Purpose statement

This module Describes the skills, Knowledge and attitude required to Perform basic

Networking. This module intended to prepare students Pursuing TVET in Level 4

Software Development. At the end of this module, the students will be able to

Establish network media connectivity, Perform Basic Network Configuration,

Maintain Network system

3

Learning outcome 1: Establish network media connectivity

Indicative content 1.1: Identification of Network requirements.

 Description of network concepts and technologies

A network is a collection of computers and devices that are connected together to

enable communication and data exchange.

Nodes: Nodes are devices that are connected to a network. These can include

computers, Servers, Printers, Routers, Switches, and other devices.

• Basic definitions: a network consists of two or more computer that are linked in

order to share resources (such as printers and CDs), exchange files, or allow

electronic communications. The computer on a network may linked through

cables, telephone lines, radio waves, satellites, or infrared light beams.

• Network classifications/types:

4

• Based on Size:

• Personal Area Network (PAN): A small network typically within a

range of a few meters, used for connecting personal devices like

smartphones, laptops, and tablets.

• Local Area Network (LAN): Covers a limited geographic area, such as a

home, office, or campus. LANs connect devices like computers, printers,

and servers.

• Metropolitan Area Network (MAN): Larger than a LAN but smaller

than a WAN, covering a city or a large campus. MANs are used by

organizations with multiple locations in a city.

• Wide Area Network (WAN): Spans a large geographic area, often

connecting LANs or MANs across different cities, regions, or countries.

The internet is the most extensive WAN.

• Global Area Network (GAN): A network that covers a global or

international scale, often using satellite links and undersea cables. The

internet can be considered a GAN.

Classifying network by components roles

• Client-Server Network: Devices are categorized as clients (requesters) and

servers (providers of services or resources). Common in corporate networks and the

internet.

• Peer-to-Peer (P2P) Network: Devices communicate directly with each other

without a central server. Often used in file-sharing applications and some blockchain

networks.

• Network benefits

Main benefits of networks include:

5

Networks offer numerous benefits across various domains and industries due to their

ability to connect devices, systems, and people. Here are some key advantages of

networks:

1. Communication

Networks enable efficient and effective communication, allowing people to share

information, collaborate, and exchange messages in real time. This is crucial for

business operations, remote work, and social interactions.

2. Resource Sharing

Devices and resources such as printers, scanners, and storage devices can be shared

across a network, reducing costs and optimizing resource utilization.

3. Flexibility

Networking enables remote access, allowing users to work from different locations

and devices. This feature is particularly useful for businesses with employees working

from home or traveling frequently.

Remote access allows users to access the network, files, and applications from

anywhere with an internet connection. This enables employees to work from home or

while traveling, increasing productivity and saving time. Hence, flexibility is one of

the major benefits of networking in computers.

4. Increased Efficiency

One of the other major benefits of networking in computers is that it reduces the time

and effort required to complete a particular task, such as updating the software on all

the devices in an organization. This may take a long time if done manually, as you

would have to update the software on each machine. This will require a lot of time.

6

But, if all the computers are connected to a network, you can easily automate the

process. This will increase efficiency and productivity while reducing downtime.

5. Optimized Convenience

Networking provides users with easy access to information and resources, which

optimizes convenience and saves time. With a network, users can access files,

applications, and other resources from any device in the network. Thus, eliminating

the need to transfer files manually or carry devices around.

6. Easy Information Sharing

One of the other benefits of networking is that it enables easy sharing of information,

data, and files among devices in a network. Thus enhancing collaboration, teamwork,

and productivity.

7. Streamline Communication

Networking enables efficient and cost-effective communication between individuals,

departments, and organizations. This feature enables easy information, ideas, and

feedback sharing, leading to better decision-making, improved problem-solving, and

faster response times.

Networking allows communication through email, instant messaging, video

conferencing, and other means, reducing the need for physical meetings and phone

calls.

8. Cost-Efficient Resource Sharing

Networking allows multiple devices to share resources, such as printers, scanners, and

storage devices. This reduces the need for duplicate devices and saves costs.

7

9. Overcome Geographic Separation

Networking enables devices to communicate and share resources even if they are

located in different physical locations.

10. Improve Storage Efficiency and Volume

Another important benefit of networking is that it enables centralized storage of data.

This improves storage efficiency and volume, reduces the need for individual storage

devices for each device in a network, and saves costs.

With a centralized storage system, files and data can be accessed and shared by

multiple devices in the network, reducing the need for duplicate files and storage

devices.

11. Cut Back on Hardware and Software Costs

Networking reduces the need for duplicate devices, software licenses, and other

resources. This lowers costs and increases the return on investment (ROI).

Advantages and Disadvantages of network

Networks, whether they are computer networks, social networks, or any other type of

interconnected systems, come with various advantages and disadvantages. Here are

some of the key advantages and disadvantages of networks:

Advantages

 Sharing devices such as printers saves money.

 Site (software ) licences are likely to be cheaper than buying several standalone

licences.

 Files can easily be shared between users.

 Network users can communicate by email and instant messenger.

8

 Security is good - users cannot see other users&#39; files unlike on stand-alone

machines.

 Data is easy to backup as all the data is stored on the file server.

Disadvantages

 Purchasing the network cabling and file servers can be expensive.

 Managing a large network is complicated, requires training and a network

manager usually needs to be employed.

 If the file server breaks down the files on the file server become inaccessible.

Email might still work if it is on a separate server. The computers can still be

used but are isolated.

 Viruses can spread to other computers throughout a computer network.

• There is a danger of hacking, particularly with wide area networks.

• Security procedures are needed to prevent such abuse, eg a firewall.

Application of network

Networks have a wide range of applications across various domains and industries.

Their primary function is to facilitate the exchange of information and resources

between different entities or nodes. Here are some common applications of networks:

 Computer Networks:

• Internet: The global network that connects millions of computers and devices

worldwide, enabling communication, information sharing, and online services.

• Local Area Networks (LANs): Networks that connect devices within a limited

geographic area, such as a home, office, or campus, to share resources like

printers and files.

9

• Wide Area Networks (WANs): Networks that span larger geographical areas,

often connecting multiple LANs and providing long-distance communication

capabilities.

• Intranets and Extranets: Internal corporate networks (intranets) and extended

networks (extranets) for secure communication and collaboration within and

between organizations.

 Telecommunications:

• Telephone Networks: Traditional voice communication networks, including

landlines and cellular networks.

• Voice over IP (VoIP): Networks that transmit voice and multimedia content

over the internet, offering cost-effective communication.

• Fiber Optic Networks: High-speed data transmission networks using optical

fibers, commonly used in long-distance and high-bandwidth applications.

 Data Centers:

• Data Center Networks: Networks within data centers that connect servers,

storage, and networking equipment to support cloud computing, web services,

and big data applications.

 Transportation:

• Traffic Control Systems: Networks used in traffic lights, sensors, and cameras

to manage traffic flow, improve safety, and reduce congestion.

• Fleet Management: Networks for tracking and managing vehicles in logistics

and transportation companies.

 Healthcare:

• Health Information Exchange (HIE): Networks that enable the secure sharing

of patient health records and medical data among healthcare providers for

improved patient care.

• Telemedicine: Networks that support remote medical consultations and

diagnosis, bringing healthcare services to remote or underserved areas.

10

 Financial Services:

• Electronic Banking: Networks that enable online banking, ATM transactions,

and electronic fund transfers.

• Stock Exchanges: Networks that facilitate trading and real-time financial data

transmission for stock markets worldwide.

 Manufacturing and Industrial Automation:

• Industrial Control Systems (ICS): Networks used in factories and industrial

environments to control machinery and automation processes.

• Internet of Things (IoT): Networks connecting various sensors and devices to

collect and transmit data for monitoring and control.

 Entertainment and Media:

• Streaming Services: Networks that deliver multimedia content, such as video

and music streaming, to users over the internet.

• Online Gaming: Networks that enable multiplayer online gaming experiences,

including cloud gaming services.

 Education:

• E-Learning: Networks that support online education platforms, virtual

classrooms, and remote learning opportunities.

 Social Networks:

• Social Media: Online platforms connecting individuals and organizations for

social interaction, content sharing, and communication.

 Agriculture:

• Precision Agriculture: Networks and IoT devices used in farming to monitor

crops, manage resources, and improve crop yields.

 Smart Cities:

• Public Wi-Fi: Networks that provide internet access in public spaces,

promoting connectivity and digital services in urban areas.

11

• Network technologies

Network technologies encompass a wide range of tools, protocols, hardware, and

software used to create and manage computer networks. These technologies enable the

efficient transfer of data, communication between devices, and the sharing of

resources. Here are some key network technologies:

• Ethernet (IEEE 802.3): Ethernet is a widely used wired networking technology that

defines how data packets should be placed on a network cable. It operates over various

media types, including copper and fiber-optic cables, and supports different data

speeds (e.g., 10/100/1000/10000 Mbps).

• Wi-Fi (IEEE 802.11): Wi-Fi technology enables wireless local area networks

(WLANs). It allows devices to connect to a network without physical cables, making it

especially useful for mobile devices like smartphones and laptops. Various Wi-Fi

standards (e.g., 802.11n, 802.11ac, 802.11ax) offer different data rates and features.

• Bluetooth: Bluetooth is a short-range wireless technology primarily used for

connecting devices like smartphones, headphones, and IoT devices. It&#39;s commonly

used for file sharing, audio streaming, and peripheral device connections.

• Cellular Networks: Cellular technology provides wireless connectivity for mobile

phones and other devices. It includes generations like 2G, 3G, 4G, and 5G, with each

generation offering improved data speeds and capabilities.

• IP (Internet Protocol): IP is a fundamental network protocol that governs how data

packets should be addressed and routed across the internet. IPv4 (Internet Protocol

version 4) and IPv6 (Internet Protocol version 6) are the most commonly used

versions.

• TCP/IP (Transmission Control Protocol/Internet Protocol): TCP/IP is a suite of

protocols used for communication over the internet and local networks. It includes

protocols like HTTP, FTP, SMTP, and DNS, which enable various network services.

12

• DNS (Domain Name System): DNS is a technology that translates human-readable

domain names (e.g., www.example.com ) into IP addresses (e.g., 192.168.1.1). It&#39;s

essential for browsing the internet.

• Firewalls: Firewalls are security devices or software that protect networks by

monitoring and controlling incoming and outgoing network traffic. They can block

malicious traffic and unauthorized access.

• Routers: Routers are network devices that connect different networks and determine

the best path for data packets to travel between them. They play a critical role in

directing traffic on the internet.

• Switches: Switches are devices that connect multiple devices within a local network

and efficiently forward data packets only to their intended recipients. They operate at

Layer 2 (Data Link Layer) of the OSI model.

• VPN (Virtual Private Network): VPN technology creates a secure and encrypted

connection over a public network, such as the internet. It&#39;s commonly used for remote

access, privacy, and secure communication.

• VoIP (Voice over IP): VoIP technology allows voice calls to be transmitted over IP

networks. It&#39;s the basis for services like Skype, Zoom, and business phone systems.

• IoT (Internet of Things) Protocols: IoT networks use various protocols such as

MQTT, CoAP, and Zigbee to enable communication between IoT devices and

platforms.

