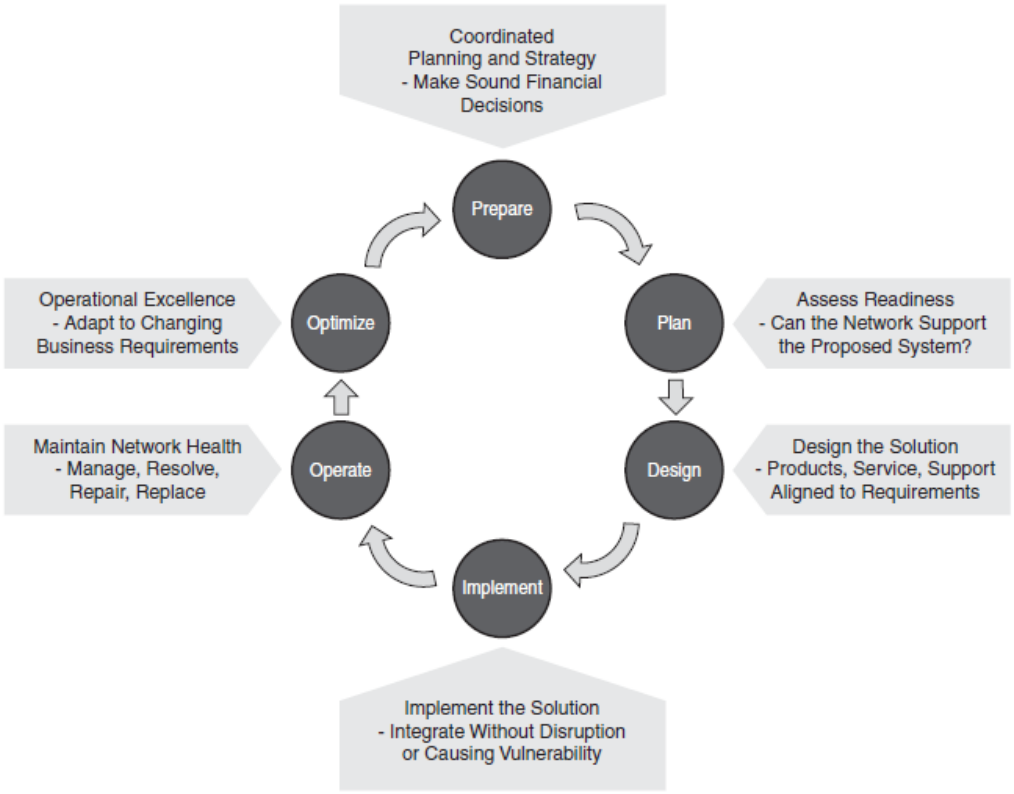


Figure 2-5 PPDIOO Network Lifecycle Influences Design

The following describes each PPDIOO phase:

■ **Prepare phase**: The Prepare phase involves establishing the organizational (business) requirements, developing a network strategy, and proposing a high-level conceptual architecture, identifying technologies that can best support the architecture. Financial justification for the network strategy is established by assessing the business case for the proposed architecture.

■**Plan phase:** This phase involves identifying the network requirements, which are based on the goals for the network, where the network will be installed, who will require which network services, and so forth. The Plan phase also involves assessing the sites where the network will be installed

and any existing networks, and performing a gap analysis to determine if the existing system infrastructure, sites, and the proposed system. A project plan helps manage the tasks, responsibilities, critical milestones, and resources required to implement the changes to the network. The project plan should align with the scope, cost, and resource parameters established in the original business requirements. The output of this phase is a set of network requirements.

■ **Design phase:** The initial requirements determined in the Plan phase drive the network design specialists' activities. These specialists design the network according to those initial requirements, incorporating any additional data gathered during network analysis. network audit (when upgrading an existing network) and through discussion with managers and network users. The network design specification that is produced is a comprehensive detailed design that meets current business and technical requirements and incorporates specifications to support availability, reliability, security, scalability, and performance. This design specification provides the basis for the implementation activities.

■ **Implement phase:** Implementation and verification begins after the design has been approved. The network and any additional components are built according to the design specifications, with the goal of integrating devices without disrupting the existing network or creating points of vulnerability.

■ **Operate phase:** Operation is the final test of the design's appropriateness. The Operate phase involves maintaining network health through day-to-day operations, which might include maintaining high

availability and reducing expenses. The fault detection and correction and performance monitoring that occur in daily operations provide initial data for the network lifecycle's Optimize phase.

■ **Optimize phase:** The Optimize phase is based on proactive network management, the goal of which is to identify and resolve issues before real problems arise and the organization is affected. Reactive fault detection and correction (troubleshooting) are necessary when proactive management cannot predict and mitigate the failures.

Benefits of the Lifecycle Approach to Network Design

The network lifecycle approach provides many benefits, including the following:

■ **lowering the total cost of network ownership:**

— Identifying and validating technology requirements

— Planning for infrastructure changes and resource requirements

— Developing a sound network design aligned with technical requirements and business goals.

— Accelerating successful implementation

— Improving the efficiency of the network and of the staff supporting it

— Reducing operating expenses by improving the efficiency of operation processes and tools.

■ **Increasing network availability:**

— Assessing the state of the network's security and its ability to support the proposed design.

— Specifying the correct set of hardware and software releases and keeping them operational and current.

— Producing a sound operational design and validating network operation.

— Staging and testing the proposed system before deployment.

— Improving staff skills.

■ **Improving business agility:**

— Establishing business requirements and technology strategies.

— Readying sites to support the system to be implemented.

— Integrating technical requirements and business goals into a detailed design and demonstrating that the network is functioning as specified.

— Expertly installing, configuring, and integrating system components.

— Continually enhancing performance.

■ **Accelerating access to applications and services:**

— Assessing and improving operational preparedness to support current and planned network technologies and services.

— Improving service-delivery efficiency and effectiveness by increasing availability, resource capacity, and performance.

— Improving the availability, reliability, and stability of the network and the applications running on it.

— Managing and resolving problems affecting the system and keeping software applications current.

Steps for Network design

The steps for designing a network are as follows:

1- Gather information to support the business and technical requirements.

2- Assess the current network.

3- Consider the applications involved.

4- Design the local-area networks.

5- Design the wide-area network.

6- Design for specific network protocols.

7-Create the design document and select network management applications.

8- Test the design.

This section provides an overview of these steps.

1- Gather information to support the business and technical requirements

The section "Customer Objectives," earlier in this chapter, covers step 1. "Assessing the Existing Network and Identifying Customer Objectives," covers this step in much more detail.

Assess the Current Network

This is the step during which you collect all data pertaining to physical, logical, traffic, and management information of the network.

Physical Assessment

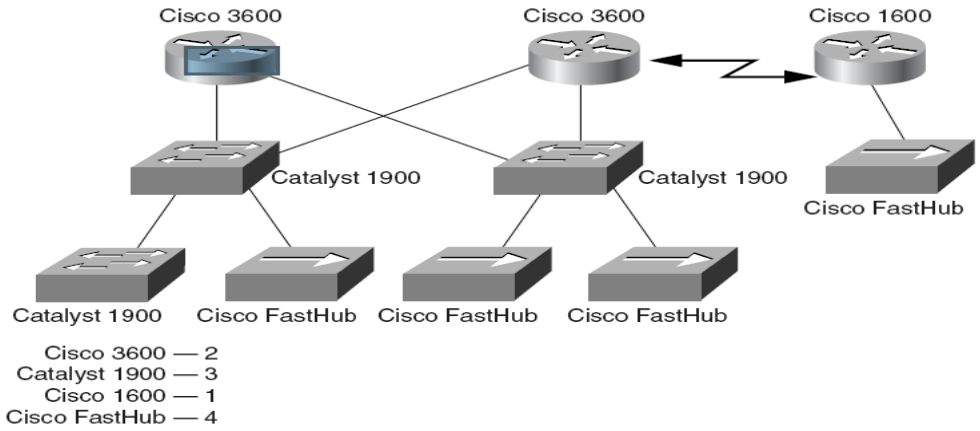
To perform a physical assessment, you need to document the physical topology of the network.

Create a diagram with all routers, switches, and hubs. For example, in Figure 1-2, a list of network devices is created and the type and amount of devices is documented.

Physical connectivity between devices should also be documented; also list the speed and type of media used between devices.

Figure 1-2 Physical Assessment

For Example (Cisco Company)



You will also need to list the LAN technologies being used. The following is a list of possible
LAN technologies:

- Ethernet
- Token Ring
- FDDI
- Fast Ethernet
- Gigabit Ethernet

Finally, document the WAN circuit information and list the WAN technologies being used.

The following is a list of possible WAN technologies used:

- Frame Relay
- Private lines
- ATM
- ISDN
- X.25

Logical Assessment

To perform the logical assessment, determine the following:

- The protocols that are being routed.
- The IP address assignment scheme.

Traffic Assessment

To perform the traffic assessment, determine the following:

- Document the traffic flows on the network.
- Determine how much traffic is on each segment.
- Locate the servers.
- Determine how much traffic is local to the segment and how much traffic is external.

Management Assessment

Determine the current tools used for network management:

- Determine whether the customer has the necessary tools to manage the network.
- Determine whether there is a management station

• Verify whether there are capacities or performance monitoring tools.

• Determine whether a network protocol analyzer is available for LAN segment Troubleshooting.

Consider the Applications Involved

A good designer needs to take into consideration the applications that the network supports.

The only reason the network is there is to provide a highway on which application information can flow.

Never ignore the applications in use.

Local Area Network Design

The designer must be able to design local-area networks that meet the customer's objectives on performance and scalability.

He must design networks in a hierarchical manner to provide scalable solutions.

He also must decide where to use hubs, switches, and routers to separate broadcast and collision domains.

Know the differences between Layer 2 and Layer 3 switching as well.

Hierarchical Network Model

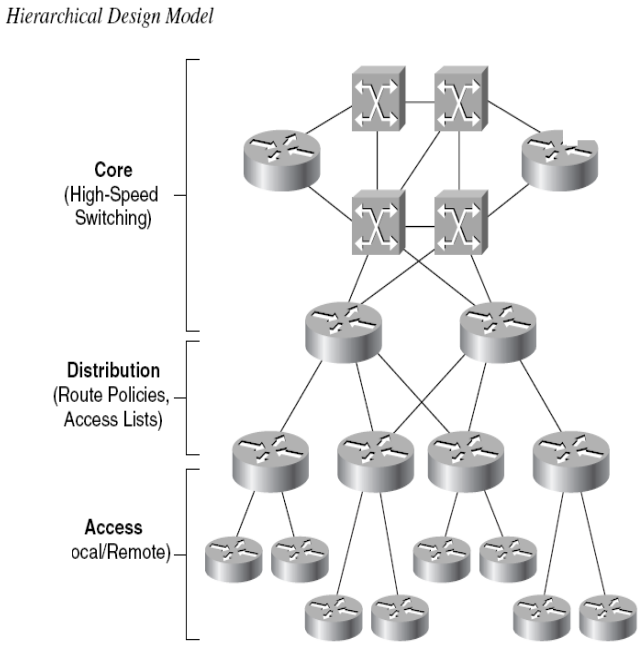


Fig. shows Hierarchal Network Model

The three-layer hierarchical model helps you design campus networks.

This model is used to simplify designing, implementing, and managing large-scale networks.

With traditional network designs, it was common practice to place the networking services at the center of the network and the users at the periphery.

However, many things in networking have changed over the past decade, including

Advancements in applications, developments in graphical user interfaces (GUIs), the

Proliferation of multimedia applications, the explosion of the Internet, and fast-paced

Changes in your users' traffic patterns.

It contains three layers: core, distribution, and access.

A well-designed network typically follows this topology.

The following sections cover the functions of the three layers, including the devices that function at the various layers.

Core Layer

The core layer, as its name suggests, is the backbone of the network. It provides a high speed connection between the different distribution layer devices.

Because of the need for high-speed connections, the core consists of high-speed switches and will not, typically, perform any type of packet or frame manipulations, such as filtering or Quality of Service.

Because switches are used at the core, the core is referred to as a layer-2 core.

The traffic that traverses the core is typically to access enterprise corporate resources: connections to the Internet, gateways, e-mail servers, and corporate applications.

Distribution Layer

Of the three layers, the distribution layer performs most of the connectivity tasks. In
Larger networks, routers are used at the distribution layer to connect the access layers
To the core. For smaller networks, sometimes switches are used. The responsibilities of the distribution layer include the following:

■ Containing broadcasts between the layers
■ securing traffic between the layers
■ providing a hierarchy through layer-3 logical addressing and route summarization
■ translating between different media types

Routers give you by far the most flexibility in enforcing your company's networking policies, since routers deal with logical addresses.
And because routers are used at the distribution layer, the implementation of your policies, at least most of them, is done here.

One of the main functions traffic that the access layer devices create. of the distribution layer is to contain broadcast and multicast.

If a broadcast storm is created in one access layer, or there is a large amount of multicast traffic from a real-time video stream, the distribution layer, by default, confines this traffic in the access layer and thus prevents
it from creating problems in other areas.

Providing Logical Addressing

Routers also provide for logical addressing of devices in your network. This makes it
Much easier to implement your networking policies, including filtering and QoS since
You control how addresses are assigned to machines: it is very difficult to do this with
Layer-2MACaddresses. Another advantage that logical addressing provides is that, again, with the correct address layout in your network, you should be able to create a highly scalable, hierarchical network.

Performing Security

Another function of this layer is to enforce your security policies. Because switches are used at the core and access layers, security is not typically implemented at these layers, given the issues of filtering MAC addresses.

Since routers deal with logical addresses, however, they make it much easier to implement your policies.

Connecting Different Media Types

If you have two different media types that you want to connect, Token Ring and

Ethernet, for instance, a router is the best solution; and since routers are used at the distribution layer, this is where this conversion takes place.

"Data Link Layer", bridges are not very good at performing translations between different media types.

However, routers do not have this problem.

Routers don't translate between media types.

Instead, they perform a de-encapsulation and encapsulation process.

From layer-2, the router strips off the frame and passes up the packet to layer-3.

At layer-3, the router makes its routing decision and queues the packet on the outbound interface.

Once again, at layer-2, the packet is encapsulated in the frame type for the corresponding media type the interface is connected to.

Access Layer

The bottom layer of the three-layer hierarchical model is the access layer. Actually, the access layer is at the periphery of your campus network, separated from the core layer by the distribution layer.

The main function of the access layer is to provide the user's initial connection to your network.

Typically, this connection is provided by a switch, or sometimes, a hub.

Sometimes if the user works at a small branch office or home office, this device can also be a router.

But in most cases, the connection is provided by a switch.

Connections

Remember that the three-layer hierarchical model is a logical, not a physical, representation.

For example, sometimes the distribution layer device might contain both switches and routers.

This combination of devices can provide both layer-2 and layer-3 functionality at the distribution layer.

This kind of setup is common at the distribution layer: sometimes the routing function sits inside the chassis of the switch, and sometimes the routing function is in a separate chassis.

No matter what configuration is used, it is important that you configure the layer-3 device correctly to create a boundary between the access and core layer devices.

The switching function that can be provided by the distribution layer is used to connect departmental services that the access layer devices commonly access.

LAN Protocols

You need to understand the characteristics of LAN protocols, including physical distance limitations of LAN technologies:

Ethernet (10Base2, 10Base5, and 10BaseT), Fast Ethernet, Gigabit Ethernet, Token Ring, and FDDI.

Use these technologies to satisfy requirements ranging from user workstations to high-bandwidth servers.

LAN Physical Design

Select the equipment to be used, keeping in mind the LAN technologies and the number of ports required for the network.

Design the Wide-Area Network

The Designer must design WAN networks that meet the customer's objectives of performance and scalability. Design

networks in a hierarchical manner. And plan for bandwidth capacity to provide scalable solutions.

Determine the WAN technologies to use, and plan for router solutions.

Transport Selection

Decide on the WAN technology to use. The following list will help you make this decision:

• Use leased lines where traffic flows are constant between point-to-point locations.

• Use ISDN for on-demand access to remote offices and for backup for another link type.

• Use Frame Relay as a high-bandwidth, cost-effective transport.

This very popular WAN protocol provides permanent virtual circuits (PVC) between routers.

Frame Relay provides characteristics such as congestion notification, discard eligibility (DE) bit, bursting, and the capability to have several PVCs on a physical port.

These and other features (such as cost) made Frame Relay a very popular WAN technology in the 1990s.

• Use X.25 when the reliability of the WAN links is suspect.

X.25 is an older WAN technology that is still widely in use and can be found running over low-speed (9600 to 64000 bps) lines.

Throughput using X.25 suffers in comparison to Frame Relay due to X.25's additional error checking.

• Use ATM when high bandwidth (155+ Mbps) is required on the core. ATM offers different Quality of Service (QoS) types, allowing traffic with varying tolerances for bandwidth and latency to travel over the same network.

Bandwidth Planning

The Designer must look at the applications being deployed at remote sites and decide on the sizing
Of WAN circuits. Rely on the analysis of existing traffic flows and past experience to help determine an appropriate bandwidth size for a circuit.
If WAN circuit utilization is more than70 percent for a long period of time, the circuit bandwidth should be increased.
When planning bandwidth allocation, consider the following:

• The type of servers that are located at the remote site.
• Whether the applications in the hub site will be accessed remotely and whether the intranet Web sites will be accessed remotely.
• Whether there are Microsoft Domain controllers or MS Exchange servers at the remote sites.
• Whether there are any database applications

Physical Design

Select the equipment to be used, keeping in mind the technologies and the number of interfaces required for the network.

