RQF LEVEL V

NETWORKING

MODULE CODE: NEWCR501

TEACHER'S GUIDE

IMPLEMENTING CONNECTIONS TO REMOTE SITE

TABLE OF CONTENTS

ACRONYMS

ADSL	Asymmetric Digital Subscriber Line
ATM	Asynchronous Transfer Mode
AVCTP	Audio/video control transport protocol
BNEP	Bluetooth network encapsulation protocol
CO	central office
CPE	Customer Premises Equipment
CSA	Client-Server Architecture
CSU/DSU	*Channel service unit/data service unit*
DCE	Data Communications Equipment
DHCP	Dynamic Host Configuration Protocol
DoD	Department of Defense
DSL	Digital Subscriber Line
DTE	Data Terminal Equipment
EIGRP	Enhanced Interior Gateway Routing Protocol
FCP	Fiber Channel Protocol
FDDI	Fiber Distributed Data Interface
FTTH	Fiber to the home
FTTP	Fiber To The Premises
HCSA	Hybrid Client-Server Architecture
HDLC	High-level Data Link Control
HIPPI	High Performance Parallel Interface
IETF	Internet Engineering Task Force
IPI	Intelligent Peripheral Interface
IPsec	Internet Protocol Security
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
L2CAP	Logical link control and adaptation protocol
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LAPB	Link Access Procedure, Balanced
MAC	*Media Access Control*
NAT	Network Address Translation
NOS	Network Operating System
NTD	Network Termination Device
OSI	*Open System Interconnection*
OSPF	Open Shortest Path First
P2P	Peer-to-peer
POP	*point of presence*
PPP	Point-to-Point Protocol
PPPOE	Point to Point Protocol Over Ethernet

PPTP	Point – to – Point Tunneling Protocol
PSTN	Public switched telephone network
RFCOMM	Radio frequency communication
RIP	Routing Information Protocol
SCP	secure copy protocols
SCSI	Small Computer System Interface
SDA	Shared Disk Architecture
SDLC	software development life cycle
SDP	Service discovery protocol
SFTP	SSH file transfer
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP/IP	Transport Control Protocol with Internet Protocol
TCS	Telephony control protocol
TLS	Transport Layer Security
TVET	Technical Vocational Education and Training
VPN	Virtual Private Network
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity

INTRODUCTION

This module is intended to the learner pursuing TVET certificate III in networking, at the end of this module the learner will be able to Plan and Design Remote connectivity, Install, Configure and Troubleshoot WAN and Document the work done, he or she will be able to work.

Learning units describe the essential outcomes of a competence

Performance criteria describe the required performance needed to demonstrate achievement of the learning unit.

By the end of the module, the trainee will be able to:

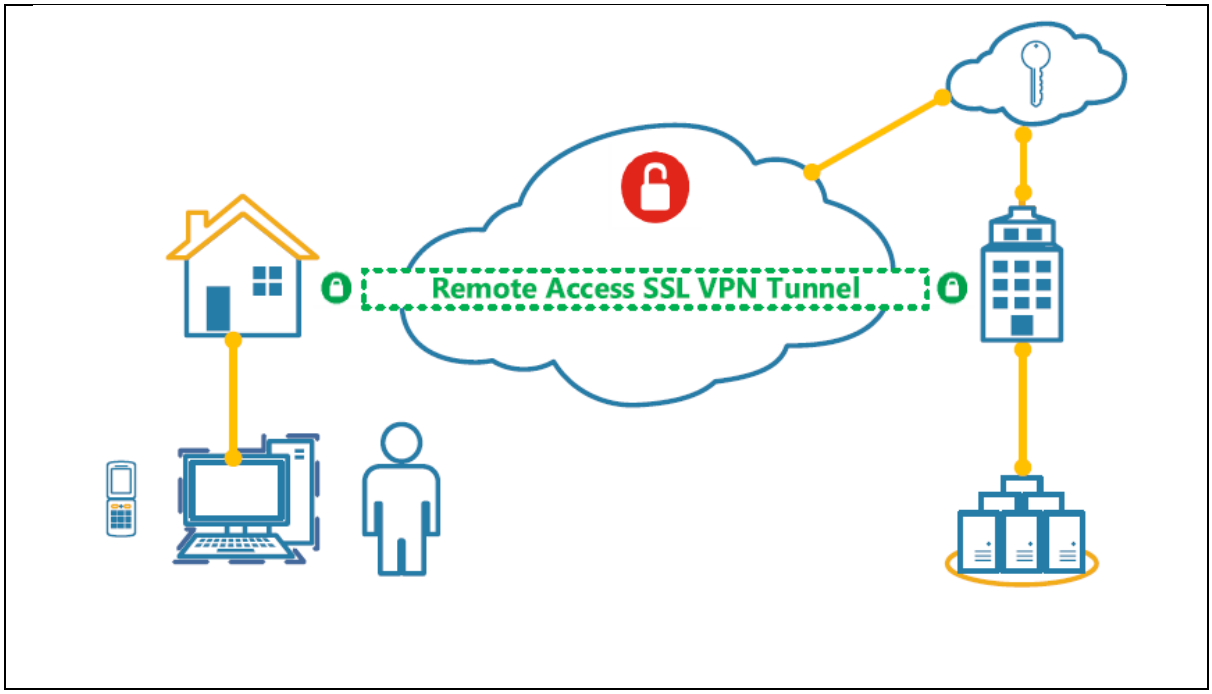
- Plan and Design Remote Connectivity.
- Install, Configure and Troubleshoot WAN
- Document of the work done

NEWCR501 – Implementing Connections to Remote site

Learning Units:

1. Plan and Design Remote connectivity
2. Install, Configure and Troubleshoot WAN and VPN
3. Document of the Work Done

LEARNING UNIT 1: PLAN AND DESIGN REMOTE CONNECTIVITY



STRUCTURE OF LEARNING UNIT

Learning outcomes:

1.1. Analyze network requirements

1.2. Analyze Enterprise facilities, existing WIFI &WIRED networks and sites

1.3. Identify security requirements

1.4. Select WAN technology, hardware and software components

1.5. Identify tools, equipment and materials used in Remote connection

1.6. Design and interpret network blueprint.

Learning outcome 1.1 Analyze network requirements

Duration: 5hrs

Learning outcome 1.1 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Identify correctly network architecture.
2. Describe correctly network applications.
3. Describe Correctly network protocols.

Resources

Equipment	Tools	Materials
Computer	Handout notes	Internet Bundles
Projector	Simulator	Video aid
Black/White board	Books	Chalks
		Marker Pens

Advance preparation:

- Sample videos of analyzing network requirements.

Indicative content 1.1.1: Network architectures

Network architecture is the design of a **computer network.** It is a framework for the specification of a network's physical components and their functional organization and configuration, its operational principles and procedures, as well as **communication protocols** used.

In **telecommunication**, the specification of a network architecture may also include a detailed description of products and services delivered via a communications network, as well as detailed rate and billing structures under which services are compensated.

The network architecture of the **Internet** is predominantly expressed by its use of the **Internet Protocol Suite**, rather than a specific model for interconnecting networks or nodes in the network, or the usage of specific types of hardware links.

- **Client-server**

In Client-server architecture, architecture of a computer network in which many clients (remote processors) request and receive service from a centralized **server** (host computer). **Client** computers provide an interface to allow a computer user to request services of the **server** and to display the results the **server** returns.

The **client-server model** describes how a **server** provides resources and services to one or more clients. **Examples** of servers include web servers, mail servers, and file servers. Each of these servers provide resources to **client** devices, such as desktop computers, laptops, tablets, and smart phones

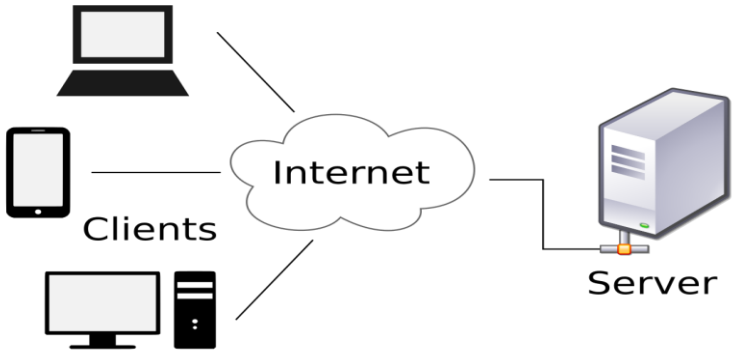


Figure 1 - Client-server network architecture

Advantages of Client/Server network:

- A Client/Server network contains the centralized system. Therefore, we can back up the data easily.
- A Client/Server network has a dedicated server that improves the overall performance of the whole system.
- Security is better in Client/Server network as a single server administers the shared resources.
- It also increases the speed of the sharing resources.

Disadvantages of Client/Server network:

- Client/Server network is expensive as it requires the server with large memory.
- A server has a Network Operating System (NOS) to provide the resources to the clients, but the cost of NOS is very high.
- It requires a dedicated network administrator to manage all the resources.

- **Peer-to-peer (P2P)**

In a **P2P network**, the "**peers**" are computer systems which are connected to each other via the Internet. Files can be shared directly between systems on the **network** without the need

of a central server. In other words, each computer on a **P2P network** becomes a file server as well as a client.

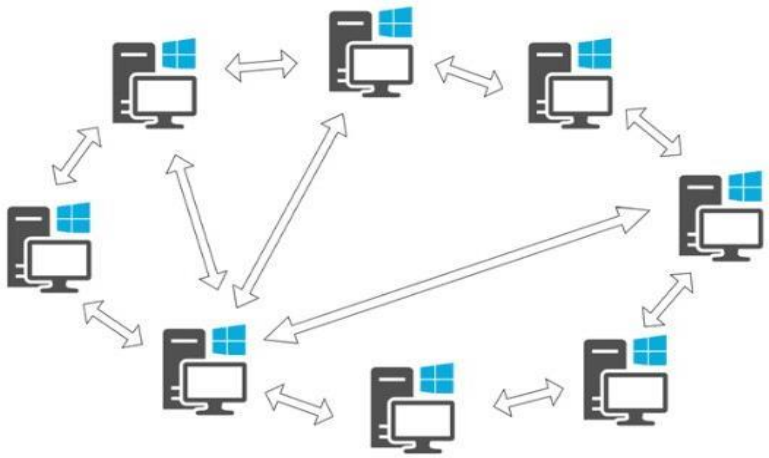


Figure 2 - Peer to peer network architecture

Advantages of Peer-To-Peer Network:

- It is easy to install and so is the configuration of computers on this network,
- All the resources and contents are shared by all the peers, unlike server-client architecture where Server shares all the contents and resources.
- P2P is more reliable as central dependency is eliminated. Failure of one peer doesn't affect the functioning of other peers. In case of Client –Server network, if server goes down whole network gets affected.
- There is no need for full-time System Administrator. Every user is the administrator of his machine. User can control their shared resources.
- The over-all cost of building and maintaining this type of network is comparatively very less.