• Network topology types

Network topology refers to the physical or logical layout of devices and connections in

a computer network. Different network topologies are used depending on the specific

requirements of the network, such as scalability, fault tolerance, and cost. Here are

some common network topology types:

13

• Star Topology:In a star network each device on the network has its own cable

that connects to a switch

or hub. A hub sends every packet of data to every device, whereas a switch only sends

a packet of data to the destination device.

Figure caption,

A star network, where devices are connected to a central hub or switch

Advantages and disadvantages of a star network

The advantages of a star network are:

 it is very reliable – if one cable or device fails then all the others will continue to

work

 it is high-performing as no data collisions can occur

The disadvantages of a star network are:

 it is expensive to install as this type of network uses the most cable (network

cable is expensive)

 extra hardware is required (hubs or switches) which adds to cost

14

 if a hub or switch fails, all the devices connected to it will have no network

connection

• Bus Topology:

• Description: In a bus topology, all devices are connected to a single

central cable (the &quot;bus&quot;).

In a bus network all the workstations

, servers and printers are joined to one cable (the bus). At each end of the cable a

terminator

is fitted to stop signals reflecting back down the bus.

Figure caption,

A bus network, connecting several workstations, servers and printers

Advantages and disadvantages of a bus network

The advantage of a bus network is:

 it is cheap to install, as it doesn&#39;t require much cable

15

 Simple and inexpensive to set up, suitable for small networks

The disadvantages of a bus network are:

 if the main cable fails or gets damaged the whole network will fail

 as more workstations are connected the performance of the network will

become slower because of data collisions

 every workstation on the network &quot;sees&quot; all of the data on the network – this is a

security risk

• Ring Topology: In a ring network each device (workstation, server, printer) is

connected to two other devices - this forms a ring for the signals to travel around. Each

packet of data on the network travels in one direction and each device receives each

packet in turn until the destination device receives it.

Figure caption,

A ring network, where each device is connected to two other devices to form a ring

Advantages and disadvantages of a ring network

16

This type of network can transfer data quickly, even if there are a large number of

devices connected because the data only flows in one direction, so there won’t be any

data collisions.

However, the real disadvantage is that if the main cable fails or any device is faulty,

then the whole network will fail.

• Mesh Topology:

• Description: In a mesh topology, every device is connected to every other

device. There are two variations: full mesh (all devices connect to all others)

and partial mesh (only some devices connect to all others).

• Advantages: High redundancy, fault tolerance, can handle heavy traffic loads.

• Disadvantages: Expensive to implement and manage, complex cabling,

scalability challenges in full mesh.

• Hybrid Topology:

“A type of topology which is built by connecting two or more different topologies.”

 For example, the arrangement of computers in an office makes ring topology. And in

another office computers are attached in the form of star topology. So if you connect

these two offices i.e. combining ring and star topology will make a hybrid topology.

17

Diagram of Hybrid Topology

You can combine various topologies that include:-

 Bus topology

 Ring topology

 Star topology

 Mesh topology

If you connect two or more topologies then the resulting hybrid topology will have

attributes of the connected topologies.

The pros and cons of hybrid topology are explained below:-

Advantages of hybrid topology

Some features of hybrid topology are:-

Strong network: If any computer in the network fails to function then other

computers in the network will not be affected.

18

Scalable: This type of network can be expanded without any problem. You just need

an additional hub to connect the new topology to the existing network of topology.

Effective: End users can share their files from one office to another and the speed of

data is also high in the network.

Combined features: When you connect two or more topologies then the resulting

topology will get benefits from all the combined topologies.

Flexible: You can add and remove nodes from the network easily without any issue.

Reliable: if there occurs any error in the network then the error can be identified and

fixes easily.

Large traffic: This topology can handle a large amount of data traffic. You will not

face any traffic issue if you expand or collapse the network. You can make a large

network easily.

Disadvantages of hybrid topology

Some drawbacks of hybrid topology are:-

Complex: As there are two or more topologies connected so the number of nodes

increases also. This will make the network very large and handling all the issues in the

nodes become difficult.

Costly:  To connect different network topologies there is needed a special hub that can

understand all the complexity of the different topologies. This type of special hub is

costly.

19

A lot of cables: As the network grows, the number of cables required to connect also

increases. It becomes difficult for a network technician to handle all the cables

together.

Example of hybrid topology

 Different office branches can be connected

 Networking in a building

 Networking in school/university

 Hospital networking

• Tree Topology (Hierarchical Topology): The below image will help you to

understand how Tree Topology works.

Advantages of Tree Topology

There are numerous benefits of the tree topology, which are as follows:

20

 If one or more nodes have failed in the network, they do not affect the entire

network. And, the network can still continue to operate, even if a single Switch

or Hub has been damaged.

 A tree topology network can be managed and maintained easily.

 In this topology, Node expansion is easy and fast.

 It contains an easy process to detect an error.

 Due to the utilization of Intelligent Hub/Switch, Tree Topology gives much

greater performance than Bus Network.

 In tree topology, the management and establishment are much like Star

Network.

 Additionally, it is much appropriate for small-sized organizations.

Disadvantages of Tree Topology

The tree topology has some disadvantages, which are as follows:

Dependent on the main bus cable

A tree topology depends upon a cable to transmit data to the whole network as the

information is passed one to one node that creates weak areas. If one node has been

damaged, it will impact the entire network, and the rest of the network will be

inaccessible.

It becomes more difficult if the event occurs in the backbone cable. Furthermore, if a

defect happens before the remainder of the tree topology&#39;s branches, the complete

system will not function correctly. Even if all devices on the other side of the problem

can still communicate with each other.

- Costly and complex to implement, failure of the backbone can disrupt the entire

network.

21

QUESTIONS

Multiple-Choice Questions

1. What is a network?

o A) A collection of devices that do not communicate

o B) A set of isolated computers

o C) A collection of computers and devices connected to enable

communication and data exchange

o D) A group of computers used for gaming

o Answer: C) A collection of computers and devices connected to

enable communication and data exchange

2. Which of the following is NOT a type of network classification based on

size?

o A) Personal Area Network (PAN)

o B) Local Area Network (LAN)

o C) Metropolitan Area Network (MAN)

o D) Small Area Network (SAN)

o Answer: D) Small Area Network (SAN)

3. Which network type covers a large geographic area, often connecting

multiple LANs across different cities or countries?

o A) Local Area Network (LAN)

o B) Personal Area Network (PAN)

o C) Wide Area Network (WAN)

o D) Metropolitan Area Network (MAN)

o Answer: C) Wide Area Network (WAN)

4. Which network topology involves devices connecting to a central hub or

switch?

22

o A) Mesh Topology

o B) Star Topology

o C) Ring Topology

o D) Bus Topology

o Answer: B) Star Topology

5. What is the primary purpose of a Peer-to-Peer (P2P) network?

o A) Centralized data management

o B) Direct communication between devices without a central server

o C) Data storage on a central server

o D) Voice communication

o Answer: B) Direct communication between devices without a central

server

6. Which type of network is typically restricted to a specific organization or

group?

o A) Public Network

o B) Private Network

o C) Hybrid Network

o D) Community Network

o Answer: B) Private Network

7. Which of the following is a benefit of networking?

o A) Increased hardware costs

o B) Reduced communication efficiency

o C) Easy information sharing

o D) Decreased flexibility

o Answer: C) Easy information sharing

8. Which network classification is based on architecture?

o A) Personal Area Network

o B) Client-Server Network

23

o C) Metropolitan Area Network

o D) Public Network

o Answer: B) Client-Server Network

9. What is one key advantage of a network?

o A) Files cannot be shared between users.

o B) Backup is complex as data is stored on individual machines.

o C) Printers and other devices can be shared, saving money.

o D) Software licenses are more expensive than standalone licenses.

o Answer: C) Printers and other devices can be shared, saving money.

10. Which of the following is a disadvantage of networks?

o A) Improved communication and collaboration

o B) Potential security risks if not managed properly

o C) Easy backup of data on a central server

o D) Reduced hardware costs

o Answer: B) Potential security risks if not managed properly

• Network components

Computer networks consist of various components that work together to facilitate

communication, data sharing, and resource access among connected devices. These

components can be categorized into several broad categories:

• End Devices:

• Computers: Such as desktops, laptops, servers, and workstations.

• Mobile Devices: Such as smartphones, tablets, and wearable devices.

• Printers: For document and image printing.

• IP Phones: Voice-over-IP (VoIP) phones for voice communication over the

network.

24

• IoT Devices: Sensors, cameras, and other Internet of Things (IoT) devices.

• Networking Hardware:

• Router: A device that connects different networks and directs traffic between

them.

• Switch: A device that connects devices within a local network and efficiently

forwards data packets based on MAC addresses.

• Hub: An older networking device that broadcasts data packets to all connected

devices.

• Access Point (AP): Facilitates wireless connectivity by allowing devices to

connect to a wired network wirelessly (Wi-Fi).

• Firewall: A security device or software that monitors and controls network

traffic, often used to protect against unauthorized access and threats.

• Modem: Converts digital data from a network into a format suitable for

transmission over specific types of media (e.g., DSL, cable, fiber).

• Gateway: Acts as an entry and exit point between different networks,

translating data formats and protocols.

• Network Infrastructure:

• Cabling: Includes Ethernet cables (e.g., CAT6), fiber-optic cables, and coaxial

cables for wired connections.

• Wireless Infrastructure: Access points, wireless controllers, and antennas for

Wi-Fi networks.

• Network Servers: Systems responsible for hosting applications, files, and

services on the network.

• Data Centers: Facilities housing network equipment, servers, and storage

devices for centralized data processing and storage.

• Racks and Cabinets: Housing units for organizing and securing network

equipment.

• Networking Software and Protocols:

25

• Operating Systems: Such as Windows, Linux, and macOS, which include

networking features and protocols.

• Network Protocols: TCP/IP, UDP, HTTP, FTP, SNMP, DNS, DHCP, etc.,

enabling communication and data transfer.

• Network Management Software: Tools for monitoring, configuring, and

managing network devices.

• Virtualization Software: Such as VMware and Hyper-V, used for creating

virtual network environments and virtual servers.

• Network Services and Applications:

• Email Services: Like Microsoft Exchange and SMTP/POP/IMAP servers.

• Web Services: Hosting websites and web applications.

• File Sharing Services: Such as Network Attached Storage (NAS) and cloud-

based file sharing platforms.

• VoIP Services: Voice over IP services for telephony and video conferencing.

• DNS Servers: Resolving domain names to IP addresses.

• DHCP Servers: Assigning IP addresses automatically to devices on the

network.

• Security Components:

• Firewalls: As mentioned earlier, protecting the network from threats.

• Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS):

Monitoring and preventing unauthorized access and attacks.

• Antivirus and Antimalware Software: Protecting end devices from malicious

software.

• Virtual Private Networks (VPNs): Securing data transmitted over public

networks.

• Authentication and Access Control Systems: Managing user access

rights and permissions.

26

 Materials

• Network Cables (twisted, coaxial, and Fiber optic)

Image 1.Twisted pair cable

Image 2. Coaxial cables

27

• Trunk: A trunk is a single channel of communication that allows multiple

entities at one end to correspond with the correct entity at the other end. It is a

“link” that carries many signals at the same time, creating more efficient

network access between two nodes.

• Connectors

A connector is a device that terminates a segment of cabling or provides an entry point

for network devices such as computers, hubs and routers. These can in turn be

differentiated according to their external appearance and connection characteristics.

Types of Connectors

1. Barrel connectors that are used to connect coaxial cables are known as BNC barrel

connectors. The following image shows BNC barrel connectors.