Design for Specific Network Protocols

In this step, take into consideration the type of protocols to be used on the network.

IP

The designer needs to design an IP address assignment scheme based on a hierarchical model.
Use VLSMs to assign networks based on the number of devices and areas on the network.
A hierarchical model for address assignment with VLSMs allows the network to take advantage
Of routing summary features supported by protocols such as EIGRP and OSPF.
Choose routing protocols that will not add significant traffic to the network.
Understand the differences between distance vector and link-state routing protocols.

Novell

Create IPX addressing schemes. Consider the broadcast characteristics of Novell's distance vector Routing Information Protocol (RIP) and Service Advertising Protocol (SAP).
RIP broadcasts its table every 60 seconds; SAP also broadcasts the SAP table every 60 seconds.
Use access lists to filter specific SAP broadcasts.
Consider the design of the distance vector IPX RIP Versus NetWare Link-Services Protocol (NLSP). EIGRP can be used on WAN links to reduce IPX traffic.

AppleTalk

Consider the AppleTalk cable ranges to assign to each interface and the zones for each area.
To overcome the limitations of the AppleTalk routing protocol RTMP, use methods such as AURP or EIGRP on the WAN.

Bridging

Transparent and source-route bridged networks have size limitations and do not scale well. To reduce the traffic of bridged protocols, limit the size of bridged networks.

Test the Design

After a design has been proposed, the next step is to verify that the design will work. For large networks, a prototype can be built; for smaller networks a pilot can be devised.

Chapter 5

Introduction to WAN Technologies – A Technical Overview

This chapter introduces the various protocols and technologies used in wide-area network (WAN) environments. Topics summarized here include point-to-point links, circuit switching, packet switching, virtual circuits, dialup services, and WAN devices.

What Is a WAN?

A *WAN* is a data communications network that covers a relatively broad geographic area that often uses transmission facilities provided by common carriers, such as telephone companies. WAN technologies generally function at the lower three layers of the OSI reference model: the physical layer, the data link layer, and the network layer. Figure 1 illustrates the relationship between the common WAN technologies and the OSI model.

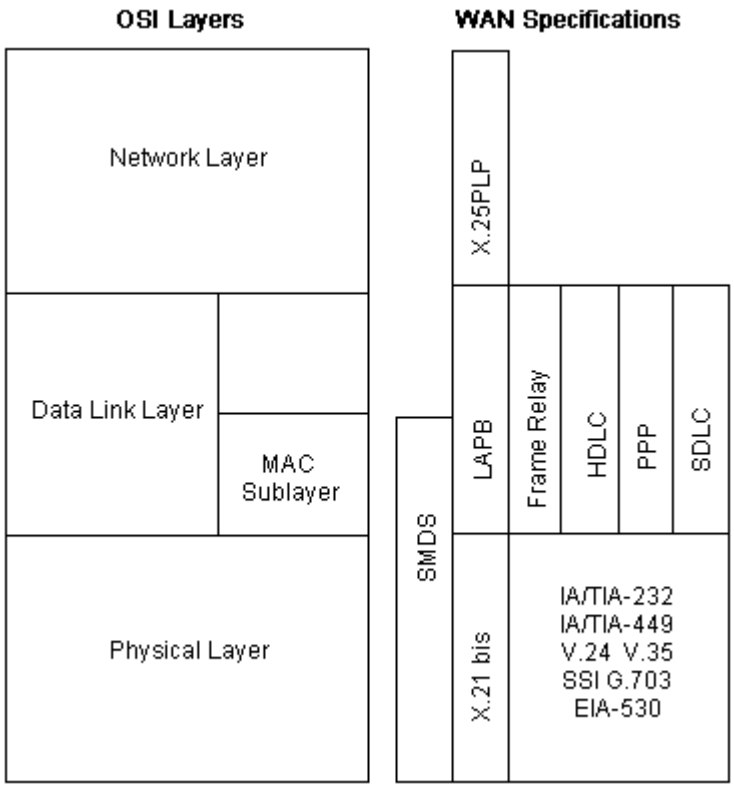


Figure 1: WAN Technologies Operate at the Lowest Levels of OSI Model

WANs are used to connect LANs and other types of networks together, so that users and computers in one location can communicate with users and computers in other locations. Many WANs are built for one particular organization and are private. Others, built by Internet service providers, provide connections from an organization's LAN to the Internet. WANs are often built using leased lines. At each end of the leased line, a router connects to the LAN on one side and a hub within the WAN on the other. Leased lines can be very expensive. Instead of using leased lines, WANs can also be built using less costly circuit switching or packet switching methods. Network protocols including TCP/IP deliver transport and addressing functions. Protocols including Packet over SONET/SDH, MPLS, ATM and Frame relay are often used by service providers to deliver the links that are used in WANs. X.25 was an important early WAN protocol, and is often considered to be the "grandfather" of Frame Relay as many of the underlying protocols and functions of X.25 are still in use today (with upgrades) by Frame Relay.

Research into wide area networks can be broken down into three areas: Mathematical models, network emulation and network simulation.

Several options are available for WAN connectivity:

Table shows several options are available for WAN connectivity

Option:	Description	Advantages	Disadvantage	Bandwidt	Sample protocol

			s	h range	s used
Leased line	Point-to-Point connection between two computers or Local Area Networks (LANs)	Most secure	Expensive		PPP, HDLC, SDLC, HNAS
Circuit switching	A dedicated circuit path is created between end points. Best example is dialup connections	Less Expensive	Call Setup	28 Kb/s - 144 Kb/s	PPP, ISDN
Packet switching	Devices transport packets via a shared single point-to-point or		Shared media across link		X.25 Frame-Relay

	point-to-multipoint link across a carrier internetwork. Variable length packets are transmitted over Permanent Virtual Circuits (PVC) or Switched Virtual Circuits (SVC)				
Cell Switching	Similar to packet switching, but uses fixed length cells instead of variable length packets.	best for simultaneous use of Voice and data	Overhead can be considerable		ATM

	Data is divided into fixed-length cells and then transported across virtual circuits				

Transmission rate usually range from 1200 bits/second to 6 Mbit/s, although some connections such as ATM and Leased lines can reach speeds greater than 156 Mbit/s. typical communication links used in WANs are telephone lines, microwave links & satellite channels.

Recently with the proliferation of low cost of Internet connectivity many companies and organizations have turned to VPN (Virtual Private Network) to interconnect their networks, creating a WAN in that way.

Point-to-Point Links

A point-to-point link provides a single, pre-established WAN communications path from the customer premises through a carrier network such as a telephone company, to a remote network. Point-to-point lines are usually leased from a carrier and thus are often called leased lines. For a point-to-point line, the carrier allocates pairs of wire and facility hardware to your line only. These circuits are generally priced based on bandwidth required and distance between the two connected points. Point-to-point links are generally more expensive than shared

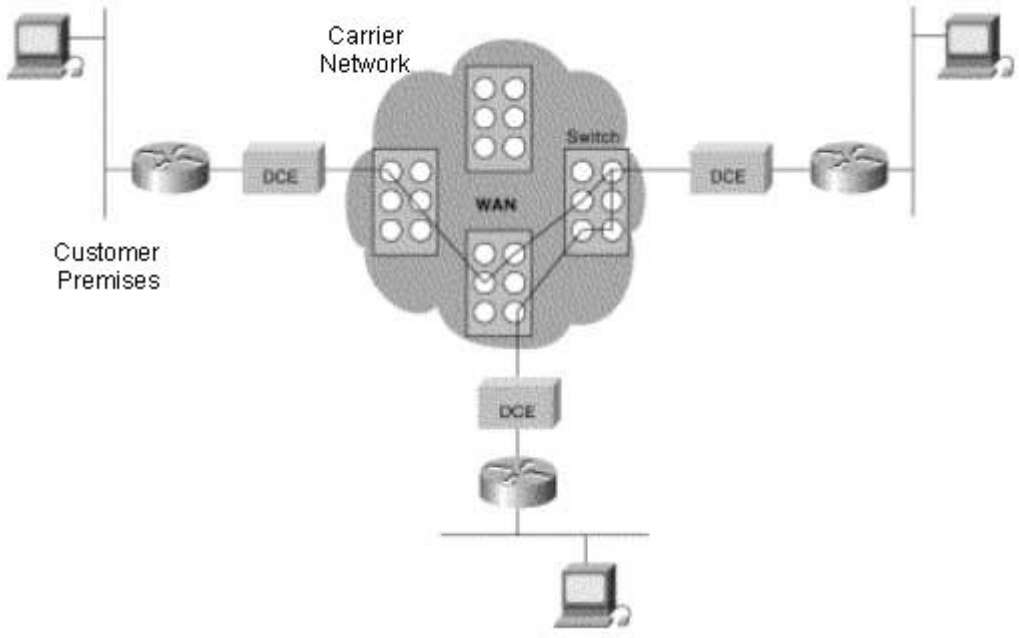
services such as Frame Relay. Figure 2 illustrates a typical point-to-point link through a WAN.

Figure 2. A Typical Point-to-Point Link Operates Through a WAN to a Remote Network

Circuit Switching

Switched circuits allow data connections that can be initiated when needed and terminated when communication is complete. This works much like a normal telephone line works for voice communication. Integrated Services Digital Network (ISDN) is a good example of circuit switching. When a router has data for a remote site, the switched circuit is initiated with the circuit number of the remote network. In the case of ISDN circuits, the device actually places a call to the telephone number of the remote ISDN circuit. When the two networks are connected and authenticated, they can transfer data. When the data transmission is complete, the call can be terminated. Figure 3 illustrates an example of this type of circuit.

Figure 3. A Circuit-Switched WAN Undergoes a Process Similar to That Used for a Telephone Call



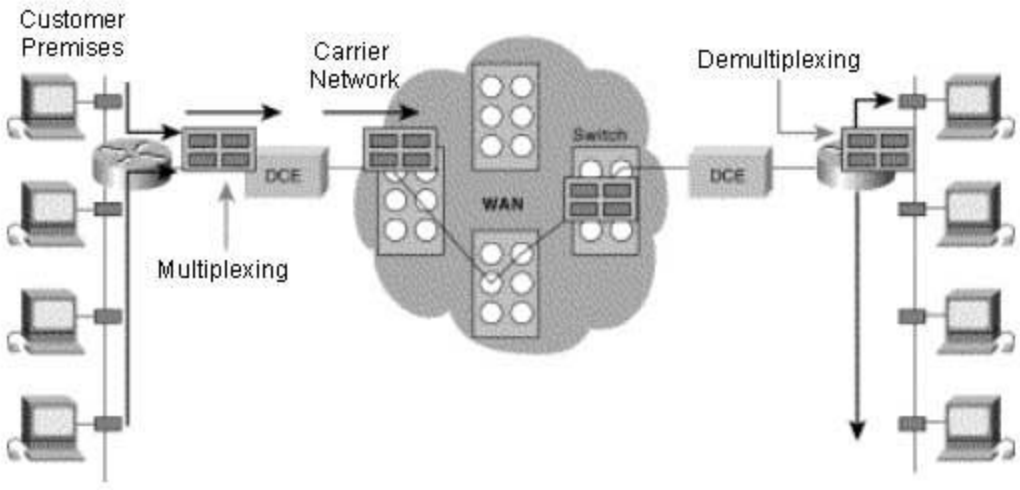
Packet Switching

Packet switching is a WAN technology in which users share common carrier resources. Because this allows the carrier to make more efficient use of its infrastructure, the cost to the customer is generally much better than with point-to-point lines. In a packet switching setup, networks have connections into the carrier's network, and many customers share the carrier's network. The carrier can then create virtual circuits between customers' sites by which packets of data are delivered from one to the other through the network. The section of the carrier's network that is shared is often referred to as a cloud.

Some examples of packet-switching networks include Asynchronous Transfer Mode (ATM), Frame Relay, Switched Multimegabit Data Services (SMDS), and X.25. Figure 4 shows an example packet-switched circuit.

The virtual connections between customer sites are often referred to as a virtual circuit.

Figure 4. Packet Switching Transfers Packets across a Carrier Network



WAN Virtual Circuits

A virtual circuit is a logical circuit created within a shared network between two network devices. Two types of virtual circuits exist: switched virtual circuits (SVCs) and permanent virtual circuits (PVCs).

SVCs are virtual circuits that are dynamically established on demand and terminated when transmission is complete. Communication over an SVC consists of three phases: circuit establishment, data transfer, and circuit termination. The establishment phase involves creating the virtual circuit between the source and destination devices. Data transfer involves transmitting data between the devices over the virtual circuit, and the circuit termination phase involves tearing down the virtual circuit between the source and destination devices. SVCs are used in situations in which data transmission between devices is sporadic, largely because SVCs increase bandwidth used due to the circuit establishment and

termination phases, but they decrease the cost associated with constant virtual circuit availability.

PVC is a permanently established virtual circuit that consists of one mode: data transfer. PVCs are used in situations in which data transfer between devices is constant. PVCs decrease the bandwidth use associated with the establishment and termination of virtual circuits, but they increase costs due to constant virtual circuit availability. PVCs are generally configured by the service provider when an order is placed for service.

WAN Dialup Services

Dialup services offer cost-effective methods for connectivity across WANs. Two popular dialup implementations are dial-on-demand routing (DDR) and dial backup.

DDR is a technique whereby a router can dynamically initiate a call on a switched circuit when it needs to send data. In a DDR setup, the router is configured to initiate the call when certain criteria are met, such as a particular type of network traffic needing to be transmitted. When the connection is made, traffic passes over the line. The router configuration specifies an idle timer that tells the router to drop the connection when the circuit has remained idle for a certain period.

Dial backup is another way of configuring DDR. However, in dial backup, the switched circuit is used to provide backup service for another type of circuit, such as point-to-point or packet switching. The router is configured so that when a failure is detected on the primary circuit, the

dial backup line is initiated. The dial backup line then supports the WAN connection until the primary circuit is restored. When this occurs, the dial backup connection is terminated.

WAN Devices

WANs use numerous types of devices that are specific to WAN environments. WAN switches, access servers, modems, CSU/DSUs, and ISDN terminal adapters are discussed in the following sections. Other devices found in WAN environments that are used in WAN implementations include routers, ATM switches, and multiplexers.

WAN Switch

A *WAN switch* is a multiport internetworking device used in carrier networks. These devices typically switch such traffic as Frame Relay, X.25, and SMDS, and operate at the data link layer of the OSI reference model. Figure 5 illustrates two routers at remote ends of a WAN that are connected by WAN switches.

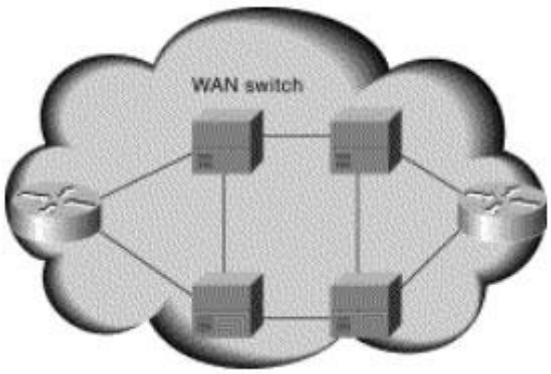


Figure 5: Two Routers at Remote Ends of a WAN Can Be Connected by WAN Switches

Access Server

An access server acts as a concentration point for dial-in and dial-out connections. Figure 6 illustrates an access server concentrating dial-out connections into a WAN.

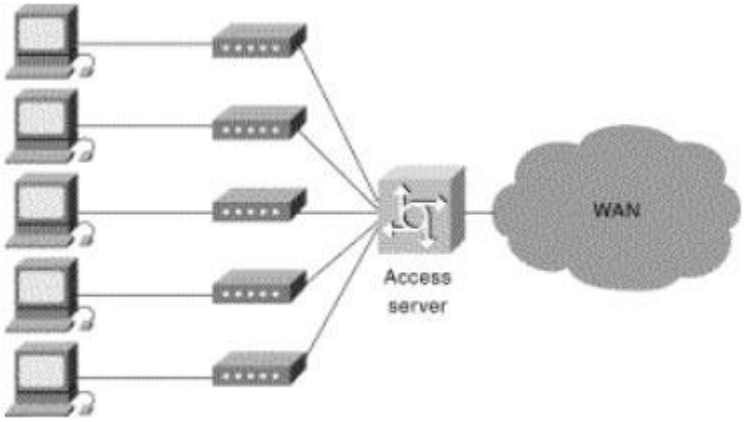
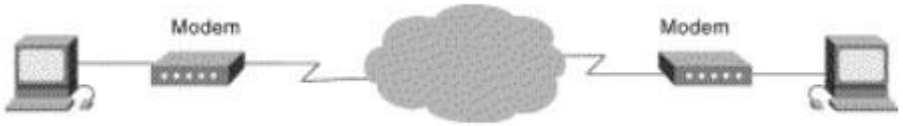


Figure 6: An Access Server Concentrates Dial-Out Connections into a WAN

Modem

A modem is a device that interprets digital and analog signals, enabling data to be transmitted over voice-grade telephone lines. At the source, digital signals are converted to a form suitable for transmission over analog communication facilities. At the destination, these analog signals are returned to their digital form. Figure 7 illustrates a simple modem-to-modem connection through a WAN.

