Introduction to Basic Network

N.H. Samad, M.R. Mat Ramli

Diterbitkan :

POLITEKNIK METrO KUALA LUMPUR
No. 2 – 14, Jalan Setiawangsa 10, Taman Setiawangsa
54200 Kuala Lumpur

Introduction to Basic Network

First Published 2021
@ Politeknik METrO Kuala Lumpur

e ISBN 978-967-2623-92-2

Perpustakaan Negara Malaysia Cataloguing-in-Publication Data

N. H. Samad, 1993-
Introduction to Basic Network / N.H. Samad, M.R. Mat Ramli.
Mode of access: Internet
eISBN 978-967-26239-2-2
1. Computer networks.
2. Computer network protocols.
3. Government publications--Malaysia.
4. Electronic books.
I. M. R. Mat Ramli, 1970-. II. Judul.
004.6

Introduction to Basic Network

Preface

This ebook introduces you to Introduction to Basic Network. It mainly focuses on the foundation of networking, the components involved in networking, and the model used to allow a device to be able to communicate with each other

It is basically designed to help students in understanding and designing a logical network diagram using "Packet Tracer" as well as to be able to explain the logic behind computer networks. Important concepts are presented in the context of infographics and diagrams, Well-chosen examples make it clear how the details of networking protocols are used

Since this ebook provides an outlook of the overall foundation of networking, after going through this material, you will find yourself at a moderate level. It will heaps your knowledge from basics to the next levels

Acknowledgement

The highest gratitude to Allah SWT because with His permission, this Introduction to Basic Network was successfully published. This ebook is published as a guide or reference for students who take the Introduction to Network course at Malaysia Polytechnic. In preparing this ebook, various challenges and obstacles need to be faced before being able to produce an ebook. We would like to express our deepest gratitude to our family, the Polytechnic e-Learning Coordinator, and colleagues for their guidance and support in the production of this ebook.

A special thanks to Mr. Mohd Safwan Bin A. Aziz for all his support and guidance in the completion of this ebook.

We would also like to thank the following for permission to reproduce copyright photos:

- Cisco
- Canva
- pngset

We hope that this ebook can be put to good use by all who use it. Thank you.

Nur Hanifah Binti A. Samad, Mohd Rizuan Bin Mat Ramli
October 2021

Table of Contents

Introduction to Basic Network

Chapter 1

Networking

Chapter 1

Introduction to Network

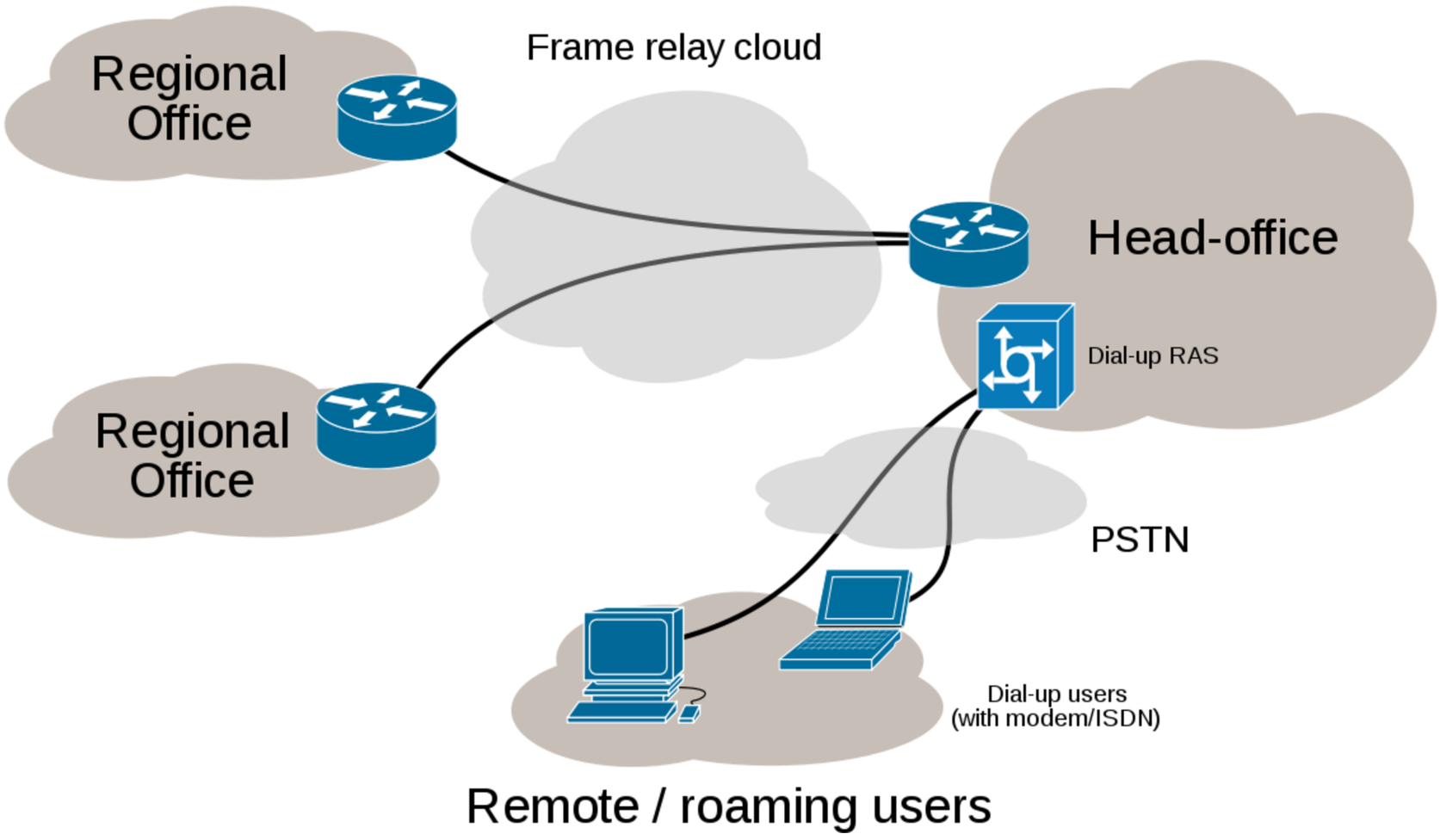
We rely on communication almost as much as we rely on air, water, food, and shelter. We are more connected than ever before in today's society because of the utilization of networks. Nowadays, in order for us to communicate we need a network even just to do a simple transaction

Network can be described as linking a computer to use for transferring to collect information and be able to communicate with each other. According to the Cambridge Dictionary network is defined as a large system consisting of many similar parts that are connected together to allow movement or communication between or along with the parts, or between the parts and a control center.

There is mainly 3 important functions of networking which is:

1. Sharing data,
2. Sharing resources and
3. Sharing application.

Chapter 1



A network allows users to share any data between the connected devices without the need for external devices such as a portable USB drive or a portable hard disk drive.

Network also allows users to share any devices such as printers between the connected computers. For example, in a small office, the main printer is connected to a LAN cable allowing all the computers in the same network able to access the printer without actually needing to use a USB cable. Furthermore, network also allows users to share an application among the connected devices.

An application is installed at two parts in application sharing:

- the server application
- the client application

Both components are used to deliver and request data or services. Users are able to use the Internet to remotely view and control a particular software application on someone else's computer in application sharing.

A network consists of two or more entities sharing resources and information

Chapter 1.1

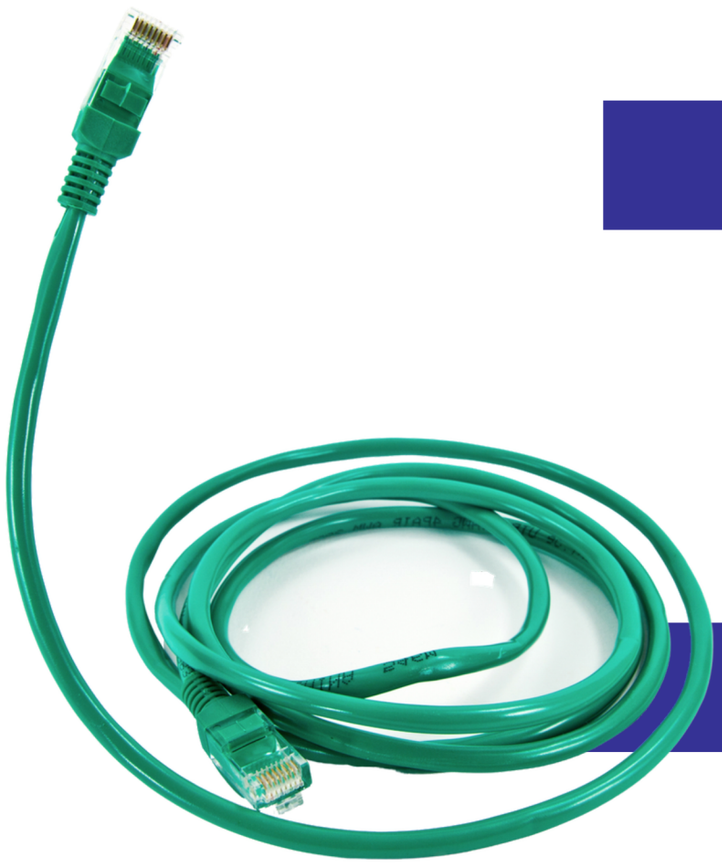
Network Component

A message's journey from source to the destination might be as simple as a single wire linking two computers or as complicated as a network that covers the world. This network architecture serves as the network's foundation. It provides a solid and trustworthy route which communication can occur,

The network infrastructure contains three categories of network components as follow.

END DEVICE

INTERMEDIARY DEVICES



NETWORK MEDIA

A network covering a larger area than a single

END DEVICE

An end device is a device that sends or receives the data in the network such as a PC, Laptop, Smartphone, or any other device that has the ability to send and receive data and is connected with the network. There are two categories of end devices which is client and server. The client is the device that receiving the data from the server meanwhile server is the device that providing or sending the data to the client.

Some examples of end devices are:

- Computers (laptops, file servers, web servers)
- Network printers
- VoIP phones
- Security cameras
- Mobile handheld devices (such as smartphones, tablets, wireless debit/credit card readers and barcode scanners)

QUICK TIPS

Client-based networks take advantage of their own powerful processors as well as the increasingly powerful computers used as typical workstations

NETWORK MEDIA

A medium is used to carry communication across a network. The medium acts as a conduit for the message's transmission from source to destination.

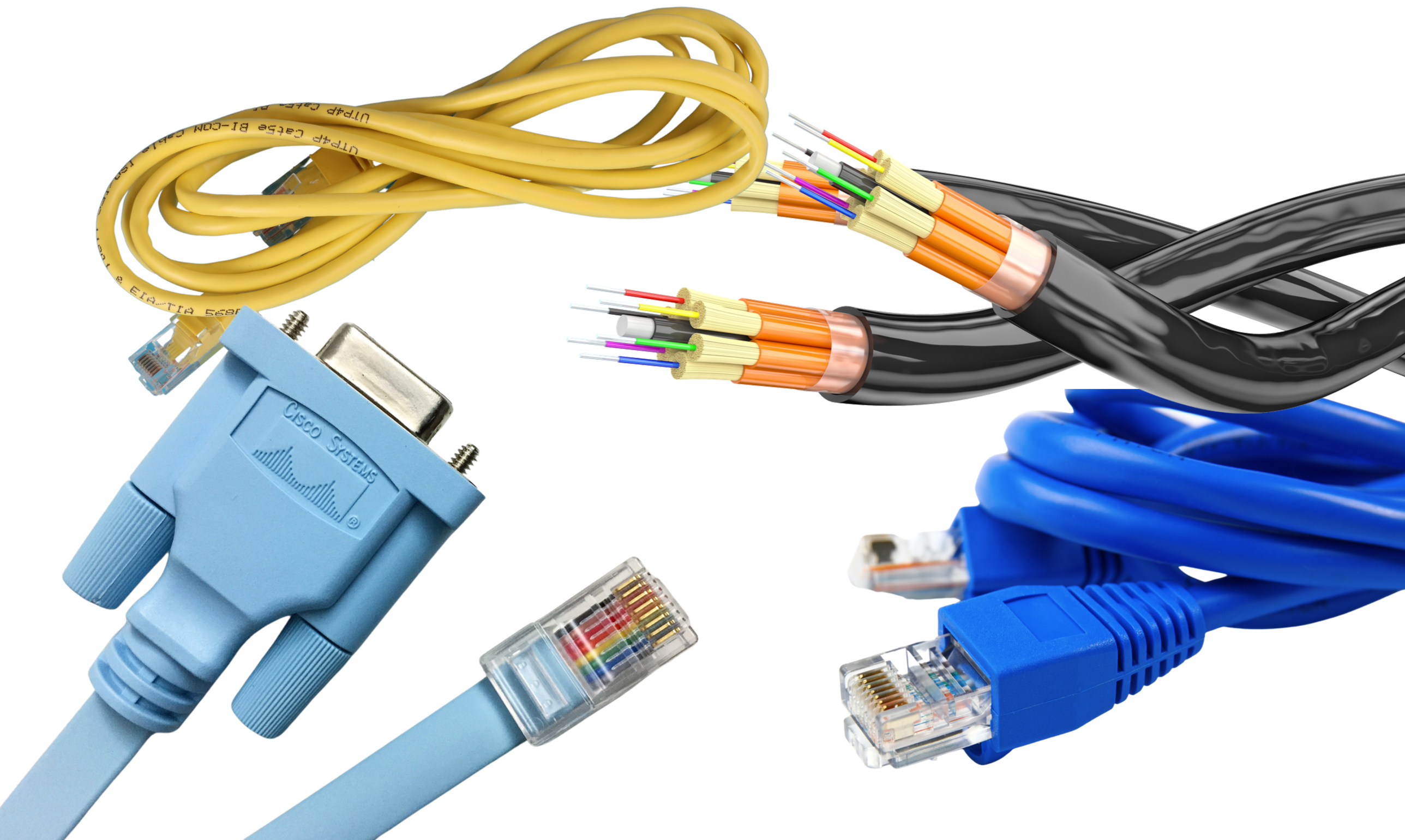
To link devices and provide a channel for data transmission, modern networks typically employ the three types of media listed below:

- Copper
- Fiber optic cable (glass or plastic)
- Wireless

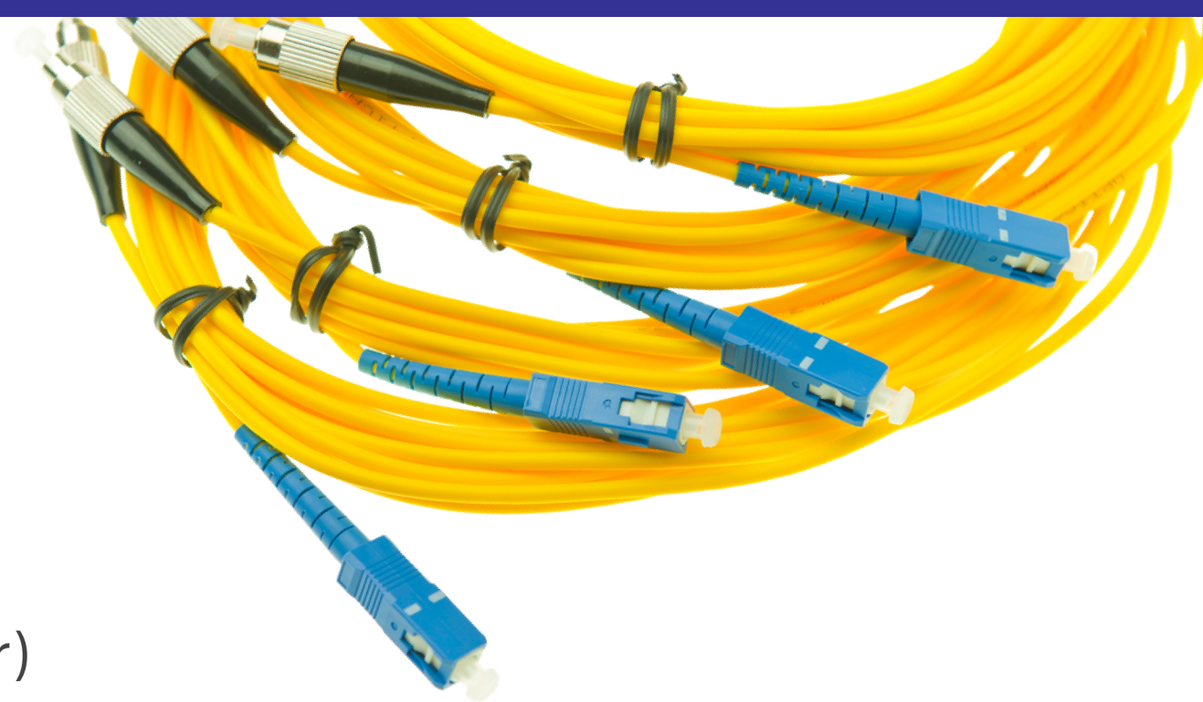
For each media type, the signal encoding that would occur in order for the message to be delivered is different. The data is encoded into electrical impulses that fit certain patterns on metallic wires.