28

Barrel connectors that are used to connect STP or UTP cables are known as Ethernet

LAN jointers or couplers. The following image shows Ethernet LAN jointers or

couplers.

29

Barrel connectors do not amplify the signals. It means, after joining, the total cable

length must not exceed the maximum supporting length of the cable. For example, a

standard UTP cable supports a maximum distance of 100 meters. You can join two

UTP cables if their sum is not more than 100.

For example, you can join the following cables.

Cable 1 (45 meters) + cable 2 (30 meters) = joint cable (75 meters = 45 meters + 30

meters)

The length of the joint cable is less than 100 meters.

But you can&#39;t join the following cables.

Cable 1 (65 meters) + cable 2 (45 meters) = joint cable (110 meters = 65 meters + 45

meters)

The length of the joint cable is more than 100 meters.

2. F connectors

An F connector is used to attach a coaxial cable to a device. F connectors are mostly

used to install home appliances such as dish TV, cable internet, CCTV camera, etc.

The following image shows F connectors.

30

Terminator connectors

When a device places signals on the coaxial cable, the signals travel along the end of

the cable. If another device is connected to the other end of the cable, the device will

receive the signal. But if the other end of the cable is open, the signals will bounce and

return in the same direction they came from. To stop signals from bouncing back, all

endpoints must be terminated.

A terminator connector is used to terminate the endpoint of a coaxial cable. The

following image shows terminator connectors.

T type connectors

31

A T connector creates a connection point on the coaxial cable. The connection point is

used to connect a device to the cable.

The following image shows T-type connectors.

RJ-11 Connectors

RJ-11 connectors have the capacity for six small pins. However, in many cases, only

two or four pins are used. For example, a standard telephone connection uses only two

pins, and a DSL modem connection uses four pins. They have a small plastic flange on

top of the connector to ensure a secure connection.

The following image shows RJ-11 connectors.

RJ-45 connectors

RJ-45 connectors look likes RJ-11 connectors, but they are different. They have 8

pins. They are also bigger in size than RJ-11. RJ-45 connectors are mostly used in

computer networks. They are used with STP and UTP cables. Some old Ethernet

32

implementations use only four of the eight pins. Modern Ethernet implementation uses

all 8 pins to achieve the fastest data transfer speed.

The following image shows RJ-45 connectors.

DB-9 (RS-232) connectors

A DB-9 or RS-232 connector connects a device over a serial port. It has 9 pins. It is

available in both male and female connectors. It is used for asynchronous serial

communication. The other side of the cable can be connected to any popular connector

type. For example, you can connect one side of the cable with a DB-9 connector and

the other side of the cable with another DB-9 connector or with an RJ-45 connector or

with a USB connector.

The following image shows DB-9 connectors.

33

One of the most popular uses of a DB-9 connector is to connect the serial port on a

computer with an external modem.

Universal serial bus (USB) connectors

USB connectors are the most popular. They support 127 devices in the series. All

modern computers have USB ports. Most devices that you can connect to the system

have USB ports. Some examples of devices that support or have USB ports are mice,

printers, network cards, digital cameras, keyboards, scanners, mobile phones, and flash

drives.

34

If the device has a USB port, you can use a cable that has a USB connector on both

ends to connect the device to the computer. If the device does not have a USB port,

you can still connect the device to the USB port. For that, you can use a cable that has

a USB connector on one side and the corresponding connector on the other.

Fiber cable connectors

A variety of connectors are used to connect fiber cables. Some popular connectors are

ST, SC, LC, and MTRJ. Let&#39;s discuss these connectors.

SC connectors

SC connectors are also known as subscriber connectors, standard connectors,

or square connectors. An SC connector connects to a terminating device by pushing

the connector into the terminating device, and it can be removed by pulling the

connector from the terminating device. It uses a push-pull connector similar to audio

and video plugs and sockets.

The following image shows SC connectors.

35

Straight tip (ST) connectors

Straight tip (ST) connectors are also known as bayonet connectors. They have a long

tip extending from the connector. They are commonly used with MMF cables. They

use a half-twist bayonet type of lock. An ST connector connects to a terminating

device by pushing the connector into the terminating equipment and then twisting the

connector housing to lock it in place.

The following image shows ST connectors.

LC connectors

36

LC connectors are known as Lucent Connectors. For a secure connection, they have a

flange on top, similar to an RJ-45 connector. An LC connector connects to a

terminating device by pushing the connector into the terminating device, and it can be

removed by pressing the tab on the connector and pulling it out of the terminating

device.

The following image shows LC connectors.

MTRJ connectors

An MTRJ connector connects to a terminating device by pushing the connector into

the terminating device, and it can be removed by pulling the connector from the

terminating device. It includes two fiber strands: a transmit strand and a receive strand

in a single connector.

The following image shows MTRJ connectors.

37

• Cable Ties :

• Cable clips

38

• Cable Sockets

• Wall plugs

39

 Tools

• Cutting Tools and Stripping tools

• Drilling Tools

40

• Fixing Tool

• Patching Panel

How to Wire a Patch Panel

• Buy a patch panel. ...

• Design a cable map. ...

41

• Remove cable jackets from incoming Ethernet cables. ...

• Remove internal plastic jackets (if any) ...

• Untwist and spread the cable wires. ...

• Set your wires to the panel connector. ...

• Complete your connections.

Internet connections are required in areas with large populations such as business

settings and work environments. In such areas where employees are spread across

various offices and floors, the computers are oftentimes connected to central servers. It

is so simple to wire the internet to the server, but obviously creates a large build-up of

cables around the server area, which must be routed and terminated with absolute care.

Because it is barely possible to hardwire each Ethernet cable, the solution is to

42

terminate the incoming cables at a patch panel. This makes it easy to connect the

server to the patch panel with the help of short cables, which can as well be moved

easily when there is a need to. To achieve this kind of wiring, consider the following

guide on how to wire a patch panel:

Buy a patch panel

When buying the patch panel, ensure it has 110 style insulation displacement

connectors. Similarly, make sure that there are enough patch connectors that can fit the

Ethernet cables. Be sure to conduct a little research so that you can buy the right patch

panel.

left arrow

right arrow

Design a cable map

This will be the only guide indicating to which panel connector a particular incoming

cable is connected. Remember, there could be a need for system upgrades changes in

future, so prepare the right map and label the patch panels accurately for this as well as

problem diagnosis.

Remove cable jackets from incoming Ethernet cables

Cable jackets must be removed from the incoming Ethernet cables, and this is best

done with the help of wire strippers . Cut the jacket approximately 1.5 inches from the

cable, remove and discard it. Wire strippers are also available in hardware and

electrical stores.

Remove internal plastic jackets (if any)

Sometimes you will be handling Cat6 type incoming Ethernet cables. These often

come with an internal plastic jacket, which too should be removed. Use wire cutters in

43

this operation and exercise absolute care. If you are using Cat5e incoming cables,

however, you will not be required to undertake this step.

Untwist and spread the cable wires

Inside the Ethernet cables, you will find four pairs of twisted wires. Unwind these

wires, but be careful not to mix them up. Four of the wires have solid colors while the

rest have a strip of white alongside the solid color.

Set your wires to the panel connector

Each of the wires should then be set to the patch panel. The connector pins are fitted

with labels containing color codes, which should guide you in selecting the type of

wire that goes to a particular connector.

Complete your connections

Using a patch panel punch down tool, press each of the wires down firmly. This

ensures that the wire is held in place by the insulation connector teeth. If this tool has a

cutting edge, place it over the cut end of your Ethernet cables to cut off any extra wire

while pressing. If it lacks the cutting edge, on the other hand, use your wire cutter to

remove the excess wires that are spread over the edges of your connector.

How to make RJ45 cable

RJ45 cable is used for connect the ALL HMI and engineer station through a switch to

communicated each other. It is used to download the any modification and which is

made in graphics in engineering station.RJ45 cable also used for communicate the

printer with computer

Required tool and materials:

• Ethernet Cable – Category 5e or CAT5e or CAT6

• RJ-45 Crimping tool

• RJ45 Crimp able Connectors

44

Introduction: There are four pairs of wires in an Ethernet cable, and an Ethernet

connector (8P8C) has eight pin slots. Each pin is identified by a number, starting from

left to right, with the clip facing away from you.

45

There is two kinds of Ethernet cable is used for communication.

• Straight Through

• Cross over cable

Straight Through cable:

STRAIGHT THROUGH Ethernet cables are the standard cable used for almost all

purposes, and are often called “patch cables”. It is highly recommend you duplicate

the color order as shown on the left. Note how the green pair is not side-by-side as are

all the other pairs. This configuration allows for longer wire runs.

Important Instruction: Always remember that both end connector clip facing away

from you when check the color.

CROSSOVER CABLES –

46

The purpose of a Crossover Ethernet cable is to directly connect one computer to

another computer (or device) without going through a router, switch or hub.

Procedure to make RJ45 cable :

Step 1: Cut into the plastic sheath about 1 inch (2.5 cm) from the end of the cut cable.

Do not cut deep which may cause damage the insulation of core.

Step 2: Unwind and pair the similar colors. Pinch the wires between your fingers and

straighten them out in a sequence of color as u want to make cable (Straight cable or

cross over cable). The color order is important to get correct

47

Step 3: A straight cut across the 8 wires to shorten them to 1/2 Inch (1.3 cm) from the

cut sleeve to the end of the wires by crimping tool. Carefully push all 8 unstrapped

colored wires into the connector. Plastic sleeve should be inserted proper in connector.

Wrong way: The plastic sleeve is not inside the connector where it can be locked into

place. The wires are too long. The wires should extend only 1/2 inch from the blue cut

sleeve. The wires do not go all the way to the end of the connector. The wires are too

short.

48

Crimping the cable: Carefully place the connector into the Ethernet Crimper and cinch

down on the handles tightly. The copper splicing tabs on the connector will pierce into

each of the eight wires. There is also a locking tab that holds the plastic sleeve in place

for a tight compression fit. When you remove the cable from the crimper, that end is

ready to use.

Test the cable: Check the continuity of both connectors each other .Check the cable

threw a cable tester or ping from a computer. To check the cable through computer

connects both connector in two computers for cross cable and straight cable connect

through a switch then ping the computer.

N.B: When you connect two devices of different types together, you use a straight

through cable. When you connect two devices of the same type together, you use a

crossover cable. All cables are straight through if you insert a network device

between two devices of the same kind.

• Crimping tools

49

Crimping tools are used for the following purposes.

• To cut the network cable of the required length from the bundle.

• To remove the outer and inner jackets of the network cable.

• To attach the connectors on both ends of the cable.

• Testing tool

50

a

Network cable testing and troubleshooting tools

A network cable testing and troubleshooting tool is used for the following purposes.

• To measure the length of a segment or network cable.

• To detect loose connectors.

• To identify an un-labeled network cable from all network cables.

• To find a break in the network cable.

• To certify the cable installation.

 Equipment

51

• Computer: A computer is a machine that can be programmed to carry out

sequences of arithmetic or logical operations (computation) automatically.

• UPS: An uninterruptible power supply (UPS) or uninterruptible power

source is a type of continual power system that provides automated backup

electric power to a load when the input power source or mains power fails. A

UPS differs from a traditional auxiliary / emergency power system or standby

generator in that it will provide near-instantaneous protection from input power

interruptions by switching to energy stored in battery packs , super capacitors .