Disadvantages of Peer-To-Peer Network:

- In this network, the whole system is decentralized thus it is difficult to administer. That is one person cannot determine the whole accessibility setting of whole network.
- Security in this system is very less viruses, spywares, Trojans; etc malwares can easily transmit over this P-2-P architecture.
- Data recovery or backup is very difficult. Each computer should have its own backup system
- Lot of movies, music and other copyrighted files are transferred using this type of file transfer. P2P is the technology used in torrents.

- **Hybrid of client-server and P2P**

The HCSA (Hybrid Client-Server Architecture), a flexible system layout that combines the advantages of the traditional Client-Server Architecture (CSA) with those of the Shared Disk Architecture (SDA), is introduced. In HCSA, the traditional CSA-style I/O subsystem is modified to give the clients network access to both the server and the server's set of disks.

A hybrid P2P network is one that has an index server containing information on the locations of resources at the center, and which uses the index server for search.

Theoretical learning Activity

In group of 2-3 members, discuss on the following task:

- ✓ Identify three types of network architectures
- ✓ Identify the advantages and disadvantages of each type of network architectures.

Points to Remember (Take home message)

Network architectures: • Client-server • Peer-to-peer (P2P) • Hybrid of client-server and P2P

Indicative content 1.1.2: Network Applications

Network application is application running on one host and provides a communication to another application running on a different host.

Examples of network applications:

- **E-mail**

Short for **Electronic mail**, it is a method of exchanging messages between people using electronic devices. Invented by Ray Tomlinson, email first entered limited use in the 1960s and by the mid-1970s had taken the form now recognized as email. Email operates across computer networks, which today is primarily the Internet

- **Web**

The World Wide Web, commonly known as the Web, is an information system where documents and other web resources are identified by Uniform Resource Locators, which may be interlinked by hypertext, and are accessible over the Internet

- **Instant messaging**

Instant messaging technology is a type of online chat that offers real-time text transmission over the Internet. A LAN messenger operates in a similar way over a local area network. Short messages are typically transmitted between two parties, when each user chooses to complete a thought and select "send".

- **Remote login**

Rlogin (**remote login**) is a UNIX command that allows an authorized user to **login** to other UNIX machines (hosts) on a network and to interact as if the user were physically at the host computer. Rlogin is similar to the better known Telnet command.

- **P2P file sharing**

Peer-to-peer file sharing is the distribution and sharing of digital media using peer-to-peer networking technology. P2P file sharing allows users to access data by using the following file sharing application softwares Xunlei, Bittorrent, uTorrent, BitComet, Vuze and Transmission, Azureus, Emule and eDonkey, Gnutella, LimeWire and Cabos, Flashget, Foxy, Goboogy, Google Talk (file-transfer), Manolito, Msn (file-transfer), Mute, Neonet, Openft, Pando, Peerenabler, Perfect-dark, Poco, Soribada, Yahoo-IM (file-transfer), etc.

- **Multi-user network games**

Multi user games are **games** where you play online with other online gamers. For example, you can play your component online; you can be playing an opponent which is sitting on the other side of the earth.

The future of **multi**-**user** networked **games** lies among others in **networking** mobile **games**.

Currently there exists a **multi**-player mobile **network** real time **game** called "**Multi**-**User** Dungeon", which is a text-based MUD story. This is a popular **game** used by over 50.000 **users**.

- **Streaming stored video clips**

Streaming video is content sent in compressed form over the Internet and displayed by the viewer in real time. With **streaming video** or **streaming** media, a Web user does not have to wait to download a file to play it.

Streaming of videos involve, storing of pre-recorded videos on servers.

- Users send request to those servers.
- Users may watch the video from the start till the end, and may pause it anytime, do a forward or reverse skip, or stop the video whenever they want to do so.

- **Internet telephone**

Internet telephony is a type of communications technology that allows voice calls and other **telephony** services like fax, SMS and other voice-messaging applications to be transmitted using the **Internet** as a connection medium. **Internet telephony** is also called IP **telephony** or broadband **telephony**.

While a traditional **phone service** uses outdated telephone **lines**, **Internet phone** uses the **Internet** to connect your **phone** calls to the public **phone** network. **Internet phone** services utilize a technology called "packet switching". First, your **Internet phone** has to convert your voice into data packets with the ATA adapter.

- **Real-time video conference**

Video conferencing is a visual communication session between two or more users regardless of their location, featuring audio and **video** content transmission in **real time**.

Examples of applications used in video conferencing: Zoom, Google Hangouts, Google Meet, GoToMeeting, Skype for Business, Cisco WebEx, etc

- **Massive parallel computing**

In computing, massively parallel refers to the use of a large number of processors to perform a set of coordinated computations in parallel.

Theoretical learning Activity

In group of 2-3 members, discuss on the following task:

a. Define the term network applications.
b. Describe the following network applications:
    1. E-mail
    2. Web
    3. Instant messaging
    4. Remote login
    5. P2P file sharing
    6. Multi-user network games
    7. Streaming stored video clips
    8. Internet telephone
    9. Real-time video conference
    10. Massive parallel computing

Points to Remember (Take home message)

List of Network Applications:

- E-mail
- Web
- Instant messaging
- Remote login
- P2P file sharing
- Multi-user network games
- Streaming stored video clips
- Internet telephone
- Real-time video conference
- Massive parallel computing

Indicative content 1.1.3: Network Protocols

1. **Bluetooth protocol**

Bluetooth is a standardized **protocol** for sending and receiving data via a 2.4GHz wireless link. It's a secure **protocol**, and it's perfect for short-range, low-power, low-cost, wireless transmissions between electronic devices. Some Bluetooth protocols are Logical link control and adaptation **protocol** (L2CAP), **Bluetooth** network encapsulation **protocol** (BNEP), Radio frequency communication (RFCOMM), Service discovery **protocol** (SDP), Telephony control **protocol** (TCS), Audio/video control transport **protocol** (AVCTP)

2. **Fiber Channel network protocols**

Fiber **Channel Protocol** (FCP) is the SCSI interface **protocol** utilizing an underlying Fiber **Channel** connection.

The Fiber **Channel** standards define a high-speed data transfer mechanism that can be used to connect workstations, mainframes, supercomputers, storage devices and displays.

Fiber **Channel** is designed to transport many **protocols**, such as FDDI, serial HIPPI, SCSI, IPI, and many more that will be listed in the section describing the **FC**-4 layer. The transfer rates **of Fiber Channel** are currently (133 Mbps,266 Mbps,530 Mbps, and 1 Gbps).

- **Fiber Distributed Data Interface,** a set of ANSI protocols for sending digital data over fiber optic cable. **FDDI** networks are token-passing networks, and support data rates of up to 100 Mbps (100 million bits) per second. **FDDI** networks are typically **used** as backbones for wide-area networks.
- **HIPPI**, short for **High Performance Parallel Interface**, is a **computer bus** for the attachment of high speed storage devices to **supercomputers**, in a **point-to-point link**. It was popular in the late 1980s and into the mid-to-late 1990s, but has since been replaced by ever-faster standard interfaces like **Fiber Channel** and **10 Gigabit Ethernet**.
- **SCSI** Small Computer System Interface is a set of standards for physically connecting and transferring data between computers and peripheral devices. The **SCSI** standards define commands, **protocols**, and electrical, optical and logical interfaces.
- **IPI** (Intelligent Peripheral Interface) is a high-bandwidth interface between a computer and a hard disk or a tape device. Devices using **IPI** can transfer data between the hard drive and RAM in the range between 3 and 25 megabytes per second.

3. **Internet Protocol Suite or TCP/IP model**

The **Internet protocol suite** is the **conceptual model** and set of **communications protocols** used in the **Internet** and similar **computer networks**. It is commonly known as **TCP/IP** because the foundational protocols in the suite are the **Transmission Control Protocol** (TCP) and the **Internet Protocol** (IP). It is occasionally known as the **Department of defense** (**DoD**) **model**

because the development of the networking method was funded by the **United States Department of defense** through **DARPA**.

The Internet protocol suite provides **end-to-end data communication** specifying how data should be packetized, addressed, transmitted, **routed,** and received. This functionality is organized into four **abstraction layers**, which classify all related protocols according to the scope of networking involved. From lowest to highest, the layers are the **link layer,** containing communication methods for data that remains within a single network segment (link); the **internet layer,** providing **internetworking** between independent networks; the **transport layer,** handling host-to-host communication; and the **application layer,** providing process-to-process data exchange for applications.

The **technical standards** underlying the Internet protocol suite and its constituent protocols are maintained by the **Internet Engineering Task Force** (IETF). The Internet protocol suite predates the **OSI model,** a more comprehensive reference framework for general networking systems.

4. OSI protocols

There are a total of seven layers. Data and information are received by each layer from an upper layer.

1. Layer 1, the Physical Layer: This layer deals with the hardware of networks such as cabling. The major protocols used by this layer include Bluetooth, PON, OTN, DSL, IEEE.802.11, IEEE.802.3, L431 and TIA 449.
2. Layer 2, the Data Link Layer: This layer receives data from the physical layer and compiles it into a transform form called framing or frame. The protocols are used by the Data Link Layer include: ARP, CSLIP, HDLC, IEEE.802.3, PPP, X-25, SLIP, ATM, SDLS and PLIP.
3. Layer 3, the Network Layer: This is the most important layer of the OSI model, which performs real time processing and transfers data from nodes to nodes. Routers and switches are the devices used for this layer. The network layer assists the following protocols: Internet Protocol (IPv4), Internet Protocol (IPv6), IPX, AppleTalk, ICMP, IPSec and IGMP.
4. Layer 4, the Transport Layer: The transport layer works on two determined communication modes: Connection oriented and connectionless. This layer transmits data from source to destination node. It uses the most important protocols of OSI protocol family, which are: Transmission Control Protocol (TCP), UDP, SPX, DCCP and SCTP.
5. Layer 5, the Session Layer: The session layer creates a session between the source and the destination nodes and terminates sessions on completion of the communication process. The protocols used are: PPTP, SAP, L2TP and NetBIOS.
6. Layer 6, the Presentation Layer: The functions of encryption and decryption are defined on this layer. It converts data formats into a format readable by the

application layer. The following are the presentation layer protocols: XDR, TLS, SSL and MIME.

7. Layer 7, the Application Layer: This layer works at the user end to interact with user applications. Q oS (quality of service), file transfer and email are the major popular services of the application layer. This layer uses following protocols: HTTP, SMTP, DHCP, FTP, Telnet, SNMP and SMPP.

5. Routing protocols

A **routing protocol** specifies how **routers** communicate with each other, distributing information that enables them to select routes between any two **nodes** on a **computer network.** Routers perform the "traffic directing" functions on the Internet; **data packets** are forwarded through the networks of the internet from router to router until they reach their destination computer

Examples of **Routing Protocols** are RIP (**Routing** Information **Protocol**), EIGRP (Enhanced Interior Gateway **Routing Protocol**) and OSPF (Open Shortest Path First).