Light pulses in the infrared or visible wavelengths are used in fiber optic communications. The various bit values are represented by patterns of electromagnetic waves in wireless transmission.

The advantages and benefits of various forms of network media vary. Not all forms of network media have the same properties or are suitable for the same use.



FIBER OPTIC



- Made of glass or plastic.(thin as hair)
- Transmit data using pulses of light.
- It is immune to EMI and is suitable for installation in environments where interference is a problem.
- Fiber optic cables support a large amount of bandwidth making it suit for high-speed data backbones (ISP connection).
- Widely used in enterprise environments and large data centers.

COPPER (UTP)

- The most commonly encountered type of network cable in North America and many other areas.
- Inexpensive, and offers high bandwidth and is easy to install
- Used to connect phone lines, hosts and network devices
- Come with many different numbers of pairs inside the jacket, but the most common number of pairs is four
- The UTP cable types which are still commonly found include Categories 5, 5e, 6, 7 and 8
- All Categories of UTP cable are traditionally terminated into an RJ-45 connector

WIRELESS

- Wireless signals follow a number of different paths to attain the destination because of reflection
- The strength of the signal reaches a receiver is lower than the transmitted signal due to signal degradation
- Experienced attenuation and noise as the signal travel far away
- Wireless signals susceptible to noise often called interference
- Signals have to be amplified (analog signal) or repeated (digital signal) to overcome attenuation

INTERMEDIARY DEVICES

An end device is a device that sends or receives the data in the network such as a PC, Laptop, Smartphone, or any other device that has the ability to send and receive data and is connected with the network. There are two categories of end devices which are client and server. The client is the device that receives the data from the server meanwhile server is the device that provides or sends the data to the client.

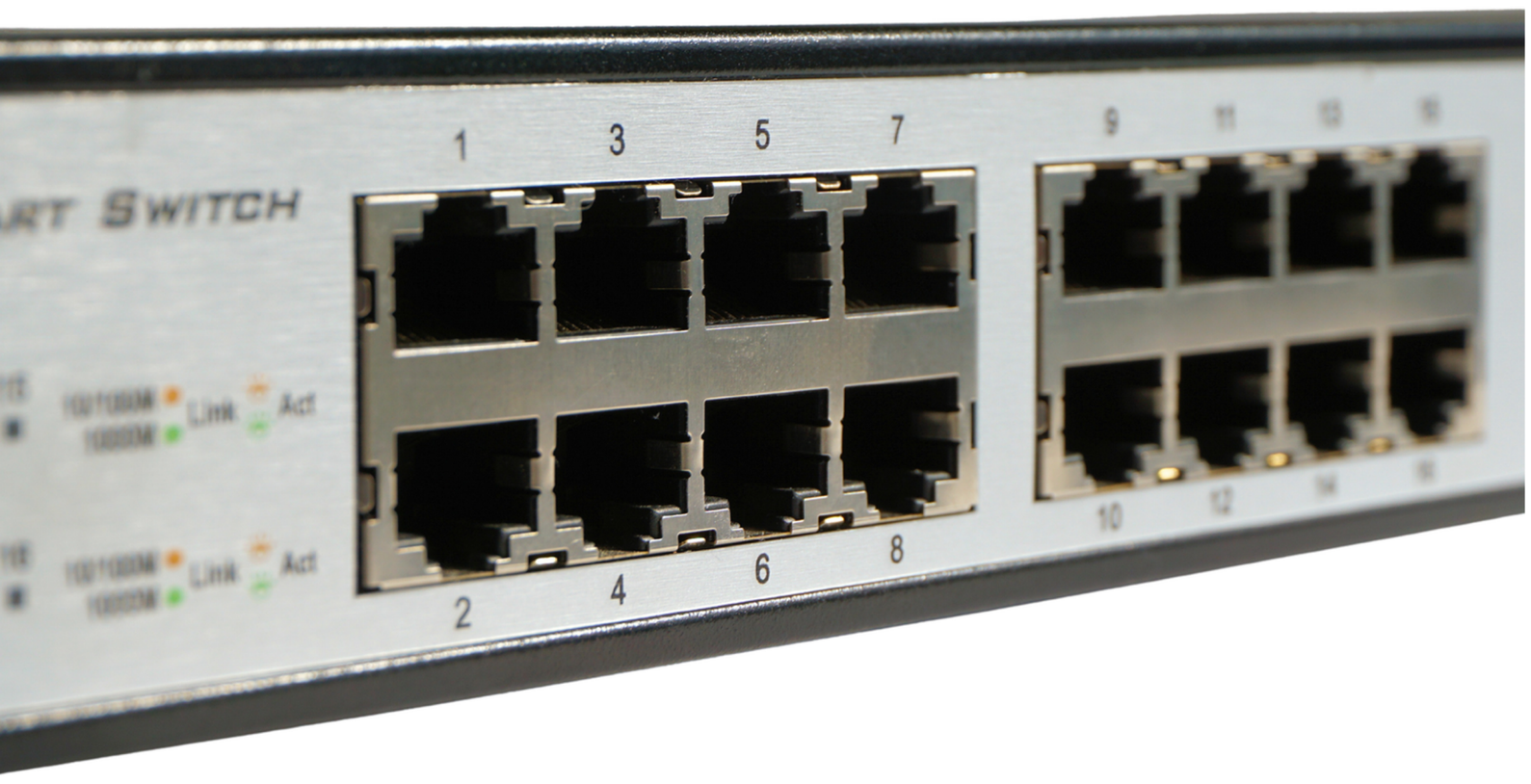
Some examples of end devices are:

- Computers (laptops, file servers, web servers)
- Network printers
- VoIP phones
- Security cameras
- Mobile handheld devices (such as smartphones, tablets, wireless debit/credit card readers and barcode scanners)

Switch

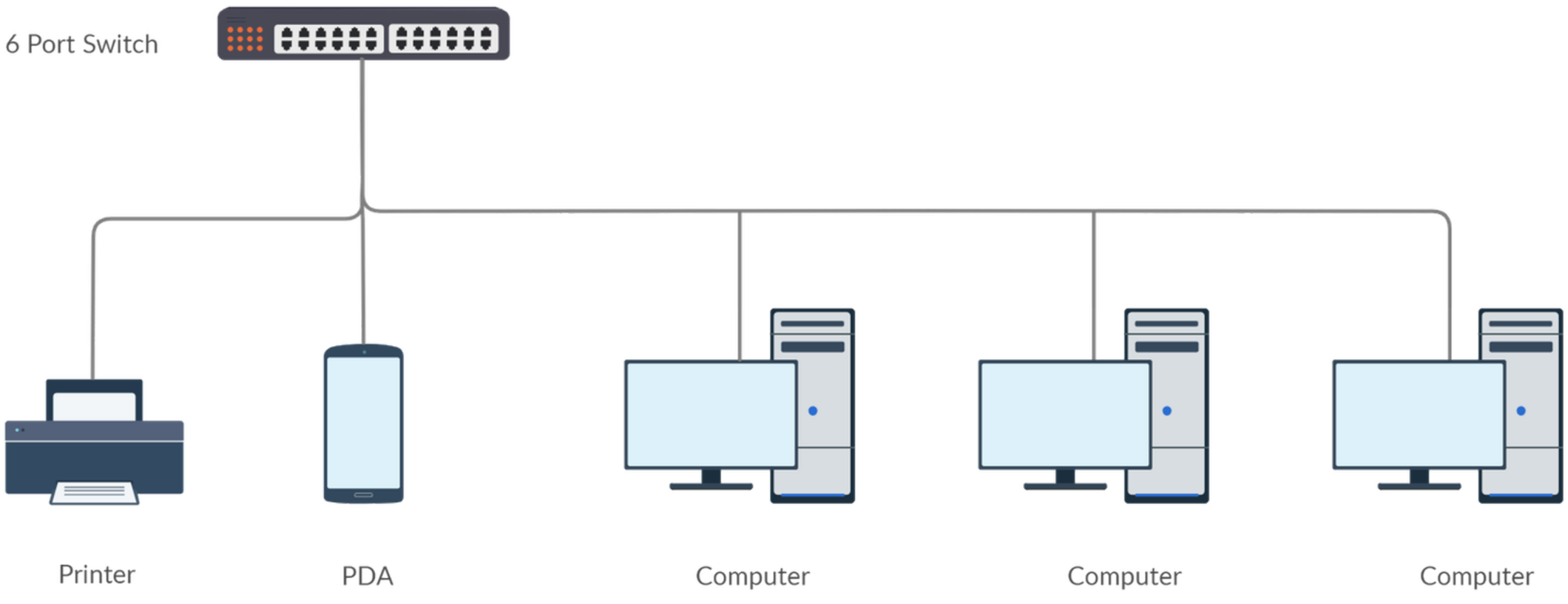
Bridges

Router



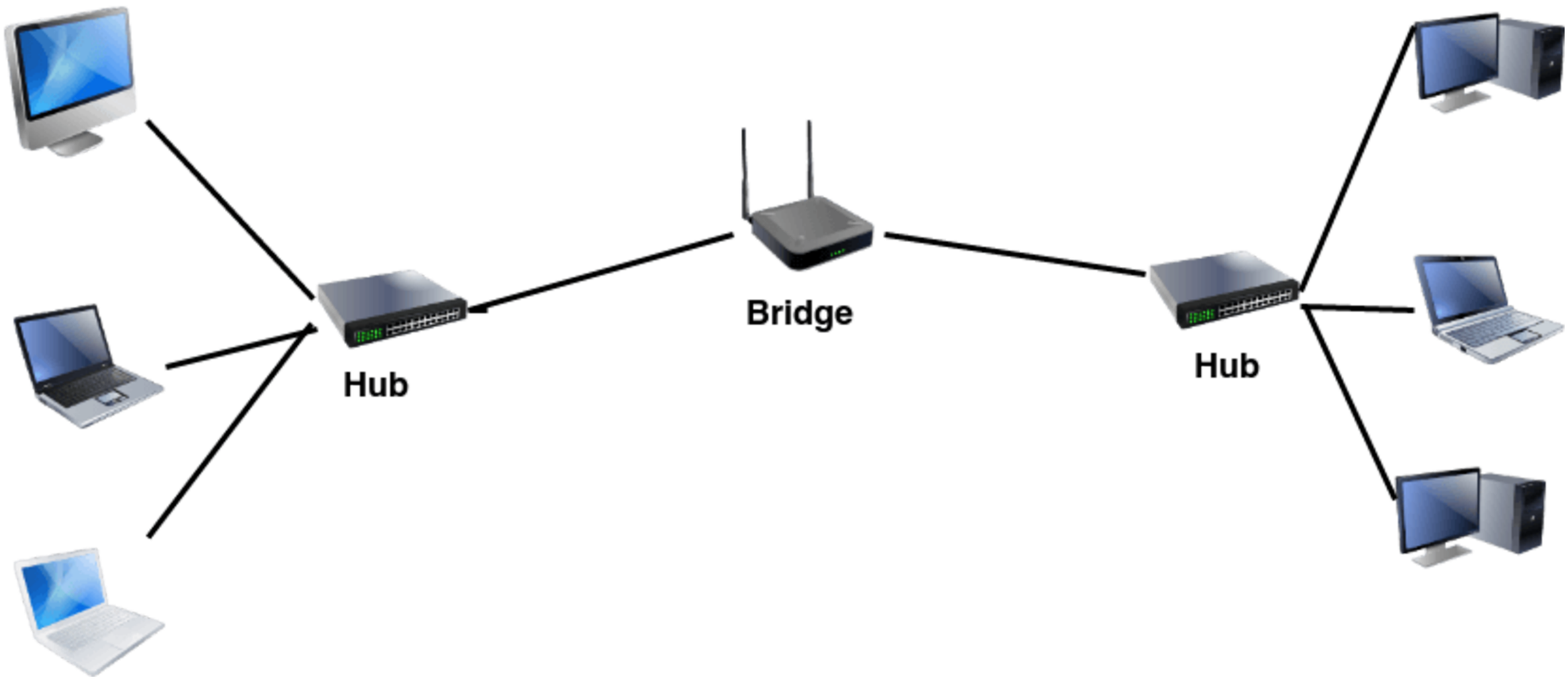
SWITCH

- Used to connect computers to the same or different network. , Bandwidth 10/100/1000 Mbps, each port is not shared
- A switch operates at the Data Link layer of the OSI model and can interpret MAC address information
- A switch able to determine whether to filter (discard) or forward packets it receives.
- It is a connectivity device that logically subdivides a network into smaller, individual collision domains.
- A switch provides better security than many other devices because they isolate one device's traffic from other devices' traffic.



HUB

- The most commonly encountered type of network cable in North America and many other areas.
- Inexpensive, and offers high bandwidth and is easy to install
- Used to connect phone lines, hosts and network devices
- Come with many different numbers of pairs inside the jacket, but the most common number of pairs is four



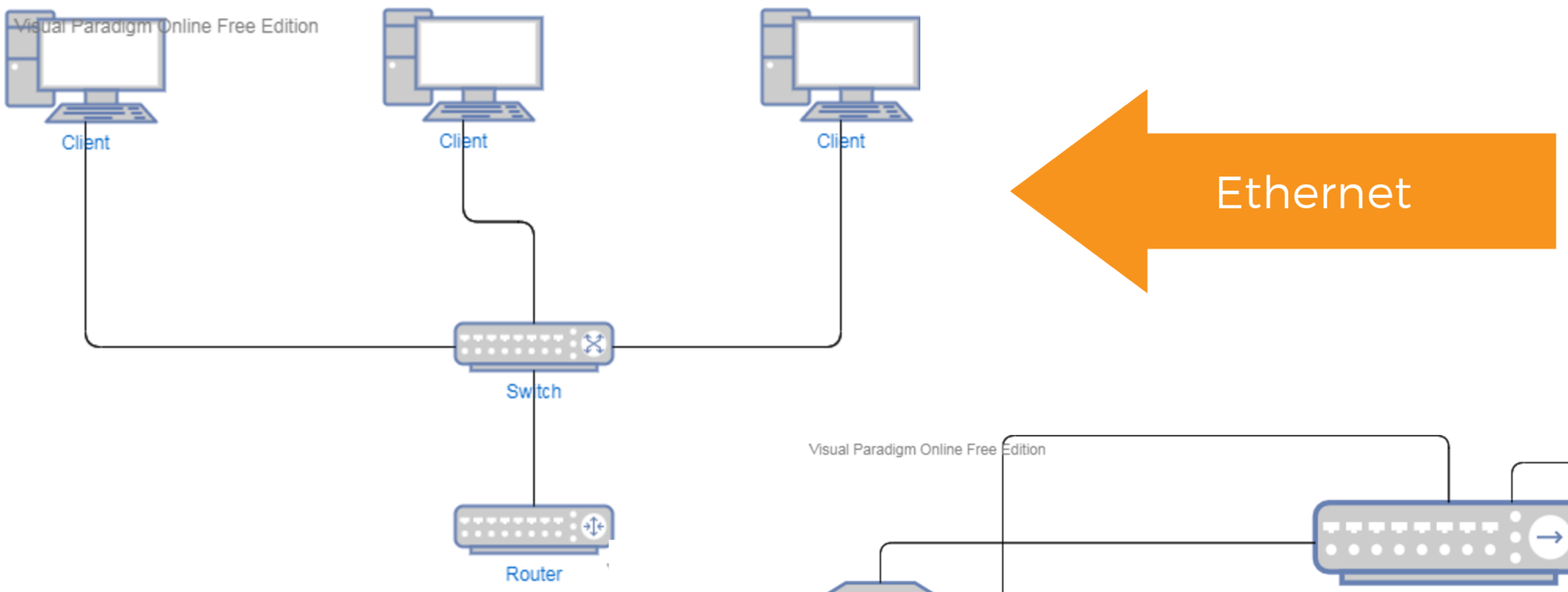
ROUTER

A router is a networking device that connects a local network to other local networks. Routers, like switches, are able to decode and read the messages that are sent to them. Routers decode the packet that is encapsulated within the frame. The packet format contains the IP addresses of the destination and source hosts.