Figure 7: A Modem Connection through a WAN Handles Analog and Digital Signals



CSU/DSU

A channel service unit/digital service unit (CSU/DSU) is a digital-interface device used to connect a router to a digital circuit like a T1. The CSU/DSU also provides signal timing for communication between these devices. Figure 8 illustrates the placement of the CSU/DSU in a WAN implementation.

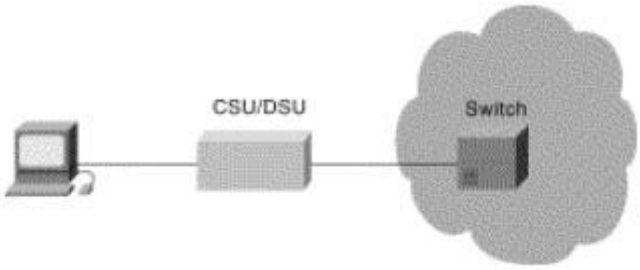


Figure 8: The CSU/DSU Stands between the Switch and the Terminal

ISDN Terminal Adapter

An ISDN terminal adapter is a device used to connect ISDN Basic Rate Interface (BRI) connections to other interfaces, such as EIA/TIA-232 on a router. A terminal adapter is essentially an ISDN modem, although it is called a terminal adapter because it does not actually convert analog to digital signals.

Packet-Switching Services

Service providers offer services that can be categorized as *packet-switching services*.

In a packet-switched service, physical WAN connectivity exists, similar to a leased line.

However, the devices connected to a packet-switched service can communicate directly with each other, using a single connection to the service.

Two types of packet-switching service are very popular today—Frame Relay and ATM.

Both are covered in this section.

Frame Relay

Point-to-point WANs can be used to connect a pair of routers at multiple remote sites.

However, an alternative WAN service, Frame Relay, has many advantages over point-to point links, particularly when you connect many sites via a WAN.

To introduce you to Frame Relay, focus on a few of the key benefits compared to leased lines.

One of the benefits is seen easily by considering Figures 4-7.

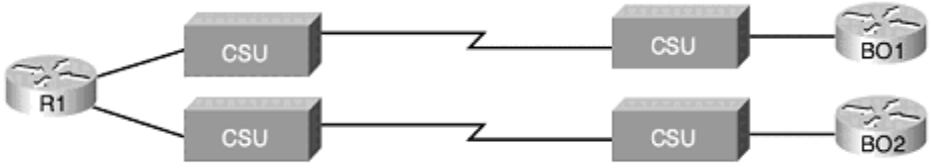


Figure 9 Two Leased Lines to Two Branch Offices

In Figure 4-7, a main site is connected to two branch offices, labeled BO1 and BO2. The main site router, R1, requires two serial interfaces and two separate CSUs.
But what happens when the company grows to 10 sites? Or 100 sites? Or 500 sites?
For each point-to-point line, R1 needs a separate physical serial interface and a separate CSU/DSU.

As you can imagine, Growth to hundreds of sites will take many routers, with many interfaces each and lots of rack space for the routers and CSU/DSUs.

Now imagine that the phone company salesperson talks to you when you have two leased lines, or circuits, installed as in Figure 4-7: "You know, we can install Frame Relay instead.

You will need only one serial interface on R1 and one CSU/DSU. To scale to 100 sites, you might need two or three more serial interaces on R1 for more bandwidth, but that's it.
And by the way, because your leased lines run at 128 kbps today**,** we'll guarantee that you can send and receive that much to and from each site.

We will upgrade the line at R1 to T1 speed (1.544 Mbps).

When you have more traffic than 128 kbps to a site, go ahead and send it! If we've got capacity, we'll forward it, with no extra charge.
And by the way, did I tell you that it's cheaper than leased lines anyway?"

You consider the facts for a moment: Frame Relay is cheaper; it's at least as fast (probably faster) than what you have now and it allows you to save money when you grow.

Frame Relay does compare very favorably with leased lines in a network with many remote sites.

The next few pages, you will see how Frame Relay works and realizes

Frame Relay Basics

Frame Relay networks provide more features and benefits than simple point-to-point WAN links, but to do that, Frame Relay protocols are more detailed.
Frame Relay networks are multi-access networks, which means that more than two devices can attach to the network, similar to LANs.

To support more than two devices, the protocols must be a little more detailed.

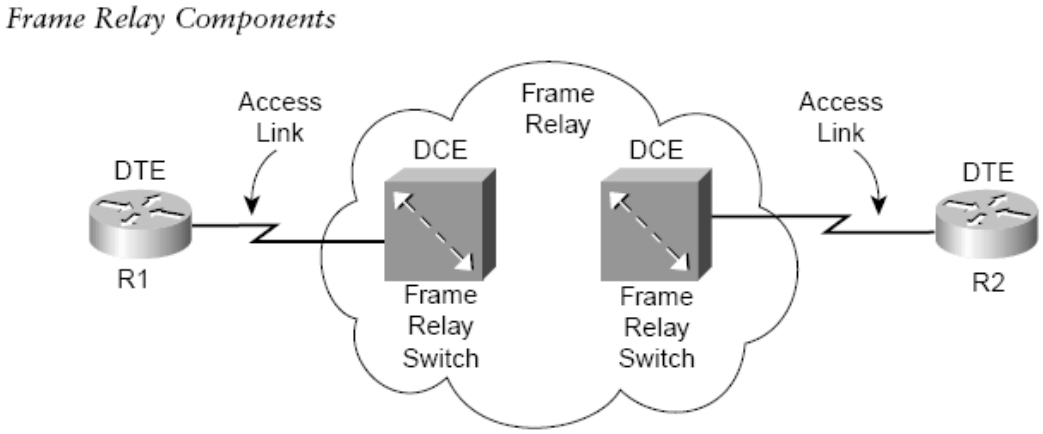


Figure 10 Frame Relay Components

Figure 4-8 reflects the fact that Frame Relay uses the same Layer 1 features as a point-to point leased line

.

For a Frame Relay services, a leased line is installed between each router and a nearby Frame Relay switch; these links are called access links.

The access links run the same speeds and use the same signaling standards as do point-to-point leased lines.

However, instead of extending from one router to the other, each leased line runs from one router to a Frame Relay switch.

The difference between Frame Relay and point-to-point links is that the equipment in the telco actually examines the data frames sent by the router.

Each frame header holds an address field called a data-link connection identifier (DLCI).

The WAN switch forwards the frame, based on the DLCI, through the provider's network until it gets to the router on the other side of the network.

Because the equipment in the Telco can forward one frame to one remote site and another frame to another remote site, Frame Relay is considered to be a form of packet switching.

However, Frame Relay protocols most closely resemble OSI Layer 2 protocols; the term usually used for the bits sent by a Layer 2 device is frame.

So, Frame Relay is also called a frame-switching service.

The terms DCE and DTE actually have a second set of meanings in the context of any

Packet-switching or frame-switching service. With Frame Relay, the Frame Relay switches are called DCE, and the customer equipment—routers, in this case—are called DTE.

In this case, DCE refers to the device providing the service, and the term DTE refers to the device needing the frame-switching service.

At the same time, the CSU/DSU provides clocking to the router, so from a Layer 1 perspective, the CSU/DSU is still the DCE and the router is still the DTE. It's just two different uses of the same terms.

Figure 4-8 depicts the physical and logical connectivity at each connection to the Frame Relay network. In contrast,

Figure 4-9 shows the end-to-end connectivity associated with a virtual circuit.

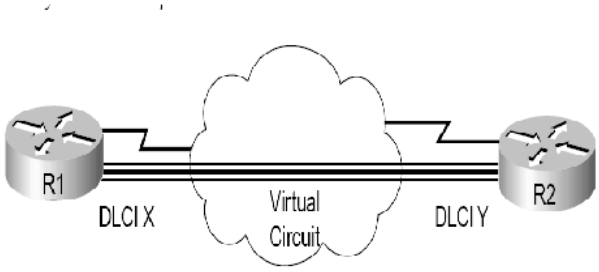


Figure11 Frame Relay PVC Concepts

The logical path between each pair of routers is called a Frame Relay virtual circuit (VC).

In Figure 4-9, a single VC is represented by the trio of parallel lines.

Typically, the service provider preconfigured all the required details of a VC; these VCs are called permanent virtual circuits (PVCs).

When R1 needs to forward a packet to R2, it encapsulates the Layer3 packet into a Frame Relay header and trailer and then sends the frame.

R1 uses a Frame Relay address called a DLCI in the Frame Relay header.

This allows the switches to deliver the frame to R2, ignoring the details of the Layer 3 packet and caring to look at only the Frame Relay header and trailer.

Just like on a point-to-point serial link, when the service provider forwards the frame over a physical circuit between R1 and R2,

with Frame Relay, the provider forwards the frame over a logical virtual circuit from R1 to R2.

Frame Relay provides significant advantages over simply using point-to-point leased lines.

The primary advantage has to do with virtual circuits. Consider Figure 4-10 with Frame Relay instead of three point-to-point leased lines.

Frame Relay creates a logical path between two Frame Relay DTEs. That logical path is called a VC, which describes the concept well.

A VC acts like a point-to-point circuit, but physically it is not, so it's virtual. For example, R1 terminates two VCs—one who's other endpoint is R2 and one who's other endpoint is R3. R1 can send traffic directly to either of the other two routers by sending it over the appropriate VC, although R1 has only one physical access link to the Frame Relay network.

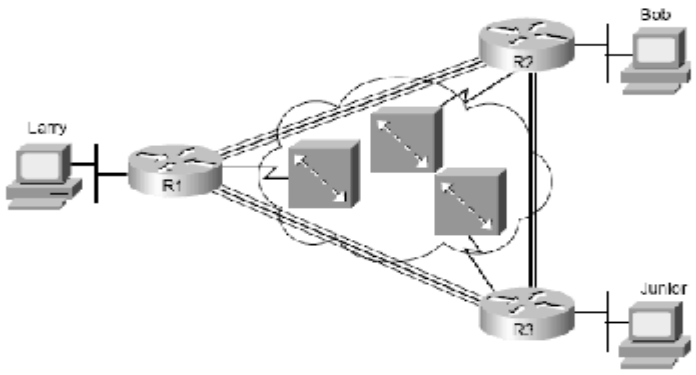


Figure 12 Typical Frame Relay Network with Three Sites

VCs share the access link and the Frame Relay network. For example, both VCs terminating at R1 use the same access link. So, with large networks with many WAN sites that need to connect to a central location, only one physical access link is required from the main site router to the Frame Relay network. If point-to-point links were used, a physical circuit, a separate CSU/DSU, and a separate physical interface on the router would be required for each point-to-point link.

So, Frame Relay enables you to expand the WAN but add less hardware to do so.

Many customers of a single Frame Relay service provider share that provider's Frame Relay network. Originally, people with leased-line networks were reluctant to migrate to Frame Relay because they would be competing with other customers for the provider's capacity inside the cloud.

To address these fears, Frame Relay is designed with the concept of a committed information rate (CIR).

Each VC has a CIR, which is a guarantee by the provider that a particular VC gets at least that much bandwidth.

You can think of CIR of a VC like the bandwidth or clock rate of a point-to-point circuit, except that it's the minimum value— you can actually send more, in most cases.

It's interesting that, even in this three-site network, it's probably less expensive to use Frame Relay than to use point-to-point links.

Now imagine an organization with a hundred sites that needs any-to-any connectivity. How many leased lines are required? 4950!

Besides that, you would need 99 serial interfaces per router.

Or, you could have 100 access links to local Frame Relay switches—1 per router—and have 4950 VCs running over them.
Also, you would need only one serial interface on each router.
As a result, the Frame Relay topology is easier for the service provider to implement, costs the provider less, and makes better use of the core of the provider's network.
As you would expect, that makes it less expensive to the Frame Relay customer as well.
For connecting many WAN sites, Frame Relay is simply more cost-effective than leased lines.

ATM and SONET

Asynchronous Transfer Mode (ATM) and Synchronous Optical Network (SONET) together provide the capability for a Telco to provide high-speed services for both voice and data over the same network.

SONET defines a method for transmitting digital data at high speeds over optical cabling, and ATM defines how to frame the traffic, how to address the traffic so that
DTE devices can communicate, and how to provide error detection. In short, SONET

Provides Layer 1 features, and ATM provides Layer 2 features over SONET. This short section introduces you to the basic concepts.

SONET

Synchronous Optical Network (SONET) defines an alternative Layer 1 signaling and
Encoding mechanism, as compared with the line types listed in Table 4-4. The motivation behind SONET was to allow the phone companies of the world to connect their COs with high-speed optical links.

SONET provides the Layer 1 details of how to pass high-speed data over optical links.

Optical cabling has fiberglass in the middle, with a light signal being sent over the fiberglass.
Optical cabling is more expensive than copper wire cables, and the devices that
Generate the light that crosses the cables are also more expensive—but they allow very high speeds.

During the same time frame of the development of SONET, the Telcos of the world wanted a new protocol to support data and voice over the same core infrastructure.

SONET was built to provide the Layer 1 high-speed links, and ATM was created to provide the capability to mix the voice and data.

Both voice and data traffic could be broken into cells; by using small ATM cells, the delay-sensitive voice traffic could be interleaved with the data traffic, without letting any congestion caused by the bursty nature of data get in the way of high quality voice.

Outside the United States, the term Synchronous Digital Hierarchy (SDH) represents the same standards as SONET.
Also, the term optical carrier (OC) represents the prefix in the names for SONET links that use a variety of different link speeds.

Table lists the different speeds supported by SONET.

Optical carrier	Speed
OC-1	52 Mbps
OC-3	155 Mbps
OC-12	622 Mbps

OC-48	2.4 Gbps
OC-192	9.6 Gbps
OC-768	40 Gbps

ATM

Asynchronous Layer 1 links Transfer Mode (ATM) provides data link layer services that run over SONET.
ATM has a wide variety of applications, but its use as a WAN technology has many similarities to Frame Relay.
When using ATM, routers connect to an ATM service via an access link to an ATM switch inside the service providers network.
For multiple sites, each router would need a single access link to the ATM network, with a VC between sites as needed.

ATM can use permanent VCs (PVCs) like Frame Relay. In fact, the basic concepts between Frame Relay and ATM are identical.

Of course, there are differences between Frame Relay and ATM—otherwise, you wouldn't need both! First, ATM relies on SONET for Layer 1 features instead of the traditional twisted-pair

specifications such as T1 and DS0. The other big difference is that ATM does not forward frames—it forwards cells. Just like packets and frames refer to a string of bits that are sent over some network, cells are a string of bits sent over a network.

Packets and frames can vary in size, but ATM cells are always a fixed 53-bytes in length.

ATM cells contain 48 bytes of payload and a 5-byte header. The header contains two fields that together act like the DLCI for Frame Relay by identifying each VC.

The two fields are named Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI).

Just like Frame Relay switches forward frames based on the DLCI, devices called ATM switches, resident in the service provider network, forward cells based on the VPI/VCI pair.

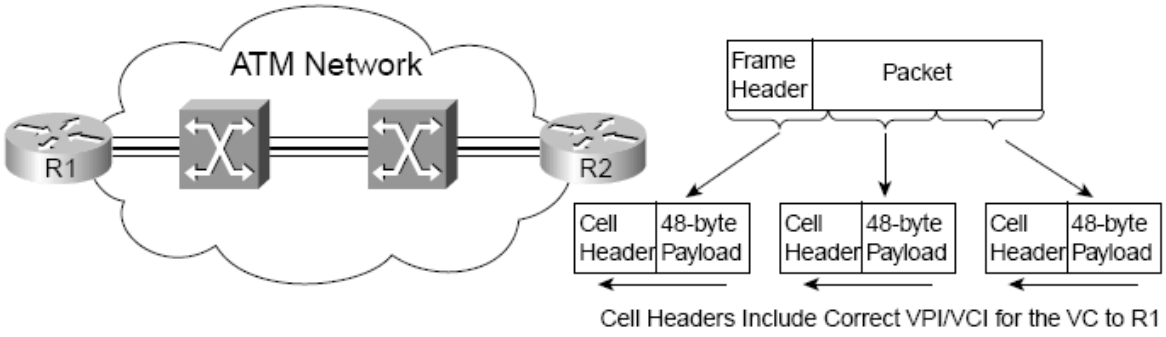
The users of a network typically connect using Ethernet, and Ethernet devices do not create cells.

So, how do you get traffic off an Ethernet onto an ATM network? When a router receives a packet and decides to forward the packet over the ATM network, the router creates the cells.

The creation process involves breaking up a data link layer frame into 48- byte-long segments.

Each segment is placed in a cell along with the 5-byte header. Figure 4-11 shows the general idea, as performed on R2.

Figure 4-11 *ATM Segmentation and Reassembly*



routers forward IP packets, but they must add a data-link header and trailer to the packet before sending it.

R2 takes the packet, adds a data-link header appropriate for ATM, and then also segments the frame into cells before sending any data. R2 takes the first 48 bytes of the frame and puts them in the payload field of a new cell; next, it takes the next 48 bytes and puts them in another cell, and so on.

The cell header includes the correct VPI/VCI pair so that the ATM switches in the ATM network know to forward the cells to R1.

R1 actually reverses the segmentation process after receiving all the cells—a process called reassembly.

The entire concept of segmenting a frame into cells, and reassembling them, is called segmentation and reassembly (SAR).