52

• Inverter: An inverter converts the DC voltage to an AC voltage. In most cases,

the input DC voltage is usually lower while the output AC is equal to the grid

supply voltage of either 120 volts, or 240 Volts depending on the country.

• Switch: A network switch is networking hardware that connects devices on a

computer network by using packet switching to receive and forward data to the

destination device. A network switch is a multiport network bridge that uses

MAC addresses to forward data at the data link layer of the OSI model.

53

• Glue gun: Hot-melt adhesive, also known as hot glue, is a form of

thermoplastic adhesive that is commonly sold as solid cylindrical sticks of

various diameters designed to be applied using a hot glue gun.

• Rack:

What is a Network Rack?

54

Known by many names, a network rack is a metal frame chassis that holds, stacks,

organizes, secures and protects various computer network and server hardware

devices. The term “network” refers to the rack actually housing this type of hardware.

Network Rack Equipment

These racks can house a lot of different types of equipment.  Network equipment is

really just an umbrella term that encapsulates various kinds of technology. Some of

these devices include the following:

• Switches – Multi-port, high-speed devices that receive data and redirect them to

the correct destination on a local area network (LAN). Information can only go

across a single network using a switch.

• Routers – Similar to switches, routers receive and forward information, but

they can carry data over multiple networks. This is why, for example, different

devices or networks can access the Internet using one single router.

• Modems – This device actually connects the source of your internet to your

router. This is typically done using an ethernet cord.

• Brackets

55

• Patch panel: A patch panel in a local area network (LAN) is a mounted

hardware assembly that contains ports that are used to connect and manage

incoming and outgoing LAN cables. A patch panel provides a way to keep large

numbers of cables organized, enabling flexible connectivity into network

hardware located in a data center or an access or wiring closet.

• Repeater

56

In telecommunications, a repeater is an electronic device that receives a signal and

retransmits it. Repeaters are used to extend transmissions so that the signal can

cover longer distances or be received on the other side of an obstruction.

10.Regenerator: : In the context of networking, a &quot;regenerator&quot; typically refers to a

network device or component that is used to boost or regenerate the strength of optical

signals. Optical signals can degrade as they travel long distances in optical fiber

cables, and regenerators are employed to restore the signal quality.

IC.1.2. Termination of Network cables

Network cables installation types.

• Open-Wire

• Aerial

• Above-Grounds Conduits

• Underground

• Underwater

57

• Built in

• Semi built in

• Open-Wire: Open-wire lines were historically used for telecommunication

purposes, including telephone and telegraph systems. Multiple wires were often

strung together, and different wires were dedicated to different communication

circuits.

• Aerial: In networking and telecommunications, the term &quot;aerial&quot; typically refers

to an antenna. An antenna is a device used to transmit and receive wireless

signals, such as radio waves, microwaves, or other electromagnetic waves.

Aerials play a crucial role in wireless communication, including wireless

networking, cellular communications, and broadcasting. Here are some key

points about aerials in networking:

Wireless Networking: Aerials are an integral part of wireless networking,

including Wi-Fi (Wireless Fidelity) and other wireless communication protocols.

Wi-Fi routers and access points are equipped with antennas to send and receive

data wirelessly to and from connected devices like laptops, smartphones, and IoT

devices.

Cellular Networks: In cellular networks, the antennas on cell towers and base

stations are often referred to as aerials. They are responsible for transmitting and

receiving signals to and from mobile devices, allowing users to make calls, send

text messages, and access mobile data services.

58

Broadcasting: In television and radio broadcasting, large aerials (antennas) are

used to transmit broadcast signals. These signals are received by the aerials of

consumer TVs and radios, allowing people to access broadcasted content.

Satellite Communication: In satellite communication, both ground-based and

satellite-based antennas are used to establish connections with satellites in orbit.

Ground stations use directional aerials to communicate with satellites, and the

satellites themselves have aerials to transmit signals back to Earth.

MIMO (Multiple Input, Multiple Output): In advanced wireless technologies

like 4G and 5G, multiple-input, multiple-output (MIMO) systems use multiple

aerials at both the transmitter and receiver to improve signal quality and increase

data throughput.

Antenna Placement: The placement and orientation of aerials are critical factors in

network design. Proper positioning can optimize signal coverage, reduce

interference, and improve network performance.

Aerials are fundamental components of wireless communication systems, enabling

the transmission of data and signals over the air. The type of aerial used depends on

the specific application, the frequency of the signals, and the desired coverage area.

Proper selection and placement of aerials are essential for the successful operation

of wireless networks.

• Above-Grounds Conduits:

59

Above-ground conduits, also known as overhead conduits or overhead cable trays, are

physical structures used in networking and telecommunications to support and protect

cables, wires, and other infrastructure components. They are typically installed above

the ground or overhead, often attached to walls, ceilings, or support structures. Above-

ground conduits have several applications in networking:

Cable Management: Above-ground conduits are commonly used to organize and

manage network cables, such as Ethernet cables, fiber optic cables, and power cables.

Making it easier to trace and replace cables when necessary.

Data Centers: In data centers, where large quantities of cables are used to connect

servers, switches, and other networking equipment, above-ground conduits are used to

route and protect cables. They help maintain cable organization and facilitate

maintenance and changes.

Suspended Ceilings: In office buildings and commercial environments, above-ground

conduits can be used to route cables through suspended(hang) ceilings, providing a

clean and organized appearance.

Maintenance Access: They allow easy access to cables for maintenance, inspection,

and future upgrades. This is particularly important in data centers and other

networking environments.

• Underground

60

&quot;Underground&quot; in the context of networking and telecommunications typically refers

to the deployment of cables, conduits, or infrastructure beneath(under) the ground.

Underground installations are common for various purposes in networking and

utilities. Here are some key aspects of underground installations in networking:

Cable Installation: Underground installations are often used to lay cables, such as

fiber optic cables and power cables, below the surface to connect buildings, data

centers, or network endpoints. This method is preferred in urban areas to reduce visual

clutter and protect cables from physical damage and environmental factors.

Conduits: Conduits, which are protective pipes or tubes, are commonly used for

routing and protecting cables underground. Conduits shield cables from moisture, soil,

and other external elements, helping to maintain the integrity of the network.

Outdoor Fiber Networks: Telecommunications providers often deploy underground

fiber optic networks to connect neighborhoods and provide high-speed internet

services. This approach offers reliability and minimizes the risk of damage from

accidents.

Data Centers: Data centers may have underground cable routes to connect different

parts of the facility.

Residential and Commercial Utilities: Utilities like electricity, water, and gas may use

underground installations to supply homes and businesses. These utilities may share

underground infrastructure with telecommunications networks, as they can use

common conduits to reduce installation costs and environmental impact.

61

• Underwater:

In networking and telecommunications, &quot;underwater&quot; typically refers to the

deployment of network infrastructure, cables, and communication systems beneath the

surface of bodies of water, such as oceans, seas, rivers, and lakes. Underwater

networking is essential for a variety of applications, including:

Submarine Communication Cables: Submarine communication cables are undersea

cables that span the ocean floors and connect continents and countries. These cables

carry the majority of international internet traffic, enabling global communication and

data exchange.

The deployment and maintenance of underwater networking infrastructure are

complex endeavors that involve specialized technology, vessels, and international

cooperation. Submarine communication cables, in particular, are critical for global

internet connectivity, and they are often installed and operated by undersea cable

consortia or telecommunications companies.

• Built in

• Semi built in

• Network cables Trunking materials

• Plastic

• Wood

• Stainless

• Plastic: Cable trunking is installed as a protective routing and covering system

for electrical cables and wires which prevents accidental damage.

62

• Wood

• Stainless

• Cable termination

• twisted pair cabling

• Fiber-optic cabling

• Coaxial cabling

63

• shielded twisted pair

3. Connection of Network Media

• Labelling

Properly labeling your network cables can be critical for a successful installation, as

well as for your network in the long run. Using labeled cables helps prevent people

from unplugging the wrong cable at the wrong time,

• Patching and Tagging

&quot;Patching and tagging&quot; typically refers to the practice of labeling and organizing

network cables, particularly in data centers, server rooms, and structured cabling

systems. Proper labeling and organization of network cables are essential for efficient

network management, troubleshooting, and maintenance. Here&#39;s what &quot;patching and

tagging&quot; involves:

1. Patching:

Patching refers to the physical connection of cables. This process involves connecting

network cables from active devices (e.g., computers, servers, switches) to passive

devices (e.g., patch panels or wall outlets) or to other active devices.

64

Patch panels are commonly used in data centers and server rooms to terminate and

manage network connections. Each port on a patch panel corresponds to a specific

location or device.

Cables are connected to the patch panel on one end and to the active devices or wall

outlets on the other end, forming the physical links in the network.

2. Tagging:

Tagging involves labeling or tagging each cable with relevant information. This is

typically done using cable labels or markers that are affixed to the cables.

Each cable is labeled with information such as its source and destination, cable type

(e.g., Cat 6, fiber optic), and unique identifier (e.g., port number, device name).

Cable labels are typically color-coded or otherwise organized to make identification

easier.

Patching and tagging offer several benefits in network management:

Easy Identification: Proper labeling allows network administrators to quickly identify

the purpose and location of each cable, simplifying troubleshooting and maintenance.

Minimized Downtime: When network issues occur, administrators can pinpoint

problems and make repairs more efficiently, reducing network downtime.

Documentation: Accurate labeling provides documentation of network connections,

which is valuable for future reference and expansion planning.

65

Improved Scalability: Well-organized cabling systems make it easier to add, move,

or change connections as network requirements evolve.

Compliance and Standards: In some industries and data centers, compliance with

labeling and documentation standards is required for regulatory reasons.

• Provide us build design

Designing a network architecture: can be a complex process that depends on

various factors, including the organization&#39;s requirements, budget, and existing

infrastructure. Below is a high-level outline for designing a network, focusing on

common components and considerations. Please note that the specific design will vary

based on your needs.

1. Requirements Gathering:

Begin by understanding the business requirements and objectives.

Identify the number of users, devices, and the types of applications that will run on the

network.

2. Network Topology:

Choose a network topology that suits your needs. Common topologies include star,

bus, ring, and mesh.

66

3. IP Addressing:

Decide on IP addressing schemes, both IPv4 and IPv6, and subnetting.

Plan for address allocation, including static and dynamic addresses.

4. Routing and Switching:

Select appropriate routers and switches. Cisco, Juniper, and other vendors offer

various options.

Configure routing protocols (e.g., OSPF, BGP) based on the network&#39;s size and

complexity.

5. Security:

Implement security measures, including firewalls, intrusion detection/prevention

systems, and access control lists (ACLs).

Encrypt sensitive data with technologies like VPNs or SSL/TLS.

6. VLANs (Virtual LANs):

Divide the network into VLANs to segregate traffic and improve security.

Plan VLAN assignments based on department, function, or security requirements.

7. Wireless Networks (Wi-Fi):

If applicable, design the wireless network with considerations for coverage, capacity,

and security.

67

Implement WPA3 security and consider guest networks.

8. Network Management:

Choose network monitoring and management tools (e.g., SNMP, Net Flow).

Set up alerting and reporting to proactively identify and resolve issues.

9. Documentation:

Maintain comprehensive network documentation, including network diagrams, IP

address assignments, device configurations, and change logs.

10. Training and Support:

Provide training for network administrators and support staff.