When a router receives a data packet on its interfaces, it will check the destination address of that packet, and forwards that data packet address to the interface that is associated with the destination address.

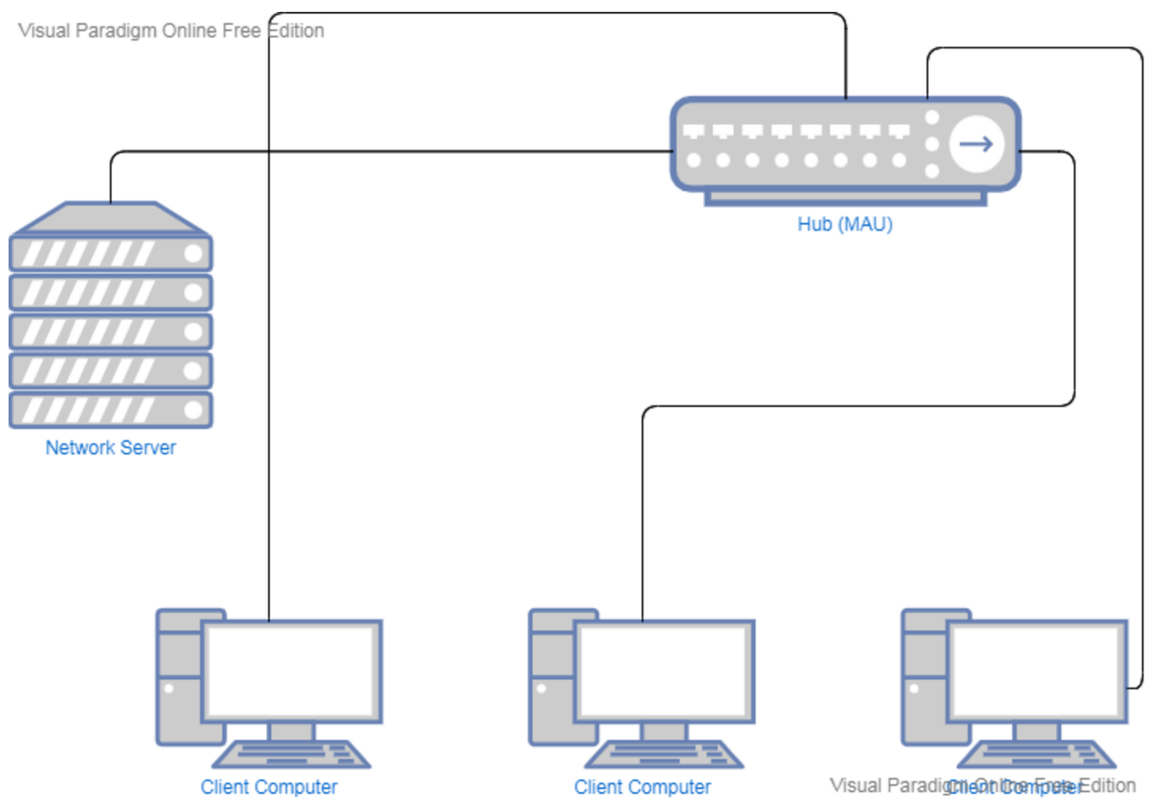
In order to successfully forward the data packets to their destination, the router keeps a record in a database table form known as the routing table of the connected network. Routing tables can be created statically or dynamically.

Some of the main functions of a router are to connect different network protocols, to break a large network into smaller networks and to connect two different media types. A router is also used to connect two different network architectures such as Token Ring and Ethernet and to access DSL services.



Ethernet

Token Ring

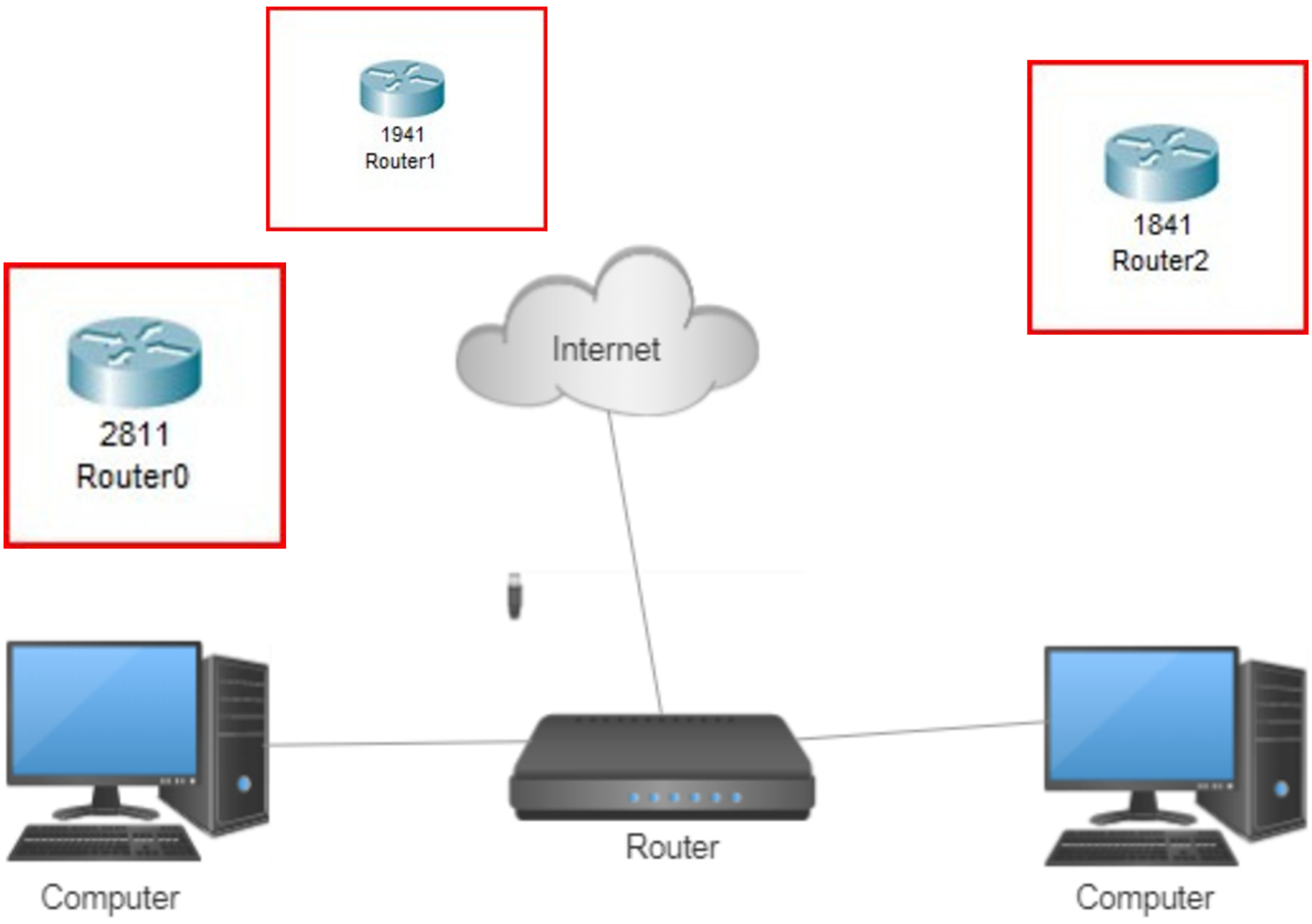


ROUTER

There are several types of a router such as The Cisco 1941 Integrated Services Router (ISR) which provides 2 integrated 10/100/1000 Ethernet ports, 2 WAN Interface Card (WIC) slots and 1 Internal Services Module slot,

The Cisco 1841 Integrated Services Router provides two fixed 10/100 (100BASE-TX) Ethernet ports, two integrated High-Speed WAN Interface Card (HWIC) slots that are compatible with WAN Interface Card (WICs) and Voice/WAN Interface Cards (VWICs), and one internal Advanced Integration Module (AIM) slot,

The Cisco 2811 Integrated Services Router provides one Enhanced Network-Module slot with two fixed 10/100 (100BASE-TX) Ethernet ports, four integrated High-Speed WAN Interface Card (HWIC) slots that are compatible with WAN Interface Card (WICs), Voice Interface Cards (VICs) and Voice/WAN Interface Cards (VWICs), and dual Advanced Integration Module (AIM) slots. The majority of each routers have a different slots and ports.



Chapter 1.2

Common Type of Network

LAN

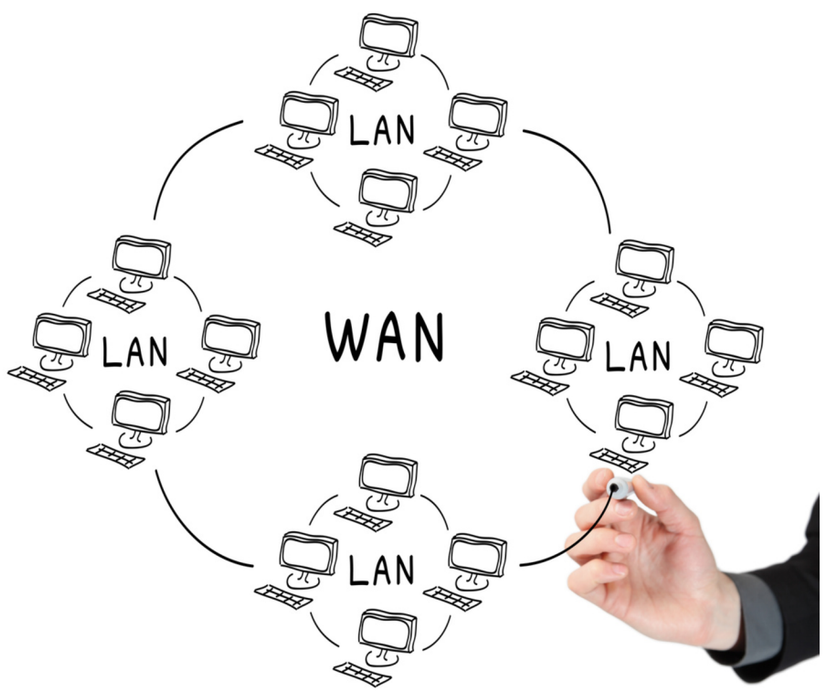
A computer network is frequently defined by the geographical location where the network is implemented. A LAN (local area network). For example, devices such as computers that are connected to each other at school, at a company,

Internet cafe, and between neighbouring homes. Local area network or LAN has a high data rate compared to others type of network and does not require telecommunications lines leased from telecommunications operators. However, the data transfer coverage area of the local area network is not so broad and communicating outside the network becomes more difficult

WAN

WAN (wide area network) connects computers across continents. The internet is the most well-known example of a WAN, as it connects billions of computers all over the world that serves as a source of information in a variety of discipline. It also offers a variety of services, including e-mail, network chat (MSN, ICQ), web, file transfer (FTP), online gaming (Ragnarok), and website traffic (Web).

Fiber optic cable usually will be used in WAN network where the cable will be implemented in the ground or passing it under the sea. There are a few WAN network characteristics such as it is used to connect one local area network with another local network so that users or computers in one location can communicate with users and computers in other locations and its covers a large area