6. VPN protocols

VPN is a Virtual Private Network that allows a user to connect to a private network over the Internet securely and privately. VPN creates an encrypted connection, known as VPN tunnel, and all Internet traffic and communication is passed through this secure tunnel. Thus, keeping the user data secure and private.

Two basic types VPN

a. Remote Access VPN

Remote access VPN allows a user to connect to a private network and access its services and resources remotely. The connection between the user and the private network happens through the Internet and the connection is secure and private.

Remote Access VPN is useful for business users as well as home users.

A corporate employee, while traveling, uses a VPN to connect to his/her company's private network and remotely access files and resources on the private network.

Home users, or private users of VPN, primarily use VPN services to bypass regional restrictions on the Internet and access blocked websites. Users conscious of Internet security also use VPN services to enhance their Internet security and privacy.

b. Site – to – Site VPN

A Site-to-Site VPN is also called as Router-to-Router VPN and is mostly used in the corporates. Companies, with offices in different geographical locations, use Site-to-site VPN to connect the network of one office location to the network at another office location.

When multiple offices of the same company are connected using Site-to-Site VPN type, it is called as Intranet based VPN. When companies use Site-to-site VPN type to connect to the office of another company, it is called as Extranet based VPN. Basically, Site-to-site VPN create

a virtual bridge between the networks at geographically distant offices and connect them through the Internet and maintain a secure and private communication between the networks.

Since Site-to-site VPN is based on Router-to-Router communication, in this VPN type one router acts as a VPN Client and another router as a VPN Server. The communication between the two routers starts only after an authentication is validated between the two.

Types of VPN protocols

a. Internet Protocol Security or IPsec:

Internet Protocol Security or IPsec is used to secure Internet communication across an IP network. IPsec secures Internet Protocol communication by authenticating the session and encrypts each data packet during the connection.

IPsec operates in two modes, Transport mode and Tunneling mode, to protect data transfer between two different networks. The transport mode encrypts the message in the data packet and the tunneling mode encrypts the entire data packet. IPsec can also be used with other security protocols to enhance the security system.

b. Layer 2 Tunneling Protocol (L2TP):

L2TP or Layer 2 Tunneling Protocol is a tunneling protocol that is usually combined with another VPN security protocol like IPsec to create a highly secure VPN connection. L2TP creates a tunnel between two L2TP connection points and IPsec protocol encrypts the data and handles secure communication between the tunnel.

c. Point – to – Point Tunneling Protocol (PPTP):

PPTP or Point-to-Point Tunneling Protocol creates a tunnel and encapsulates the data packet. It uses a Point-to-Point Protocol (PPP) to encrypt the data between the connection. PPTP is one of the most widely used VPN protocol and has been in use since the time of Windows 95. Apart from Windows, PPTP is also supported on Mac and Linux.

d. Secure Sockets Layer (SSL) and Transport Layer Security (TLS):

SSL (Secure Sockets Layer) and TLS (Transport Layer Security) create a VPN connection where the web browser acts as the client and user access is restricted to specific applications instead of entire network. SSL and TLS protocol is most commonly used by online shopping websites and service providers. Web browsers switch to SSL with ease and with almost no action required from the user, since web browsers come integrated with SSL and TLS. SSL connections have https in the beginning of the URL instead of http.

e. OpenVPN:

OpenVPN is an open source VPN that is useful for creating Point-to-Point and Site-to-Site connections. It uses a custom security protocol based on SSL and TLS protocol.

f. Secure Shell (SSH):

Secure Shell or SSH creates the VPN tunnel through which the data transfer happens and also ensures that the tunnel is encrypted. SSH connections are created by a SSH client and data is transferred from a local port on to the remote server through the encrypted tunnel.

7. ADSL technologies

Asymmetric Digital Subscriber Line (ADSL) is a type of **DSL broadband** communications technology used for connecting to the Internet. ADSL allows more data to be sent over existing copper telephone lines **(POTS),** when compared to traditional modem lines. A special filter, called a **micro filter,** is installed on a subscriber's telephone line to allow both ADSL and regular voice (telephone) services to be used at the same time.

ADSL requires a special ADSL modem and subscribers must be in close geographical locations to the provider's central office to receive ADSL service. Typically, this distance is within a radius of 2 to 2.5 miles. ADSL supports data rates of from 1.5 to 9 Mbps when receiving data (known as the **downstream** rate) and from 16 to 640 Kbps when sending data (known as the **upstream** rate).

Theoretical learning Activity

In group of 2-3 members, discuss on the following task:

a. Define the term network protocols.
b. Describe the following network Protocols:
   - Bluetooth protocol
   - Fiber Channel network protocols
   - Internet Protocol Suite or TCP/IP model
   - OSI protocols
   - Routing protocols
   - VPN protocols
   - ADSL technologies

Points to Remember (Take home message)

List of Network Protocols:

- Bluetooth protocol
- Fiber Channel network protocols
- Internet Protocol Suite or TCP/IP model
- OSI protocols
- Routing protocols
- VPN protocols
- ADSL technologies

Learning outcome 1.1 formative assessment

Written assessment

I. Answer the following questions by **True** or **False**

1. Client/Server doesn't require a dedicated network administrator to manage all the resources. ……
2. client-server model describes how a server provides resources and services to one or more clients. …….
3. In Client/Server, the files can be shared directly between systems on the network without the need of a central server. ……
4. Network architecture is the design of a computer network. …….
5. Remote access VPN allows a user to connect to a public network and access its services and resources remotely. …….
6. Security is better in Client/Server network as a single server administers the shared resources. …….
7. The hybrid network is the combination of client-server and peer to peer network. …….
8. The network architecture of the Internet is a specific model for interconnecting networks or nodes in the network rather than expressing its use of the Internet Protocol Suite. …….
9. There is no need for full-time System Administrator in peer to peer Network. …….

II. Match the following Network Protocols in **Column B** with their corresponding meaning in **Column A,** and write the answers in Column of **Answer.**

Answer	**Column A**	**Column B**
1. …..	1. It is similar to Telnet.	**A.** E-mail
2. …..	2. It is an information system where documents are identified by Uniform Resource Locators.	**B.** Instant messaging
3. …..	3. it is a method of exchanging messages between people using electronic devices.	**C.** Internet telephone
4. …..	4. It is a type of online chat that offers real-time text transmission over the Internet.	**D.** Massive parallel computing
5. …..	5. It allows users to access data by using the application like Bit torrent.	
6. …..		
7. …..		
8. …..		
9. …..		
10. …..		

	6. The content sent in compressed form over the Internet and displayed by the viewer in real time 7. These are the games where you play online with other online gamers. 8. It is a type of communications technology that allows voice calls 9. It is a visual communication session between two or more users regardless of their location, featuring audio and video content transmission in real time. 10. It refers to the use of a large number of processors to perform a set of coordinated computations in parallel.	**E.** Multi-user network games **F.** P2P file sharing **G.** Real-time video conference **H.** Remote login **I.** Streaming stored video clips **J.** Web **K.** Bluetooth

III. **Provide short answers to the following questions**

1. Enlarge the following terms:
    a. FDDI
    b. BNEP
    c. AVCTP
    d. HIPPI
2. List down three (3) protocols that operate at layer 4 of OSI Model
3. Enumerate three (3) routing protocols in full word.

ANSWERS

I. Answer the following questions by **True** or **False**

1. False **2. True** **3. False** **4. True** **5. False** **6. True**
7. True 8. **False** **9. True**

II. Matching questions

1. H 2.J 3.A 4.B 5.F 6.I 7.E 8.C 9.G 10.D

III. Short answer questions:

1. Enlarge the following terms:
    a. **FDDI:** Fiber Distributed Data Interface
    b. BNEP: Bluetooth network encapsulation protocol
    c. AVCTP: Audio/video control transport protocol
    d. HIPPI: High Performance Parallel Interface.
2. Three (3) protocols that operate at layer 4 of OSI Model
   Answer: TCP, UDP, SPX, DCCP and SCTP.
3. Three (3) routing protocols in full word.
    - Routing Information Protocol
    - Enhanced Interior Gateway Routing Protocol
    - Open Shortest Path First

Learning outcome 1.2 Analyze Enterprise facilities, existing Wi-Fi & Wired network and sites

Duration: 2hrs

Learning outcome 1.2 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Define the term network analysis correctly.
2. Analyze effectively enterprise facility and existing networks

Resources

Equipment	Tools	Materials
Computer	Handout notes	Internet Bundles
Projector	Simulator	Video aid
Black/White board	Books	Chalks
		Marker Pens

Advance preparation:

- Sample videos representing different enterprise network.

Indicative content 1.2.1: Enterprise facility and Existing networks analysis

Network Analysis

A **network** is a collection of two or more computers connected together for sharing information and resources such as printer. **Network analysis** involves the analysis of physical equipment and logical configuration of network that are operating currently and predicting the network usage for future due to the current.

- **Physical Design**

Because **physical network** diagrams depict the entire topology of the **physical network**, they can include a number of different components: Connections: connections are critical to a **physical network** diagram. Connectors (aka connections) depict the **physical** cabling that connects **physical** devices in a **network**.

- **Logical Design**

A **logical network** is one that appears to the user as a single, separate entity although it might in fact be either an entity created from multiple **networks** or just a part of a larger **network**. A **logical network** is defined by its IP addressing scheme.

- **Wired network technologies**

A **wired network** is a common type of **wired** configuration. Most **wired networks** use **Ethernet** cables to transfer data between connected PCs. In a small **wired network**, a single router may be used to connect all the computers. Larger **networks** often involve multiple routers or switches that connect to each other.

- **Wireless network technologies**

Wireless networks are computer **networks** that are not connected by cables of any kind. The use of a **wireless network** enables enterprises to avoid the costly process of introducing cables into buildings or as a connection between different equipment locations.

Other **examples** of applications of radio **wireless technology** include GPS units, garage door openers, **wireless** computer mouse, keyboards and headsets, headphones, radio receivers, satellite television, broadcast television and cordless telephones.

- **Networks devices**

Networking hardware, also known as network equipment or computer networking devices, are electronic devices which are required for communication and interaction between devices on a computer network. Specifically, they mediate data transmission in a computer network.

Examples are Hub, Switch, Router, Bridge, Gateway, Modem, Repeater, Access Point.

- **Networks nodes**

In a communications **network**, a **network node** is a connection point that can receive, create, store or send data along distributed **network** routes.

Theoretical learning Activity

In group of 2-3 members, discuss on the following task:

a. Define the term network analysis.
b. Identify the elements to consider while analyzing network.

Points to Remember (Take home message)

Network analysis is the process of finding the voltages across, and the currents through, all **network** components.