Learning outcome 2: Perform Basic Network Configuration

Indicative content 2.1Classification of IP Addresses

What Is an IP Address?

IP address stands for internet protocol address; it is an identifying number that is

associated with a specific computer or  computer network . When connected to

the  internet , the IP address allows the computers to send and receive information.

How do IP Addresses Work?

An IP address allows computers to send and receive data over the internet. Most IP

addresses are purely numerical, but as internet usage grows, letters have been added

to some addresses.

Types of IP Addresses

There are four different types of IP addresses: public, private, static, and dynamic.

While the public and private are indicative of the location of the network—private

68

being used inside a network while the public is used outside of a network—static and

dynamic indicate permanency.

A static IP address is one that was manually created, as opposed to having been

assigned. A static address also does not change, whereas a dynamic IP address has

been assigned by a (DHCP) server and is subject to change. Dynamic IP addresses are

the most common type of internet protocol addresses. Dynamic IP addresses are only

active for a certain amount of time, after which they expire. The computer will either

automatically request a new lease, or the computer may receive a new IP address.

An IP address can be compared to a  Social Security Number  (SSN) since each one is

completely unique to the computer or user it is assigned to. The creation of these

numbers allows routers to identify where they are sending information on the internet.

They also make sure that the correct devices are receiving what is being sent. Much

like the post office needs a mailing address to deliver a package, a router needs an IP

address to deliver to the web address requested.

What Are the Different Types of IP Addresses?

Consumer IP Addresses: These are the IP addresses of individuals and businesses

who use the internet. Consumer IP addresses could be either public or private

addresses. Typically, devices use private IP addresses within a network and a public

IP addresses outside a network. For example, each device within the same network is

assigned a unique private IP address, whereas a public IP can be accessed directly

over the internet and is assigned to your network router by your ISP.

Public IP addresses come in two types: dynamic IP addresses and static IP addresses.

Dynamic IP Addresses: A dynamic IP address refers to an address assigned to a

device temporarily by an ISP. Dynamic IP addresses are typically assigned to devices

such as computers, smartphones, or routers. They provide a level of anonymity and

security as the IP address changes periodically, making it more difficult to track a

specific device or user. When a device connects to the ISP&#39;s network, it is assigned an

69

available IP address from a pool. This address is then borrowed for a specific duration

before being returned to the pool and assigned to another device.

Static IP Addresses: A static IP address is a fixed address assigned to a device that

remains constant. They are typically used for hosting websites or running servers. By

having a fixed IP address, users can easily connect domain names to their servers,

ensuring that their  websites  or services are always accessible. Static addresses are

manually configured either on the device itself or by the network administrator. Static

IP addresses are typically provided by the user’s ISP or network administrator, and

typically come at an additional cost.

IP address versions

What Is IP?

The Internet Protocol (IP) is a set of networking rules that enable computers to

communicate over the Internet. IP has two primary purposes:

• Enable different computers to exchange data over the Internet while ensuring

sent files arrive at the correct destination.

• Identify every device and domain that connects to the Internet by assigning  a

unique IP address  (a series of digits that identify a specific computer or device).

When you send something online, the IP breaks data into smaller chunks

called packets. Each packet has attached IP info that ensures whatever you send

reaches the right recipient. This process occurs automatically and looks like this:

• The sender&#39;s computer connects to the Internet via  a local router , either at home

or within an office  server room .

• The router (which has a  static IP address  that never changes) assigns a

temporary (a.k.a. dynamic) IP address to the device to enable communication.

70

• IP converts files into datagrams with a header (info consisting of IP

source/destination and metadata) and the payload (the data itself).

• The protocol nests data into  packets .

• IP breaks down data packets ( fragmentation ) and sends them over the Internet to

the specified IP address.

• Once data reaches its destination, IP rebuilds the file (reassembly) to allow

access.

The Internet Protocol does not assign IP addresses at random. A non-profit

organization called Internet Corporation for Assigned Names and Numbers (ICANN)

allocates IP addresses to Internet Service Providers (ISPs) who assign addresses to

end-user devices.

Most networks combine IP with  TCP (Transmission Control Protocol)  or  UDP (User

Datagram Protocol)  to form a connection between devices. All three are a part of the

broader Internet Protocol Suite (TCP/IP) that governs rules for routing and receiving

data over a network.

What Is IPv4?

IPv4 is the first major version of the Internet Protocol that&#39;s been the go-to

communication model for the Internet since the 1980s.

IPv4 assigns 32-bit IP addresses to devices. Each address has four groups of numbers

(8-bit sections called octets) separated by a period, such as:

192.158.1.38

The value of each octet ranges from  0 to 255, so the IPv4 model includes every

address between 0.0.0.0 and 255.255.255.255. All IPv4 addresses have two parts:

• The network ID (the first three octets) that indicates which network the device

is on.

71

• The host ID (the fourth octet) that identifies the specific device on that network.

For example, if your home network has a 192.168.1.1 address, 192.168.1 is the

network ID, while the final octet (1) is the host ID. In most networks, the router gets

the .1 value by default.

IPv4 enables the creation and use of 4,294,967,296 unique addresses (more

commonly expressed as 2^32). In the 1980s and 1990s, over 4 billion available

addresses seemed sufficient to meet the demand of the online world.

The most common technique for reusing IPv4 addresses is Network Address

Translation (NAT).  NAT  enables you to represent a group of devices with a single IP

address, which conserves  bandwidth  and slows down the depletion(reduction) of IP

addresses.

We view IP addresses in human-readable notations, such as 66.94.29.13. However,

computers only understand binary format, so the address we see as 66.94.29.13 stands

for 01000010.01011110.00011101.00001101 in the &quot;computer language.&quot;

IPv4 Features

72

Here are the main features of IPv4:

• Creates 32-bit IP addresses.

• Addresses use four 1-byte decimal numbers separated by a dot, a format that a

human can easily read and even remember.

• Connectionless protocol.

• Requires small amounts of memory to store address info in the network.

• Supported by nearly all devices and websites on the Internet.

• Offers video libraries and conferences.

• Enables the creation of a simple virtual communication layer over

diversified(different) devices.

What Is IPv6?

IPv6 is the latest Internet Protocol version and the successor to IPv4. IPv6 aims to

fulfill the need for more IP addresses, the main issue of the previous IP. Another

common name for IPv6 is IPng (Internet Protocol next generation).

IPv6 uses 128-bit hexadecimal IP addresses. This model enables 2^128 unique

addresses (over 340 undecillion, which is 340 with 36 zeros).

IPv6 addresses are significantly longer than IPv4 variants (eight 16-bit blocks with

groups of four symbols, often called hextets or quartets) and are alphanumeric. Also,

whereas IPv4 relies on periods for formatting, IPv6 uses colons, such as in this

example:

2001:0db8:0000:0001:0000:ff00:0032:7879

The model omits leading zeros (like in IPv4), and you&#39;ll sometimes find IP addresses

that have a double colon (::) that designate any number of 0  bits  (such as

1201:2db7::fa00:0040:6669, in which the third, fourth, and fifth hextets are 0000).

73

While IPv6 is more sustainable than IPv4, the majority of the Internet still uses

IPv4. Upgrading all the routers,  servers , and  switches  that have used IPv4 for decades

takes a lot of time and money.

IPv6 Features

Here are the main features of IPv6:

• A 128-bit hexadecimal address scheme.

• Both stateful and stateless configurations.

• Auto-configuration capabilities.

• Support for  Quality of Service (QoS) .

• Better multicast routing and simpler header format than IPv4.

• End-to-end connectivity at the IP layer, so there&#39;s no need for NAT.

• Integrated Internet Protocol Security (IPSec) with built-

in  authentication ,  encryption , and privacy support.

IPv4 vs IPv6: What’s the difference?

Both IPv4 and IPv6 identify connected devices on the network. However, there are

slight differences in the way they operate. IPv6 is the newer IP version and was

introduced to address the limitations IPv4 posed on the availability of IP addresses.

The following is a list of differences between IPv4 and IPv6:

• IPv4 is 32-bit, whereas IPv6 is 128-bit.

• In IPv4, binary bits are separated by a dot (.); IPv6 separates binary bits by a colon

(:).

• IPv4 follows the numeric addressing method and IPv6 is  alphanumeric .

74

• IPv4 offers 12 header fields and IPv6 offers eight header fields.

• IPv4 has  checksum  fields but IPv6 doesn&#39;t.

• IPv4 supports broadcast address, which is a type of special address that transmits

data packets to every node on the network. IPv6 doesn&#39;t support broadcast, but

instead uses a multicast address, which is a logical identifier for a collection of

hosts on a network.

• IPv4 supports  Variable Length Subnet Mask , but IPv6 doesn&#39;t.

Looking up an IP address

There are many ways to look up the IP address of a device. However, the simplest way

is to type what is my IP address? into an internet browser, such as  Google Chrome .

The returning address will be the public IP address of the requesting device.

Windows 10 and Windows 11

• Select Start&gt;Settings&gt;Network &amp; internet&gt;Wi-Fi and the  Wi-Fi network  you&#39;re

connected to.

• Under Properties, look for your IP address listed next to IPv4 address.

Identification of IP address classes

IP Address Classification Based on Operational Characteristics

There are three different types of IP addresses within this classification.

75

1. Unicast IP Addresses

This is an address of a single interface which are used for one-to-one communication.

Unicast IP addresses are used to direct packets to a specific host.

2. Multicast IP Addresses

Multicast IP addresses are used for one-to-many communication. Multicast messages

are sent to IP multicast group addresses. The packets reach multiple destinations,

however, not every single one of them.

3. Broadcast IP Addresses

This type of IP is used to send data to all the possible destinations within the broadcast

domain.

IP Address Terminology

Static means the IP address never changes as long as you stay with the same provider

or same server.

Dynamic means the IP address can change from time-to-time.

76

Public means the IP address can be visited from any computer in the world.

Private means the IP address can only be used by those on the same network.

Shared means other people use your IP address for their connection or websites.

Dedicated means no one else uses your IP address for their connection or websites.

Class identifies the range of your IP address and the default subnet mask.

• A class - 0 to 127 with default mask of 255.0.0.0

• B class - 128 to 191 with default mask of 255.255.0.0

• C class - 192 to 223 with default mask of 255.255.255.0

• D class - 224 to 247 (not currently used) or D class - 224 to 239 (not currently

used)

• E class - 248 to 255 (not currently used) or E class - 240 to 255 (not currently

used)

•

Identification of IP address classes

There are two versions of IP addresses, IPv4 and IPv6. In this tutorial, we will discuss

how IPv4 organizes IP addresses. In IPv4, there are 4,294,967,296 IP addresses. These

addresses are organized into five IP classes. These classes are A, B, C, D, and F.

Before we understand how IP addresses are organized in these classes, let&#39;s briefly

discuss how IP addresses are written and structured.

IP addresses notation

Computers understand only the binary system. The binary system uses bits to store and

process data. A bit can store only two values: zero (0) and one (1). If the

77

value &#39;zero&#39; is stored, the bit is known as the OFF bit. If the value &#39;one&#39; is stored, the

bit is known as ON bit. The binary system uses a unique combination

of ON and OFF bits for each letter and number.

Using IP addresses in the binary format is not easy. But the good news is that unless

you are a software developer or a network administrator, you never need to write and

use IP addresses in binary notation. You can write and use them in decimal format.

The software program that you use to assign the IP address on the interface

automatically converts the assigned IP address into binary format.