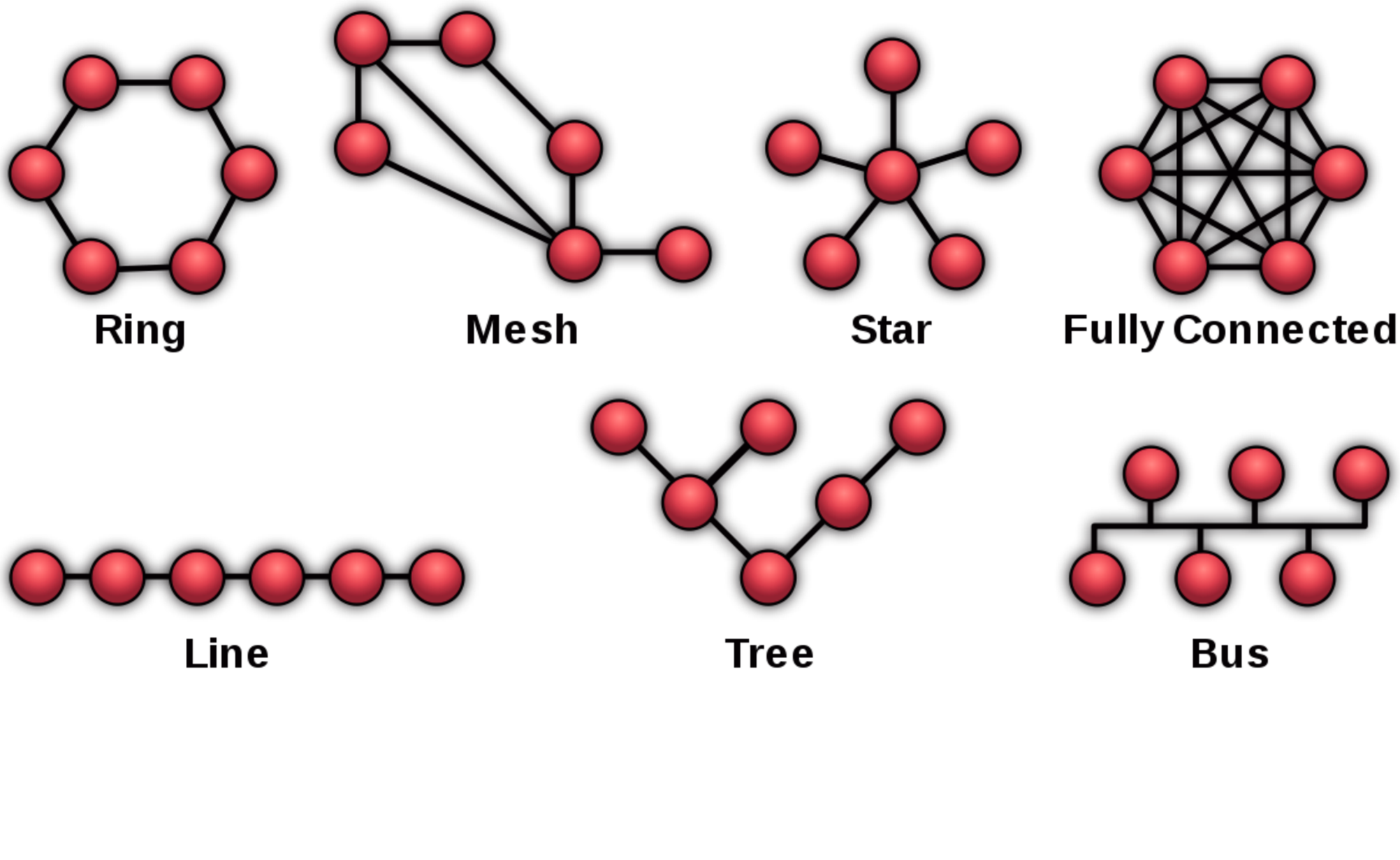
Chapter 1.3

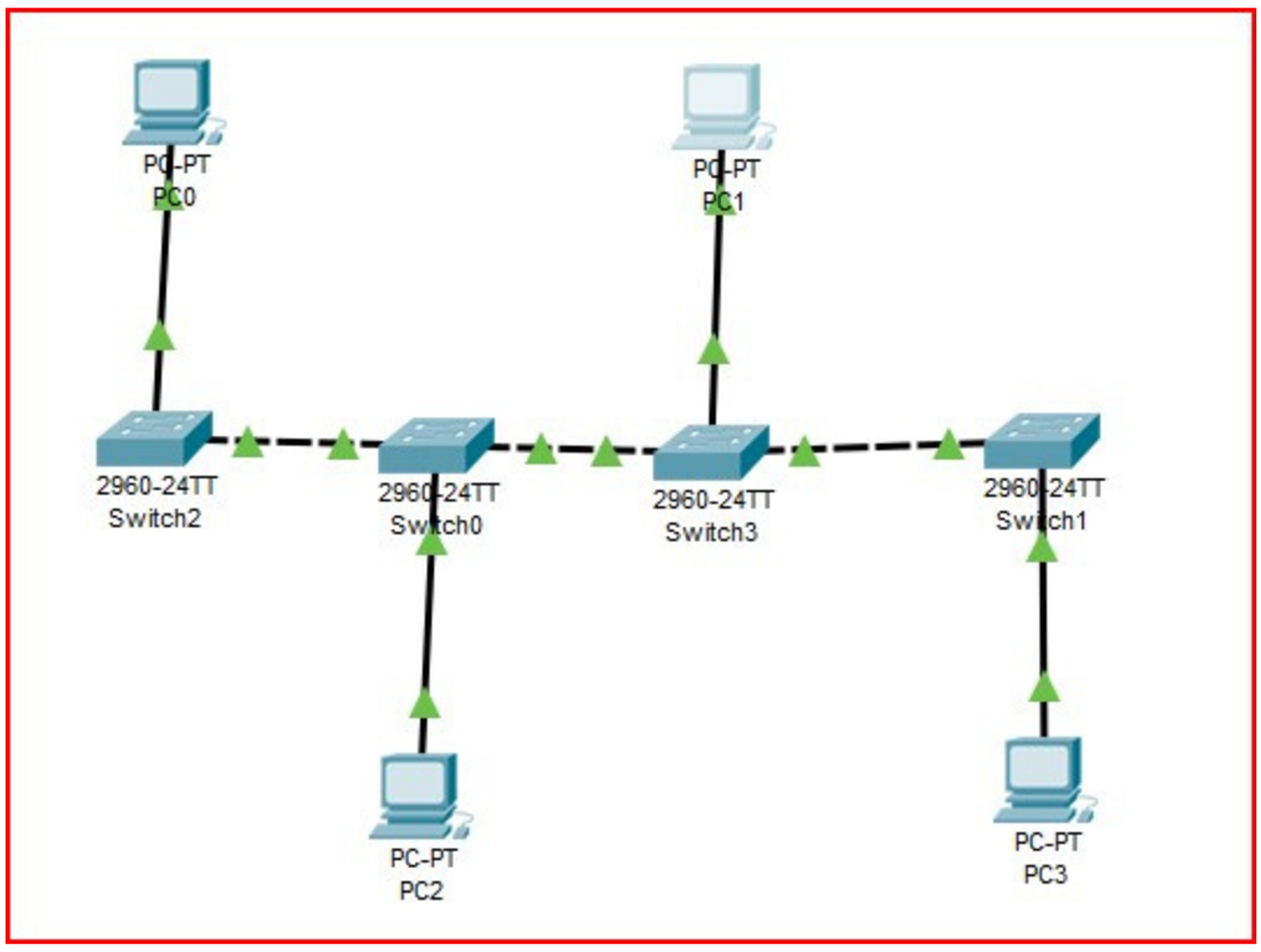
Common Network Topology

The network topology is the link that connects end users to a data centre and connects data centre equipment. It's critical to choose a topology that meets both the data center's and the end users' requirements. If the data centre is responsible for serving a mission-critical application and network availability is important, a topology with several levels of redundancy, such as full-mesh, is the best option.

In the event that a cable or node in the network/data centre breaks, this design will assist prevent network disruptions. If the data center's supported application isn't mission-critical, and network disruptions aren't a major issue, then a less expensive data centre could be appropriate

If the application supported by the data center is less critical and network outages would not cause a serious problem, then a less expensive topology, such as star or extended star, would be more appropriate





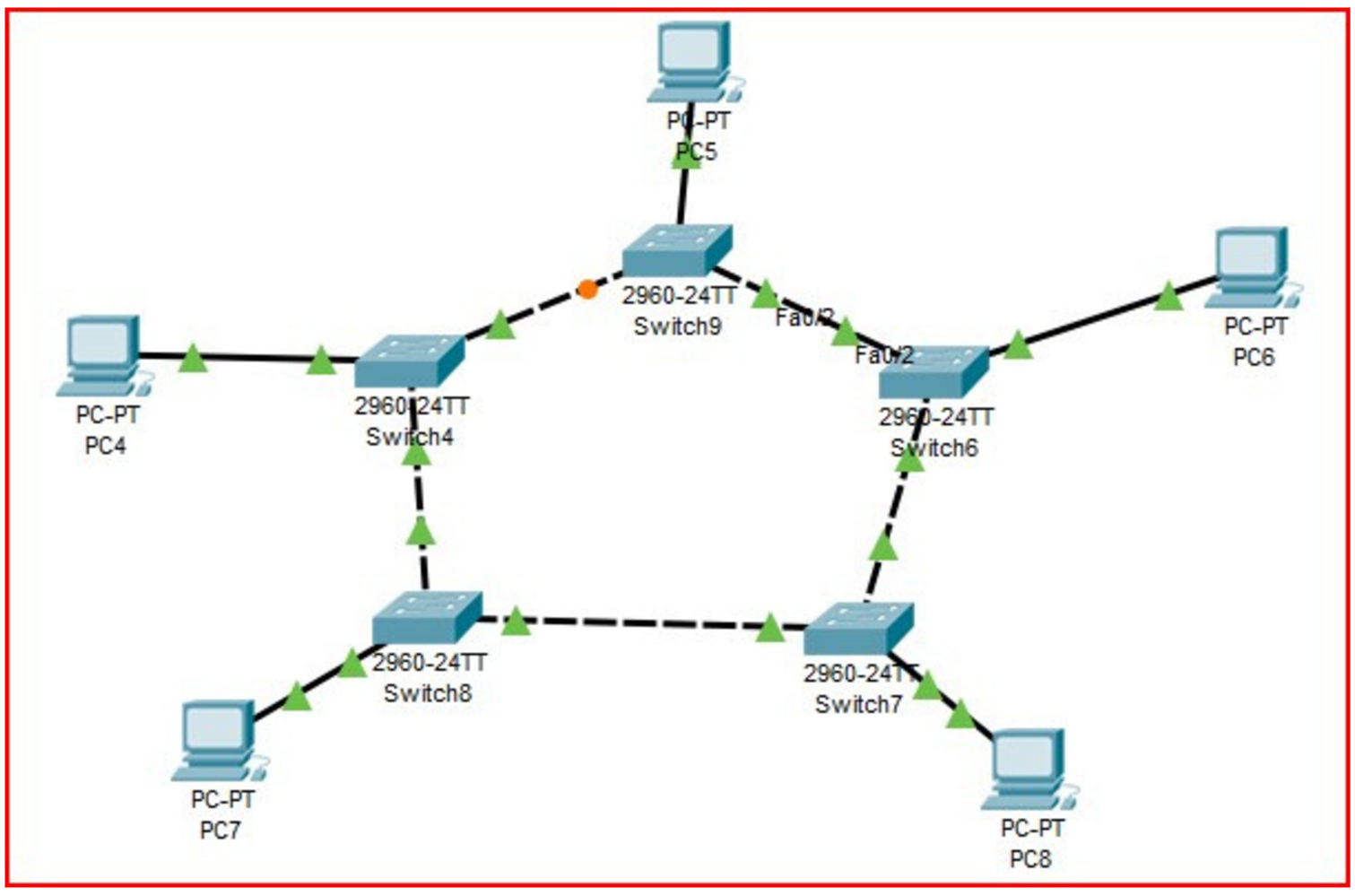
BUS TOPOLOGY

TWhen all of the network's nodes are linked to a single cable, it's called a bus topology. A backbone is a term used to describe a single cable. For early coaxial cable Ethernet networks, bus topology was utilised for 10Base-2, ThinNet, and 10Base-5, ThickNet. Messages sent by a node are broadcast to all nodes on the network under this architecture.

The message is only accepted and processed by the designated recipient node. This network architecture is simple to set up and inexpensive to maintain. Both ends of the backbone cable must be terminated in this topology. If the backbone isn't terminated, signals will likely bounce back from the cable's end, resulting in data collisions and noise.

If the backbone isn't terminated, the signal will bounce back from the cable's end, producing data collisions and noise that might damage the network. The primary disadvantages of this network design are the limited number of computers that may be linked to the network and the fact that all nodes are connected by a single backbone connection.

A network using a bus topology can only support a few dozen machines. If the network's performance surpasses this limit, issues are likely to arise. The entire network will become unstable and may stop functioning if the backbone connection linking all of the nodes fails.



RING TOPOLOGY

When all of the nodes in a network are connected in a circle, it is called a ring topology. Each node in the network serves as a repeater, ensuring that the signal remains strong across the network. A node will create a signal that is targeted to a specific computer on the network, and the signal will then be transmitted clockwise or counterclockwise through the network.

It's crucial to remember that in a network with this architecture, all signals must flow in the same direction. The quantity of data collision and noise on the network is reduced as a result. The signal will pass via each node until it reaches its final destination.

If the backbone isn't terminated, the signal will bounce back from the cable's end, producing data collisions and noise that might damage the network. The primary disadvantages of this network design are the limited number of computers that may be linked to the network and the fact that all nodes are connected by a single backbone connection.

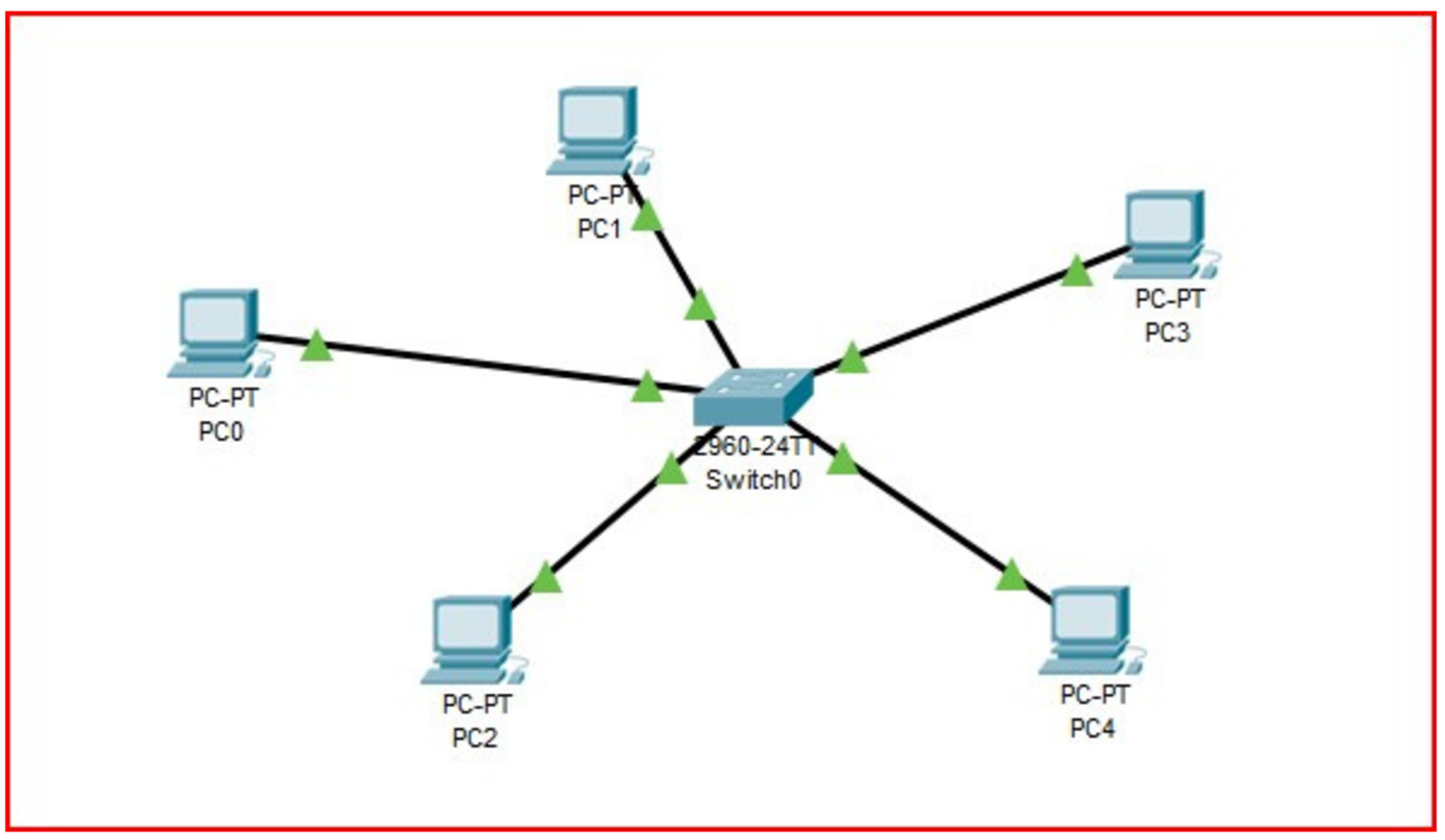
Typically this type of network will use a Token Ring protocol, which enables only one computer to broadcast a signal at a time, which is commonly used in this sort of network. The primary disadvantage of this architecture is that if one or more of the nodes or the cables connecting them break, the network would become unstable and could stop working. A double ring topology is the answer to this flaw. In the event of a failure, the double ring adds a secondary cable for redundancy.

STAR TOPOLOGY

The star and extended star topologies are the most common Ethernet network topologies. This sort of network is simple to set up, affordable and offers greater redundancy than other topologies, such as the bus topology. The star topology is set up by connecting all of the network's nodes to a single central device.

Even if a single node or cable breaks, the network can continue to function because of the central link. The most significant disadvantage of this architecture is that if the central device fails, the network would become unstable or stop working. Small, concentrated networks benefit the most from the star architecture. Sub-central devices are connected to the central device in the extended star architecture.

Sub-central devices are connected to the central device in the extended star architecture. This architecture is beneficial for big networks because it allows for the organising and subnetting of IP address assignments inside the network. Large networks that may cover an entire building benefit from the extended star topology.



Introduction to Basic Network

Chapter 2

Network Model

Chapter 2

Computer Network Models

Computer networks use cables, fibre optics, or wireless communications to link nodes such as computers, routers, and switches. Devices in a network can interact and exchange information and resources through these links.

Networks follow protocols, which define how communications are sent and received. These protocols enable devices to communicate with one another. An Internet Protocol, or IP address, is a string of digits that uniquely identifies a device and allows other devices to identify it on a network.

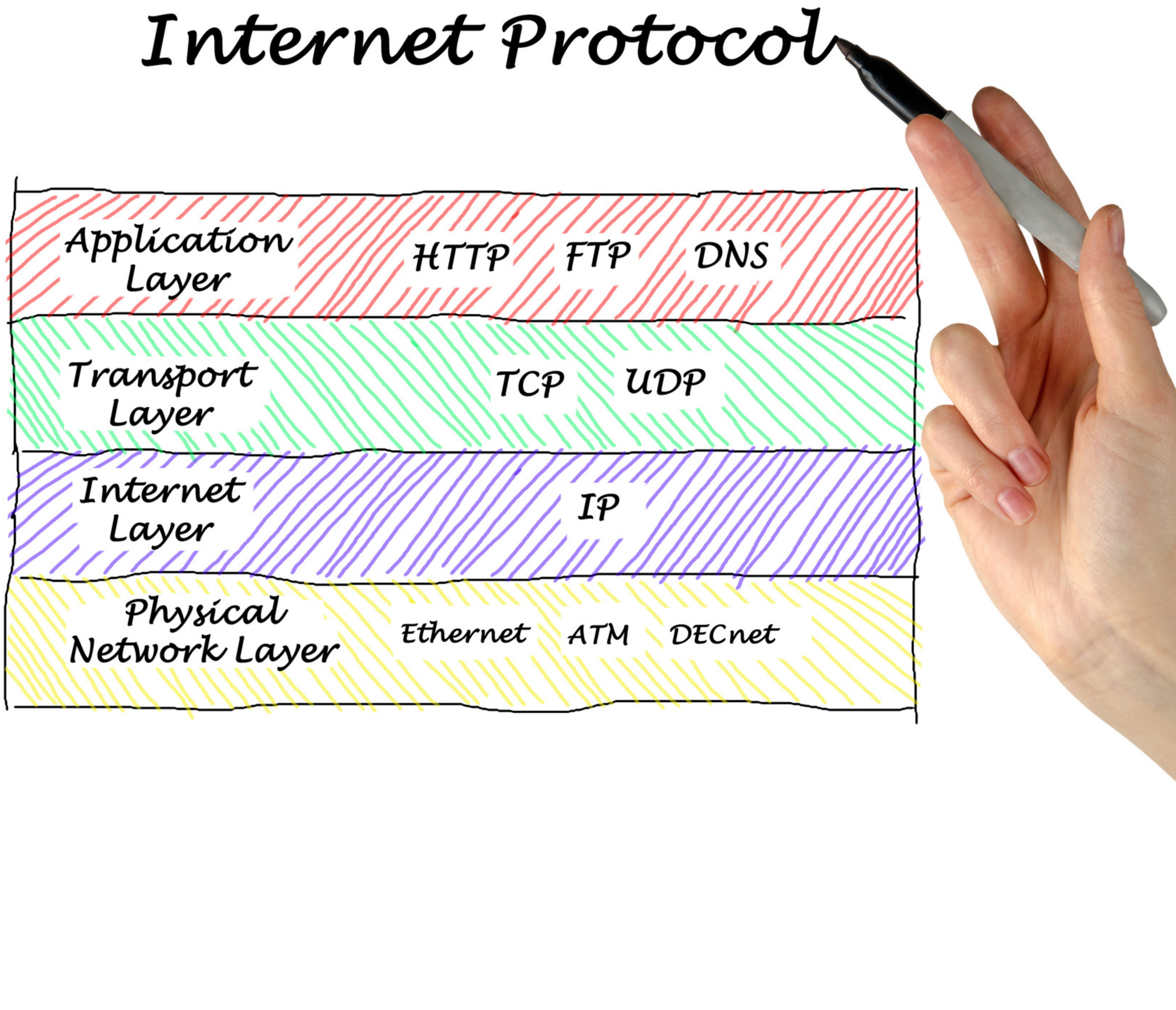
Routers are virtual or physical devices that help networks communicate with one another. Routers examine data to identify the most efficient path for it to reach its final destination.