Learning outcome 1.2 formative assessment

Written assessment

Answer the following statements by **True** if the statement is correct, or **False** if the statement is incorrect.

a. A logical network is defined by its IP addressing scheme. ……
b. a network device is a connection point that can receive, create, store or send data along distributed network routes. ……
c. computer networking devices are electronic devices which are required for communication and interaction between devices on a computer network. ……
d. Most wired networks use Fibre optic cables to transfer data between connected PCs. ……
e. Network analysis involves the analysis of physical equipment and logical configuration of network that are operating currently and predicting the network usage for future due to the current. ……
f. physical network diagrams depict small part of the physical network topology. ……
g. Wireless networks are computer networks that are not connected by cables of any kind. ……

Answers: a. True, b. False, c. True, d. False, e. True, f. False, g. True

Learning outcome 1.3. Identify Security Requirements

Duration: 3hrs

Learning outcome 1.3 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Identify the requirements for secure remote access

Resources

Equipment	Tools	Materials
Computer Projector Black/White board	Handout notes Simulator Books	Internet Bundles Video aid Chalks Marker Pens

Advance preparation:

- Sample videos for Secured remote access

Indicative content 1.3.1: Requirements for secure remote access

The requirements for secure remote access are the followings:

- Give users easy access to business resources from any location or device
- Find a solution to minimize your cost of ownership
- Find a solution offering comprehensive and extensible endpoint analysis checks
- Find a vendor that can provide an integrated application delivery infrastructure
- Find a solution that supports granular authorization policies and true application-level control
- Find a solution that overcomes the limitations of network access control
- Find a vendor with a staying power, a global reach and a strong vision

Theoretical learning Activity

In group of 2-3 members, discuss on the following task:

- Identify the requirements for secure remote access.

Points to Remember (Take home message)

The requirements for secure remote access:

- Give users easy access to business resources from any location or device
- Find a solution to minimize your cost of ownership
- Find a solution offering comprehensive and extensible endpoint analysis checks
- Find a vendor that can provide an integrated application delivery infrastructure
- Find a solution that supports granular authorization policies and true application-level control
- Find a solution that overcomes the limitations of network access control
- Find a vendor with a staying power, a global reach and a strong vision

Learning outcome 1.3 formative assessment

Written assessment

Complete the following sentence by **YES** is it is a requirement for secure remote access, otherwise **NO**

a. Give users easy access to business resources from any location or device …….
b. Find a solution to Maximize your cost of ownership. …….
c. Find a solution offering comprehensive and extensible endpoint analysis checks …….
d. Find a vendor that can provide an integrated application delivery infrastructure …….
e. Find a solution that supports granular authorization policies and true application-level control …….
f. Find a solution that causes the limitations of network access control …….
g. Find a vendor with a staying power, a global reach and a strong vision…….

ANSWERS

a. YES b. NO c. YES d. YES e. YES f. NO g. YES

Learning outcome 1.4. Select WAN technology, hardware and software components

Duration: 3hrs

Learning outcome 1.4 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Identify correctly WAN technologies
2. Identify correctly communication devices
3. Differentiate correctly extranet from intranet.
4. Identify correctly tools for communications

Resources

Equipment	Tools	Materials
Computer Projector Black/White board	Handout notes Simulator Books	Internet Bundles Video aid Chalks Marker Pens

Advance preparation:

- Sample videos representing WAN Technologies, hardware and components.

Indicative content 1.4.1: Network technology.

✓ **Network Technologies**

ISPs can use are several WAN access connection options to connect the local loop to the enterprise edge. These WAN access options differ in technology, speed, and cost. Each has distinct advantages and disadvantages. Familiarity with these technologies is an important part of network design.

As shown in Figure below, an enterprise can get WAN access in two ways.

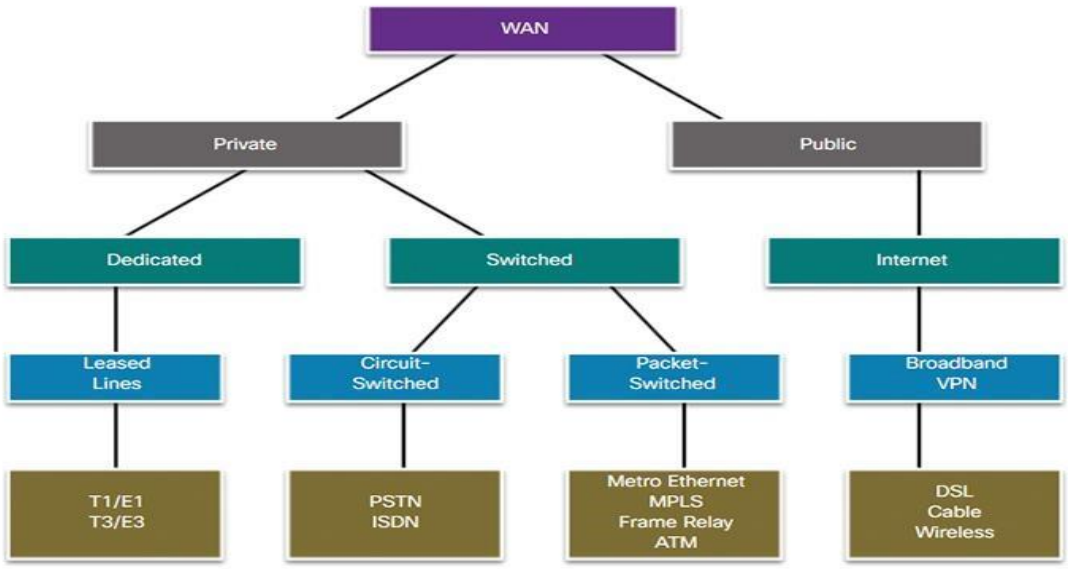


Figure 3 - WAN Access Options

Private WAN technologies: Service providers may offer dedicated point-to-point leased lines, Dialup, circuit-switched links, such as **Public switched telephone network (**PSTN) or Integrated Services Digital Network (ISDN), and packet-switched links, such as Ethernet WAN, Asynchronous Transfer Mode (ATM), or Frame Relay.

Public WAN technologies: Service providers provide Internet access using broadband services such as Digital Subscriber Line (DSL), cable, and satellite access. ***Broadband connections*** are typically used to connect small offices and telecommuting employees to a corporate site over the Internet. Data traveling between corporate sites over the public WAN infrastructure should be protected using VPNs.

Frame Relay systems are commonly being replaced by Ethernet WANs.

✓ **Communication Devices**

The following list is not exhaustive, and other devices may be required, depending on the WAN access technology chosen.

- ***Dialup modem*:** Voice band modems are considered to be a legacy WAN technology. A voice band modem *modulates* (that is, converts) the digital signals produced by a computer into voice frequencies. These frequencies are then transmitted over the analog lines of the public telephone network. On the other side of the connection, another modem *demodulates* the sounds back into a digital signal for input to a computer or network connection.
- ***Access server***: This server controls and coordinates dialup modem, dial-in, and dial out user communications. Considered to be a legacy technology, an access server may have a mixture of analog and digital interfaces and support hundreds of simultaneous users.
- ***Broadband modem***: This type of digital modem is used with high-speed DSL or cable Internet service. Both operate in a similar manner to the voice band modem but use higher broadband frequencies to achieve higher transmission speeds.
- ***Channel service unit/data service unit (CSU/DSU)***: Digital leased lines require a CSU and a DSU. A CSU/DSU can be a separate device like a modem, or it can be an interface on a router. The CSU provides termination for the digital signal and ensures connection integrity through error correction and line monitoring. The DSU converts the line frames into frames that the LAN can interpret and vice versa.
- ***WAN switch***: This multiport internetworking device is used in service provider networks. These devices typically switch traffic, such as Frame Relay or ATM, and operate at Layer 2.
- ***Router:*** This device provides internetworking and WAN access interface ports that are used to connect to the service provider network. These interfaces may be serial connections, Ethernet, or other WAN interfaces. With some types of WAN interfaces, an external device, such as a DSU/CSU or modem (analog, cable, or DSL), is required to connect the router to the local service provider.

Core router/Multilayer switch: This router or multilayer switch resides within the middle or backbone of the WAN, rather than at its periphery. To fulfill this role, a router or multilayer switch must be able to support multiple telecommunications interfaces of the highest speed used in the WAN core. It must also be able to forward IP packets at full speed on all of those interfaces. The router or multilayer switch must also support the routing protocols being used in the core.

- ✓ **Intranet and Extranet**

VPNs maintain the same security and management policies as a private network. They are the most cost effective method of establishing a virtual point-to-point connection between remote users and an enterprise customer's network.

There are three main types of VPNs.

- **Access VPNs**—Provide remote access to an enterprise customer's intranet or extranet over a shared infrastructure. Access VPNs use analog, dial, ISDN, digital subscriber line (DSL), mobile IP, and cable technologies to securely connect mobile users, telecommuters, and branch offices.
- **Intranet VPNs**—Link enterprise customer headquarters, remote offices, and branch offices to an internal network over a shared infrastructure using dedicated connections. Intranet VPNs differ from extranet VPNs in that they allow access only to the enterprise customer's employees.
- **Extranet VPNs**—Link outside customers, suppliers, partners, or communities of interest to an enterprise customer's network over a shared infrastructure using dedicated connections. Extranet VPNs differ from intranet VPNs in that they allow access to users outside the enterprise.

✓ **Tools to communication**

The followings are just a few of many communication tools available today:

- **Smart phones:-**These communication devices boast cutting-edge features, such as GPS navigation, voice-activated virtual assistants, predictive typing and video calling.
  Users can download apps that further enhance their mobile experience. They can scan QR codes with their smartphones, pay their bills on the go and check the stock market in real time.
- **Laptops:** Today, these communication tools are used mostly for work. However, laptops have some advantages over smart phones and tablets. Let's take software development. Even though you can design an app or a website on your tablet, it's easier to do in on a laptop or desktop computer.
  If you're a blogger or copywriter, doing your work on a tablet can be difficult. The small screen may cause eyestrain and affect your productivity. Additionally, laptops have a larger storage capacity compared to smart phones and tablets, letting you save large files and access them with ease.
- **Tablets:** They're portable and have all the functionalities of a smartphone and more. If you're a business owner, it's important to target customers across all devices and channels. Your website needs to be responsive and provide a seamless mobile experience. The same goes for your advertising campaigns, which need to be customized for each device so you can target the right audience in the right context.
- **VOIP/Internet telephony:** Nowadays, more and more organizations are carrying voice communications over the internet. They use Skype and other platforms to interview potential employees, hold video conferences and make international calls. These communication modes are cheaper and more convenient than traditional phone services. VoIP (Voice over Internet Protocol), has emerged as one of the most popular communication tools worldwide. Small businesses can save as much as 75 percent on local calls by switching to VoIP. Higher productivity, greater flexibility and more efficient message management are just a few of the benefits linked to this service.

- **Intranet:** An intranet is a private network that can be accessed by authorized users within an organization. Companies use an intranet to streamline communication between employees, share documents and keep them up-to-date with the latest industry news. This technology ensures everyone is on the same page, allowing for more efficient collaboration.
- **Social networks and forums:** Social media is widely used by individuals and corporations worldwide. It has the power to drive business decisions, increase brand awareness and connect customers with their favorite brands. It's also one of the most important communication tools, making it easier for brands to reach their target audience and get their message across.