If you are a software developer or a network administrator, you can also use IP

addresses in decimal format. But you should also understand how IP addresses work in

the binary system. Since interfaces use the binary system to process IP addresses,

learning IP addresses in binary format can make your IP related tasks easy.

In short, you can write and use IP addresses in two notations: binary notation and

decimal-dotted notation. In binary notation, all the individual bits of each byte are

expressed as a binary number. In decimal notation, all four binary bytes are converted

and expressed to their decimal equivalent numbers.

In this session,we will understand IP classes in both notations.

IP addresses structure

An IP address consists of 32 bits. These bits are divided into four sections. Sections

are separated by a dot (.). Each section contains 8 bits. 8 bits are equal to 1 byte or 1

octet. The following image shows how bits are organized in an IP address.

78

By using 32 bits with two possible values for each position, the binary system can

create 4,294,967,296 (2 32 ) unique combinations or IP addresses. These addresses can

be used without any addressing scheme or with an addressing scheme that arranges

them in such a way that it becomes easier to access them.

If addresses are used without any addressing scheme, all routers on the network will

need to store the address of each and every interface on the network. Depending on the

size of the network, this may affect routing. If the network size is small, it can make

routing slow. If the network size is moderate, it can make routing very slow. If the

network size is large, it can make routing completely impossible.

For efficient routing, addresses are organized into the hierarchical addressing scheme.

In this scheme, all addresses are divided into five classes and each address is divided

into two addresses: the network address and the host address.

IP address classes

Based on the following rules, IP addresses are categorized into five classes; A, B, C,

D, and E.

• In class A, the first bit of the first byte always remains OFF (0).

• In class B, the first bit of the first byte always remains ON and the second bit of the

first byte always remains OFF.

79

• In class C, the first two bits of the first byte always remain ON and the third bit of the

first byte always remains OFF.

• In class D, the first three bits of the first byte always remain ON and the fourth bit of

the first byte always remains OFF.

• In class E, the first four bits of the first byte always remain ON.

By turning all remaining bits of the first byte ON and OFF, we can make the first and

last address of that class.

The following table lists the value of the first byte or octet in both notations.

Class Fix bits First address

(binary notation)

Last address

(binary notation)

First address

(decimal

notation)

Last address

(decimal

notation)

A 0 00000000 01111111 0 127

B 10 10000000 10111111 128 191

C 110 11000000 11011111 192 223

D 1110 11100000 11101111 224 239

E 1111 11110000 11111111 240 255

Network and host addressing

In the second level of the hierarchical addressing scheme, each address is further

divided into two addresses: the network address and host address.

Network addresses are used to combine multiple IP addresses in a group while host

addresses are used to provide a unique identity to each IP address in the group. A

network address is the group address. All group members use the same network

address. A host address is a unique address in the group.

80

To learn more about how the network addresses and host addresses work, you can

check the following tutorial.

IP address, Network address, and Host address Explained

The length of network addresses and host addresses in IP addresses are different in all

IP classes. In class A, the first bits are reserved for the network address. The

remaining 24 bits are available for the host address. In class B, the first 16 bits are

reserved for the network address while the last 16 bits are available for the host

address. In class C, the first 24 bits are reserved for the network address while the

last 8 bits available for the host address.

The following image shows how bits are defined for network addresses and host

addresses in each IP class.

In IP addresses, host bits are flexible. Administrators can adjust the length of host bits

to meet the requirements of their networks. They can use host bits as network bits to

utilize maximum addresses from all available addresses. If hosts bits are used as the

network bits, this is known as the subnetting.

Class D and E are not used for the host addressing. Class D addresses are used for

multicast addresses. Class E addresses are reserved for research and development

purposes. Multicast addresses are explained in the following tutorial.

81

The subnet mask

IP addresses use an additional component to distinguish between network addresses

and host addresses. This component is known as the subnet mask. In simple words,

the subnet mask tells, how many bits in the IP address are used as the network address

and how many bits are left for the host address.

IP addresses are always written with the subnet mask. The following table lists the

default subnet mask for all IP classes.

Class Decimal

notation

Binary notation

A 255.0.0.0 11111111.00000000.00000000.00000000

B 255.255.0.0 11111111. 11111111.00000000.00000000

C 255.255.255.0 11111111. 11111111. 11111111.00000000

Identifying the class of an IP address (decimal notation)

If an IP address is written in the decimal notation, check the value of the first section

or octet and use the following rules to identify the class of the IP address.

• If the value is in the range 1 to 127, the address belongs to class A.

• If the value is in the range 128 to 191, the address belongs to class B.

• If the value is in the range 192 to 223, the address belongs to class C.

• If the value is in the range 224 to 239, the address belongs to class D.

• If the value is in the range 240 to 255, the address belongs to class E.

Identifying the class of an IP address (binary notation)

If an IP address is written in the binary notation, you can use the following rules to

identify the class of the IP address.

• If the first bit is OFF, the address belongs to class A.

82

• If the first bit is ON and the second bit is OFF, the address belongs to class B.

• If the first two bits are ON and the third bit is OFF, the address belongs to class C.

• If the first three bits are ON and the fourth bit is OFF, the address belongs to class D.

• If the first four bits are ON, the address belongs to class E.

Examples of IP addresses

Decimal notation Binary notation

1.2.3.4

255.0.0.0

00000001.00000010.00000011.00000100

11111111.00000000.00000000.00000000

10.10.10.10

255.0.0.0

00001010.00001010.00001010.00001010

11111111.00000000.00000000.00000000

25.147.191.14

255.0.0.0

00011001.10010011.10111111.00001110

11111111.00000000.00000000.00000000

95.86.75.4

255.0.0.0

01011111.01010110.01001011.00000100

11111111.00000000.00000000.00000000

127.0.0.1

255.0.0.0

01111111.00000000.00000000.00000001

11111111.00000000.00000000.00000000

Examples of class A IP addresses are the following.

Examples of class B IP addresses are the following.

Decimal notation Binary notation

129.12.36.42

255.255.0.0

10000001.00001100.00100100.00101010

11111111.11111111.00000000.00000000

168.172.1.1

255.255.0.0

10101000.10101100.00000001.00000001

11111111.11111111.00000000.00000000

83

175.66.43.12

255.255.0.0

10101111.01000010.00101011.00001100

11111111.11111111.00000000.00000000

145.186.175.234

255.255.0.0

10010001.10111010.10101111.11101010

11111111.11111111.00000000.00000000

190.60.152.25

255.255.0.0

10111110.00111100.10011000.00011001

11111111.11111111.00000000.00000000

Examples of class C IP addresses are the following.

Decimal

notation

Binary notation

192.168.1.1

255.255.255.0

11000000.10101000.00000001.00000001

11111111.11111111.11111111.00000000

210.20.30.40

255.255.255.0

11010010.00010100.00011110.00101000

11111111.11111111.11111111.00000000

216.123.145.16

255.255.255.0

11011000.01111011.10010001.00010000

11111111.11111111.11111111.00000000

220.86.76.43

255.255.255.0

11011100.01010110.01001100.00101011

11111111.11111111.11111111.00000000

220.60.80.100

255.255.255.0

11011100.00111100.01010000.01100100

11111111.11111111.11111111.00000000

84

Indicative content 2.2: Calculation of IP addresses subnet masks

• Introduction to subnet masks

A subnet mask is a 32-bit number created by setting host bits to all 0s and setting

network bits to all 1s. In this way, the subnet mask separates the IP address into the

network and host addresses. The “255” address is always assigned to a broadcast

address, and the “0” address is always assigned to a network address.

• Definition:Subnetting is the process of dividing a large network into smaller,

more manageable subnetworks or subnets. It offers several benefits in terms of

network management, security, and efficiency. Here are some of the key

benefits of subnetting:

• Benefits of subnetting

Efficient IP address utilization: Subnetting allows you to break down a large IP

address space into smaller segments, which helps optimize the allocation of IP

addresses. This is especially important in a world where IPv4 addresses are becoming

increasingly scarce.

Network segmentation: Subnets can be used to logically segment a network, which

enhances network organization and management. Different subnets can be assigned to

different departments, teams, or functions within an organization, making it easier to

manage and troubleshoot network issues.

Improved network performance: Smaller subnets can reduce broadcast traffic, as

broadcast packets are limited to the devices within the same subnet. This helps

improve overall network performance by reducing unnecessary network traffic.

85

Enhanced security: Subnetting can be used to isolate sensitive or critical parts of a

network from the rest of the network. This provides an additional layer of security by

limiting the scope of potential security breaches or attacks.

Simplified troubleshooting: When a network is divided into smaller subnets, it

becomes easier to identify and isolate issues. Troubleshooting and diagnosing

problems are more efficient because you can narrow down the affected portion of the

network.

Improved network management: Subnetting simplifies the management of IP

addresses, routing tables, and network devices. It enables network administrators to

apply access control policies, quality of service (QoS), and other network services

more effectively.

Questions

Q. Why use subnets?

A. Subnets will enhance network security, efficiency, and performance, and create a

speedier set of route maps for data.

Q. How can my company use subnets?

A. Locate a highly qualified engineer by utilizing the search function at Field

Engineer .

Q. How many hosts can a subnet have?

A. If you subtract the number of network bits from the number of total bits, you can

calculate the total number of hosts a subnet can have.

Q. What sort of networks would be best for subnetting?

A. Small networks don’t require subnets. However, large LANs are prime candidates

as IP address allocation will be impactful with group devices to maximize

organization.

86

Q. What is an IP class?

A. IP classification is complex. However, in layman’s terms, IP classes range from A -

E. Class A, B, and C are used for host addresses without exception. Class D is for

multicasting. And Class E is rarely used within networks of companies.

• Binary system

The binary system is a numeral system that uses a base of 2. In contrast to the decimal

system, which uses base 10 and has ten digits (0 through 9), the binary system uses

only two digits: 0 and 1. This system is fundamental in computer science and digital

electronics because it aligns with the binary logic of on and off, high and low voltage,

and true and false states.

Here are some key points about the binary system:

Digits: In the binary system, each digit is called a &quot;bit,&quot; which is short for &quot;binary

digit.&quot; A bit can have one of two values, either 0 or 1.

Place Value: Just like in the decimal system, the binary system uses place value. Each

position from right to left represents a power of 2. For example, in the binary number

1101, the rightmost digit is 2^0, the next is 2^1, the next is 2^2, and the leftmost digit

is 2^3.

Counting: Counting in binary follows a simple pattern. It goes from 0 (represented as

0 in binary) to 1 (also represented as 1 in binary). Then, when you add 1 to 1, it

&quot;carries over&quot; just like in the decimal system, becoming 10 in binary (which is

87

equivalent to 2 in decimal). The pattern continues: 11 (3 in decimal), 100 (4 in

decimal), 101 (5 in decimal), and so on.

Representation in Computers: Computers use binary internally to represent all data

and instructions. Each piece of data, such as numbers, characters, and even the

program itself, is represented in binary. This is because digital electronic devices work

with electrical voltage that can be either high (1) or low (0).

Boolean Logic: The binary system aligns with Boolean logic, where 0 typically

represents &quot;false&quot; or &quot;off,&quot; and 1 represents &quot;true&quot; or &quot;on.&quot; This is fundamental in

computer programming and digital circuit design.

Binary is the basis for all digital communication and computation. It&#39;s used for

encoding, storage, processing, and transmission of data in computers and other digital

systems, making it a fundamental concept in the field of information technology.