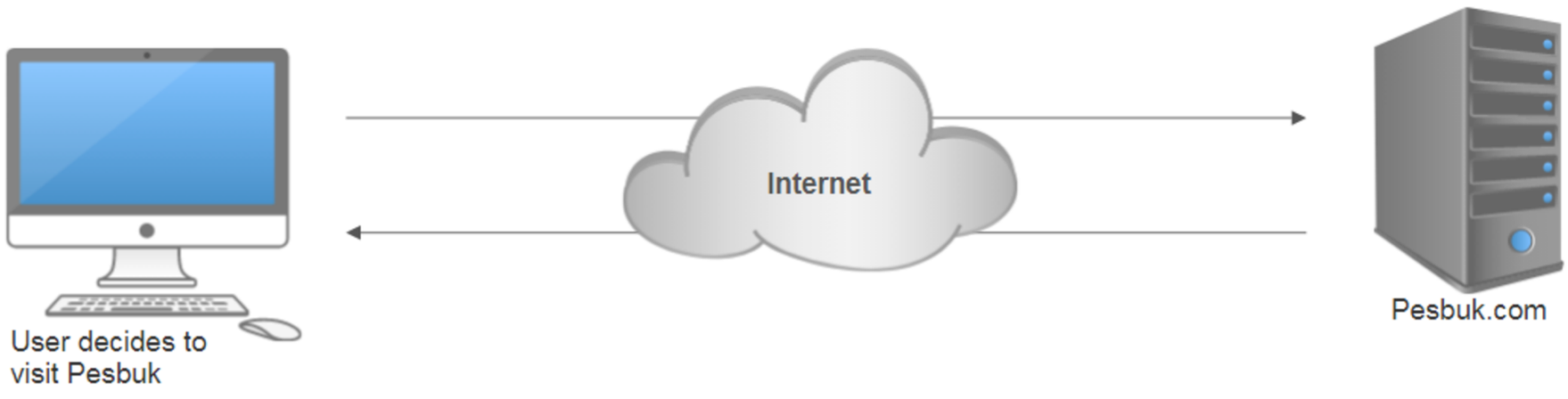
Switches in a network link devices and handle node-to-node communication, ensuring that data packets flowing across the network reach their final destination.

Network model is used to enable a connection between a computer to another computer sharing information and data. There are two models that have been developed which is OSI Model and TCP/IP Model. Every computer that wants to connect to each other has implemented a TCP/IP model into their system.

TCP/IP MODEL

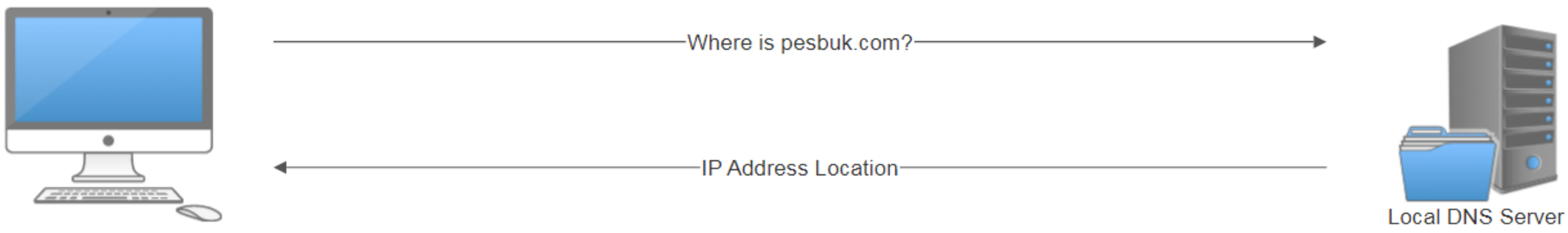
TCP/IP model can be defined as a set of rules and standards on how computers can communicate with each other. TCP/IP is also called TCP/IP stack is a model that consists of 4 big layers that are Layer 1-Physical Layer, Layer 2-Network Layer, Layer 3-Transport Layer and Layer 4-Application Layer. Each of the layers in TCP/IP stacks defines a protocol used when a computer is connected. For example, Physical Layer involving a media connection such as an Ethernet cable whereas in Network Layer involving IP Addresses and routers. All devices need to use IP Addresses to communicate over the internet since TCP/IP Model was implemented in the computer system.



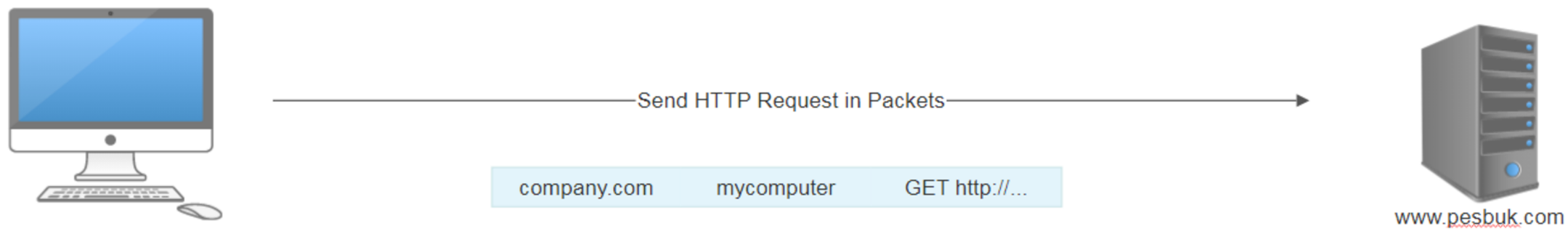


NETWORK LAYERING DIAGRAM

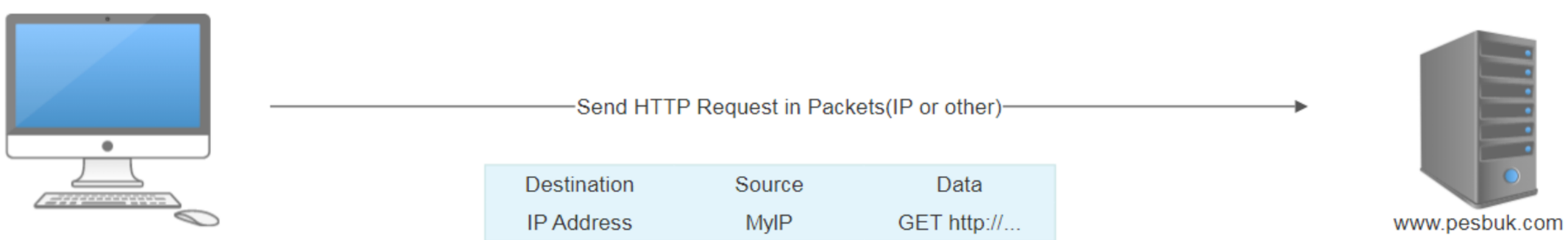
LAYER APPLICATION



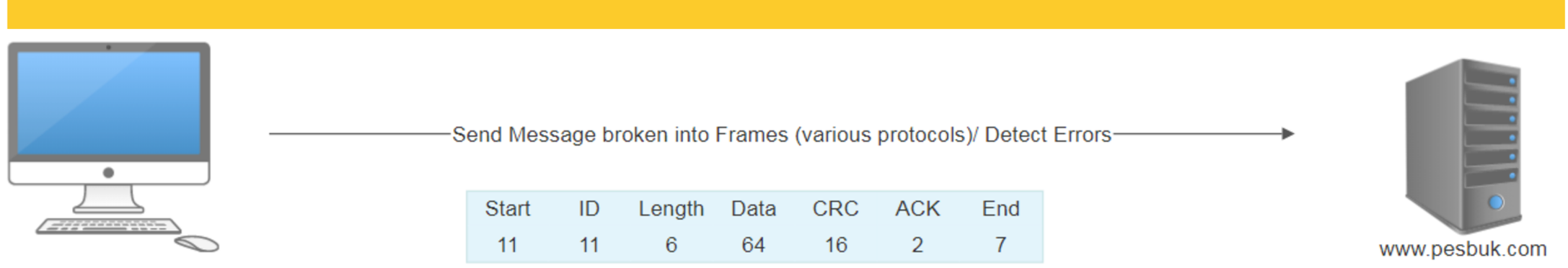
LAYER TRANSPORT



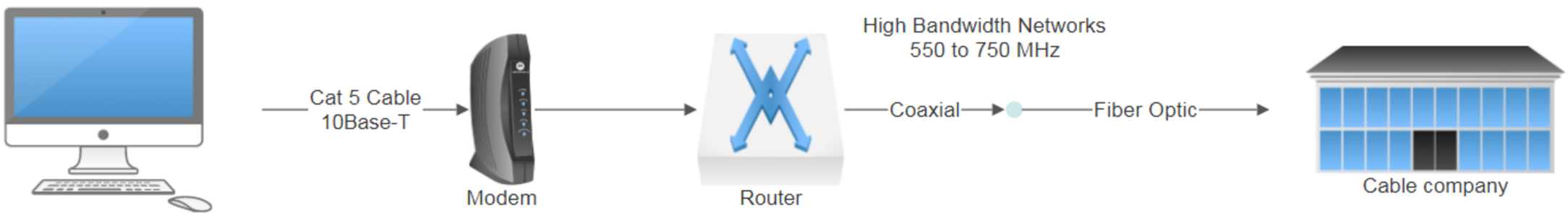
LAYER NETWORK



LAYER DATA LINK



LAYER PHYSICAL



OSI MODEL

OSI Model stands for Open System Interconnect. OSI Model is an architectural approach to developing a network communication enabling computers to share information with each other. There are 7 layers that divide up the tasks so that each layer is responsible for only a subcomponent of the overall communication process. This helps to facilitate consistency when developing new applications, protocols or devices. Each layer is arranged from Layer 7 to Layer 1-Physical Layer. Each layer in OSI Model is only aware of the layer above it and the layer below it. For example, there is no layer above Application Layer other than the users thus Application Layer is only aware of Presentation layer.

As communication between devices begins, a packet begins at the top layer (application layer) on the sending side and travels down the stack to the bottom. Each layer will add a standard or protocol to the packet to get it into a format that can be transferred across the physical wire. It is then transmitted and accepted by the lowest layer (Physical Layer) on the receiving side. The packets travel up the receiving side until ultimately arriving at the Application Layer of the recipient.

For example, in order for Person A to be able to send an email to Person B, Person A has used an email application to type the message and the application layer accepts the packet and sends it down the stack. The packet travel across the wire and the recipient will decapsulate the packet and sending the packet up to the application layer of the recipient on Person B's computer

LAYER 1 (PHYSICAL LAYER)

Physical Layer is responsible for the transmission of digital data bits from the source devices to the destination device over the physical network communications media such as Ethernet cable. As its name implies, this layer involving a physical device and hardware. There are four main functions in the Physical Layer which begins with the definition of the hardware specifications including the details for cable, connectors, network interface cards, repeaters and hubs. There a less configuration or programming on Physical Layer.

The next function is encoding and signalling used to transform data from bits, 1s and 0s, into electrical signals. The signals then send over the network. Next is topology, physical network design and data transmission (wired or wireless) which is actually sending and receiving the data. This considering things such as LAN and WAN. There is also bit rate control which is the transmission rate or the number of bits per second to avoid users overwhelming the physical media by sending too many signals.

In Layer 1 the bit 1s and 0s can be seen coming down from the data link/Layer 2. Then at the physical layer, the bits are converted into electrical signals that can travel the physical transmission medium. It is then received on the other side by the physical layer of the recipients. The electrical impulses will be converted back into bits of 1s and 0s and sent up to the data link layers on the receiving side. Each layer (both source and destination) communicates only with its counterpart layer on the other side.

The physical layer is the lowest layer. This layer provides mechanical, electrical, and other functional aids available to enable or disable, they maintain and transmit bits about physical connections

LAYER 2 (DATA LINK LAYER)

Data Link Layer responsible for node-to-node data delivery where the specific sender and receiver is identified. Layer 2 receive data coming down from Network Layer and passing it to the physical layer.

During the process, Layer 2 creates a frame and adds a physical address which is also known as Media Access Control (MAC) Address. The frame identifies the beginning and the end of any given transmission just like a frame around a picture outline or borders the picture.

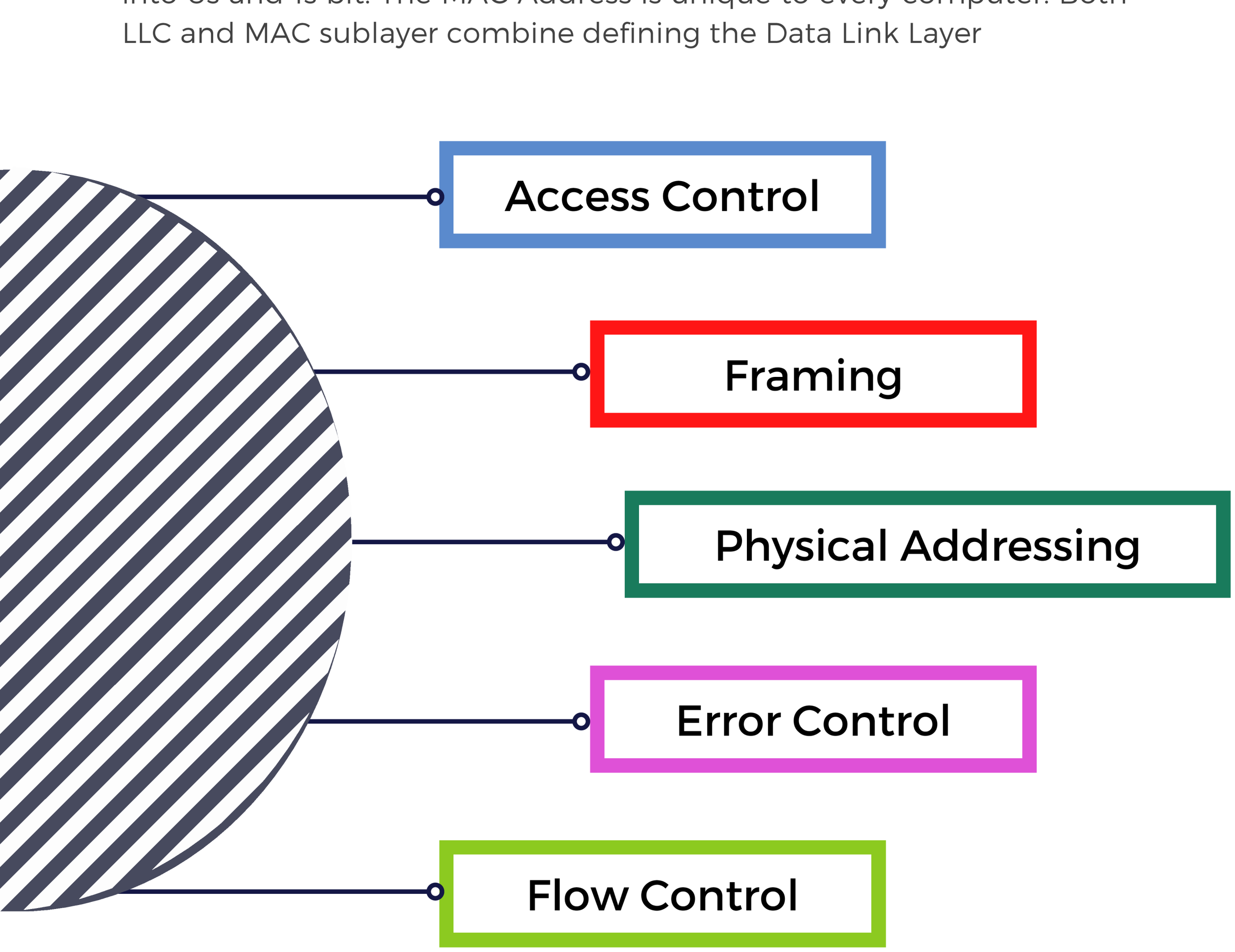
Layer 2 also handles error-free transfer thus the other layer can assume error-free transmission over the medium. Several other functions of Data Link Layer are frame traffic control, frame sequencing, frame acknowledgement detecting and recovering errors occurring at the physical layer,

Frame delimiting and frame error checking. These are all implemented at the data link layer to just implement some form of management to the communications to avoid users accessing the media at the same time.