Because of its similar function to Frame Relay, ATM also is considered to be a type of packet switching service.

However, because it uses fixed-length cells, it more often is called a cell switching Service.

WAN Terminology Related to Packet Switching

You have already read about how both Frame Relay and ATM are considered to be packet switching services but how, more often,

Frame Relay is called a frame-switching service and ATM is called a cell-switching service.

Table lists the key terms about WANs, plus a few related terms and a brief explanation.

Dedicated Circuit	Another Term for a Leased Point-to-Point Line
Packet switching	Service in which each DTE device connects to a Telco using a single physical line, with the possibility of being able to forward traffic to all other sites. The Telco switch makes the forwarding decision based on an address in the packet header.
Frame switching	In concept, it is identical to packet switching. However, when the protocols match OSI Layer 2 more than any other layer, it is called frame switching.

	Frame Relay is a frame-switching technology.
Cell switching	In concept, it is identical to packet switching. However, because ATM DTEs break frames into small, fixed-length cells; these services are also called cell switching. ATM is a cell-switching technology.
Circuit switching	A circuit is a point-to-point link between only two sites, much like a leased line. However, circuit switching refers to the process of dialing, setting up a circuit, and then hanging up—in other words, the circuit is switched on and off.

Chapter 6

Java, Collections

Introduction

In this chapter, we consider the Java ***collections framework***, which contains prepackaged data structures, interfaces and algorithms for manipulating those data structures. Some examples of collections are the cards you hold in a card game, your favorite songs stored in your computer, the members of a sports team and the real-estate records in your local registry of deeds (which map book numbers and page numbers to property owners).

With collections, programmers use existing data structures, without concern for how they are implemented. This is a marvelous example of code reuse. Programmers can code faster and can expect excellent performance, maximizing execution speed and minimizing memory consumption. In this chapter, we discuss the collections framework interfaces that
list the capabilities of each collection type, the implementation classes, the algorithms that process the collections, and the so-called ***iterators*** and enhanced for statement syntax that "walk through" collections.

The Java collections framework provides ready-to-go, reusable componentry—you do not need to write your own collection classes, but you can if you wish to. The collections are standardized so that applications can share them easily without concern with for details of their implementation. The collections framework encourages further reusability. As new data structures and algorithms are developed that fit this framework, a large base of programmers will already be familiar with the interfaces and algorithms implemented by those data structures.

2 Collections Overview

A C***ollection*** is a data structure—actually, an object—that can hold references to other objects.

Usually, collections contain references to objects that are all of the same type. The collections framework interfaces declare the operations to be performed generically on various types of collections. Figure 7.1 lists some of the interfaces of the collections framework. Several implementations of these interfaces are provided within the framework. Programmers may also provide implementations specific to their own requirements.

The collections framework provides high-performance, high-quality implementations of common data structures and enables software reuse. These features minimize the amount of coding programmers need to do to create and manipulate collections. The classes and interfaces of the collections framework are members of package java.util. In the next section, we begin our discussion by examining the collections framework capabilities for array manipulation.

Interface	Description
`Collection`	The root interface in the collections hierarchy from which interfaces `Set`, `Queue` and `List` are derived.
`Set`	A collection that does not contain duplicates.
`List`	An ordered collection that can contain duplicate elements.
`Map`	Associates keys to values and cannot contain duplicate keys.
`Queue`	Typically a first-in, first-out collection that models a waiting line; other orders can be specified.

Fig. 7.1

3 Class Arrays

Class ***Arrays*** provides static methods for manipulating arrays. Class Arrays provides high-level methods, such as **sort** for sorting an array, **binarySearch** for searching a sorted array, **equals** for comparing ***arrays*** and ***fill*** for placing values into an array. These methods are overloaded for primitive-type arrays and Object arrays. In addition, methods sort and ***binarySearch*** are overloaded with generic versions that allow programmers to sort and search arrays containing objects of any type. Figure.2 demonstrates methods fill, sort, ***binarySearch*** and equals. Method main (lines 65–85) creates a Using Arrays object and invokes its methods.

Line 17 calls static method **fill** of class **Arrays** to populate all 10 elements of ***filledIntArray*** with 7s. Overloaded versions of fill allow the programmer to populate a specific range of elements with the same value.

Line 18 sorts the elements of array ***doubleArray***. The ***static*** method sort of class ***Arrays*** orders the array's elements in ascending order by default. We discuss how to sort in descending order later in the chapter. Overloaded versions of sort allow the programmer to sort a specific range of elements.

Lines 21–22 copy array ***intArray*** into array ***intArrayCopy.*** The first argument ***(intArray)*** passed to System method ***arraycopy*** is the array from which elements are to be copied. The second argument (0) is the index that specifies the starting point in the range of elements to copy from the array. This value can be any valid array index. The third argument ***(intArrayCopy)*** specifies the destination array that will store the copy. The fourth argument (0) specifies the index in the destination array where the first

copied element should be stored. The last argument specifies the number of elements to copy from the array in the first argument. In this case, we copy all the elements in the array.

Line 50 calls ***static*** method ***binarySearch*** of class ***Arrays*** to perform a binary search on ***intArray,*** using value as the key. If value is found, ***binarySearch*** returns the index of the element; otherwise**,** ***binarySearch*** returns a negative value. The negative value returned is based on the search key's insertion point—the index where the key would be inserted in the array if we were performing an insert operation. After ***binarySearch*** determines the insertion point, it changes its sign to negative and subtracts 1 to obtain the return value. For example, in Fig.2, the insertion point for the value 8763 is the element with index 6 in the array. Method ***binarySearch*** changes the ***insertion point*** to –6, subtracts 1 from it and returns the value –7. Subtracting 1 from the insertion point guarantees that method ***binarySearch*** returns positive values (>= 0) if and only if the key is found. This return value is useful for inserting elements in a sorted array.

```java
// Fig. 19.2: UsingArrays.java
// Using Java arrays.
import java.util.Arrays;

public class UsingArrays
{
   private int intArray[] = { 1, 2, 3, 4, 5, 6 };
   private double doubleArray[] = { 8.4, 9.3, 0.2, 7.9, 3.4 };
   private int filledIntArray[], intArrayCopy[];

   // constructor initializes arrays
   public UsingArrays()
   {
      filledIntArray = new int[ 10 ]; // create int array with 10 elements
      intArrayCopy = new int[ intArray.length ];

      Arrays.fill( filledIntArray, 7 ); // fill with 7s
      Arrays.sort( doubleArray ); // sort doubleArray ascending

      // copy array intArray into array intArrayCopy
      System.arraycopy( intArray, 0, intArrayCopy,
         0, intArray.length );
   } // end UsingArrays constructor

   // output values in each array
   public void printArrays()
   {
      System.out.print( "doubleArray: " );
      for ( double doubleValue : doubleArray )
         System.out.printf( "%.1f ", doubleValue );

      System.out.print( "\nintArray: " );
      for ( int intValue : intArray )
         System.out.printf( "%d ", intValue );

      System.out.print( "\nfilledIntArray: " );
      for ( int intValue : filledIntArray )
         System.out.printf( "%d ", intValue );

      System.out.print( "\nintArrayCopy: " );
      for ( int intValue : intArrayCopy )
         System.out.printf( "%d ", intValue );

      System.out.println( "\n" );
   } // end method printArrays

   // find value in array intArray
   public int searchForInt( int value )
   {
```

Fig 7.2 (Part 1 of 2)

```
50          return Arrays.binarySearch( intArray, value );
51       } // end method searchForInt
52
53       // compare array contents
54       public void printEquality()
55       {
56          boolean b = Arrays.equals( intArray, intArrayCopy );
57          System.out.printf( "intArray %s intArrayCopy\n",
58             ( b ? "==" : "!=" ) );
59
60          b = Arrays.equals( intArray, filledIntArray );
61          System.out.printf( "intArray %s filledIntArray\n",
62             ( b ? "==" : "!=" ) );
63       } // end method printEquality
64
65       public static void main( String args[] )
66       {
67          UsingArrays usingArrays = new UsingArrays();
68
69          usingArrays.printArrays();
70          usingArrays.printEquality();
71
72          int location = usingArrays.searchForInt( 5 );
73          if ( location >= 0 )
74             System.out.printf(
75                "Found 5 at element %d in intArray\n", location );
76          else
77             System.out.println( "5 not found in intArray" );
78
79          location = usingArrays.searchForInt( 8763 );
80          if ( location >= 0 )
81             System.out.printf(
82                "Found 8763 at element %d in intArray\n", location );
83          else
84             System.out.println( "8763 not found in intArray" );
85       } // end main
86    } // end class UsingArrays
```

```
doubleArray: 0.2 3.4 7.9 8.4 9.3
intArray: 1 2 3 4 5 6
filledIntArray: 7 7 7 7 7 7 7 7 7 7
intArrayCopy: 1 2 3 4 5 6

intArray == intArrayCopy
intArray != filledIntArray
Found 5 at element 4 in intArray
8763 not found in intArray
```

Fig 7.2 (Part 2 of 2)

Lines 56 and 60 call ***static*** method equals of class ***Arrays*** to determine whether the elements of two arrays are equivalent. If the arrays contain the same elements in the same order, the method returns ***true***; otherwise, it returns ***false.*** The equality of each element is compared using ***Object*** method ***equals***. Many classes override method equals to perform the comparisons in a

manner specific to those classes. For example, class ***String*** declares equals to compare the individual characters in the two ***Strings*** being compared. If method ***equals*** is not ***overridden***, the original version of method equals inherited from class ***Object*** is used.

4 Lists

A ***List*** (sometimes called a ***sequence***) is an ordered ***Collection*** that can contain duplicate elements. Like array indices, ***List*** indices are zero based (i.e., the first element's index is zero). In addition to the methods inherited from ***Collection, List*** provides methods for manipulating elements via their indices, manipulating a specified range of elements, searching for elements and getting a ***ListIterator*** to access the elements.

Interface List is implemented by several classes, including classes ***ArrayList, LinkedList*** and ***Vector***. Autoboxing occurs when you add primitive-type values to objects of these classes, because they store only references to objects. Class ***ArrayList*** and ***Vector*** are resizable-array implementations of ***List.*** Class ***LinkedList*** is a linked list implementation of interface ***List.***

Class ***ArrayList's*** behavior and capabilities are similar to those of class ***Vector***. The primary difference between ***Vector*** and ***ArrayList*** is that objects of class ***Vector*** are synchronized by default, whereas objects of class ***ArrayList*** are not. Also, class Vector is from Java 1.0, before the collections framework was added to Java. As such, Vector has several methods that are not

part of interface ***List*** and are not implemented in class ***ArrayList,*** but perform identical tasks. For example, Vector methods ***addElement*** and add both append an element to a ***Vector***, but only method add is specified in interface ***List*** and implemented by ***ArrayList.*** Unsynchronized collections provide better performance than synchronized ones. For this reason, ***ArrayList*** is typically preferred over ***Vector*** in programs that do not share a collection among threads.

4.1 *ArrayList* and *Iterator*

Figure 7.3 uses an ***ArrayList*** to demonstrate several ***Collection*** interface capabilities.

The program places two ***Color*** arrays in ***ArrayLists*** and uses an ***Iterator*** to remove elements in the second ***ArrayList*** collection from the first ***ArrayList*** collection.

Lines 10–13 declare and initialize two ***String*** array variables, which are declared final, so they always refer to these arrays. Recall that it is good programing practice to declare constants with keywords ***static*** and ***final***. Lines 18–19 create ***ArrayList*** objects and assign their references to variables ***list*** and ***removeList,*** respectively. These two lists store ***String*** objects. Note that ***ArrayList*** is a generic class as of Java SE 5, so we are able to specify a type argument (***String*** in this case) to indicate the type of the elements in each list. Both ***list*** and ***removeList*** are collections of ***Strings***. Lines 22–23 populate ***list*** with ***Strings*** stored in array ***colors***, and lines 26–27 populate ***removeList*** with ***Strings*** stored in array ***removeColors*** using ***List*** method ***add.*** Lines 32–33 output each element of ***list.*** Line 32 calls ***List*** method

size to get the number of ***ArrayList*** elements. Line 33 uses ***List*** method ***get*** to retrieve individual element values. Lines 32–33 could have used the enhanced for statement. Line 36 calls method ***removeColors*** (lines 46–57), passing ***list*** and ***removeList*** as arguments. Method ***removeColors*** deletes ***Strings*** specified in ***removeList*** from the list collection. Lines 41–42 print ***list's*** elements after ***removeColors*** removes the ***String*** objects specified in ***removeList*** from the ***list***.

```
1  // Fig. 19.3: CollectionTest.java
2  // Using the Collection interface.
3  import java.util.List;
4  import java.util.ArrayList;
5  import java.util.Collection;
6  import java.util.Iterator;
7
8  public class CollectionTest
9  {
10    private static final String[] colors =
11       { "MAGENTA", "RED", "WHITE", "BLUE", "CYAN" };
12    private static final String[] removeColors =
13       { "RED", "WHITE", "BLUE" };
14
15    // create ArrayList, add colors to it and manipulate it
16    public CollectionTest()
17    {
18       List< String > list = new ArrayList< String >();
19       List< String > removeList = new ArrayList< String >();
20
21       // add elements in colors array to list
22       for ( String color : colors )
23          list.add( color );
24
25       // add elements in removeColors to removeList
26       for ( String color : removeColors )
27          removeList.add( color );
28
29       System.out.println( "ArrayList: " );
30
31       // output list contents
32       for ( int count = 0; count < list.size(); count++ )
33          System.out.printf( "%s ", list.get( count ) );
34
35       // remove colors contained in removeList
36       removeColors( list, removeList );
```

Fig. 7.3 (Part 1 of 2)

```
37
38        System.out.println( "\n\nArrayList after calling removeColors: " );
39
40        // output list contents
41        for ( String color : list )
42           System.out.printf( "%s ", color );
43     } // end CollectionTest constructor
44
45     // remove colors specified in collection2 from collection1
46     private void removeColors(
47        Collection< String > collection1, Collection< String > collection2 )
48     {
49        // get iterator
50        Iterator< String > iterator = collection1.iterator();
51
52        // loop while collection has items
53        while ( iterator.hasNext() )
54
55           if ( collection2.contains( iterator.next() ) )
56              iterator.remove(); // remove current Color
57     } // end method removeColors
58
59     public static void main( String args[] )
60     {
61        new CollectionTest();
62     } // end main
63  } // end class CollectionTest
```

```
ArrayList:
MAGENTA RED WHITE BLUE CYAN

ArrayList after calling removeColors:
MAGENTA CYAN
```

Fig. 7.3 (Part 2 of 2)

Method ***removeColors*** declares two ***Collection*** parameters (line 47) that allow any ***Collections*** containing strings to be passed as arguments to this method. The method accesses the elements of the first ***Collection (collection1)*** via an ***Iterator***. Line 50 calls ***Collection*** method ***iterator*** to get an Iterator for the ***Collection.*** Note that interfaces ***Collection*** and ***Iterator*** are generic types. The loop-continuation condition (line 53) calls ***Iterator*** method ***hasNext*** to determine whether the ***Collection*** contains more elements. Method ***hasNext*** returns ***true*** if another element exists and ***false*** otherwise.

The if condition in line 55 calls ***Iterator*** method ***next*** to obtain a reference to the next element, then uses method ***contains*** of the

second ***Collection*** (***collection2)*** to determine whether ***collection2*** contains the element returned by ***next.*** If so, line 56 calls ***Iterator*** method ***remove*** to remove the element from the ***Collection collection1.***

Chapter 7

The Main Algorithm

After the input stage has been finished (the user finished entering the data required by the tool) then the program will enter the following stage which is the business layer or the main algorithm stage which will be covered below.
This algorithm consists of number of steps to reach finally to the output stage as follow:

1-Switches Calculations:

In this part we attempt to find access switches needed by each room, we find the number of switches in each room, specifications of each switch and also the location of the switches according to number of nodes and type of them(PCs ,servers……).
We find also edge switches needed for the floors or the buildings.
And finally we find the core switch specifications needed for the overall area.
The previous design follows the standard of switching hierarchy which was mentioned early in the chapter of the computer network design.

1-1-Access switches calculations:

1- After the user enter the number of nodes inside each room then we add number of nodes to the original number entered by the user to offer redundancy for the switch for future use.
The redundancy is according to specific percentage which is 25% from the number of nodes entered by the user.

2- We first determine the numbers of ports of the switch according to the number of nodes after adding redundancy.

3- The switch with the required specifications will be queried from the data base and added to the room.

4- The switch location is determined in diagonal with the door, i.e. left the two corners of the door of the room and chooses the switch to be in one corner of the opposite wall.

1-2-Edge switches calculations:

1- Also here we make redundancy in consideration, where as there are numbers of rooms are active (i.e. contains nodes inside it) there also passive rooms (which do not contain any nodes) so for future use we offer redundancy percentage for the edge switch, this percentage is calculated as follow:
if the number of access switches in each active rooms + 60% of the number of passive rooms reach to 12, then we use edge switch of 12 port, and so on till the last edge switch which depends on the rest number of the access switches (i.e. for example if the number of access switches in each active rooms +60% the number of passive rooms reach to 8, then we use edge switch of 8 port and so on).

1-3-Core switches calculations:

After the edge switches are determined then a core switch of number of ports equals to the number of edge switches with redundancy added will be chosen.
Also a redundant core switch will be added for reliable network.