• Types of Subnetting

There are two types of Subnetting FLSM and VLSM. In FLSM, all subnets have

equal number of host addresses and use same Subnet mask. In VLSM, subnets have

flexible number of host addresses and use different subnet mask.

FLSM Subnetting and VLSM Subnetting

There are two types of Subnetting: FLSM and VLSM. In FLSM, all subnets have an

equal number of host addresses and use the same subnet mask. In VLSM, subnets have

a flexible number of host addresses. They use a subnet mask based on the number of

hosts.

Default IP subnets have a large number of IP addresses. Most networks do not need

too many IP addresses. If they use the default subnet, all unused IP addresses become

useless. To utilize free IP addresses, we use subnetting.

88

Subnetting allows us to break default IP subnets. There are two types of subnetting:

FLSM and VLSM.

FLSM stands for Fixed Length Subnet Mask. In it, we break the default IP subnet into

the same-sized subnets. For example, if the default subnet has 12 IP addresses, we can

break it into three equal-sized subnets having 4 IP addresses in each.

VLSM stands for Variable Length Subnet Mask. In it, we break the default IP subnet

into subnets having various sizes. For example, if the default subnet has 12 IP

addresses, we can break it into two subnets where the first subnet has 8 IP addresses

and the second subnet has 4 IP addresses.

Differences between FLSM Subnetting and VLSM Subnetting

The following table lists the differences between FLSM and VLSM.

FLSM (Fixed Length Subnet Masks)

Subnetting

VLSM (Variable Length Subnet Masks)

Subnetting

All subnets are equal in size. Subnets are variable in length.

All subnets have an equal number of hosts. Subnets have a variable number of hosts.

All subnets use the same subnet mask. Subnets use different subnet masks.

It is easy to configure and manage. It is complex in configuration and

administration.

It wastes a lot of IP addresses. It wastes minimum IP addresses.

It is also known as classful subnetting. It is also known as classless subnetting.

It supports both classful and classless

routing protocols.

It supports only classless routing

protocols.

89

1. Fixed Length Subnetting

Fixed length subnetting also called as classful subnetting. Fixed length subnetting

hold the following properties.

• Sizes of all sub networks are same.

• Subnets of all sub networks are same.

• All the sub networks have equal number of hosts.

2. Variable Length Subnetting

Variable length subnetting also called as classless subnetting. Variable length

subnetting hold the following properties.

• Sizes of all sub networks are not same.

• Subnets of all sub networks are not same.

• All the sub networks do not have the equal number of hosts.

What is CIDR?

Classless Inter-Domain Routing (CIDR) is an IP address allocation method that

improves data routing efficiency on the internet. Every machine, server, and end-user

device that connects to the internet has a unique number, called an IP address,

90

associated with it. Devices find and communicate with one another by using these IP

addresses. Organizations use CIDR to allocate IP addresses flexibly and efficiently in

their networks.

What are the different IP address formats?

An IP address has two parts:

• The network address is a series of numerical digits pointing to the network&#39;s unique

identifier

• The host address is a series of numbers indicating the host or individual device

identifier on the network

Until the early 1990s, IP addresses were allocated using the classful addressing

system. The total length of the address was fixed, and the number of bits allocated to

the network and host portions were also fixed.

Classful addresses

An IPv4 address consists of 32 bits. Each string of numbers separated by the period

consists of 8 bits, represented by 0 to 255 in numerical forms. Organizations could

purchase three classes of IPv4 addresses.

Class A

A Class A IPv4 address has 8 network prefix bits. For example, consider 44.0.0.1,

where 44 is the network address and 0.0.1 is the host address.

Class B

A Class B IPv4 address has 16 network prefix bits. For example, consider 128.16.0.2,

where 128.16 is the network address and 0.2 is the host address.

91

Class C

A Class C IPv4 address has 24 network prefix bits. For instance, consider

192.168.1.100, where 192.168.1 is the network address and 100 is the host address.

Classless addresses

Classless or Classless Inter-Domain Routing (CIDR) addresses use variable length

subnet masking (VLSM) to alter the ratio between the network and host address bits in

an IP address. A subnet mask is a set of identifiers that returns the network address’s

value from the IP address by turning the host address into zeroes.

A VLSM sequence allows network administrators to break down an IP address space

into subnets of various sizes. Each subnet can have a flexible host count and a limited

number of IP addresses. A CIDR IP address appends a suffix value stating the number

of network address prefix bits to a normal IP address.

For example, 192.0.2.0/24 is an IPv4 CIDR address where the first 24 bits, or 192.0.2,

is the network address.

What are the limitations of classful IP addressing that CIDR overcomes?

Before Classless Inter-Domain Routing (CIDR), IP addresses were classful and

created inefficiencies. We discuss some of these shortcomings next.

Inflexible IP addressing

In a classful addressing system, each class supported a fixed number of devices:

• Class A supported 16,777,214 hosts

• Class B supported 65,534 hosts

• Class C supported 254 hosts

92

The classful arrangement was inefficient when allocating IP addresses and led to a

waste of IP address spaces.

For example, an organization with 300 devices couldn’t have used a Class C IP

address, which only permitted 254 devices. So, the organization would’ve been forced

to apply for a Class B IP address, which provided 65,534 unique host addresses.

However, only 300 devices would’ve been connected, which would’ve left 65,234

unused IP address spaces.

Limitations in network design

Classful IPs limited your ability to combine networks as required. For example, these

IP addresses belong to different class C networks in the classful architecture:

• 192.168.1.0

• 192.168.0.0

As a network administrator, you couldn’t have combined both networks because the

class C subnet mask was fixed as 255.255.255.0.

What are the benefits of CIDR?

With Classless Inter-Domain Routing (CIDR), your organization has more flexibility

in assigning IP addresses and routing data between devices.

Reduce IP address wastage

CIDR provides flexibility when you determine the network and host identifier

assignments on an IP address. You can use CIDR to provision the required number of

IP addresses for a particular network and reduce wastage. Besides, CIDR reduces

routing table entries and simplifies data packet routing.

Create supernets flexibly

93

A supernet is a group of subnets with similar network prefixes. CIDR allows

flexibility in creating supernets, which isn’t possible in conventional masking

architecture. For example, your organization can combine IP addresses into a single

network block using a notation like this:

• 192.168.1 /23

• 192.168.0 /23

This notation applies a subnet mask of 255.255.254.0 to the IP address, which returns

the first 23 bits as the network address. The router needs only one routing table entry

to manage data packets between devices on the subnets.

How does CIDR work?

Classless Inter-Domain Routing (CIDR) allows network routers to route data packets

to the respective device based on the indicated subnet. Instead of classifying the IP

address based on classes, routers retrieve the network and host address as specified by

the CIDR suffix.

It’s important to understand CIDR blocks and CIDR notation to learn how CIDR

works.

CIDR blocks

A CIDR block is a collection of IP addresses that share the same network prefix and

number of bits. A large block consists of more IP addresses and a small suffix.

The Internet Assigned Numbers Authority (IANA) assigns large CIDR blocks to

regional internet registries (RIR). Then, the RIR assigns smaller blocks to local

internet registries (LIR), which then assign them to organizations. Meanwhile, private

users apply for CIDR blocks from their internet service providers.

94

CIDR notation

CIDR notation represents an IP address and a suffix that indicates network identifier

bits in a specified format. For example, you could express 192.168.1.0 with a 22-bit

network identifier as 192.168.1.0/22.

95

Steps to calculate subnet

96

Question

• You have sub-netted your class C network 192.168.1.0 with a subnet mask of

255.255.255.240. Please list the following:

• Number of Network

• Number of hosts per network

• Full range of the first three networks

• Usable address range from those first three network

Indicative content 2.3:

 Configuration of Basics Network Device.

Device Configuration Modes

Host name

Banner message

Reload Device

Configure port

97

Configure Device passwords

Save configuration

BASIC CONFIGURATIONS OF A SWITCH

Switch&gt;enable

Inter the configuration mode

Switch #configure terminal

Set the switch name to KIGARAMA TSS

Switch(config)#hostname KIGARAMA TSS

SECURING A SWITCH

Set privileged exec mode password

KIGARAMA TSS(config)#enable password ABC

Set secret password

KIGARAMA TSS(config)#enable secret 123

Protect console port

KIGARAMA TSS(config)#line console 0

KIGARAMA TSS(config-line)#password abcd

KIGARAMA TSS(config-line)#login

KIGARAMA TSS(config-line)#exit

Protect vty port

KIGARAMA TSS(config)#line vty 0 4

KIGARAMA TSS(config-line)#password ABC

KIGARAMA TSS(config-line)#login

KIGARAMA TSS(config-line)#exit

98

Set banner message

KIGARAMA TSS(config)#banner motd +

Enter TEXT message. End with the character &#39;+&#39;.

UNAUTHORISED ACCESS IS PROHIBITED!!

+

Exit the configuration mode and enter the privileged exec mode

KIGARAMA TSS(config)#END

KIGARAMA TSS#

Save configurations

KIGARAMA TSS#copy running-config startup-config

KIGARAMA TSS#conf t

Switch(config)#interface vlan 1

Set the IP address, subnet mask, and default gateway for the management interface.

The IP address must be valid for the local network where the switch is installed.

Switch(config-if)#ip address 192.168.1.2 255.255.255.0

Switch(config-if)#exit

Switch(config)#ip default-gateway 192.168.1.1

Switch(config)#end

Save the configuration by using the copy running-configuration startup-configuration

command.

99

Indicative content 2.4:Assigning IP Address Static

How to set a static IP address on Windows 10 and 11

To set a static IP address in Windows 7, 8, and 10:

• Click Start Menu &gt; Control Panel &gt; Network and Sharing Center or

Network and Internet &gt; Network and Sharing Center.

• Click Change adapter settings.

• Right-click on Wi-Fi or Local Area Connection.

• Click Properties.

• Select Internet Protocol Version 4 (TCP/IPv4).

• Click Properties.

• Select Use the following IP address.

• Enter the IP address, Subnet mask, Default gateway, and DNS server.

• Click OK.

Dynamic

100

On Windows 10, you can configure a network adapter to use a static IP address

manually, or you can use an automatically assigned configuration using the local

Dynamic Host Configuration Protocol (DHCP) server.

Although using a  static IP address is recommended  for devices that provide services to

network users, as its configuration never changes, it may come a time when you may

no longer need this configuration, and a dynamically assigned network configuration

will be more suited.

If you use a static IP address and need to switch to a dynamic configuration, it’s

possible to perform this task in several ways, including using the Settings app, Control

Panel, Command Prompt, and even PowerShell.

In this  guide , you’ll learn the steps to remove a static IP address configuration to

obtain a dynamic configuration from the DHCP server on  Windows 10 .

Change to dynamic IP address (DHCP) from Settings

To enable DHCP to obtain a TCP/IP configuration automatically on Windows 10, use

these steps:

• Open Settings on Windows 10.

• Click on Network &amp; Internet.

• Click on Ethernet or Wi-Fi.

• Click the network connection.

• Under the “IP settings” section, click the Edit button.

101

• Use the Edit IP settings drop-down menu and select the Automatic

(DHCP) option.

• Click the Save button.

102

Change to dynamic IP address (DHCP) from Control Panel

To configure a network adapter to use a dynamic IP address using Control Panel, use

these steps:

• Open Control Panel.

• Click on Network and Internet.