LAYER 2 (DATA LINK LAYER)

The Data Link Layer is subsequently divided into two sublayers which is the Logical Link Control (LLC) sublayer and Media Access Control (MAC) sublayer. LLC sublayer provides an interface between media access methods and Network Layer protocols. The LLC sublayer determines if communication is connectionless or connection-oriented.

The MAC sublayer is responsible for the connection to the physical media. The MAC Address, a 12-digit hexadecimal number will be applied to the frame before passing it down to Layer 1 transforming into 0s and 1s bit. The MAC Address is unique to every computer. Both LLC and MAC sublayer combine defining the Data Link Layer



LAYER 3 (NETWORK LAYER)

Network Layer is responsible for packet addressing, converting logical to a physical address or physical to logical address depends on the direction. The physical or MAC address is always the same and never changes meanwhile the logical address a.k.a the IP address can be changed at any time and it resides entirely at the network layer. Any valid IP address can be applied during the configuration process of the network interface. The IP address is more flexible and reusable where it can be renewed at any time. Each IP address identifies the device's host network and the location of the device on the host network. When one device sends data to another the data includes a header that includes the IP address of the sending device and the IP address of the destination device.

Network layer is also responsible for source to destination delivery using a particular method that is routing. Routing would not be used if all of the systems are in the same network even a logical IP address would not be needed because the MAC address would be sufficient. Every device within the same network would be able to distinguish each other by their unique MAC addresses. However, in two separate networks routing is needed as a way to connect those networks.

Network layer takes services from the data link layer and then provides services to the transport layer depending on the direction of the packet either it is travelling up or travelling down the stack. . In term of the function of Network Layer, there are subnet control within any given subnet that is bordered by a router where it can implement control such as throttling, subnet usage accounting can keep tracks of frame and address mapping. Network Layer also responsible on internetworking provides the capability for one network to communicate with another network

LAYER 3 (NETWORK LAYER)

By internetworking also provide a logical connection between different networks and combine various networks to form a larger network. Within a larger environment, they will typically subnet their networks into smaller units. Logical addressing combines a large number of networks creating a very large environment up to the size of the Internet. But logical addressing has to define an addressing scheme to uniquely identify each device on internetwork.

There are packetizing in Network Layer which creates packet upon receiving data from upper layers. The packets are created by way of encapsulation which is basically surrounding a packet with more information on either side. The IP protocol that resides at the network layer defines packet format which contains the IP Address of sending and receiving device. Fragmentation is also implemented at this layer. Fragmentation involves dividing larger packets into smaller fragments so it can then be easily sent out on a physical medium.

Layer 3 provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing

LAYER 4 (TRANSPORT LAYER)

Transport Layer manage end to end message delivery from the source right through to the destination and providing error checking along the way to ensure there are no duplication or errors during the data transfer. Ultimately so that messages arrive intact and in the correct order.

As far as the layer itself, it resides at the core of the OSI model. As packets are travelling up the stack, the transport layer takes its services from the network layer below it and then provides services to the application layers above it.

Meanwhile, as the packet travels down the stack, one of the primary functions is the segmentation of any given message. It accepts the message from the session layer and passes it to network layer below it. The message has been divided up into packets.

Some of the other functions include message acknowledgement and traffic control depending on the protocol that's being used. Other functions include session multiplexing due to any system might communicate with any number of other systems thus it multiplexes that connection together with over one logical link.

It's also tracking which messages belong to which sessions and its also implement service point addressing to ensure that a correct packet arrives not only at the correct system but are processed by the correct application.

LAYER 4 (TRANSPORT LAYER)

Transport Layer also implementing flow control to prevent a source device from sending data packets at a faster rate than the destination can handle whereas error control is to ensure the entire message arrives without error. TCP and UDP protocols reside at this layer. TCP is a connection-oriented transmission meanwhile UDP is a connectionless transmission. TCP protocol provides reliable transport of data and the receiving device sends an acknowledgement upon successfully receiving the packet.

The sender and the receiver implementing what's known as synchronization which then is acknowledged. Both sender and receiver establishing a rule of communication that both agreed upon. Once the acknowledgement and synchronization are complete, then the connection is established and at that point, devices can start sending the data.

In a connectionless transmission, something using the UDP protocols the receiver does not acknowledge the receipt of a packet. The sending device simply assumes the packet arrived successfully. This kind of transmission is not reliable but it enables faster communication between the devices. As its name Transport Layer indicates the actual movement of the data from point A to point B.

Layer 4 of the OSI Model: Transport Layer provides transparent transfer of data between end-users, providing reliable data transfer services to the upper layers. The transport layer controls the reliability of a given link through flow control, segmentation and desegmentation, and error control.

LAYER 5 (SESSION LAYER)

Session Layer is responsible for the beginning, maintenance and end of any given communication between two devices. Before a computer can connect to a server, it must first authenticate by providing a user name and password. The session layer is responsible for authentication and establishing a connection following authentication. Once a connection is established, the session layer examines if the connected computer is authorised to access the data. The session layer also performs the role of authorisation checking.

The session layer also ensures that the data received from the server in the form of data packets belong to the correct application. For example, when you access your Facebook profile through your browser, the data transferred from the Facebook server is transferred to your web browser application, and thus the session layer aids in session management

Layer 5, or the session layer, is the network mechanism for opening, closing, and generally managing communication sessions between end-user applications and their processes. Some examples of protocols used in layer 5 include: AppleTalk Session Protocol (ASP) and AppleTalk Data Stream Protocol (ADSP)

LAYER 6 (PRESENTATION LAYER)

The data from the application layer is in the form of letters and integers like 1234, ERFF, and so on. For example, the presentation layer transforms these letters and numbers into a machine-readable format known as binary formats, such as 100111101.

The presentation layer encrypts the data at the sender side before transmission to preserve the sensitivity of the data, and the presentation layer decrypts the data at the receiver side. The presentation layer encrypts and decrypts data using the Secure Sockets Layer Protocol (SSL).

Presentation Layer also compresses the data to make it smaller so that it can be sent across the network more quickly. This compression can be either lossy or lossless.

Layer 6, or the presentation layer, serves as the data translator between an application or process and the network. This layer is responsible for the formatting and subsequent delivery of data to the application layer either for processing or display.

LAYER 7 (APPLICATION LAYER)

The final layer in the OSI Model is Application Layer. It serves as the window for users and application processes accessing network services. It is the interface between the program and the rest of the protocol stack. The user directly interacts with the application but the program itself did not reside within Application Layer instead the protocols within the Application Layer that directly support that program and allow it to access the appropriate network services.

For example, when a computer wants to connect to a network, the device will use the DHCP network services to request an IP address using an interface of an application to do so. Application Layer allowing users to interact with applications. The application accepts user input and passes data down to the lower layers.

For instance, using email, person A just types in message into the Gmail interface. Gmail accepts it and sends it on its way down the stack. So, this allows for easier application compatibility and implementation. Essentially, applications do not have to be re-written for different types of network environments.

There are some widely used network services that reside within Application Layer such as FTP and DNS.

Layer 7 refers to the top layer in the 7-layer OSI Model of the Internet. It is also known as the "application layer." It's the top layer of the data processing that occurs just below the surface or behind the scenes of the software applications that users interact with.

FILE TRANSFER PROTOCOL (FTP)

It is mostly used to move web page files from their developer to a computer that serves other computers on the internet as a server

DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

It is mostly used to move web page files from their developer to a computer that serves other computers on the internet as a server

DOMAIN NAME SYSTEM (DNS)

The method for translating alphabetic names into numeric Internet Protocol (IP) addresses on the Internet

SIMPLE MAIL TRANSFER PROTOCOL (SMTP)

A set of communication guidelines that allow software to transmit an electronic mail over the internet

INTERNET MESSAGE ACCESS PROTOCOL (IMAP)

An application layer protocol is used to receive the emails from the mail server. It is the most commonly used protocol like POP3 for retrieving the emails

NETWORK FILE SYSTEM (NFS)

Is a file system that allows data to be stored and retrieved from various drives and directories across a shared network

POST OFFICE PROTOCOL VERSION 3 (POP3)

Is an Internet standard protocol for storing and retrieving messages from Simple Mail Transfer Protocol (SMTP) hosts

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

A protocol for managing internet-connected devices

HYPERTEXT TRANSFER PROTOCOL SECURE (HTTPS)

Combination of HTTP with Secure Socket Layer (SSL)/Transport Layer Security (TLS) to provide secured internet access through a browser

HYPER TEXT TRANSFER PROTOCOL (HTTP)

Provides internet access for all types of networking environment through a web browser

HOW DNS WORKS?

Computer browser request to visit https://www.canva.com/

Company or local DNS is checked and the requested URL is not found

ISP DNS is also checked next and unable to find the requested URL

Root DNS is checked and the IP address of 206.15.10.145 is returned to the computer

The computer receives IP address and prompts the browser to open the given address

HOW DHCP WORKS?

1 **DHCPDiscover**

IP Address requested

DHCPOffer 2

IP Address offer

3 **DHCPRequest**

IP Address selection

DHCPAck 4

IP Address
acknowledgement

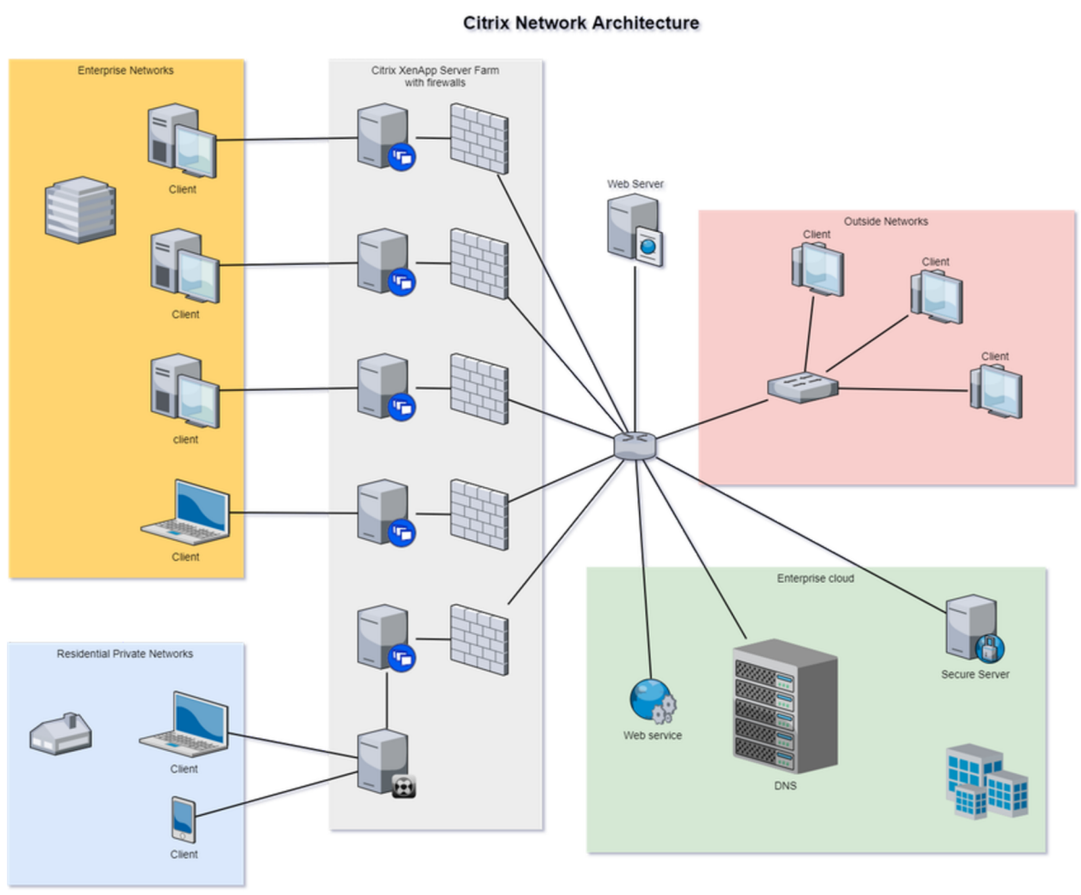
Introduction to Basic Network

Chapter 3

Design a Small Network

Chapter 3

Design a Small Network



It's critical to balance the requirements and wants of individuals who will be using the network with the budget of those who will be paying for it when establishing a new computer network, whether it's for a small scale or a big scale.

Balance security problems with the need for fast access to information; incorporate redundancy into the network in anticipation of failures and standardise hardware and software to keep maintenance expenses in control are some key things to consider that may not be on anyone's wish list.

Computer Network is never built directly. A good network engineer will create a logical design of it first. A logical structure assists in detailed analysis. There are a few software uses to design a logical network diagram i.e packet Tracer, Edraw Network Diagram Software etc.

Cisco Packet Tracer (CPT) is a multi-tasking network simulation software that can be used to perform and analyze various network activities such as the implementation of different topologies, selection of optimum path based on various routing algorithms, creation of appropriate servers, subnetting, and analysis of various network configuration and troubleshooting commands.

In order to start communication between end-user devices and to design a network, users need to select appropriate networking devices like routers, switches, hubs and make physical connections by connecting cables to serial and fast Ethernet ports from the component list of packet tracer.