2-cables calculations:

In this part we attempt to find the design of cables required in the network beginning from each room till the overall area.
We find the cables lengths, types and its connections or topologies.

2-1-Room path calculations:

In this part the path from each node to the switch, its length and its cost is calculated.

2-2-Floor or building cables calculations:

In this part the path from each access switch to its edge switch, its length and its cost is calculated.

2-3- Area Cable Calculations:

In this part the path from each core switch to each edge switch and its cost is calculated.

Chapter 8

Final Words

Conclusion:

We took about a year on our project, made a lot and learned a lot. But in a nutshell we concluded the following points as what the software can give to its users and what we learned in the process.

1. The tool provides an entire LAN design even for amateur users; giving a complete infrastructure including different network components. Such as routers, switches, servers, access points, and even the transmission media needed to link all network portions.

2. Making an easy way for designing using simple GUI; one of our main targets of the project was making even the amateur inexperienced user able to work and use our tool in an easy manner. Thanks to the Java GUI that made this task easy, with its various classes and fast approach methods.

3. Saves a lot of time for users in making the design process; "The Network Planning Tool" actually saves a lot of time of severe calculations and searching for the main design methodology and how to make your design follows the regulations of customer objectives and business requirements.

4. Calculating the total cost for users as an initial reference for the needed budget for the project; an approximate cost for the design is provided by the software. Which can be set by the user, as our project gives the option of changing the cost of different components used in the design. This was one of the main targets which had to be covered, because any design documentation contains in its main topics a lot of issues related to the cost.

5. Guarantee availability and scalability for future update in the network; when the business grows faster, the network of this business must be flexible enough to catch up with such updates…stiff networks, which neglects redundancy suffers when

updates are needed. The owner of the business doesn't want to change the whole network each time updates are needed.

6. Redundancy prediction is one of the key features of the tool; as stated in the previous point, the achievement of a flexible network is made by making sure an easy upgrade can be done with few changes and minimum cost. This goes from calculations of passive rooms to ports and up to cable lengths.

7. Network design and management are not separated sciences; Network science must be aware of the current news and updates concerning business life.

8. We became more familiar with the Java programming language and the use of data structures; using Java in implementing our tool added to us more and more experience in dealing with Java, also designing the adequate algorithm which follows the Java programming rules, and of course linking the database with the Java project.

9. We became aware of the main network hierarchies of LAN protocols and different network basics; learning more about networks was one of the main steps in our project which uses different network principles and hierarchies in its core, this is to provide a reliable design that fits the current network protocols.

Future Work:

Though we covered most of our goal that we intended for the project there were some that we now hope to achieve and add in the future updates for the project after gaining more experience in networking field.

1. The project's name is "Network Planning Tool" by that we meant LAN designs and WAN designs. But unfortunately we couldn't correctly implement the WAN idea so we postponed it in future releases.

2. The LAN design using Ethernet is more or less achieved. But the addition of the Wi-Fi technology is now crucial duo business requirements. But we needed more experience in the Wi-Fi field to achieve this goal and hoping that we learn more about that field so that it can also be added to the tool.

3. We made it possible to link different buildings in a designated area, and to make various areas on the same project. But what we wanted is to link different areas between each other but this will be after completely understanding WAN designs.

4. The idea of adding NATing and IP addressing came across our minds, but we focused on the basic design of a certain network. In future releases after improving the design we would like to add this as an extra feature, so the tool can be more comprehensive for the business requirements.

5. The basic GUI design of the software could be improved to have a modern look. Our idea was to make it simple as possible, but with more experience in Java swing we really aim to a more modernized look.

6. One of the suggestions that came across our minds was to improve the database so that it can be updated from the internet; Updates from prices to new modern network components.

7. We are not aiming for the stars or anything but with updates from the internet an AI for choosing from those parts would come in handy.

8. Then again the main algorithm of the projects could use more tweaks to work better and choose more efficiently between switches, routers…etc.

9. One of the hardest parts was when we were trying to make the user able to save his project but we didn't have enough experience to know how to implement a "save project" and its components. And this is considered one of our highest priorities.

10. As mentioned before we are not aiming for the stars, but we really hope that one day Cisco Solutions could adopt our project.

A final word:

All of us became able to work in a team applying the main principles of team work and project management.

Working in a team work is one of the main issues that must be gained during our work on the project. So organizing our ideas and distributing different jobs in a way so that it matches our final goal taught us a lot on how to work within a team following the manager's instructions and to be an effective part of a team.

Appendix

Tutorial

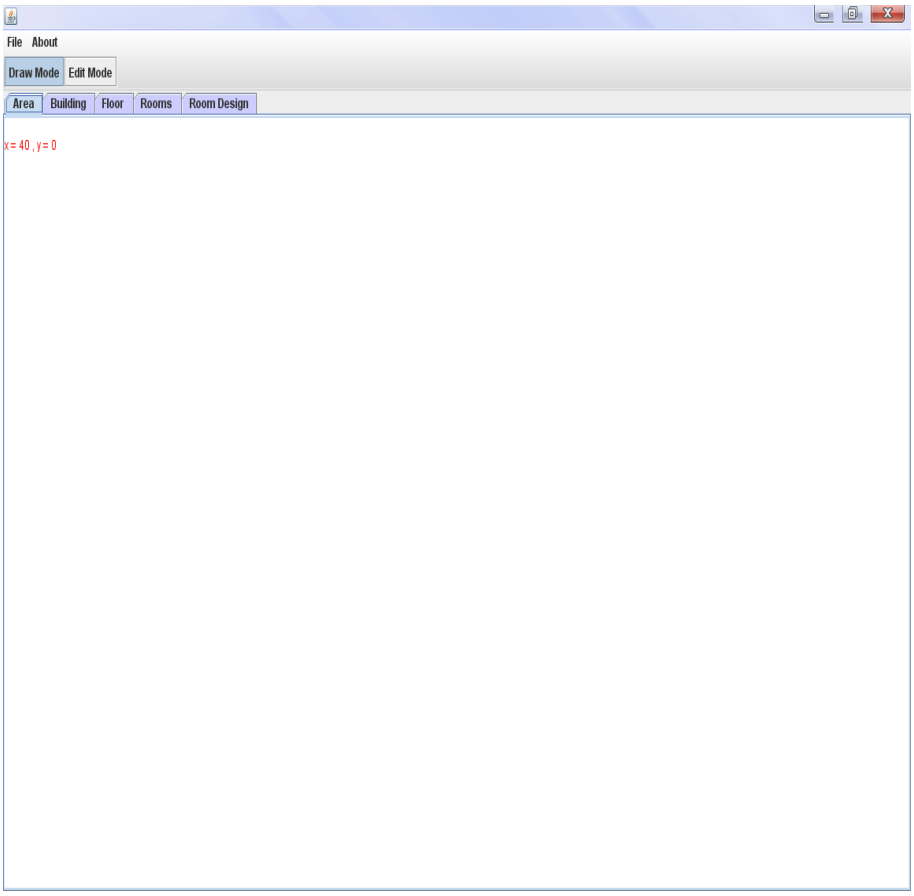
The Input Layer (How To Enter The Data)

The Input layer:

There are screen shots from the program to follow it when using the program:

1-The program interface:

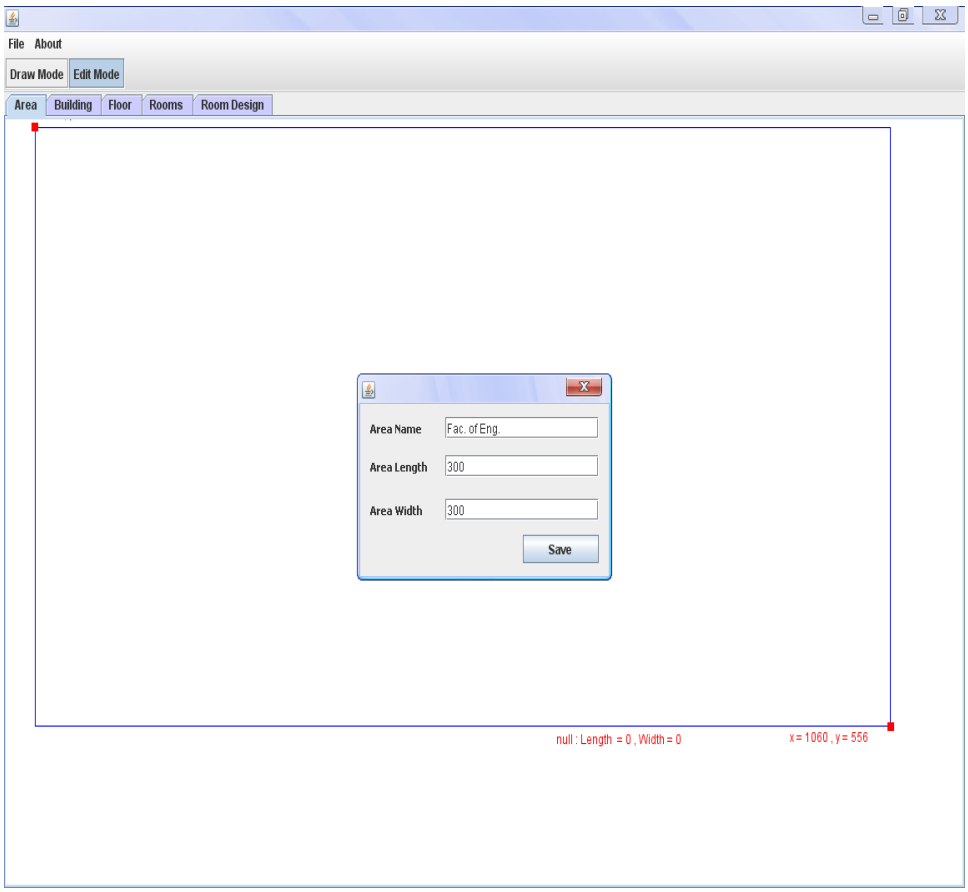
When the user opens the tool this window will appear:



There are two modes: one mode is for drawing and another mode for editing the wrong drawings.
The user then needs to start drawing so the following are the steps to do that

2-Area drawing:

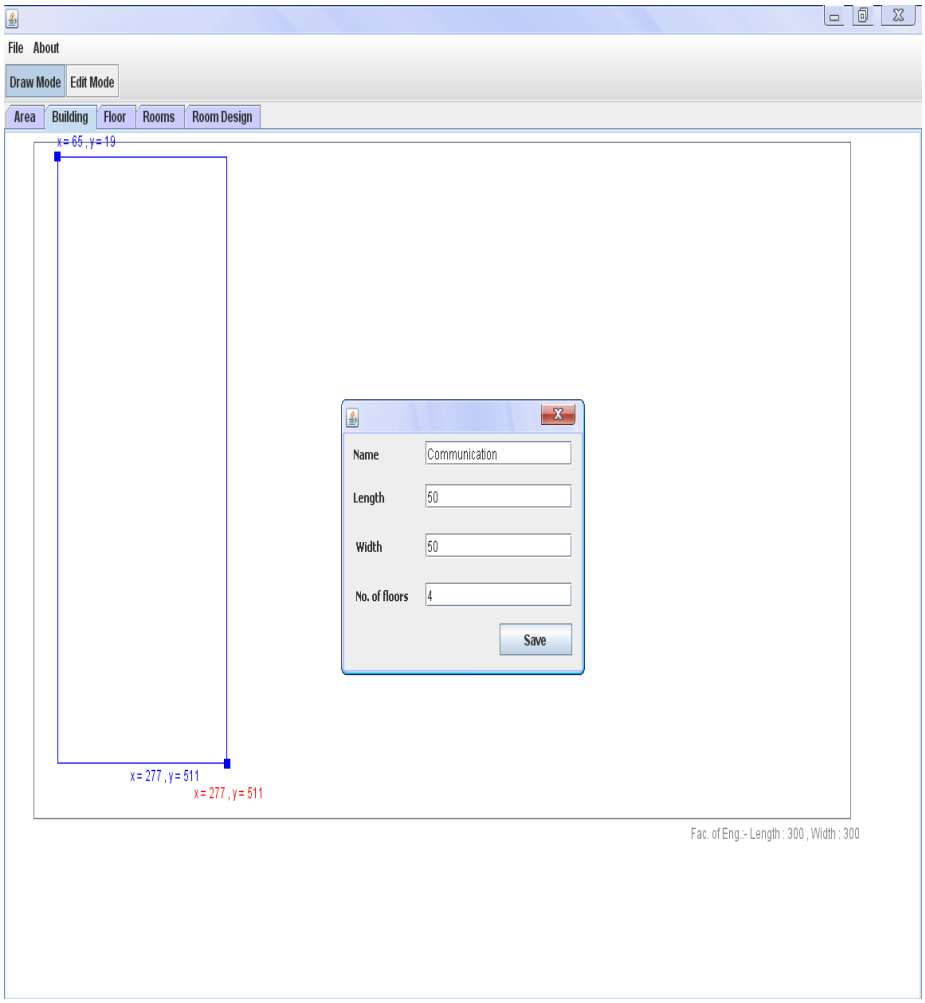
First click on the button of the draw mode button then area button, then by mouse you can click and draw the area by dragging the mouse, when you left the mouse, you must enter the properties of the area such as the area name, length and width as in the figure below.



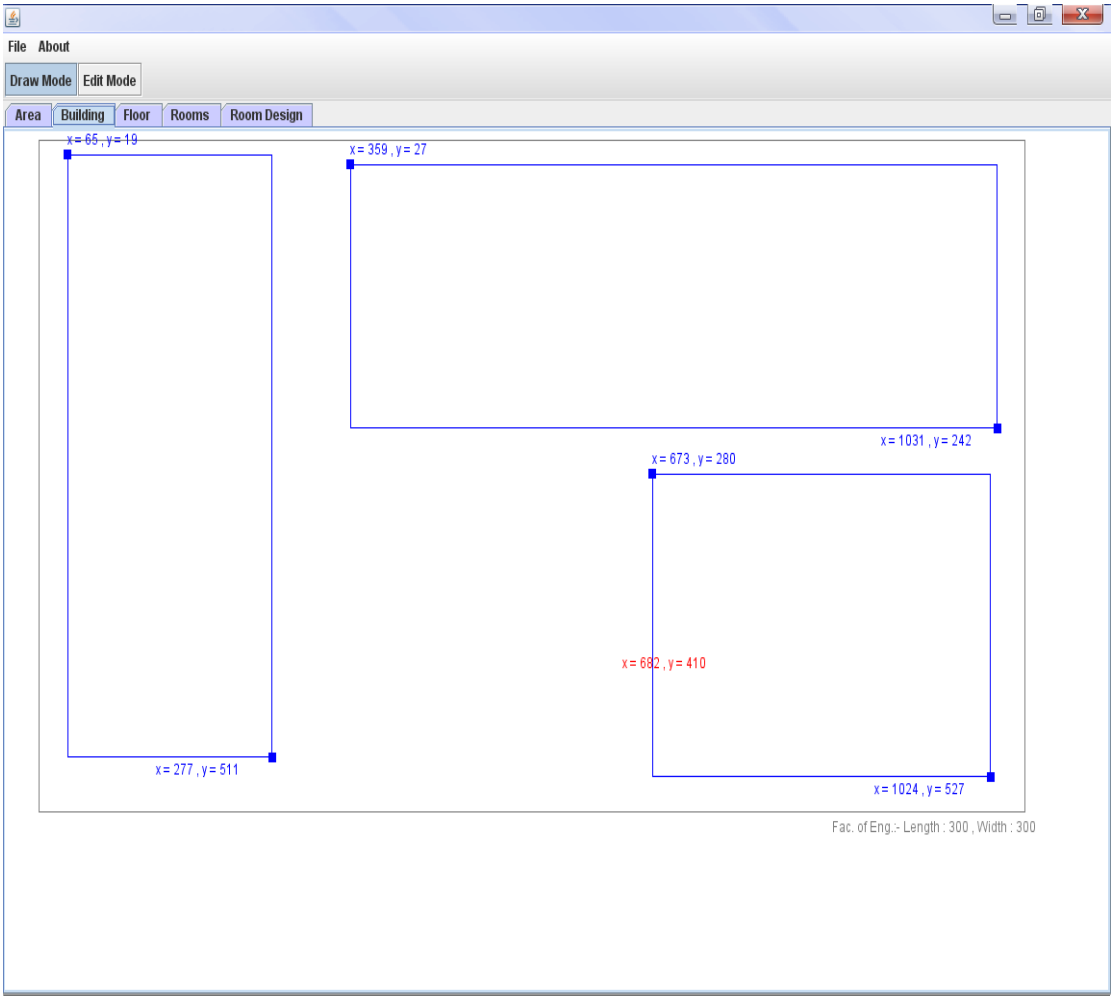
You can use the option of the tool to resize or move the figure have been drawn, but in this case you must enter the area properties again.