Companies can harness the power of social media to strengthen their online presence and improve customer experience. For example, customers leave valuable feedback on your Facebook business page. Here you can address their concerns and get better insights into your audience.

Forums can be a valuable communication tool. As a business owner, you can use these platforms to learn more about your customers' needs and wants. You can also reply to their questions, recommend products and find ideas for your marketing campaigns.

Messenger apps, chat bots, email, internal blogs and tracking software are also useful and often essential communication tools. Businesses can leverage modern technology to attract and engage customers, address their inquiries and deliver a superior experience across all devices.

 **Theoretical learning Activity**

In group of 2-3 members, discuss on the following task:

a. Private WAN technologies
b. Public WAN technologies
c. WAN devices
    1. Dialup modem
    2. *Access server*
    3. *Broadband modem*
    4. *Channel service unit/data service unit (CSU/DSU*
    5. *WAN switch*
    6. *Router*
    7. *Core router/Multilayer switch*
d. Types of VPN:
    1. Access VPN
    2. Intranet VPN
    3. Extranet VPN

b. Communication tools:
    1. Smart phone
    2. Laptop
    3. Tablet
    4. VoIP/Internet Telephony
    5. Intranet
    6. Social network and forums

Points to Remember (Take home message)

An enterprise can get WAN access in two ways:

- ***Private WAN technologies:***
    - Dedicated point-to-point leased lines
    - Dialup
    - Public switched telephone network (PSTN)
    - Integrated Services Digital Network (ISDN)
    - Ethernet WAN
    - Asynchronous Transfer Mode (ATM)
    - Frame Relay.
- ***Public WAN technologies***:
    - Digital Subscriber Line (DSL)
    - Cable
    - Satellite access.
- List of WAN devices:
    - Dialup modem
    - *Access server*
    - *Broadband modem*
    - *Channel service unit/data service unit (CSU/DSU*
    - *WAN switch*
    - *Router*
    - *Core router/Multilayer switch*
- There are three main types of VPNs.
    - Access VPNs
    - Intranet VPNs
    - Extranet VPNs
- **Communication tools:** Smart phone, Laptop, Tablet, VoIP/Internet Telephony, Intranet, Social network and forums, Messenger apps, chat bots, email, internal blogs and tracking software

Learning outcome 1.4 formative assessment

Written assessment

1. List down four (4) private WNA technologies.
2. Enumerate five (5) WAN devices.
3. What are the types of VPN?
4. List down five examples of communication tools.

ANSWERS

1. Private WAN technologies:

- Dedicated point-to-point leased lines
- Dialup
- Public switched telephone network (PSTN)
- Integrated Services Digital Network (ISDN)
- Ethernet WAN
- Asynchronous Transfer Mode (ATM)
- Frame Relay.

2. List of WAN devices:

- Dialup modem
- *Access server*
- *Broadband modem*
- *Channel service unit/data service unit (CSU/DSU*
- *WAN switch*
- *Router*
- *Core router/Multilayer switch*

3. The main types of VPNs.

- Access VPNs
- Intranet VPNs
- Extranet VPNs

4. **Communication tools are:** Smart phone, Laptop, Tablet, VoIP/Internet Telephony, Intranet, Social network and forums, Messenger apps, chat bots, email, internal blogs and tracking software

Learning outcome 1.5 Identify tools, equipment and materials used in Remote connection

Duration: 3hrs

Learning outcome 1.5 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Identify correctly the tool for remote connection
2. Identify the equipment used for remote connection

Resources

Equipment	Tools	Materials
Computer Projector Black/White board	Handout notes Simulator Books	Internet Bundles Video aid Chalks Marker Pens

Advance preparation:

- Sample Videos that represent remote connection.

Indicative content 1.5.1: Remote connection tools

Remote connection tools

- **Telnet**: is a network protocol that allows a user on one computer to log into another computer that is part of the same network.

The purpose of telnet is to provide a bidirectional interactive text-oriented communications facility using a virtual terminal connection.

- **SSH**: Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. Typical applications include remote

command-line, login, and remote command execution, but any network service can be secured with SSH. ... Windows 10 uses OpenSSH as its default SSH client.

SSH is typically used to log into a remote machine and execute commands, but it also supports tunneling, forwarding TCP ports and X11 connections; it can transfer files using the associated SSH file transfer (SFTP) or secure copy (SCP) protocols. SSH uses the client-server model.

The purpose of SSH is to support encrypted data transfer between two computers. It can be used to support secure logins; file transfers or general purpose connects. Servers maintained by ITS require SSH-based connections in most cases.

- **Remote desktop:** Remote desktop is a program or an operating system feature that allows a user to connect to a computer in another location, see that computer's desktop and interact with it as if it were local. remote computer is a computer to which a user does not have physical access, but which he or she can access or manipulate via some kind of computer network. Remote desktop software allows a person to control a remote computer from another computer.

Theoretical learning Activity

In group of 2-3 members, discuss about the following tack:

- Define the following remote connection tools:
    a. Telnet
    b. SSH
    c. Remote desktop

Points to Remember (Take home message)

Remote connection tools: Telnet**,** SSH**,** Remote desktop

Indicative content 1.5.2: Equipment used in remote connection

Equipment used in remote connection

- **Router:** A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. Data sent through the internet, such as a web page or email, is in the form of data packets.
- **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.

- **Cables:** To connect two or more computers or networking devices in a network, network cables are used. There are three types of network cables; coaxial, twisted-pair, and fiber-optic.
- **PC**: A personal computer (PC) is a multi-purpose computer whose size, capabilities, and price make it feasible for individual use. Personal computers are intended to be operated directly by an end user, rather than by a computer expert or technician.

- **Sever:** A server is a computer that serves information to other computers. These computers, called clients, can connect to a server through either a local area network or a wide area network, such as the internet. A server is a vital piece of your IT infrastructure.

 **Theoretical learning Activity**

In group of 2-3 members, discuss about the following tack:

Define the following equipment used in remote connection:

a. Router
b. Switch
c. Cable
d. PC
e. Server

 **Points to Remember (Take home message)**

The **equipment used in remote connection** are: Router, Switch, Cable, PC, Serve

 **Learning outcome 1.5 formative assessment**

Written assessment

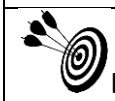
1. Give any three remote connection tools.
2. Differentiate router from server.
3. List down any three types of network cables.

ANSWERS

1. **Remote connection tools**: Telnet, SSH, Remote desktop
2. A **router** is a networking device that forwards data packets between computer networks. While, **server** is a computer that serves information to other computers called clients.
3. **Three types of network cables**; coaxial, twisted-pair, and fiber-optic.

Learning outcome 1.6 Design and interpret network blueprint.

Duration: 5hrs



Learning outcome 1.6 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Identify correctly network design principles
2. Identify correctly network design tools

Resources

Equipment	Tools	Materials
Computer	Handout notes	Internet Bundles
Projector	Simulator	Video aid
Black/White board	Books	Chalks
		Marker Pens

Advance preparation:

- Sample videos representing network design
- Installed network design tools

Indicative content 1.6.1: Network design principles and tools

Network design principles

- **Functionality:** Your all network applications and devices should be performing all the functions properly. You have to make sure, does your network infrastructure suppose the all the services running in your network? For example, you are using the Microsoft dot net then you have the enough bandwidth and hardware to work your applications to work efficiently.
- **Scalability:** Is the ability to add additional resources, for example, routers, switches, servers, memory, disks, and CPUs to an architecture without redesigning it
- **Adaptability:** For any architecture, change during a life cycle is inevitable. An architecture must be adaptable enough to accommodate growth and changes in technology, business, and user needs. Within the customer's financial constraints and growth plans, design and architecture that allows for adaptability.
- **Manageability:** You can manage your network using different tools like Cisco works or tools that can improve control over the network like capacity management, monitoring performance and detecting fault. You also need to manage the network security.
- **Cost effectiveness:** the degree to which something is effective or productive in relation to its cost.
- **Efficiency:** You can provide the efficiency with placing the best hardware and software in the network. Also make sure that your network equipment is cost effective, you can also build the most efficient network with choosing the most suitable and cost effective hardware and software. You can provide the efficiency with QoS, AAA and filtering.
- **Performance:** You also need to focus of network performance during designing the network, make sure that all your applications and devices have bandwidth they need.

Network design Tools

- **eDraw Max** is another network mapping tool with a Microsoft-inspired user interface. Over 200 map template designs can be exported into PNG, JPEG and PDF formats. eDraw is more of a generalist diagram tool rather than a specific network mapper. However, its capacity to map out flow charts and complex layouts makes it a solid choice for drawing up a network plan.
- **CONCEPTDRAW PRO** For medium size enterprises, Concept Draw Pro stands its ground against every other network-mapping program on this list. The user interface (clearly inspired by Microsoft Visio) allows you to create a variety of visual displays of your network environment as well as export Visio files.

- **Lucid chart** is one of the less known network mapping platforms that packs a tremendous punch. If you're looking to fast track your map production, then look no further. From the outset you can launch straight into a template and start building your IT environment.
- **Intermapper** is one of the pricier network mapping tools on this list. This program is available for users on Windows, Linux, and Mac, making it a flexible platform in terms of deployment. Intermapper was built with auto discovery in mind and will automatically locate devices throughout your network and record them on a map.
- **CADE (FREE)** In terms of network diagramming solutions, CADE takes a back-to-basics approach. While there is no fancy GUI, you'll find that there is an extensive 2D vector editor. CADE is a free application that can be downloaded online. This makes CADE a good choice for teams looking for a suitable remote deployment platform. As a welcome addition, remote users can contribute in real time to a drawing on the web. Once you've finished creating your drawings, you can also export them in EMF, JPG, XAML or PDF format.
- **LANFLOW** As the name suggests, LanFlow is tailor made for mapping out networks. As a result, it is a great choice for network administrators looking for a topology tool with a simple user interface. Everything in LanFlow is drag and drop, so if you want to add a new element to your diagram, all you need to do is click and move it.
- **Network Notepad** is a freeware application available for Windows made specifically for mapping out network elements. While Network Notepad doesn't have an extensive autodiscovery feature, it does have the Cisco Discovery Protocol Neighbor Tool (CPD), which can speed up the discovery process. The CPD tool allows the user to search through their network devices and pull information from elements with CDP information.

Practical learning Activity

In group of two members, design network representing your school with the following specific criteria:

- Each department in your school should have its own router.
- All routers inside your school must be connected to a single router that receive internet from ISP.
- The end devices must access the network through switch.
- The design must have design colors that differ from one department to another.

Checklist

Criteria	Yes	No
✓ Each department has its own router.		
✓ All routers are connected to a single router that receive internet from ISP.		
✓ The end devices can access the network through switch.		
✓ The design has design colours that differ from one department to another.		