• Click on Network and Sharing Center.

• On the left pane, click the “Change adapter settings” option.

• Right-click the network adapter and select the Properties option.

• Select the “Internet Protocol Version 4 (TCP/IPv4)” option.

• Click the Properties button.

103

• Select the “Obtain an IP address automatically” option.

• Select the “Obtain the following DNS server address automatically” option.

104

• Click the OK button.

After completing the steps, the statically assigned TCP/IP configuration will no longer

be available, and the computer will automatically request a dynamic network

configuration from the network.

Automatic

Windows 10

1. Right-click on the Windows icon then select Network Connections.

2. Under Advanced network settings click on Change adapter options.

105

3. Right-click on Wi-Fi then select Properties.

106

If your computer is connected wired to the router, right-click on Ethernet then

select Properties.

4. Select Internet Protocol Version 4 (TCP/IPv4) then click on Properties.

107

5. Select Obtain an IP address automatically then click OK.

108

Indicative content 2.5: Testing network Interconnection

• Physical Testing

• Unit Testing

• Integration Testing

Diagnostic/troubleshooting tools

The Network Diagnostic Tool (NDT) is a client/server program that provides network

configuration and performance testing to a user’s desktop or laptop computer.

a) Ping: What Is Ping?

The ping utility relies on the Internet Control Message Protocol (ICMP) at the internet

layer of TCP/IP. Its most basic use is to confirm network connectivity between two

hosts. Ping sends out an ICMP echo request to which it expects an ICMP echo reply

response.

109

You can perform this test by using either the destination node&#39;s hostname or IP

address:

ping remoteserver07

ping 10.1.1.42

If either of these commands returns ICMP echo reply messages, network connectivity

exists between the two devices. However, when these commands fail, ping can tell us

a lot about what might be wrong.

• This utility(service) is used to provide a basic connectivity test between the

requesting host and a destination host.

• this is done by using the Internet Control Message Protocol (ICMP) which has

the ability to send an echo packet to a destination host and a mechanism to listen

for a response from this host.

• Simply stated, if the requesting host receives a response from the destination

host, this host is reachable.

b) Ipconfig/ifconfig

110

- The utilities that can be used to find out this IP configuration information include the

ipconfig utility on Windows machines and the ifconfig utility on Linux/\*nix based

machines.

Learning outcome 3: Maintain Network system

Indicative content 3.1: Perform preventive maintenance.

• Hardware preventive maintenance

What Is Network Maintenance?

That “network” itself involves your entire portfolio of physical IT assets, like

the hardware and servers, and non-physical IT assets, like the software and cloud

access — also known as your IT ecosystem.

111

The basic of maintaining your network — and the basis of a successful regular

network maintenance plan — typically include the following:

• Schedule regular cleaning

• Setting of preventive measures: involves implementing various security

measures to protect the network and its assets from potential threats and attacks.

Ex. Access control

• Check physical Equipment condition: in networking is crucial to ensure the

reliability and performance of network devices.

• Check environment condition.: involves assessing various factors that can

impact the performance, reliability, and security of a network.

Software preventive maintenance

• Regular change of network device credentials

• Network monitoring software Licencing /Application

• Updating and Upgrading network monitoring software and device Firmware

NB: An update typically refers to a modification or addition to a piece of

software, firmware, or a system to fix bugs, enhance features, or improve

security.

An upgrade involves installing a new version of software, firmware, or a

system that provides significant changes or improvements over the previous

version.

Firmware is a type of software that is embedded in hardware to control and

manage the functionality of the hardware device.

 Indicative content 3.2: Perform corrective maintenance.

Hardware corrective maintenance

112

• Identification of common problem and their causes

• Repair/Replace damaged equipment.

Software corrective maintenance

• Troubleshoot network configuration.

• Check network status

• Update network configuration

 Troubleshooting network

• Introduction to troubleshoot

Troubleshooting is a systematic approach to solving a problem. The goal of

troubleshooting is to determine why something does not work as expected and

explain how to resolve the problem. The first step in the troubleshooting process is

to describe the problem completely.

Basic network troubleshooting

Adapter resources

Verify that the network adapter is installed correctly and detected by the computer

with no conflicts.

If conflicts exist or the network adapter is detected as an &quot;Other device,&quot; the network

card is not installed correctly. Try letting Windows re-detect and install the network

113

card by removing the network adapter and any other conflict devices from Device

Manager and then rebooting the computer. If Windows re-detects the card but does not

find the drivers, download the latest network card drivers from the computer

manufacturer&#39;s website or the network card manufacturer&#39;s website.

Verify connections

Wired network

If this is a wired network, verify the network cable is connected correctly and make

sure the LEDs (light-emitting diode) next to the network jack are properly illuminated.

For example, a desktop computer network card with a solid green LED or light usually

indicates that the card is either connected or receiving a signal. If the green light is

flashing, this is an indication of data is transmitting. The picture shows a LAN (local

area network) port with two LED indicators next to the RJ-45 port. With this port, one

LED lights up if connected properly, and one flashes when transmitting data.

If there are no lights or they&#39;re orange or red, the card may be bad, not connected

properly, or may not be receiving a signal from the network. If you&#39;re on a small

network and can check the hub , switch , or router , verify the cables are connected

correctly, and it has power. If, after checking the connections, the LED indicators

appear bad, the network adapter, port, or cable may be defective.

Wireless network

114

If you&#39;re using a laptop with a wireless network , look for the laptop&#39;s Wi-Fi button and

make sure it is turned on. Many laptops have a Wi-Fi button that allows the wireless

network to be turned on and off. The Wi-Fi button may be above the keyboard, on the

front edge of the laptop, or integrated with an F key . The pictures are examples of a

Wi-Fi button and Wi-Fi indicator on an F key that are enabled.

If the button is turned on, make sure you&#39;re using the correct Wi-Fi hotspot by right-

clicking the Network icon in the Windows Notification Area and clicking &quot;Connect to

a network.&quot; Usually, the network with the strongest connection (the most bars) is your

wireless router.

Finally, when connecting to most wireless networks, you need to enter the proper

SSID (service set identifier) password to connect to the network. If the incorrect

password is entered, you won&#39;t be able to access the network.

Adapter functionality

Verify the network card can ping itself using the ping command . Windows users can

ping the computer from a Windows command line . Unix and Linux users can ping

from the shell .

To ping the card or the localhost, type either of the following commands:

ping 127.0.0.1

or

ping localhost

115

Executing either of the above commands should get replies from the network card. If

you get an error, or the transmission fails, the network card is not connected correctly,

has the incorrect or outdated drivers installed, or is defective.

Make sure the network card is physically installed in the computer correctly by

removing it and re-inserting it again. Check the network card manufacturer&#39;s website

for the latest drivers and install those drivers. If the network card is defective, it needs

to be replaced.

Connect to the router

If your network has a router , make sure the computer is connecting to the router with

the following commands.

Determine the router&#39;s address

Using the ipconfig command (or ifconfig command for Linux), determine the router&#39;s

address by looking at the Gateway address. Below are the steps for Microsoft

Windows users. Linux users can substitute ipconfig for ifconfig.

• Open the Windows command line.

• At the command prompt, type ipconfig and press Enter . Output similar to the

following example should appear.

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : computerhope.com.

IP Address. . . . . . . . . . . . : 192.168.1.103

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Default Gateway . . . . . . . . . : 192.168.1.1

The Default Gateway is the address of your router. Most home routers have a gateway

address that starts with 192.168, like the address shown above. Assuming your

gateway address is 192.168.1.1, attempt to ping the router to see if it can send and

receive information by running the following command.

116

ping 192.168.1.1

If you get replies from the router, the connection between your router and computer is

good, and you can skip to the next step .

If you don&#39;t receive replies from the router, either the router is not set up properly or

there&#39;s a bad connection between the router and computer. Reset your router to make

sure it is not a problem with your router by following the following steps.

• Turn off the power to the computer and leave it off.

• Unplug the power to your router and cable modem or DSL modem .

• Leave the power cables disconnected for 10-15 seconds and then plug in your

modem and then your router again.

• Finally, turn on your computer again and repeat this step to see if you can ping

your router.

If you have a wireless network, and you cannot ping your wireless router using the

above steps, turn the computer off again. Connect the computer directly to the router

using an Ethernet cable. If this does not work, contact the manufacturer of the router

for additional support or replacement.

Firewall

If your computer network utilizes a firewall , make sure all required ports are open,

especially port 80, which is the HTTP (hypertext transfer protocol) port. If possible,

disable the firewall software or disconnect the computer from the firewall to make sure

it is not causing the network problems.

Troubleshoot process

• Collecting Network System information

• Analysing current Network Status

117

• Identification of common problem

• Implementation of solution

 Elaboration of maintenance report

Ways of reporting

a) Oral

An oral report, also known as an oral presentation or spoken report, is a method of

conveying information verbally to an audience. It involves presenting key points,

findings, or details on a particular topic through spoken words rather than written

documents.

b) Used Tools, materials, and Equipment.

c) Written

A written report is a formal document that conveys information, analysis, findings, or

recommendations on a particular subject. Reports are commonly used in various

professional, academic, and business settings to communicate information in a

structured and organized manner.

d) Video documentation

Video documentation&quot; refers to the process of creating visual records in the form of

videos to capture events, activities, procedures, or information.

When creating video documentation, it&#39;s important to consider factors such as video

quality, clarity of audio.

e) Report elements

118

A network maintenance report provides a summary of activities performed to maintain

and manage a computer network. Here are the key elements commonly included in a

network maintenance report:

1. Report Header:

o Date: The date when the network maintenance was conducted.

o Report ID: A unique identifier for tracking and reference purposes.

o Network Information: Details about the network, including its scope, location,

and any relevant specifications.

2. Maintenance Personnel:

o Names and signatures of the individuals or team responsible for performing the

network maintenance.

3. Maintenance Details:

o Description of Work: A summary of the specific maintenance tasks performed on

the network.

o Maintenance Type: Indicate whether it was routine/preventive maintenance or

corrective maintenance.

o Duration: The time taken to complete the maintenance activities.

4. Configuration Changes:

o Details of any changes made to the network configuration.

o Configuration files updated or modified.

5. Software Updates and Patching:

o Information on any software updates, patches, or firmware upgrades applied to

network devices.

o Versions before and after the update.

6. Security Measures:

o Any security-related actions taken during maintenance.

119

o Overview of firewall configurations, intrusion detection/prevention system

updates, etc.

7. Troubleshooting and Issue Resolution:

o Details of any network issues encountered and the steps taken to troubleshoot and

resolve them.

o Any preventive measures implemented to avoid similar issues in the future.

8. Backup and Recovery:

o Information on network data backups performed.

o Details of any disaster recovery tests conducted.

9. Documentation Updates:

o Any changes made to network documentation.

o Updated network diagrams, configurations, and documentation of new devices.

10. Recommendations:

o Suggestions for future network improvements or enhancements.

o Any proposed changes to enhance network performance or security.

11. Photographs and Documentation:

o Visual documentation of the network infrastructure.

o Photographs of equipment, cabling, and any physical changes made.

12. Cost Information:

o Breakdown of costs associated with the network maintenance, including labor,

materials, and any external services.

13. Signatures and Approvals:

o Signatures of maintenance personnel, network administrators, and other relevant

stakeholders.

o Approval signatures indicating that the network maintenance activities were

completed satisfactorily.

f) Status after maintenance

120