2-Building drawing:

You can draw the number of buildings inside this area as long as the area is enough, as shown in the figure below, after you left the mouse, dialogue box of building properties will appear to fill it as follow:



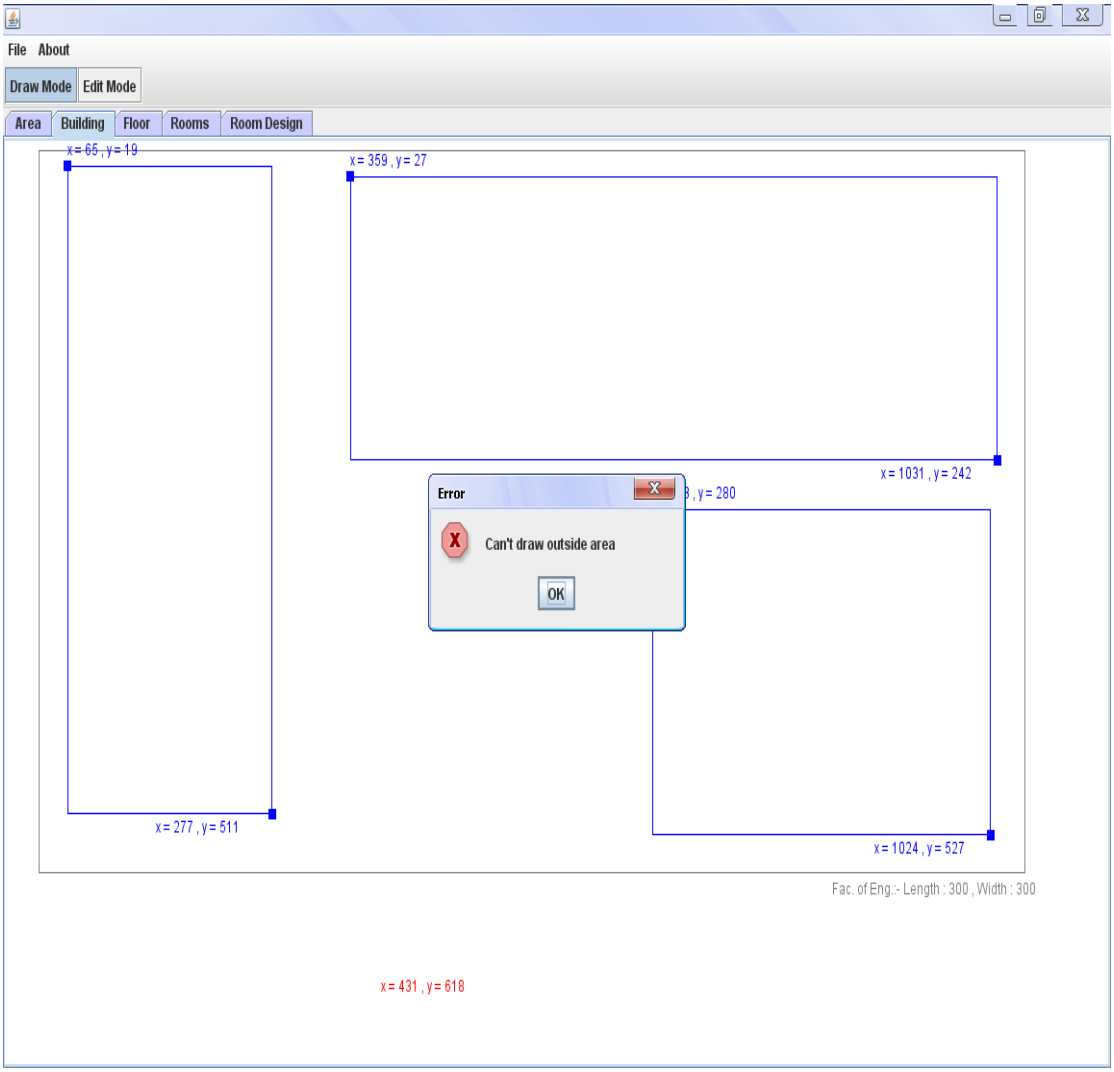
You can draw the other buildings in the same manner, as follow:



Also here you can move the building or make resize for it, you can do that from the edit mode, otherwise (from the drawing mode) it will give error message and return to the previous shape.

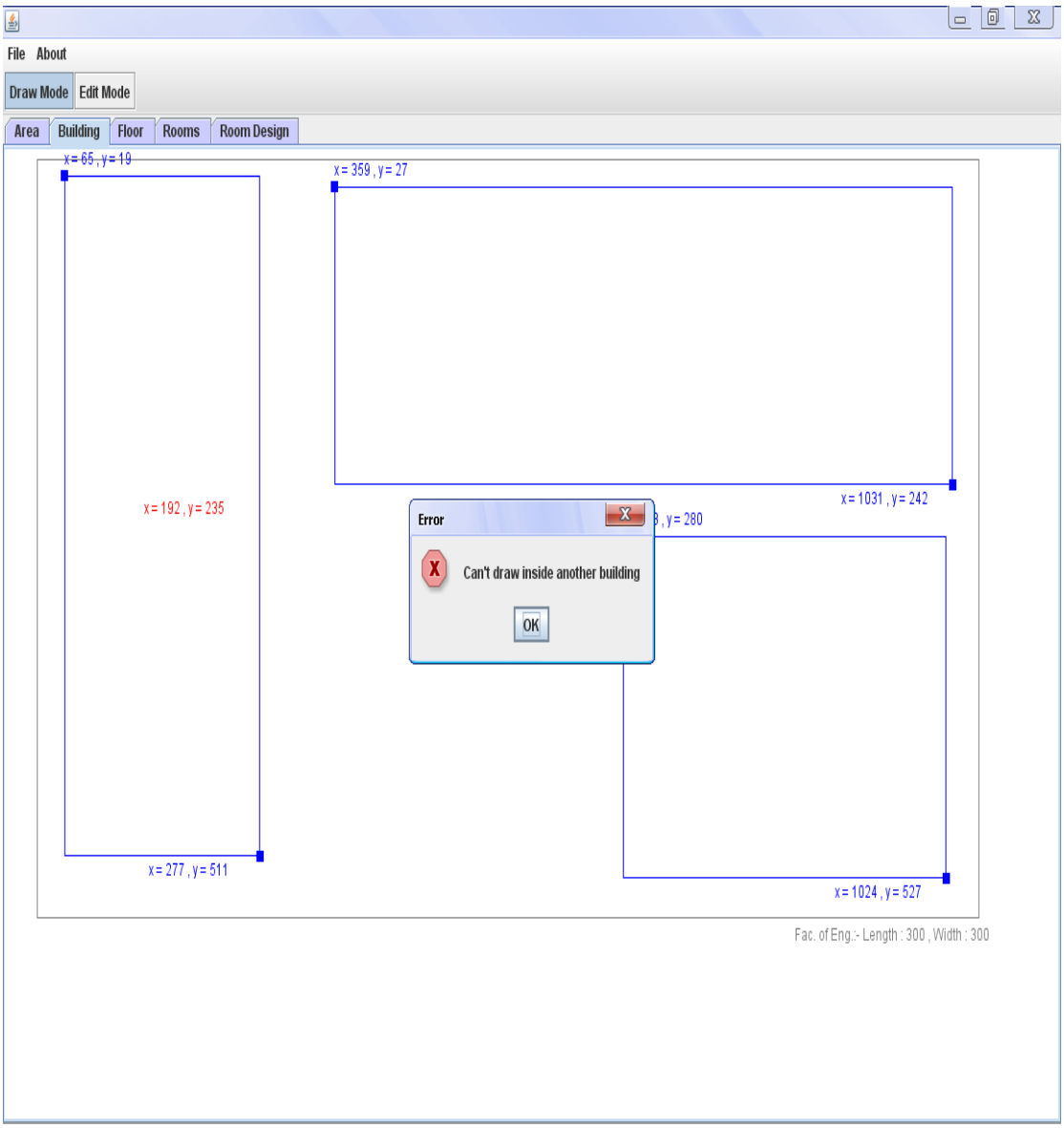
Here there are number of validations takes place as follow:

1-Building can't be drawn from out side the area, if you d, error message will appear as follow:



Note that: the red pointer (numbers x=, y=) is the start of the new building which is out of area.

2-Building can't be drawn from other building, if you do error message will appear as follow:



Note that: the red pointer (numbers x=, y=) is the start of the new building which is inside another building.

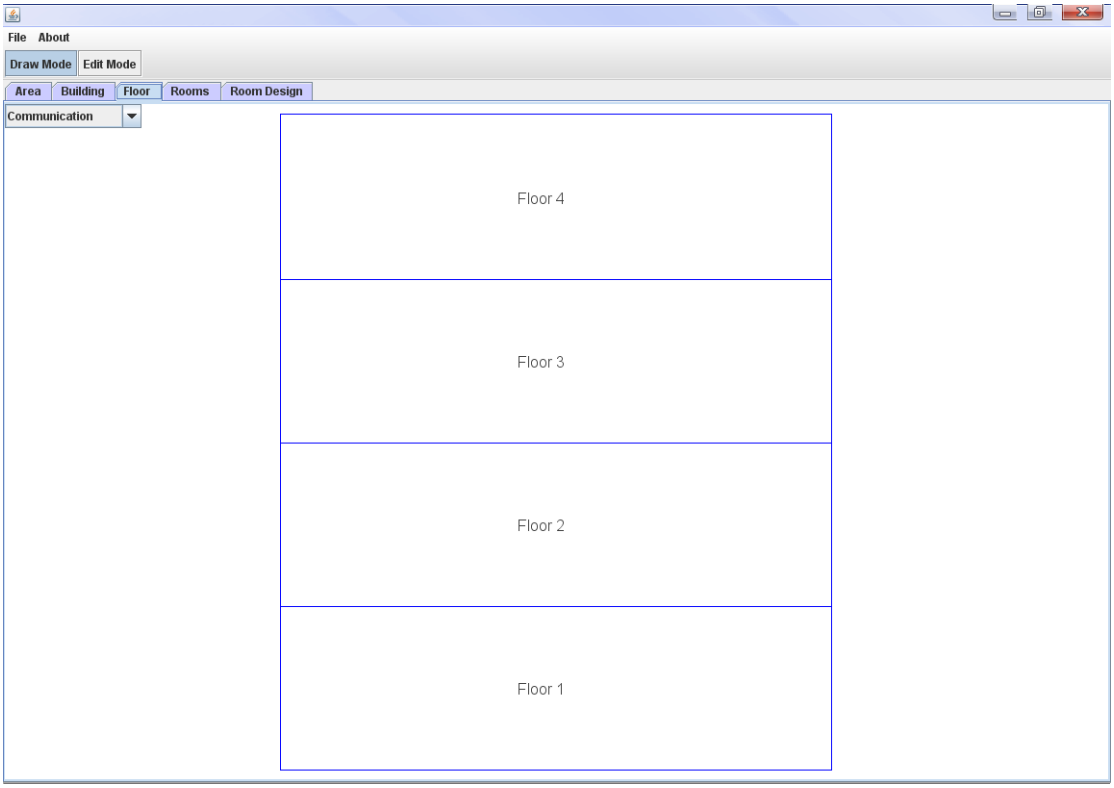
3-If the building during drawing moved out of the area it will be erased automatically.

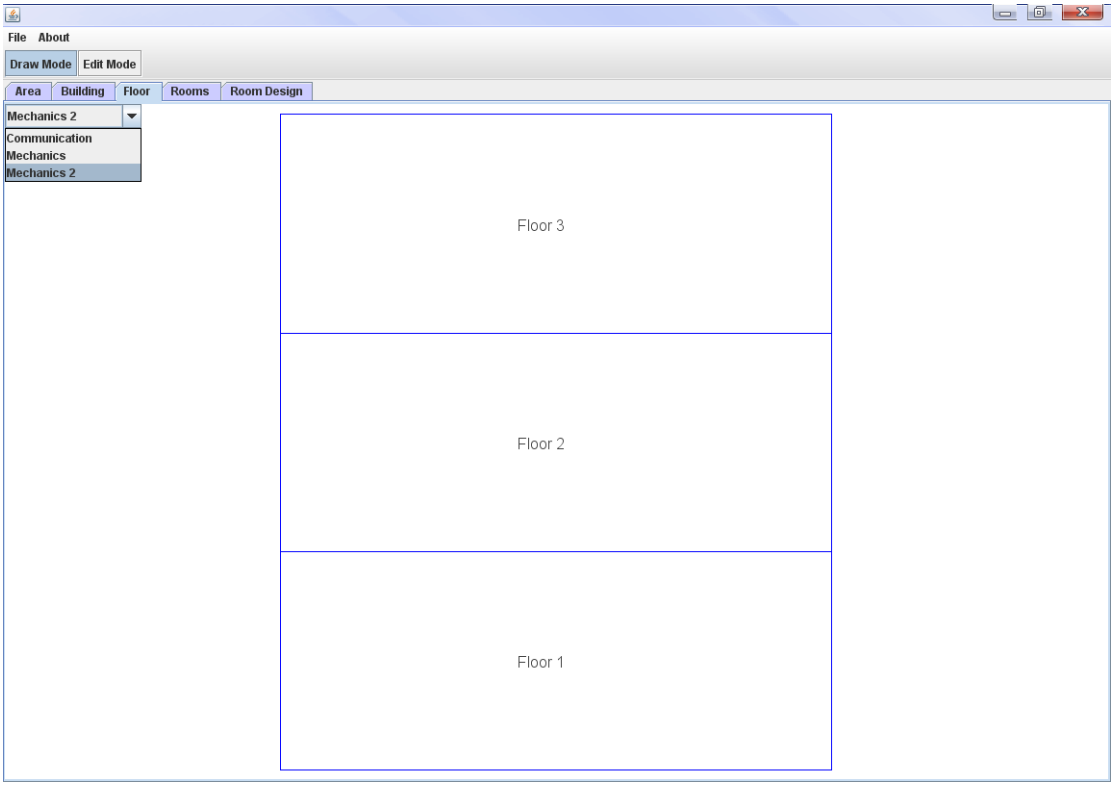
4-there is check (validate) on the area of the drawn buildings with respect to the overall area.

5-you should draw the rectangle of the building from left to right, otherwise (from right to left) you should make move to the figure from the edit mode.

3-Floor drawing:

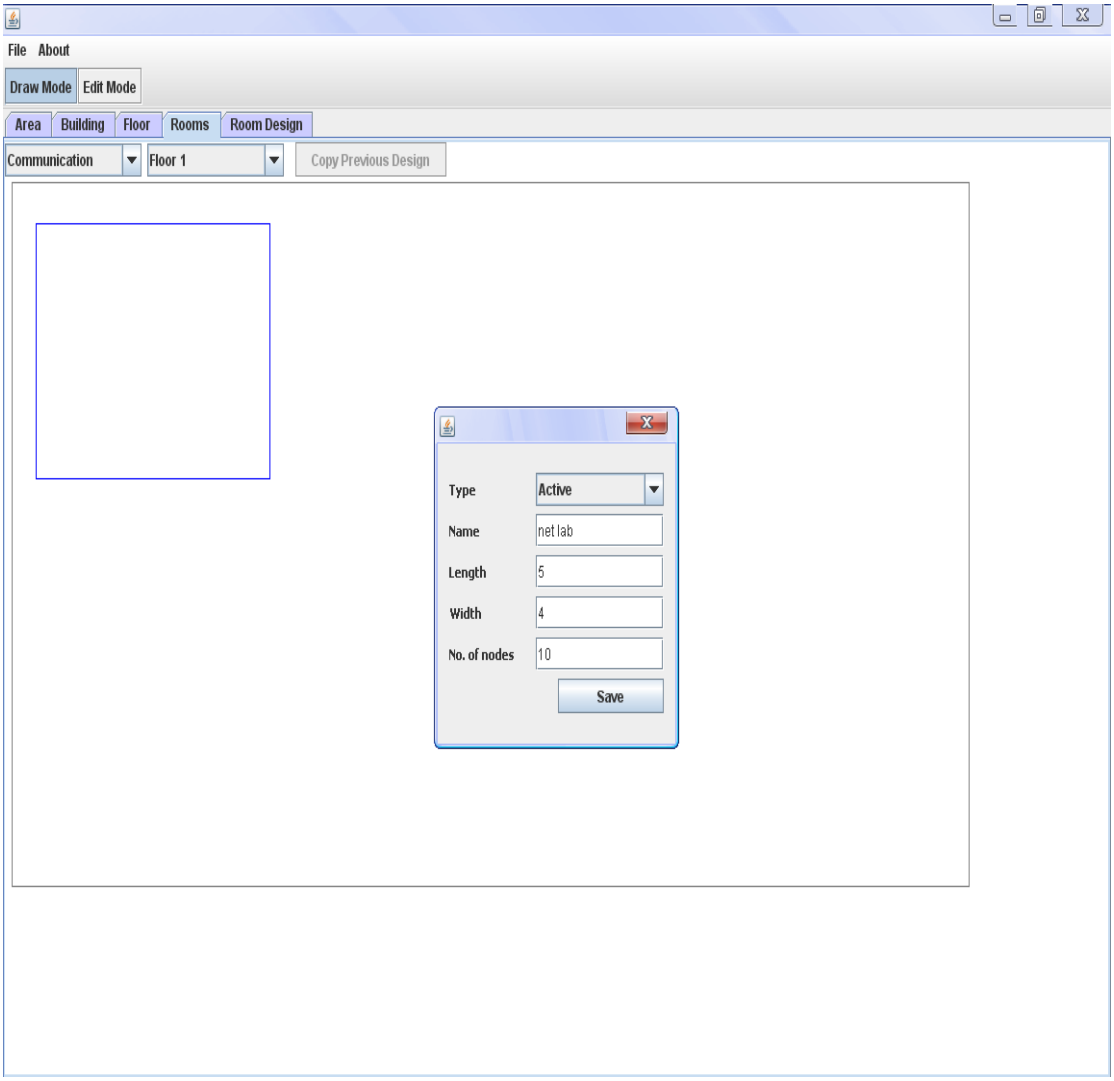
When you enter the number of floors in the dialogue box of the building properties, the floors will be drawn automatically just click on the floor button as follow:





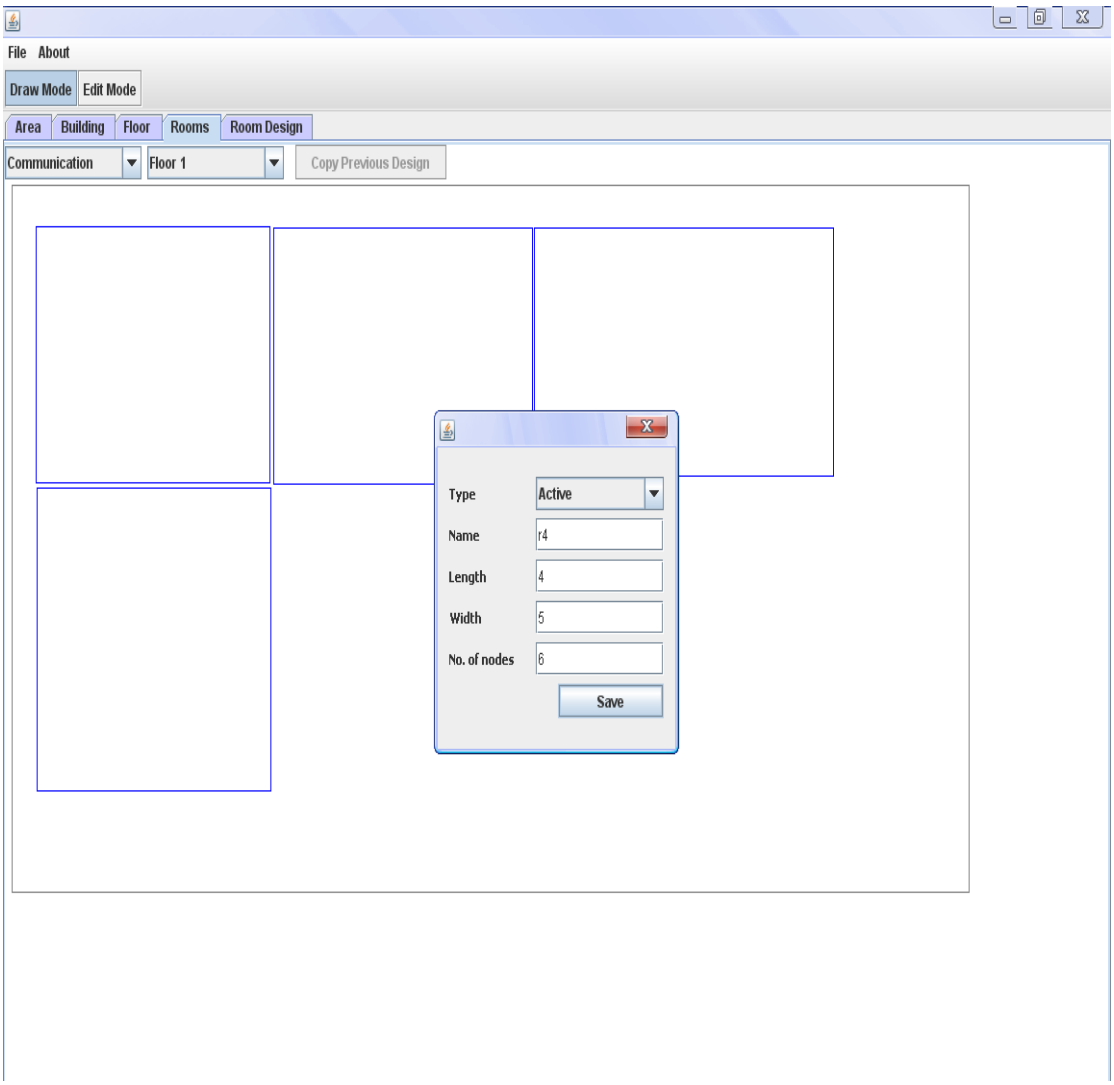
3-Room drawing:

Click on the room button then choose the building then the floor then draw the room inside it after you left the mouse the properties of the room will appear as follow:



In the properties box first choose if the room is active (i.e. contains nodes) or passive (doesn't contain nodes) if you choose passive then the field of No. of nodes will be disabled, otherwise you must enter the No. of nodes,

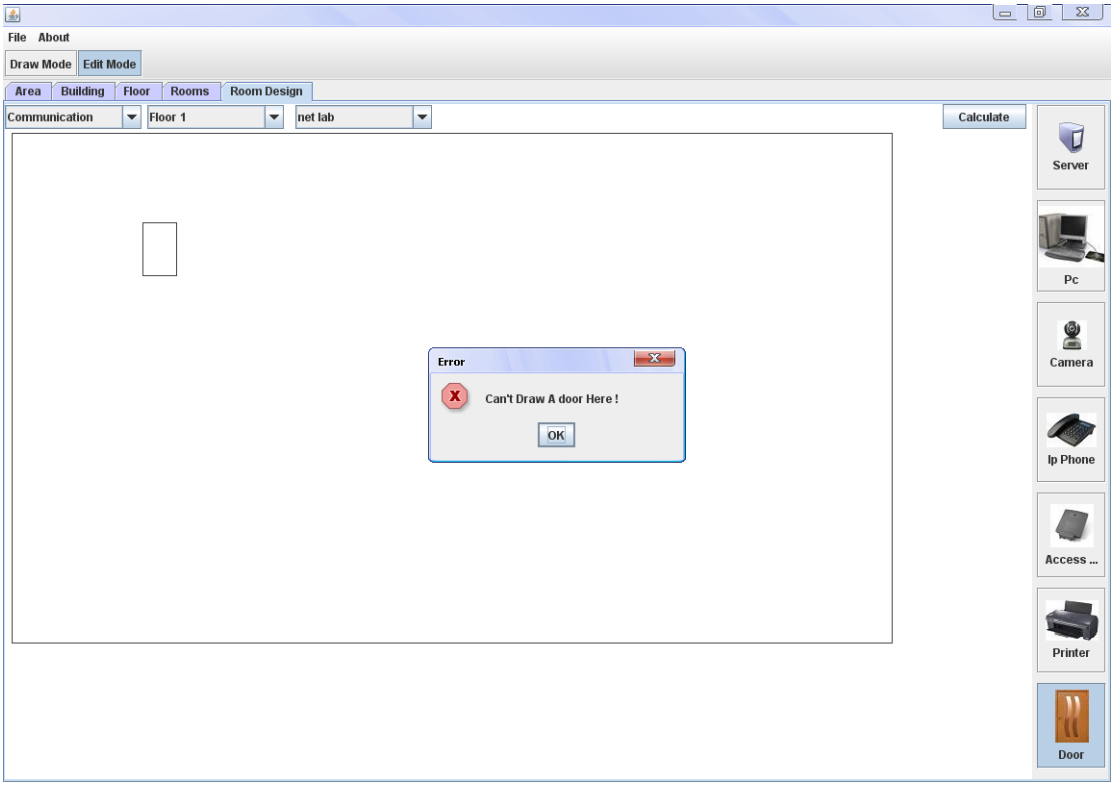
You can draw the number of rooms you want in the same manner as follow:



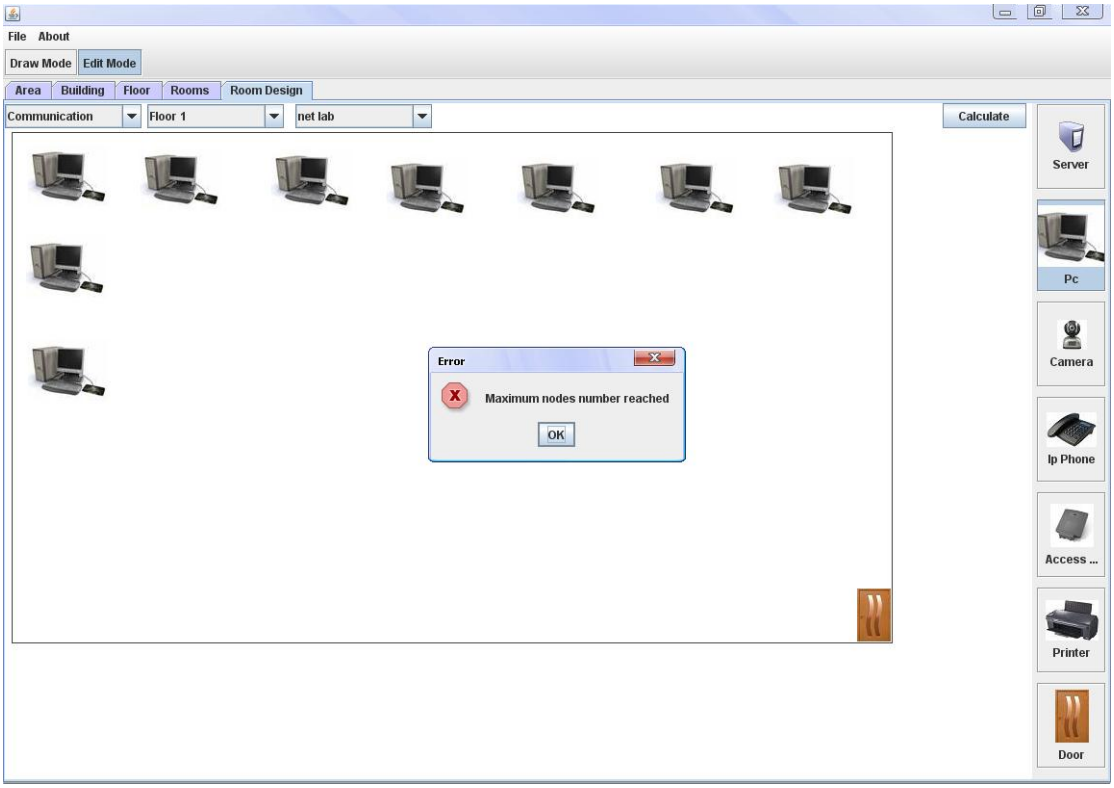
3-Room design:

After drawing the rooms then press the button of room design to draw the door at each room at any corner at the room, you can't draw the door at any place except the corners, if the door is in the middle of the wall, please approximate it to the nearest corner, Also you should draw one door only. So if there are more than one door, please choose the important one then draw it.

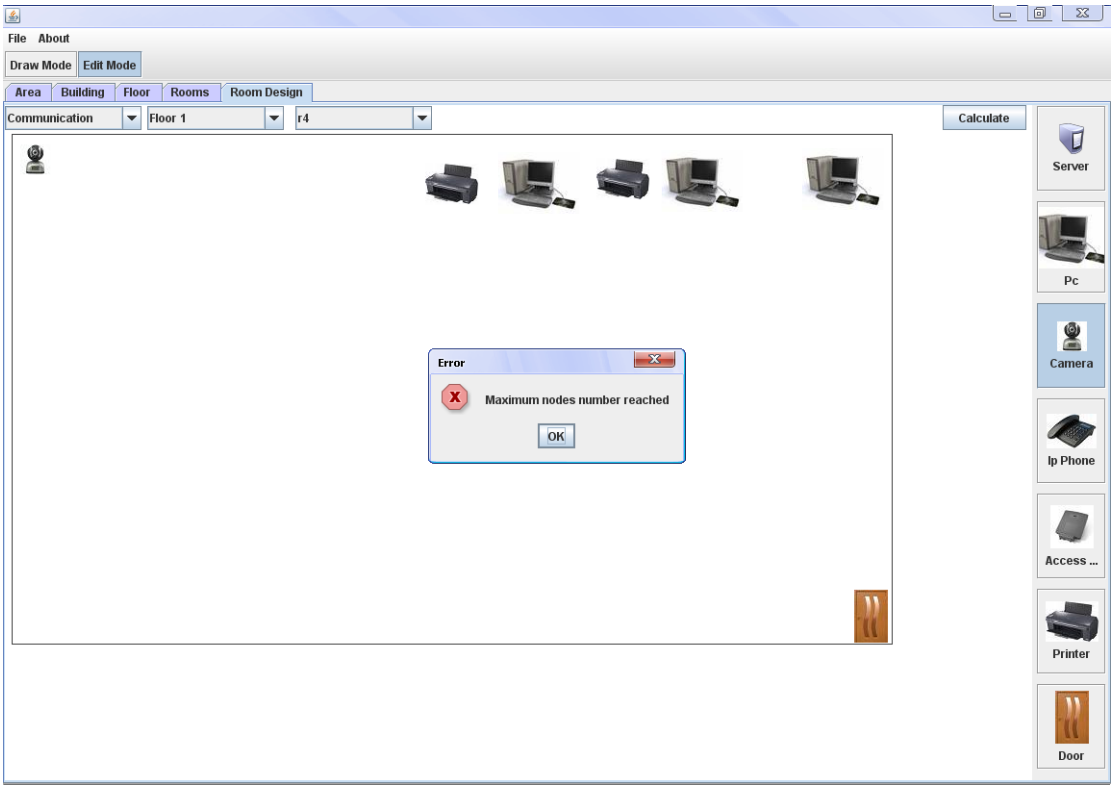
Select the door icon from the tool box right the page.



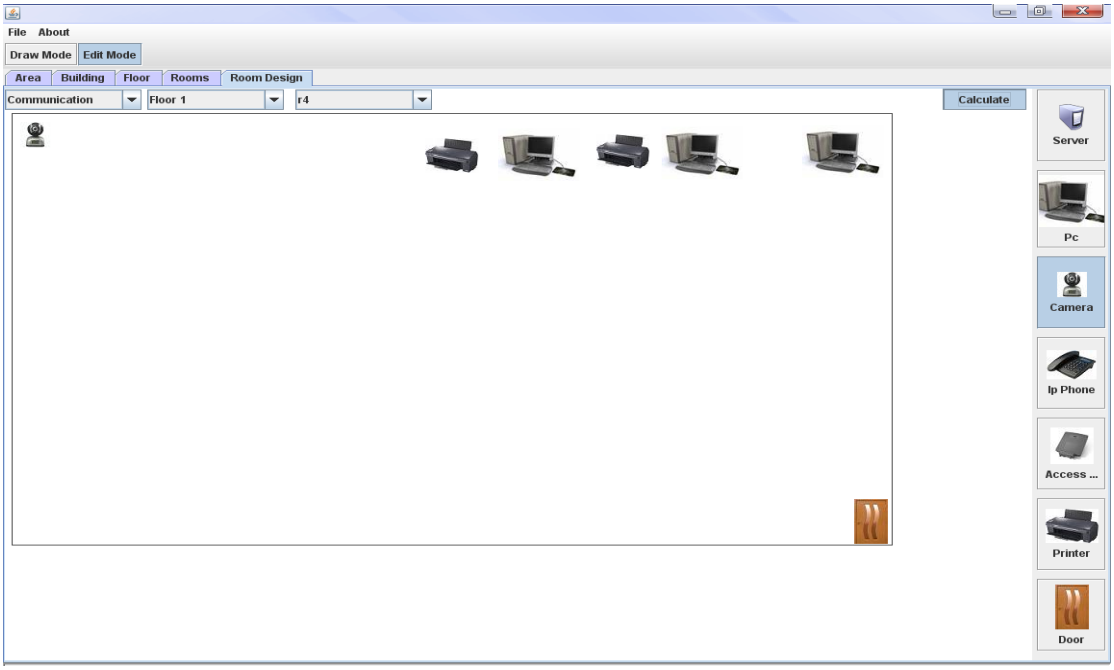
And then design the nodes inside the room by pressing at the shape of the node you want (PC, server …) as follow:



After you enter the number of nodes you have been written in the room properties dialogue box, and draw nodes larger than this number, a message will appear to inform you that maximum nodes number reached.