Points to Remember (Take home message)

Network design principles

- Functionality
- Scalability
- Adaptability
- Manageability
- Cost effectiveness
- Efficiency
- Performance

Network design Tools

- eDraw Max
- CONCEPTDRAW PRO
- Lucid chart
- Intermapper
- CADE
- LANFLOW
- Network Notepad

Learning outcome 1.6 formative assessment

Practical assessment

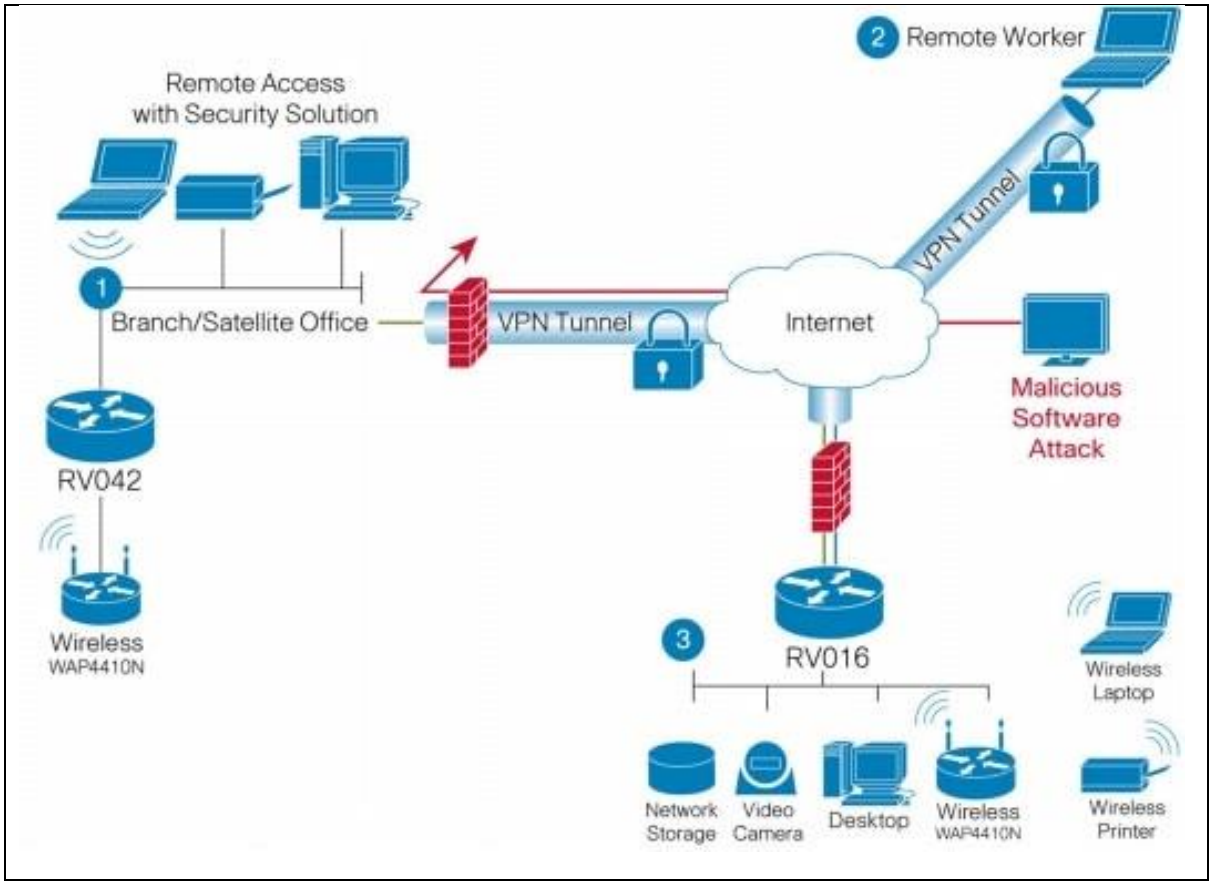
In group of two members, design network representing your school with the following specific criteria:

- Each department in your school should have its own router.
- All routers inside your school must be connected to a single router that receive internet from ISP.
- The end devices must access the network through switch.
- The design must have design colours that differ from one department to another.

Checklist

Criteria	**Yes**	**No**
✓ Each department has its own router.		
✓ All routers are connected to a single router that receive internet from ISP.		
✓ The end devices can access the network through switch.		
✓ The design has design colours that differ from one department to another.		

LEARNING UNIT 2: INSTALL, CONFIGURE AND TROUBLESHOOT WAN AND VPN



STRUCTURE OF LEARNING UNIT

Learning outcomes:

2.1. Configure and verify a serial WAN configuration
2.2. Configure and verify WAN Protocols
2.3. Configure and verify a site to site VPN
2.4. Troubleshoot WAN Network
2.5. Configure and verify an ADSL connection

Learning outcome 2.1 Configure and verify a serial WAN configuration

Duration: 2hrs

Learning outcome 2.1 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Identify correctly WAN devices.
2. Identify correctly WAN Connection types.
3. Identify physical parameters for WAN connections.

Resources

Equipment	Tools	Materials
Computer	Handout notes	Internet Bundles
Projector	Simulator	Video aid
Black/White board	Books	Chalks
Switch	Console cable	Marker Pens
Router		Cables
Modem(CSU/DSU)		
Communication Server		

Advance preparation:

- Sample videos representing WAN Devices, WAN Connection types, or WAN Connection parameters.

Indicative content 2.1.1: WAN Devices

WAN Devices

- **Router*:*** Provides internetworking and **WAN** access interface ports that are used to connect to the service provider network. These interfaces may be serial connections or other WAN interfaces. With some types of **WAN** interfaces, an external device such as a DSU/CSU or modem (analog, cable, or DSL) is required to connect the router to the service provider's local ***point of presence (POP).***
- **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.
- **Modem (CSU/DSU):** A **CSU/DSU** (Channel Service Unit/Data Service Unit) is a hardware device about the size of an external **modem** that converts a digital data frame from the communications technology used on a local area network (LAN) into a frame appropriate to a wide-area network (WAN) and vice versa.
- ***Access server:*** Concentrates dial-in and dial-out user communications. An access server may have a mixture of analog and digital interfaces and support hundreds of simultaneous users.
- ***WAN switch***: A multiport internetworking device used in carrier networks. These devices typically switch traffic such as Frame Relay, ATM, or X.25 and operate at the data link layer of the OSI reference model. ***Public switched telephone network (PSTN) switches*** may also be used within the cloud for circuit-switched connections such as ***Integrated Services Digital Network (ISDN)***or analog dialup

Theoretical learning Activity

In group of 2-3 members, discuss on the following WAN Devices:

a. Switch
b. Router
c. Modem (CSU/DSU)
d. Access server
e. WAN switch

Points to Remember (Take home message)

WAN Devices: - Switch

- Router
- Modem (CSU/DSU)
- Access server
- WAN switch

Indicative content 2.1.2: WAN Connection types

There are three types of WAN connection are as follows.

- **Circuit switched technologies**

- In circuit switches network every time before transferring data over the WAN, new connection gets establish after data transfer over the connection get closed.
- In this technique generally data is transferred through single connection or single route.
- Integrated Service Digital Network (ISDN), shown in picture below, is an example of a circuit-switched network.

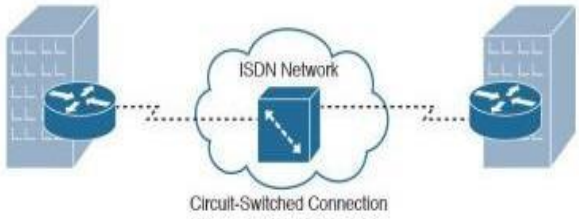


Figure 4 - Circuit-Switched Connection

Circuit switching requires a dedicated physical connection between the sending and receiving devices. For example, parties involved in a phone call have a dedicated link between them for the duration of the conversation. When either party disconnects, the circuit is broken, and the data path is lost. This is an accurate representation of how circuit switching works with network and data transmissions. The sending system establishes a physical connection, and the data is transmitted between the two. When the transmission is complete, the channel is closed.

- **Packet-switched technologies**

- In packet switched network uses virtual connection for transferring data, it for transferring data create connection on first data transmission and used it as a permanent connection.
- It is faster than circuit switched network.
- It is used for multi path communication.
- A Frame Relay network, shown in figure below, is an example of a packet-switched network.

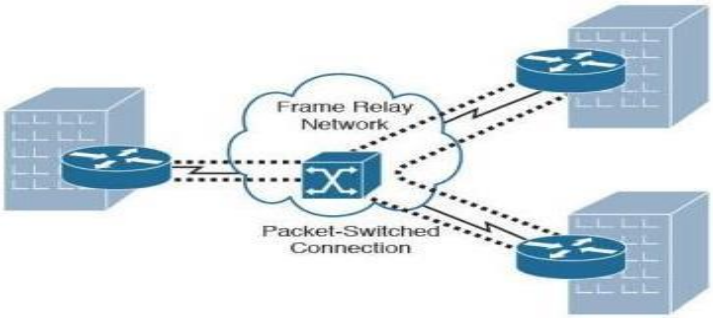


Figure 5 - Packet-switched technologies

In packet switching, messages are broken into smaller pieces called packets. Each packet is assigned source and destination addresses. Packets are required to have this information because they do not always use the same path or route to get to their intended destination.

Packets can take an alternative route if a particular route is unavailable for some reason.

- **Point-to-Point technologies**

Point-to-point connection refers to a communications connection between two communication endpoints or nodes. An example is a telephone call, in which one telephone is connected with one other, and what is said by one caller can only be heard by the other. This is contrasted with a *point-to-multipoint* or *broadcast* connection, in which many nodes can receive information transmitted by one node. Other examples of point-to-point communications links are leased lines and microwave radio relay.

Theoretical learning Activity

In group of 2-3 members, discuss on the following types of WAN connections:

a. Circuit switched technologies
b. Packet-switched technologies
c. Point-to-Point technologies

Points to Remember (Take home message)

Types of WAN connections:

- Circuit switched technologies
- Packet-switched technologies
- Point-to-Point technologies

Indicative content 2.1.3: Physical Parameters for WAN Connections

Physical Parameters for WAN Connections

- **Customer Premises Equipment (CPE):** The devices and inside wiring located at the premises of the subscriber, connected with a telecommunication channel of a carrier. The subscriber either owns or leases the CPE. A subscriber, in this context, is a company that arranges for WAN services from a service provider or carrier.
- **Data Communications Equipment (DCE):** Also called data circuit-terminating equipment, the DCE consists of devices that put data on the local loop. The DCE primarily provides an interface to connect subscribers to a communication link on the WAN cloud.
- **Data Terminal Equipment (DTE):** The customer devices that pass the data from a customer network or host computer for transmission over the WAN. The DTE connects to the local loop through the DCE.
- **Local loop:** The copper or fiber cable that connects the CPE at the subscriber site to the central office (CO) of the service provider. The local loop is sometimes called the "last mile."
- **Demarcation point:** A point established in a building or complex to separate customer equipment from service provider equipment. Physically, the demarcation point is the cabling junction box, located on the customer premises, that connects the CPE wiring to the local loop. It is usually placed for easy access by a technician. The demarcation point is the place where the responsibility for the connection changes from the user to the service provider. This is very important, because when problems arise, it is necessary to determine whether the user or the service provider is responsible for troubleshooting or repair.
- **Central office (CO):** A local service provider facility or building where local cables link to long-haul, all-digital, fiber-optic communications lines through a system of switches and other equipment.