Chapter 3.1

Configuring a router connection

PART A:

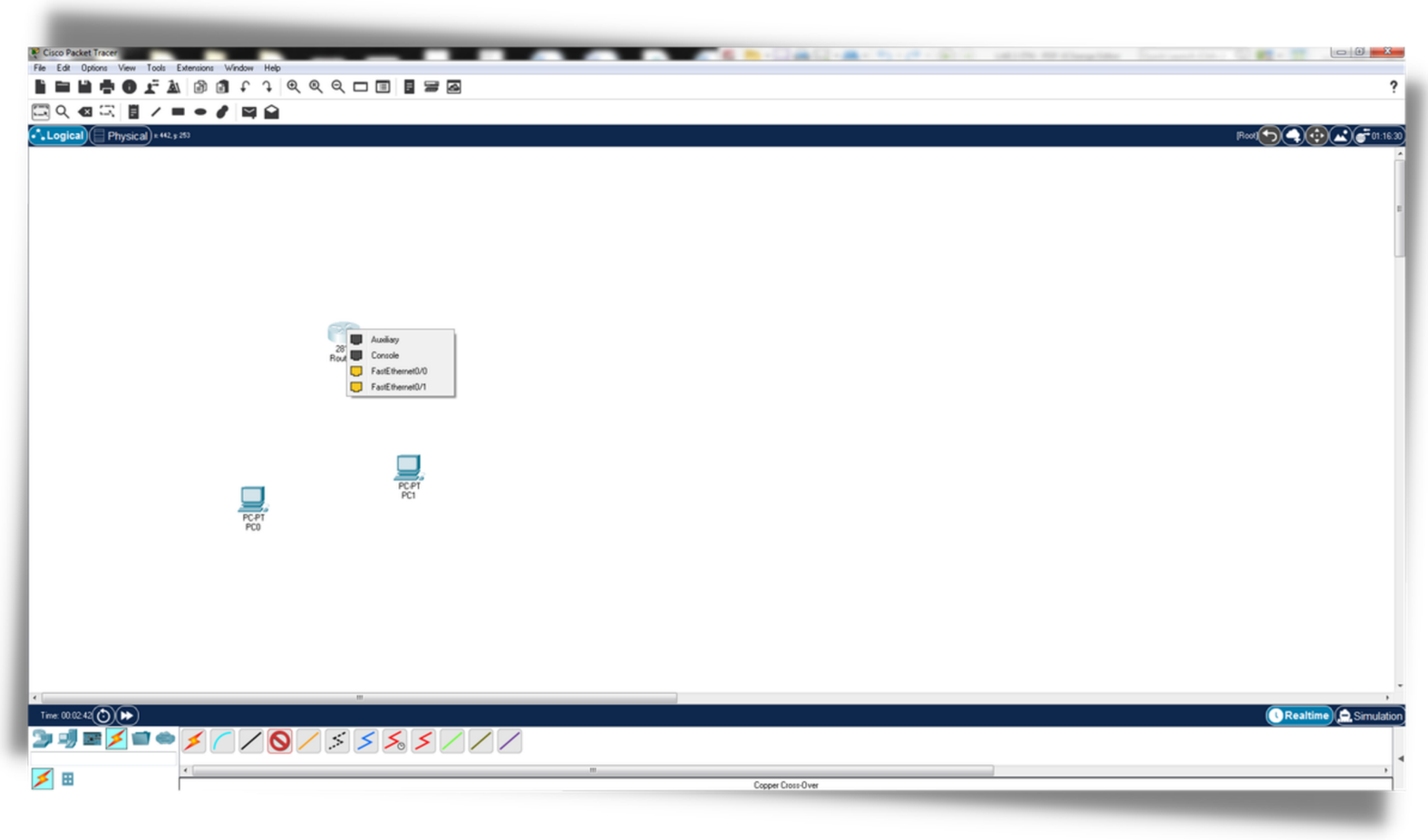
1. Select the router from the lower left-hand corner, and drag it into the center of the sandbox screen

2. Choose router 2811 from the bottom left-hand corner and drag it into the sandbox screen

3. Select the computer from the bottom left-hand corner and drag them into the sandbox screen

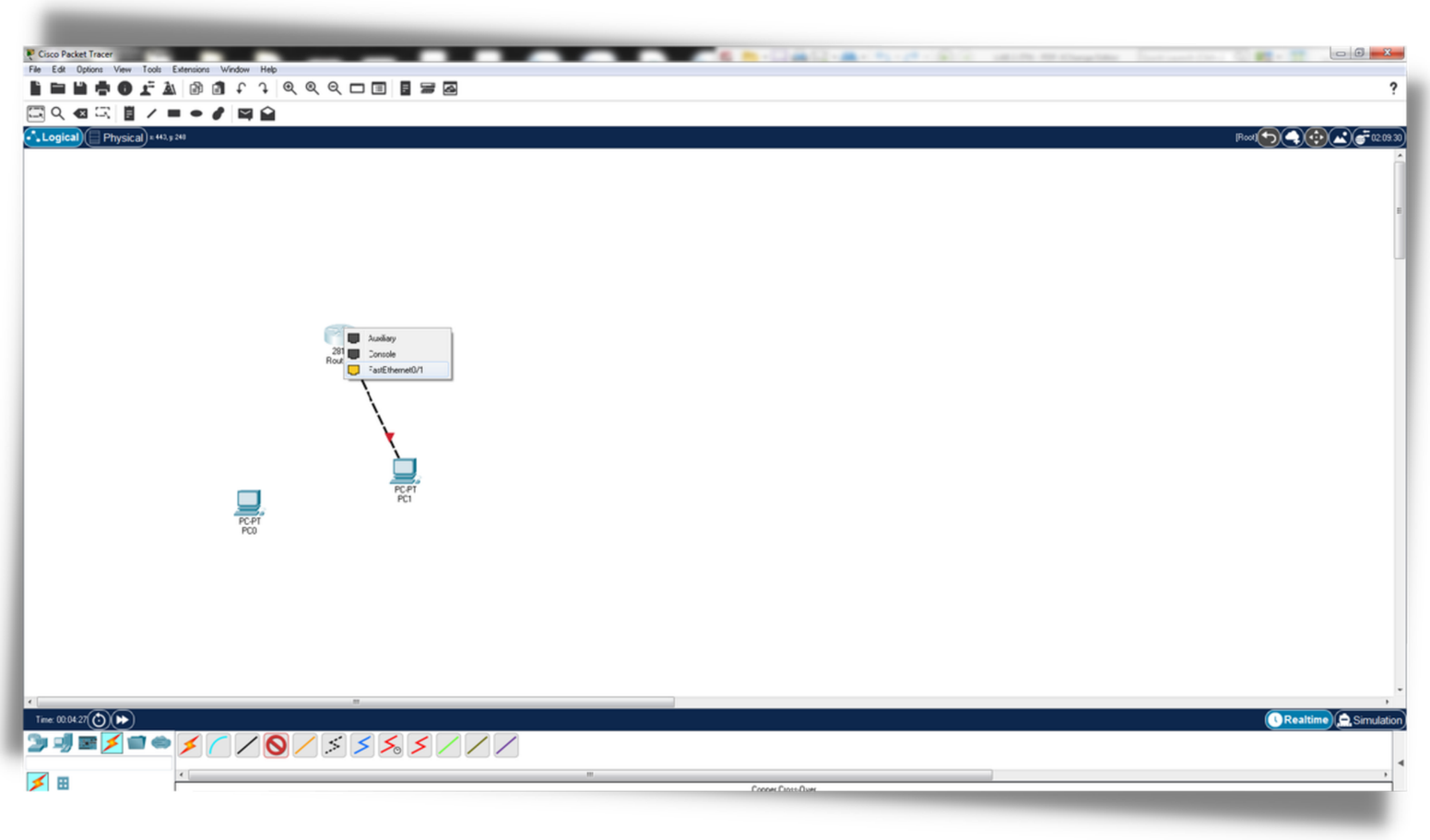
4. Choose the second computer from the bottom left-hand corner and drag them to the sandbox screen

5. Select copper cross-over cable from the second menu to the immediate right



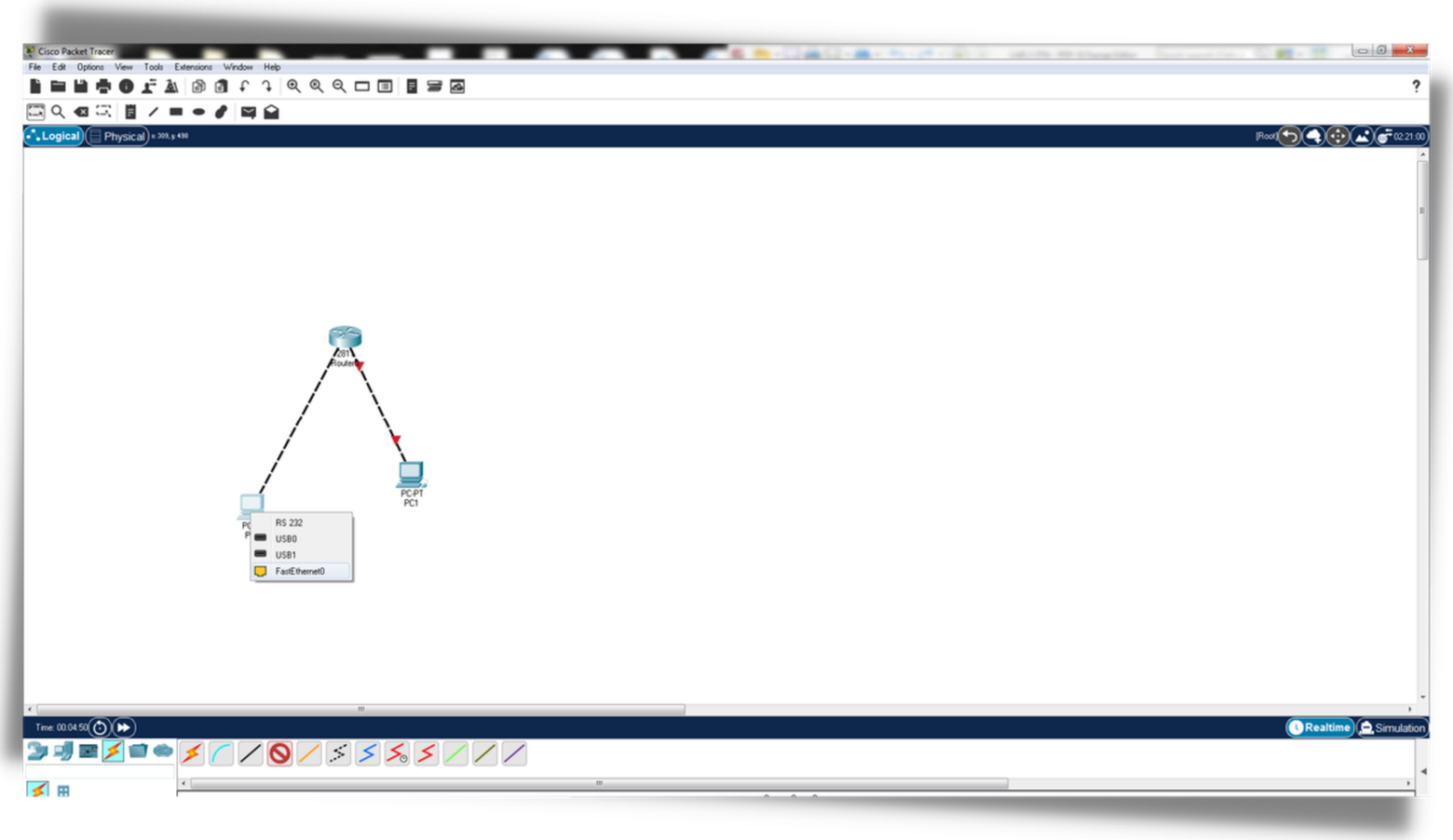
Chapter 3.1

6. Click on Router0, and connect the cable via FastEthernet0/1 as seen below



8. Click the PC0 and select FastEthernet0/0

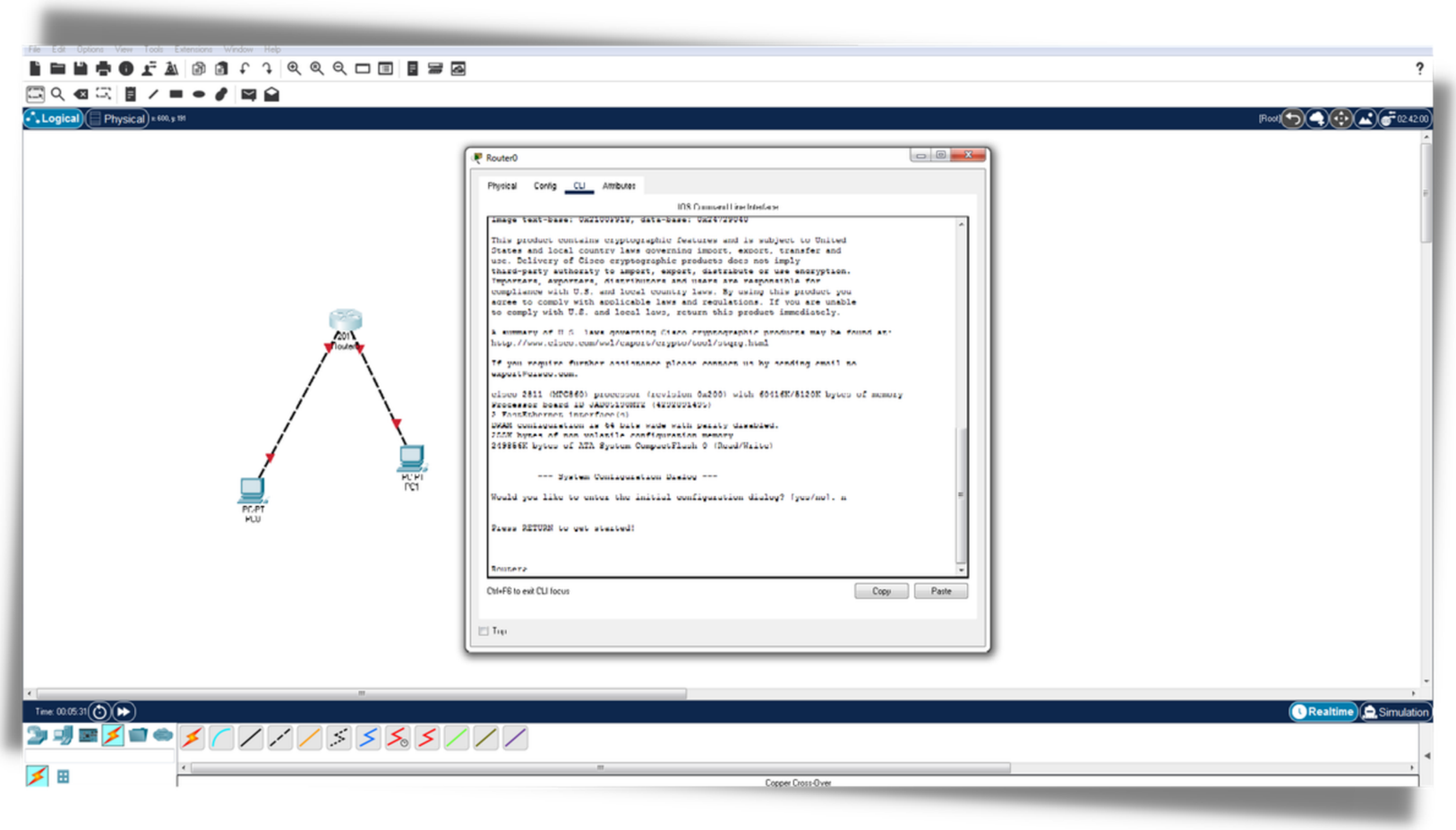
9. Repeat the same operation to PC0



Chapter 3.1

PART B:

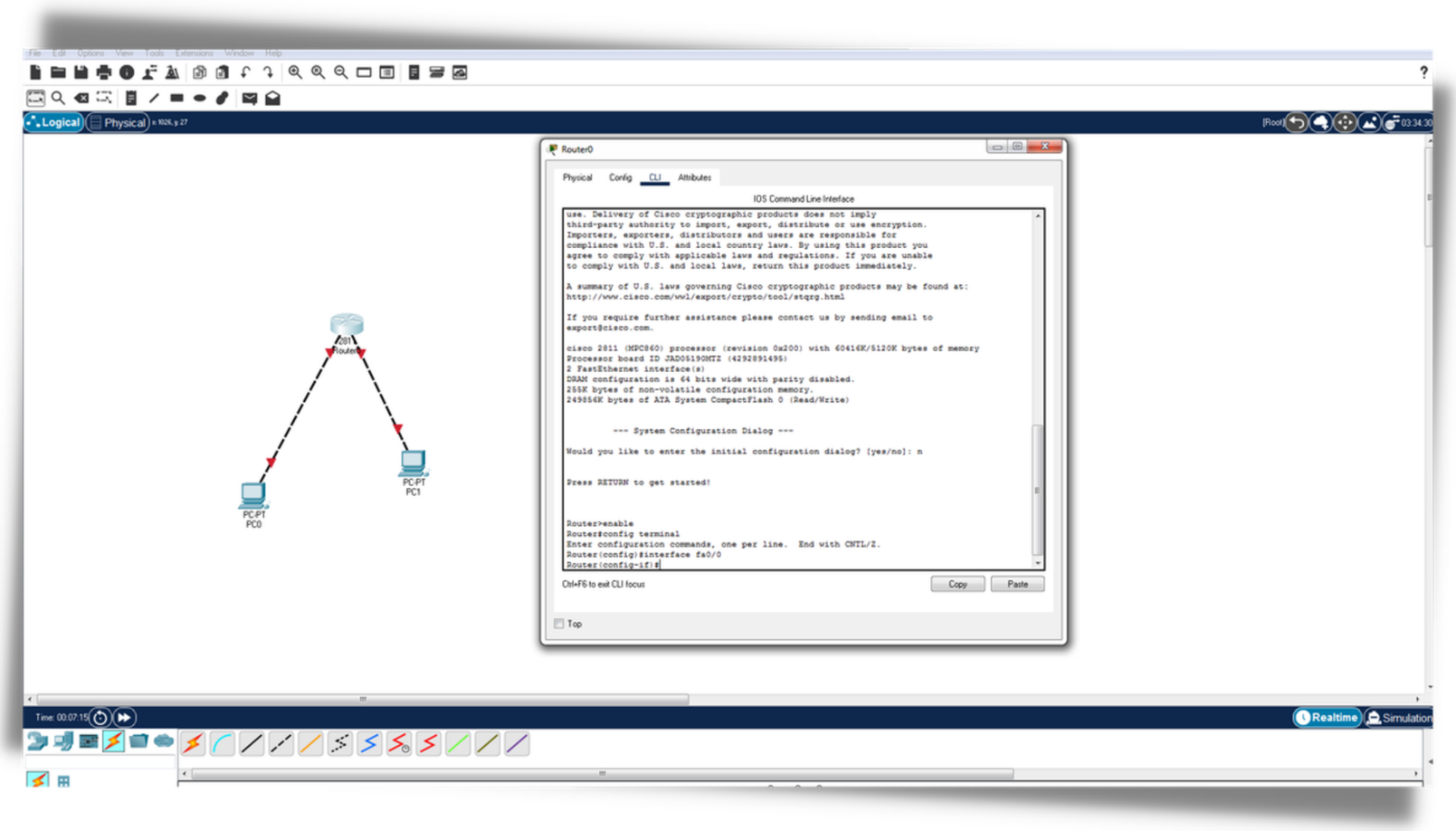
1. Select the Router0 and click on the CLI tab to access the configuration menu to open the Ethernet ports to allow communication