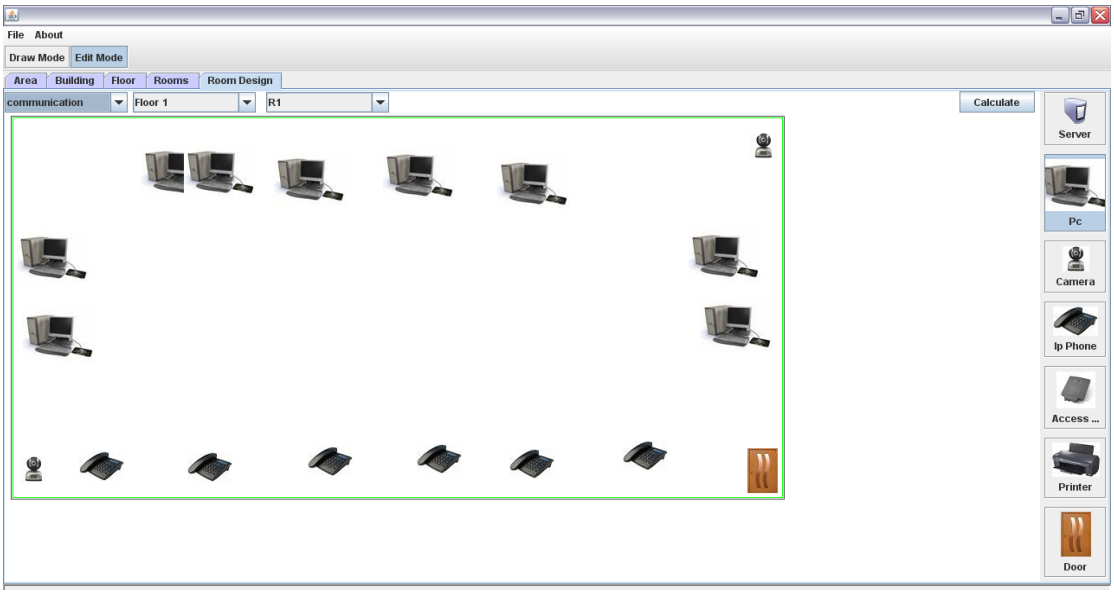


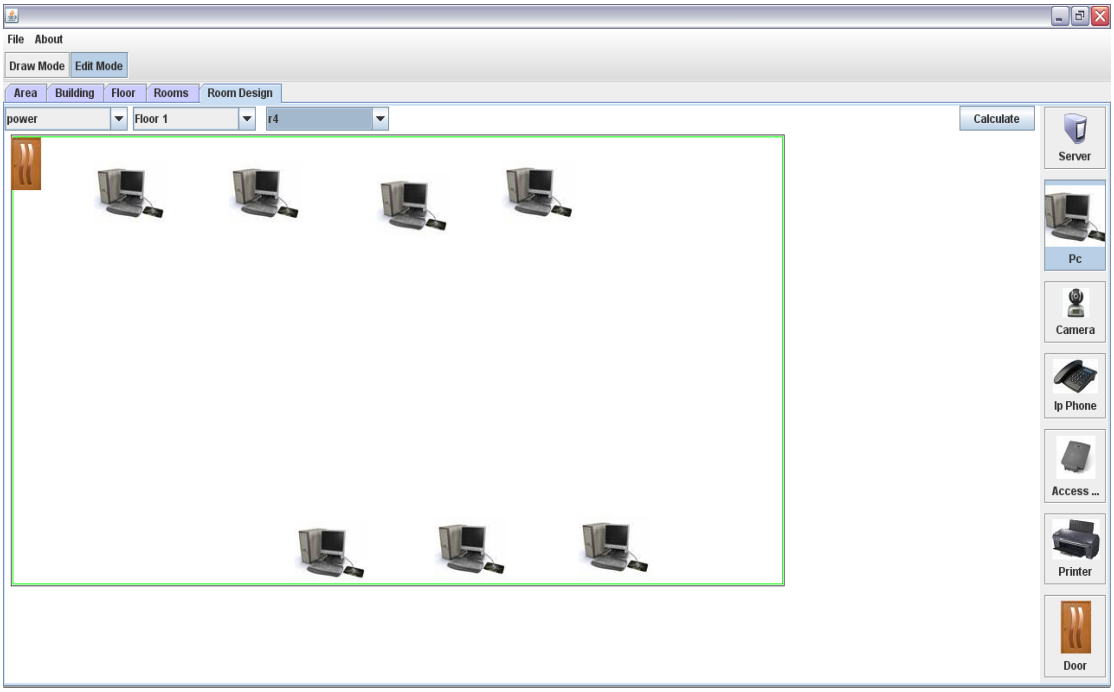
After finishing the design of each room, and to see the output of the program press calculate button to start design, as shown:



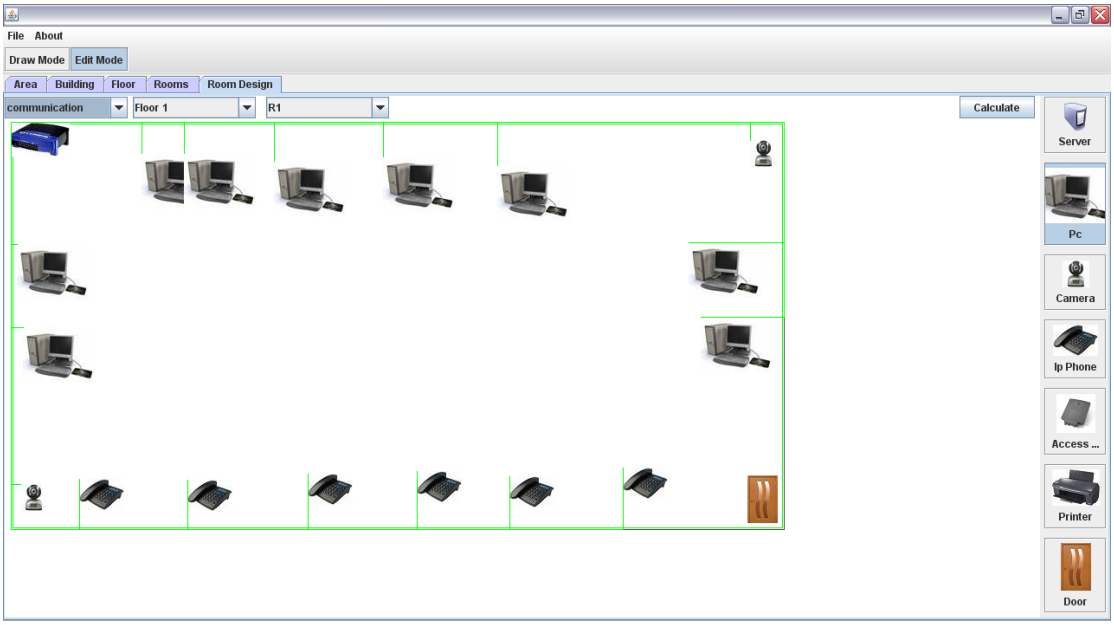
2-The output layer:

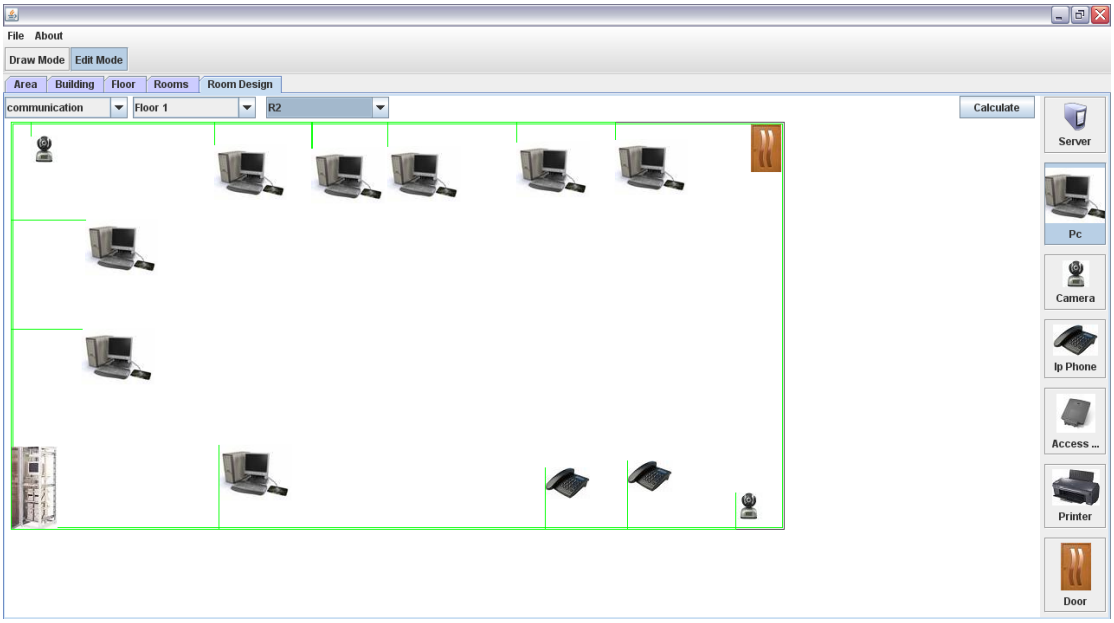
For the following simple example, if the input(site) consists of 2 buildings the first one contains one floor with 2 rooms and the second one of 2 floors the first one of 2 rooms also, the screen shots of the previous design are:

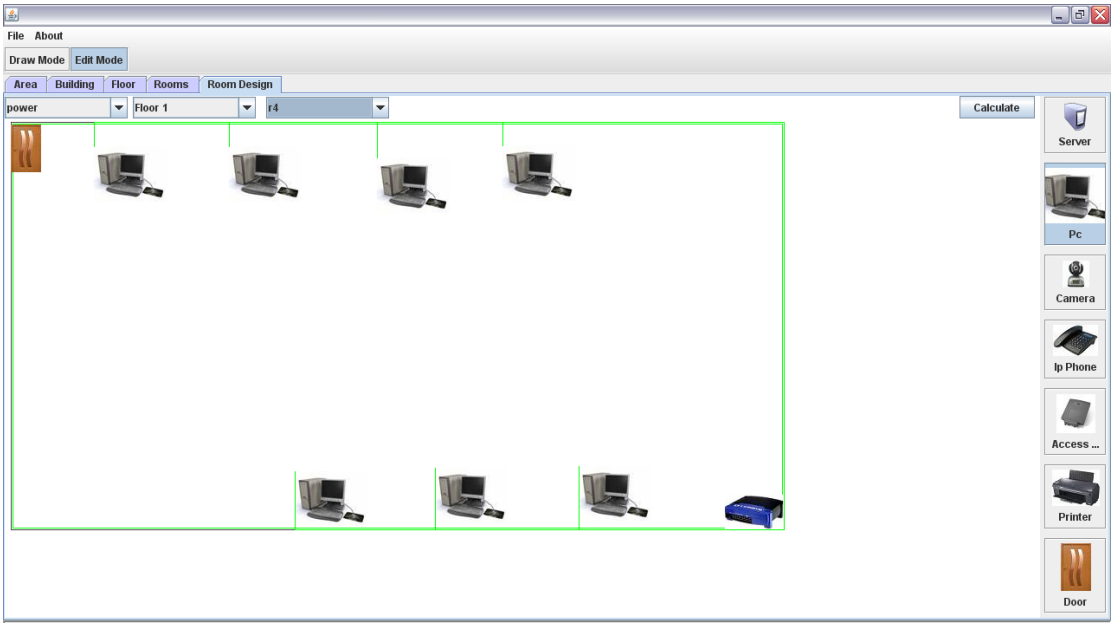




The output of this design is shown in the following screen shots:

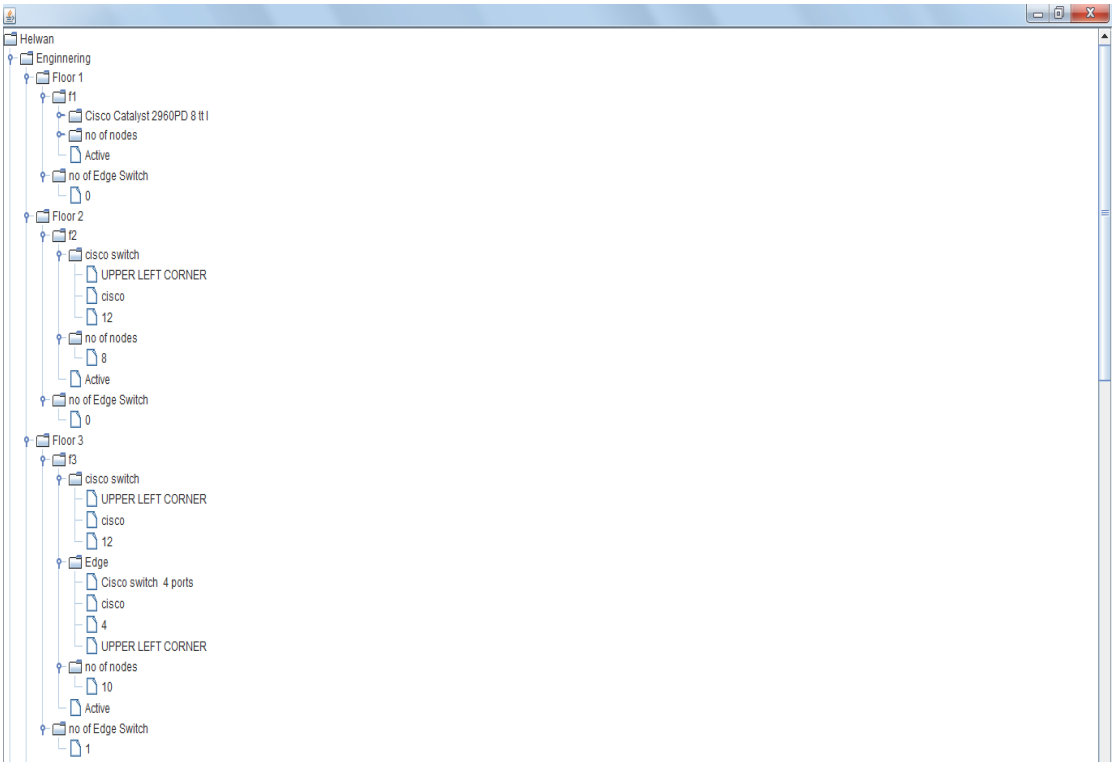


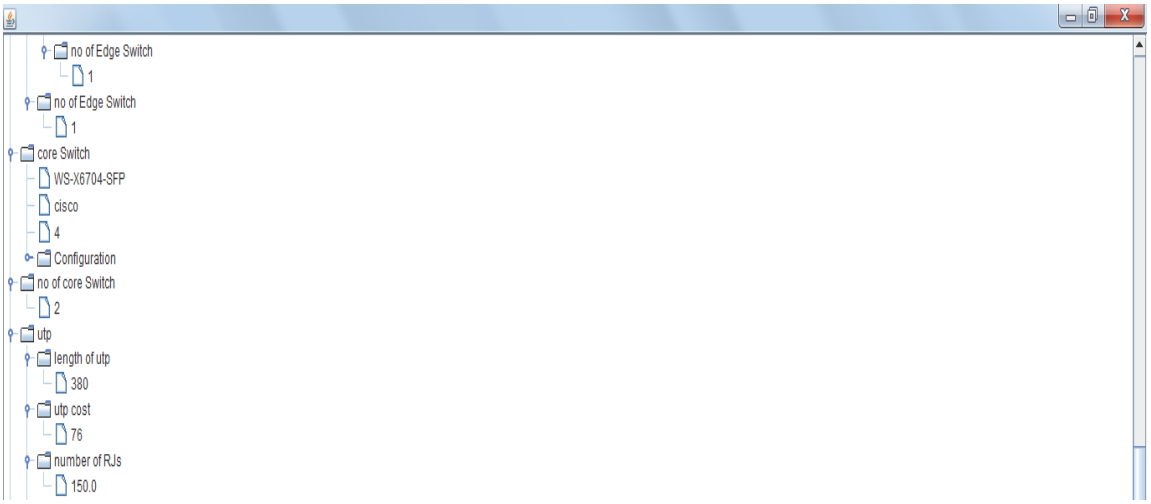

File
About
Draw Mode
Edit Mode
Area
Building
Floor
Rooms
Room Design
communication
Floor 1
R2
Calculate
Server
Pc
Camera
Ip Phone
Access ...
Printer
Door


File
About
Draw Mode
Edit Mode
Area
Building
Floor
Rooms
Room Design
power
Floor 1
r4
Calculate
Server
Pc
Camera
Ip Phone
Access ...
Printer
Door

Appendix

The following screen shot summarize the overall design in details as a tree:





Contributions

(In the java coding)

Name	Packages
Milad Shaker	org.networkplanner.topologies org.networkplanner.daofactory org.networkplanner.cost
Peter George	org.networkplanner.configrations org.networkplanner.designers org.networkplanner.validations
Ayman Mohamed	org.networkplanner.gui org.networkplanner.util org.networkplanner.vo
Ahmed Hagag	org.networkplanner.shapes org.networkplanner.images org.networkplanner.connections

Refrences:

CCDA Curriculum:

1. CCDA Self-Study: Designing for Cisco Internetwork Solutions; Diane Teare
2. Cisco CCDA Training Kit; Priscilla Oppenheimer
3. Inside Scoop to Cisco CCDA Certification: Exam 640-441; Mark A. Poplar
4. CCDA Cisco Certified Design Associate Study Guide: (Exam 640-441); Syngress Media, Inc

Communications and LAN Planning:

5. Data and Computer Communications, 8th Edition; William Stallings
6. Data Communications and Networking, 4th Edition; Behrouz A. Forouzan
7. NetCap: a tool for the capacity planning of Ethernet LANs; Vekiarides, L.
8. Installation of LANs-the pitfalls and hardware requirements; Capon, T.
9. A knowledge-based planner of LAN; Ginkou Ma; Hsiu-Ju Hsu ; Ronlon Tsai; Jiann-Liang Chen
10. Capacity planning of LAN using network management; Jha, S.K.; Howarth, B.R.
11. Network planning and tuning in switch-based LANs; Wenjian Qiao; Ni, L.M.

Java:

12. Java: How to Program, 8th Edition; Deitel
13. Java collections: an introduction to abstract data types, data structures, and algorithms; David A. Watt; Deryck F. Brown
14. Data Structures in Java; W. Collins
15. Object-Oriented Data Structures using Java 3rd Edition; Nell Dale; Daniel Joyce; Chip Weems
16. Java Generics and Collections; O'Reilly
17. Java Swing; O'Reilly
18. Java for Programmers; Paul J. Deitel; Harvey M. Deitel