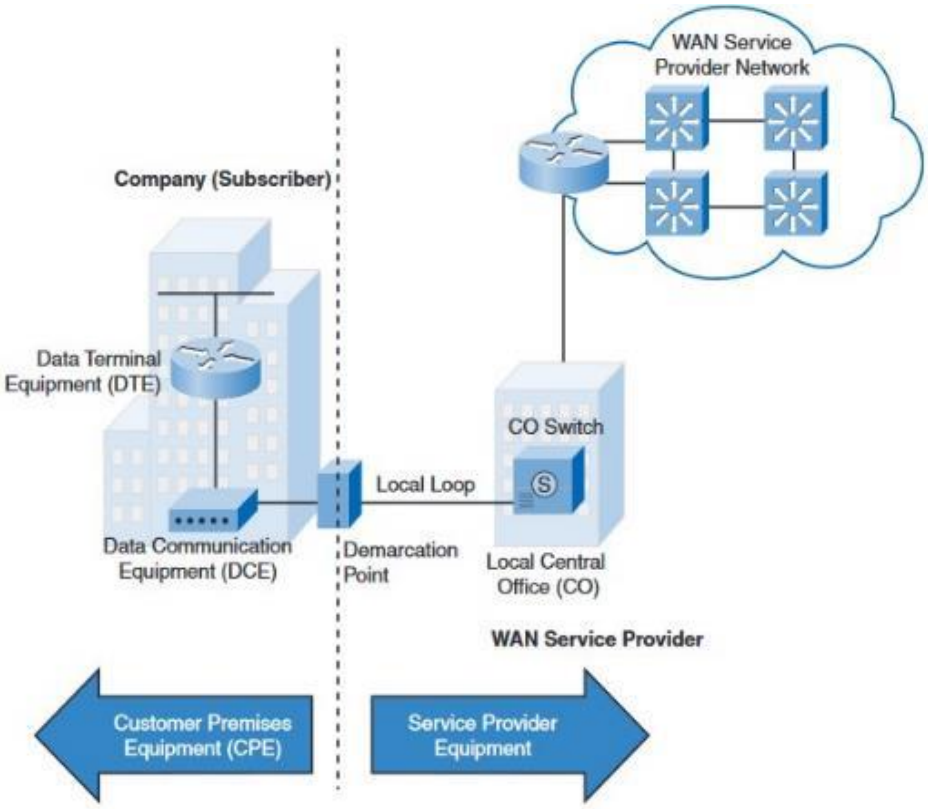


Figure 6 - WAN Physical Layer Terminology

Theoretical learning Activity

In group of 2-3 members, discuss on the following Physical Parameters for WAN Connections:

a. Customer Premises Equipment (CPE)
b. Data Communications Equipment (DCE)
c. Data Terminal Equipment (DTE)
d. Local loop
e. Demarcation point
f. Central office (CO)

Points to Remember (Take home message)

Physical Parameters for WAN Connections:

- Customer Premises Equipment (CPE)
- Data Communications Equipment (DCE)
- Data Terminal Equipment (DTE)
- Local loop
- Demarcation point
- Central office (CO)

Learning outcome 2.1 formative assessment

Written assessment

1. List down four examples of WAN Devices.
2. What are the types of WAN Connections?
3. Enumerate physical parameters for WAN connections

ANSWERS

1. Examples of **WAN Devices**: Switch, Router, Modem (CSU/DSU), Access server, WAN switch.
2. Types of **WAN Connections:** Circuit switched technologies, Packet-switched technologies, Point-to-Point technologies
3. **Physical parameters for WAN connections**:
    - Customer Premises Equipment (CPE)
    - Data Communications Equipment (DCE)
    - Data Terminal Equipment (DTE)
    - Local loop
    - Demarcation point
    - Central office (CO)

Learning outcome 2.2 Configure and Verify WAN Protocols

Duration: 5hrs

Learning outcome 2.2 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Configure properly the IP Parameters
2. Configure properly WAN Protocols and technologies.
3. Test correctly WAN connections and WAN speed

Resources

Equipment	Tools	Materials
Computer Projector Switch Router Modem (CSU/DSU) Communication server	Books Handout notes Reference books Simulator	Internet Cards Antennas Cables Video aid

Advance preparation:

- Sample videos representing configuration of WAN Protocols

Indicative content 2.2.1: Configuration of IP Parameters

Configuration of IP parameters

- **Dynamic IP Configurations**

A dynamic IP address is an IP address that an ISP lets you use temporarily. If a dynamic address is not in use, it can be automatically assigned to a different device. Dynamic IP addresses are assigned using either DHCP

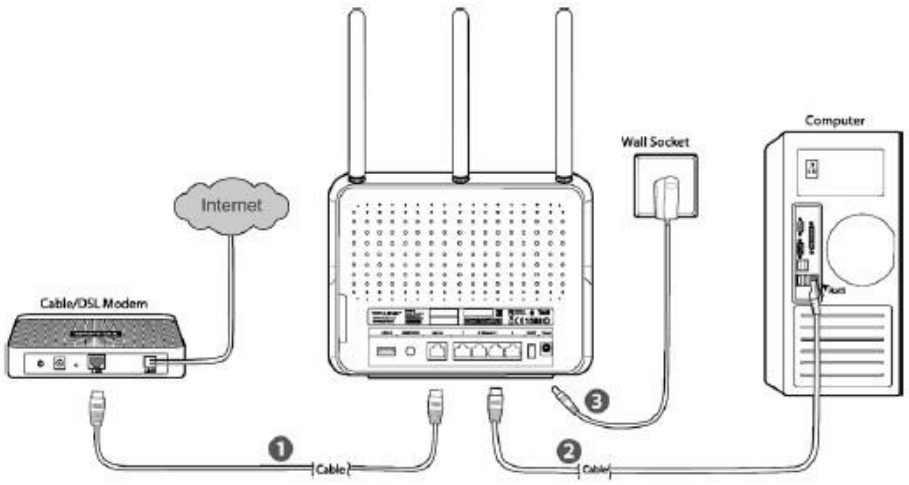
Step 1: Preparation

Note: Make certain you do have internet access directly via your modem or community network.

Step 2: Connect your Network

Take C8 as an example. If there is no modem, regard your internet source as a modem, like an Ethernet cable through a wall.

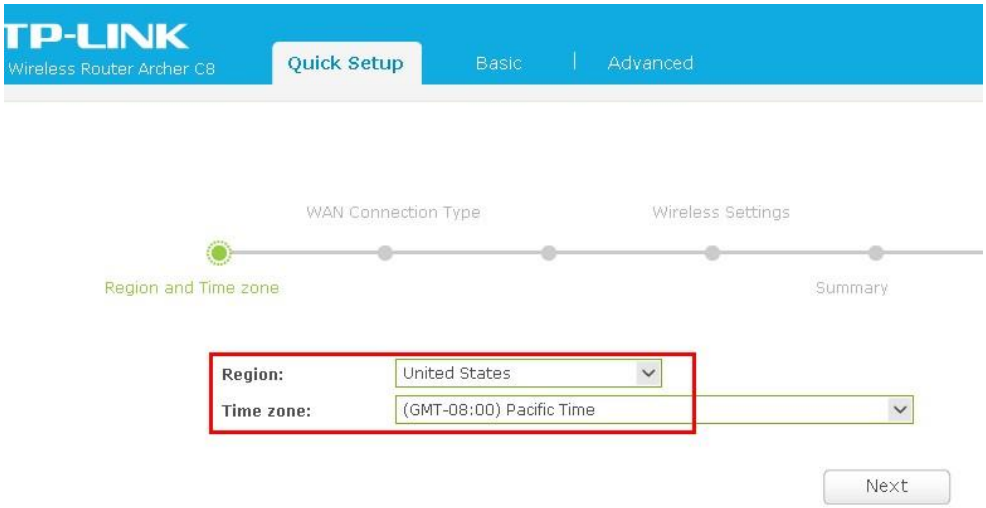
1) Turn off your Cable modem, C8 and computer.
2) Connect the WAN port of C8 to the Cable modem with Ethernet cable.
3) Connect your computer to any of the LAN ports (yellow one) of C8
4) Power on C8 and computer. Don't power on the modem before logging into the router.



Step 3: Log in to the C8's web management page

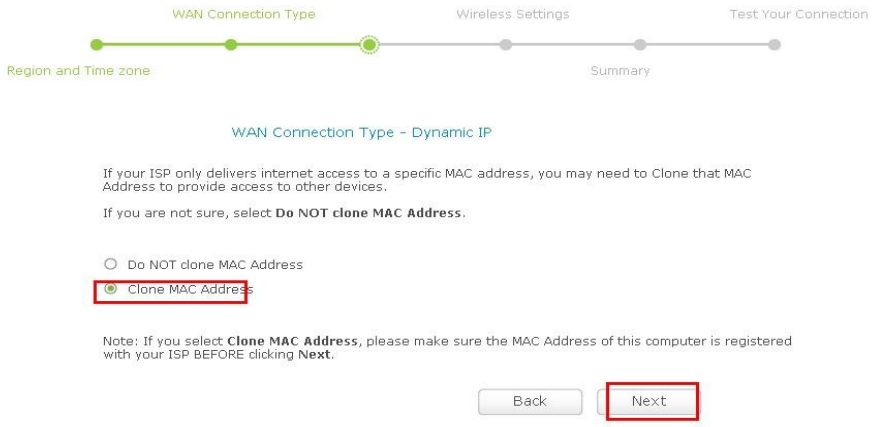
Step 4: Power on the cable modem.

Step 5: After logging into the router, you will see Quick Setup→ choose the Region and Time Zone→ Next.

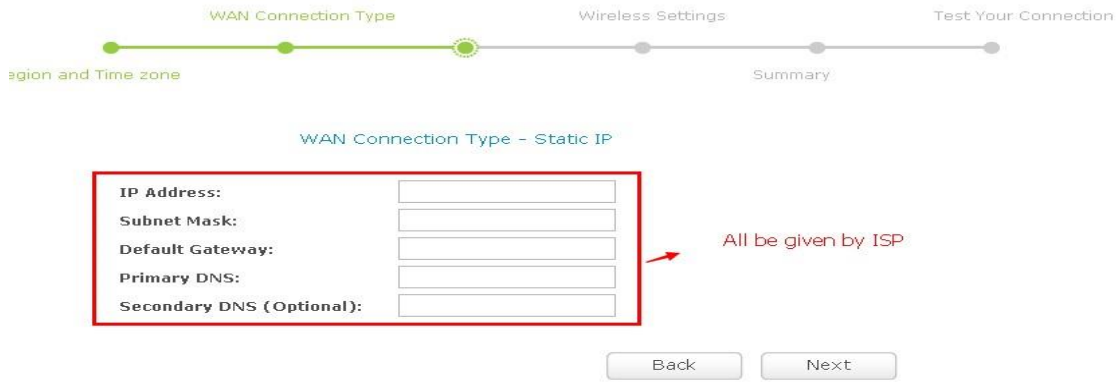


Step 6: WAN Connection Type choose Dynamic IP " →Next.