2. Type enable to get to privileged mode

3. Type config terminal (or config t) to access the configuration menu

4. Type interface fastethernet0/1 to access Ethernet0/0

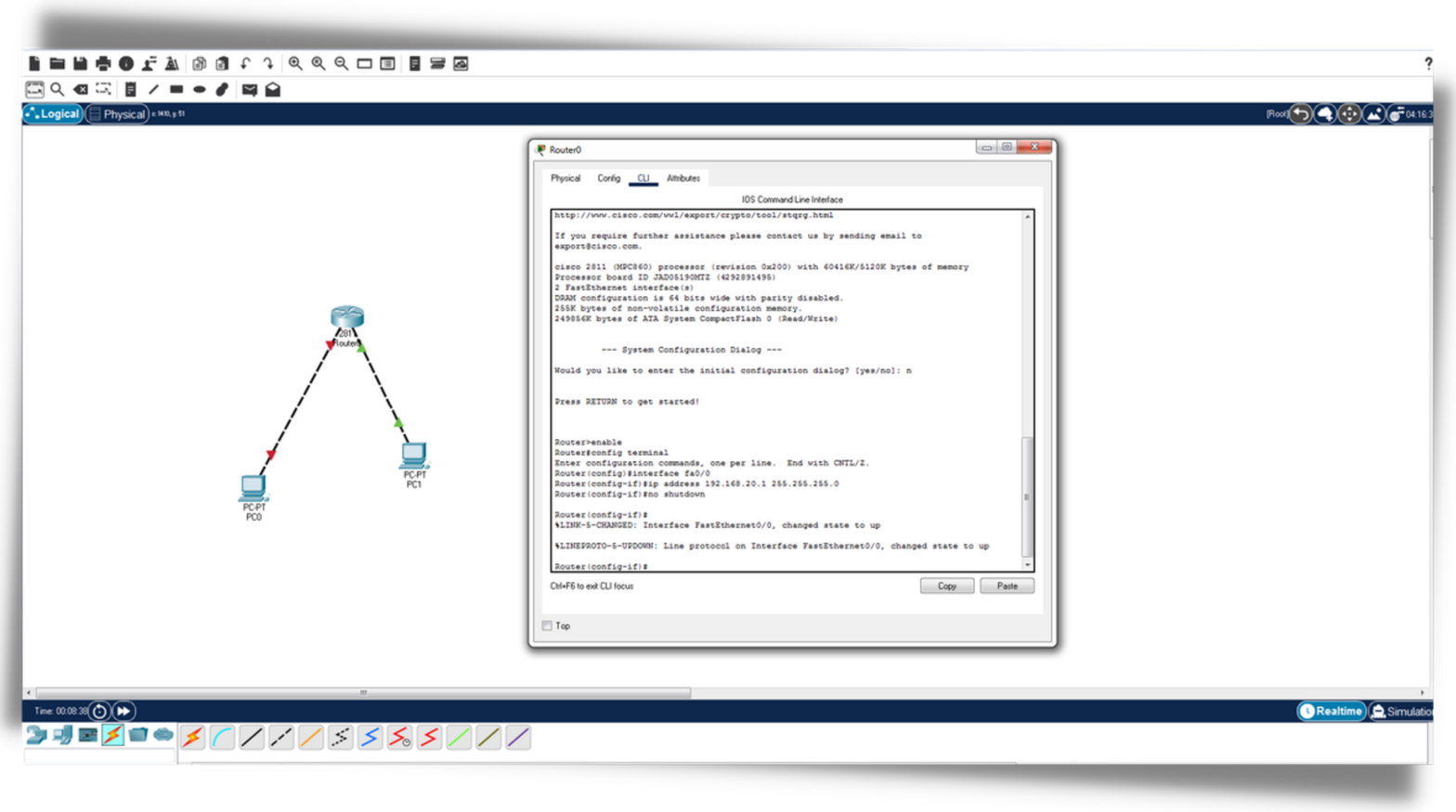


Chapter 3.1

PART B:

5. Type IP address 192.168.20.1 255.255.255.0 to assign an IP address and subnet mask to the interface

6. Type no shutdown to open the interface up



6. Press Ctrl + Z to go back to the previous mode

6. Type interface fastethernet0/0 and enter IP address 192.168.20.1 255.255.255.0

7. Type no shutdown

Chapter 3.1

PART C:

1. The last step is to configure the gateway on each desktop computer

2. Click on PC0 to bring up the configuration menu

3. Then click the FastEthernet tab on the left column under global setting to set the actual computer's IP address to be on the network

4. Type interface fastethernet0/0 to access Ethernet0/0

5. Type IP address 192.168.10.1 255.255.255.0 to assign an IP address and subnet mask to the interface

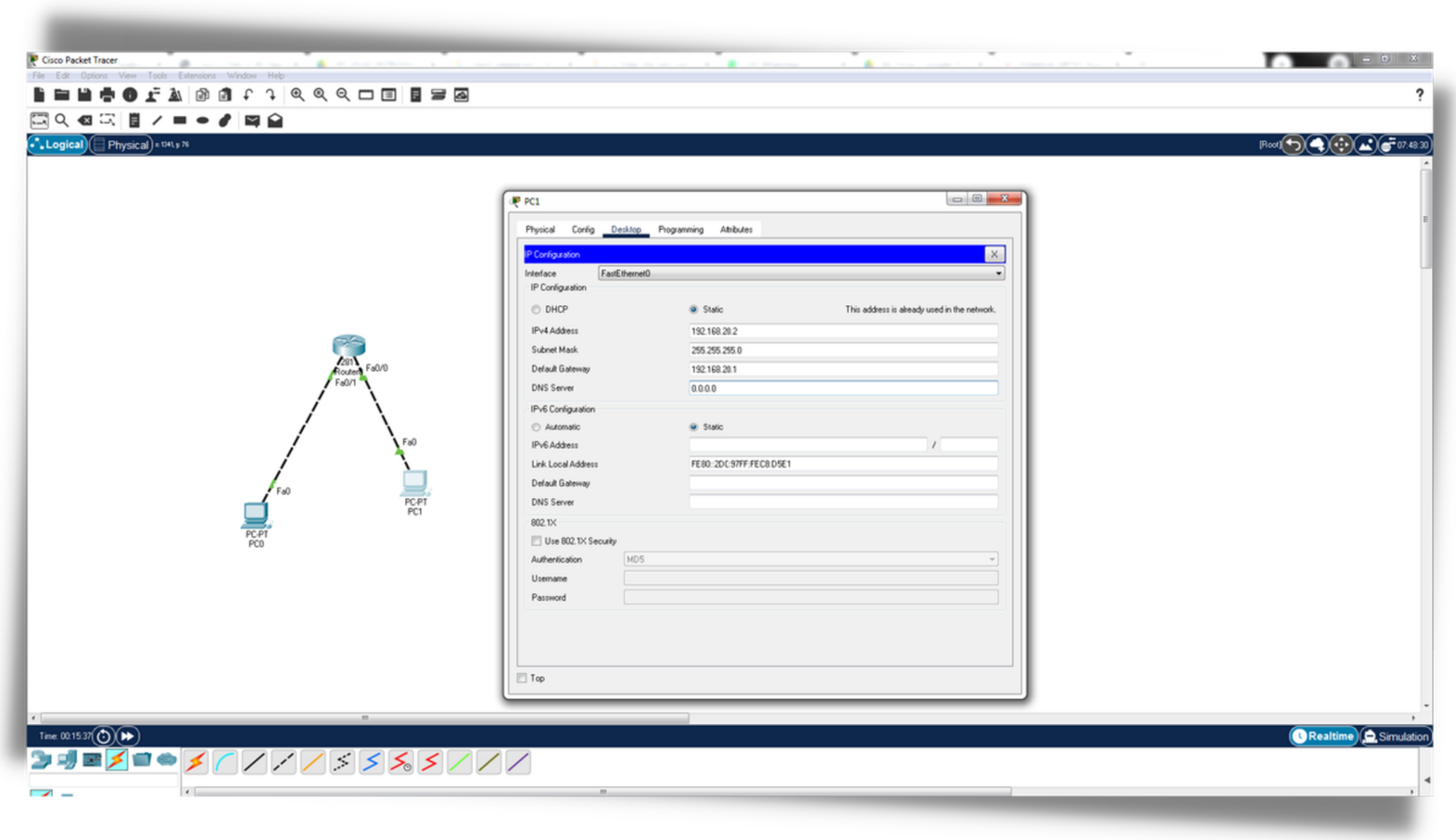
6. Use 192.168.10.1 for the gateway address, 192.168.10.2 for the IP address, and 255.255.255.0 for the subnet mask

Chapter 3.1

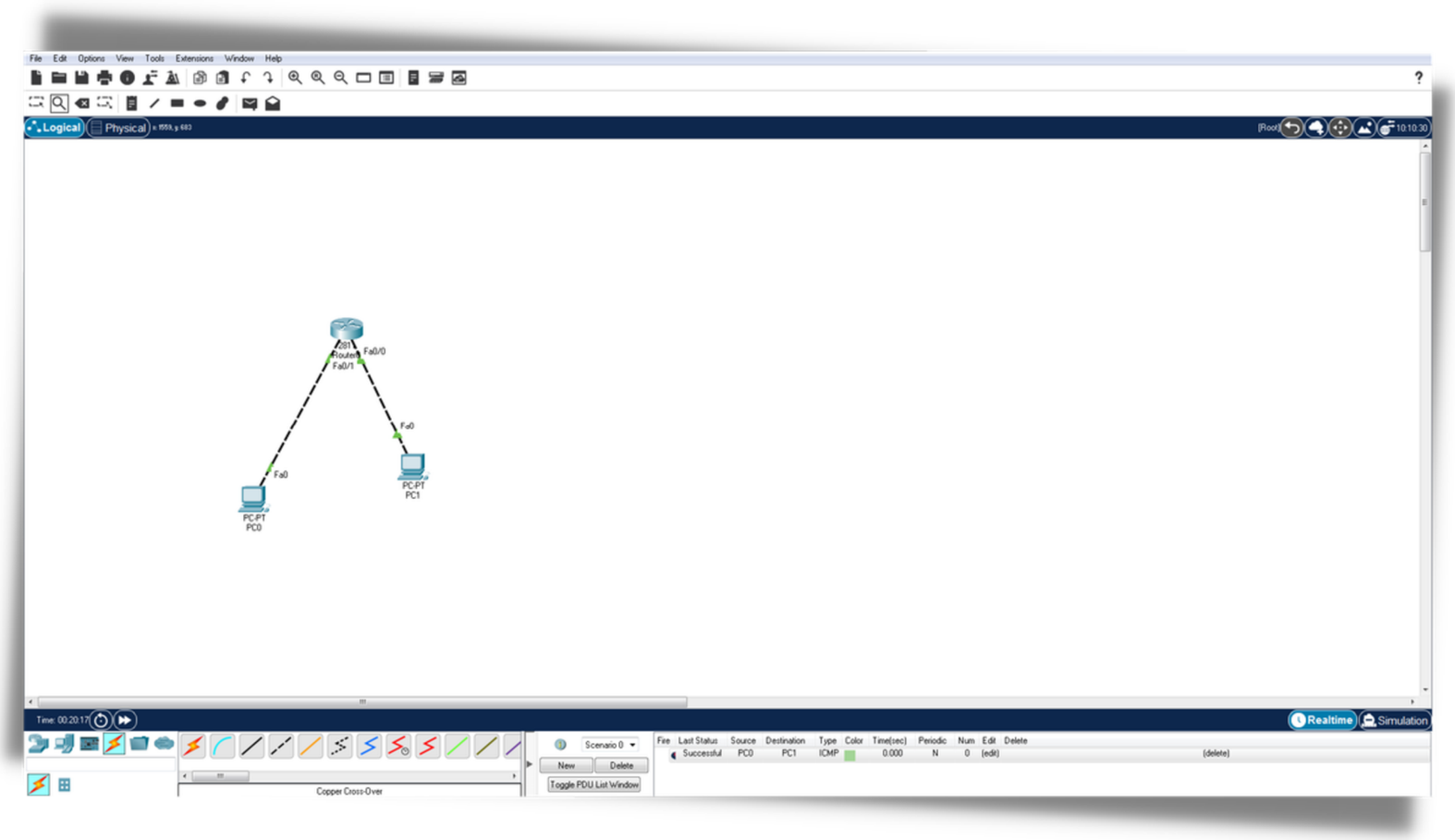
PART C:

7. Repeat the steps on PC0, use 192.168.20.1 for the gateway address, 192.168.20.2 for the IP address 255.255.255.0 for the subnet mask

8. Click on add simple PDU packet to sending out a packet of information from PC0 to PC1



9. Check the "Successful" message box on the lower right of the screen



Introduction to Basic Network

Appendix

References

References

1. Garima Jain, Nasreen Noorani, Nisha Kiran, Sourabh Sharma, Designing & simulation of topology network using Packet Tracer, International Research Journal of Engineering and Technology (IRJET), 2(2), 2015
2. Cisco Networking Academy. (2020). Introduction to Networks Companion Guide (CCNAv7). Cisco Press
3. West, J., Andrew, J., & Dean, T. (2018). Network+ Guide to Networks (8th Edition). Course Technology Press. (ISBN: 133756933X)
4. Dean. T. (2012). Network+ Guide to Networks. Course Technology (6th Edition). (ISBN: 9781133608196). Boston: Cengage Learning
5. https://www.computernetworkingnotes.com/networking-tutorials/computer-networking-devices-explained-with-function.html
6. https://www.computernetworkingnotes.com/networking-tutorials/networking-basic-concepts-and-fundamentals-explained.html
7. https://www.dnsstuff.com/what-is-network-topology
8. https://www.mvorganizing.org/how-do-computer-networks-work/
9. https://www.tutorialspoint.com/Computer-Network-Components
10. https://smallbusiness.chron.com/client-server-programming-42314.html
11. https://beginnersbook.com/2019/03/computer-network-components/
12. https://www.ibm.com/cloud/learn/networking-a-complete-guide
13. https://networkencyclopedia.com/post-office-protocol-version-3-pop3/
14. https://www.studytonight.com/computer-networks/comparison-osi-tcp-model
15. https://www.guru99.com/difference-tcp-ip-vs-osi-model.html
16. https://www.freepik.com/vectors/business : Business vector created by macrovector
17. https://www.microsoft.com/en-us/microsoft-365/business-insights-ideas/resources/tips-for-mapping-your-network-diagram

Introduction to Basic Network

eISBN 978-967-2623-92-2

(online)