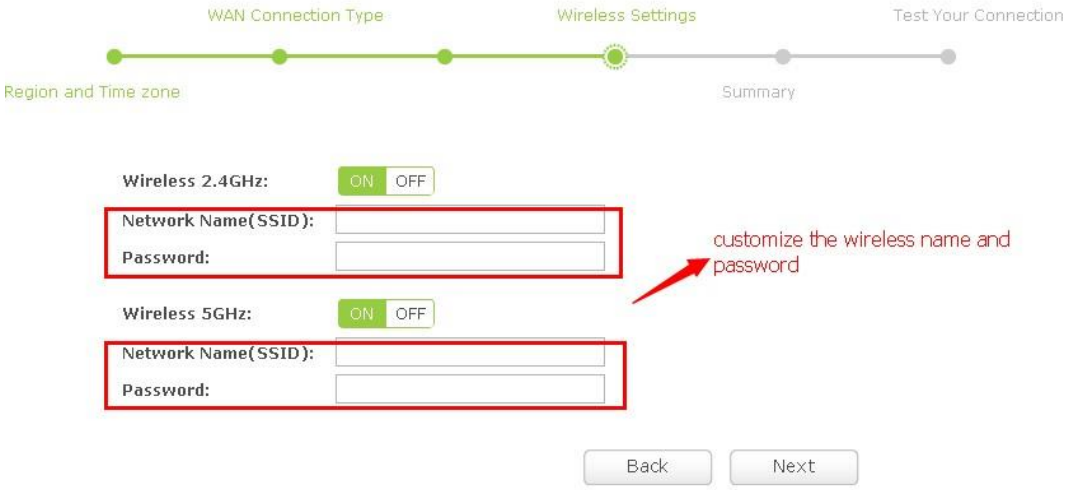
Click **Clone MAC Address** to clone your PC's MAC address to WAN MAC Address of the router→Next.



Note: If your ISP provides Static IP, the WAN Connection Type you may choose **Static IP** and put in the specific IP information from your ISP→ Next.



Step 7: Customize your own wireless network names and passwords for wireless 2.4GHz and 5GHz→Next.

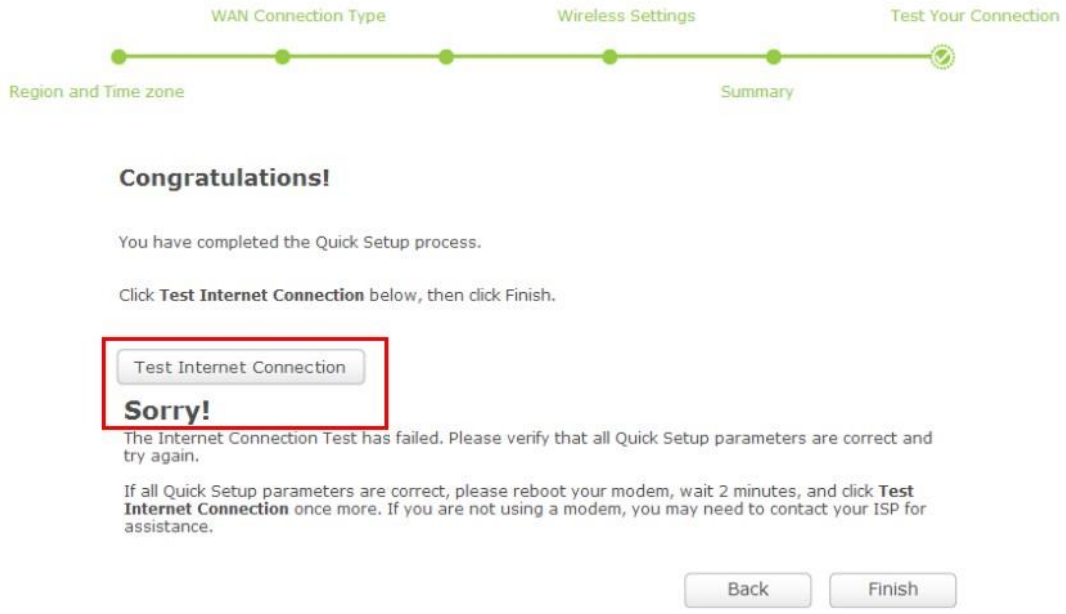


Step 8: Click **Save** to save the settings**.**

Step 9: Click **Test Internet Connection**. If it is configured successfully, you will see the message **Success**, then click **Finish** to close the Quick Setup.

If the test is failed, please go **Back** to confirm the settings and try again.

Moreover, connect your computer directly to your modem and see whether you have internet access.



Step 10: Power cycle the cable modem and router

After the configurations, powering cycle your network can make your network work more stable.

1) Turn the cable modem off firstly, then turn your router and computer off, and leave them off for about 2 minutes;
2) Turn the router on firstly and wait about 1 minute, and then power on your computer.

3) urn the cable modem on, and wait till the modem works stable (All LED lights work normally).
4) Repeat the steps 1-3 above until you connect to the Internet.

The above steps done by using Web interface (GUI). So, the following commands are used in CLI interface, starting from global configuration mode.

Router(config)#ip dhcp pool N1

(dhcp initialization)

Router(dhcp-config) #network 192.168.1.0 255.255.255.0

(Network address + Subnet mask.)

Router(dhcp-config) #default-router 192.168.1.1

(Default gateway)

Router(dhcp-config) #ip dhcp excluded-address 192.168.1.4 192.168.1.5

(to exclude ip from 4 to 5)

Router(dhcp-config) #End

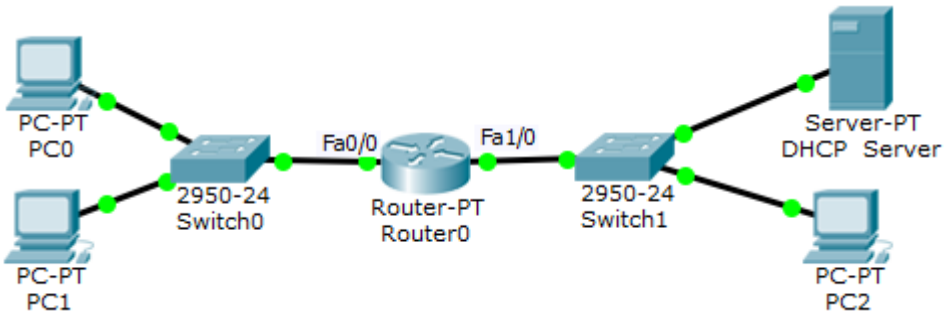
(finish configuration)

Router#copy running-config start up-config

(saving configuration)

Now, we are done by going through the configuration of Dynamic IP by using Web interface, and CLI interface. So, let's see how to do it by using network server:

Given the following network exhibit,



Configure Manually the **DHCP Server** for its **DHCP pools** and its IP configuration. The IP address is 192.168.1.10 and the default gateway will be the routers interface's IP address that is face (Fa1/0) to DHCP server; eg: 192.168.1.1.

For the subnets 192.168.1.0 and 10.10.0.0 there must be two **DHCP pool**. The assignments will be done on **DHCP Server** manually after enabling **DHCP protocol.**

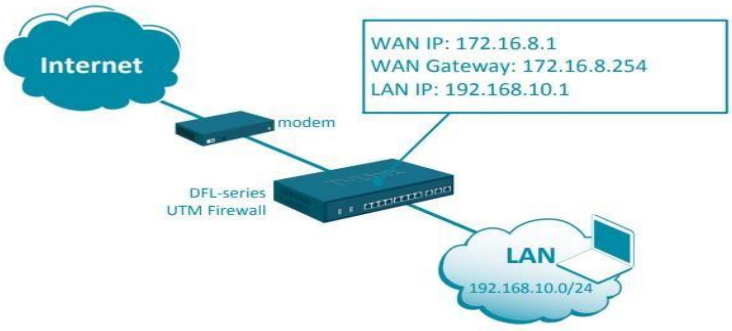
In router0, the following configuration will be done for two different subnet **DHCP** achievement:

Router0 # **config terminal**
Router0(config)# **interface fa0/0**
Router0(config-if) # **ip address 10.10.0.1 255.255.255.0**
Router0(config-if) # **ip helper-address 192.168.1.10**
Router0(config-if) # **no shutdown**
Router0(config-if) # **exit**
Router0(config)# **interface fa1/0**
Router0(config-if) # **ip address 192.168.1.1 255.255.255.0**
Router0(config-if) # **ip helper-address 192.168.1.10**
Router0(config-if) # **no shutdown**
Router0(config-if) # **end**
Router0# **copy run start**

After this configuration, we can try **dynamic IP assignment** on PC by selecting the **dynamic option** on IP configuration screen, then PCs get their IP configuration from **DHCP Server.**

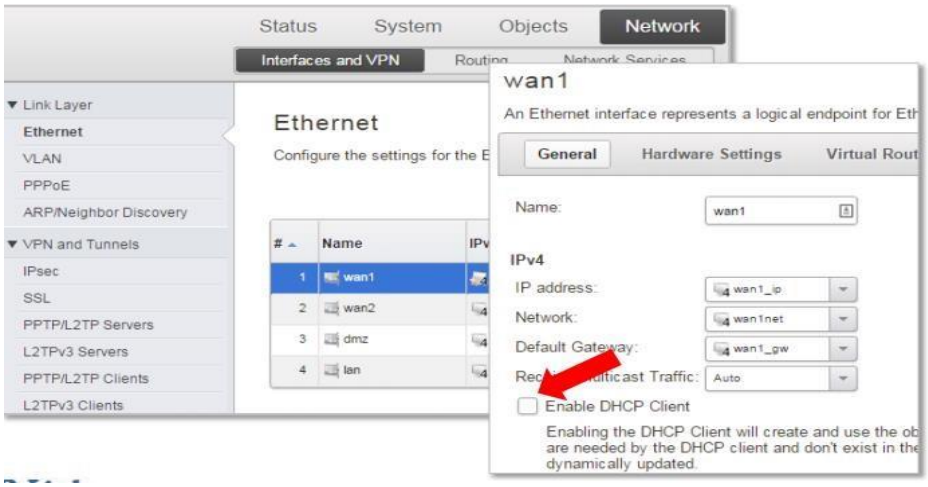
- **Static IP Configurations**

A static IP address is an IP address that was manually configured for a device instead of one that was assigned by a DHCP server.



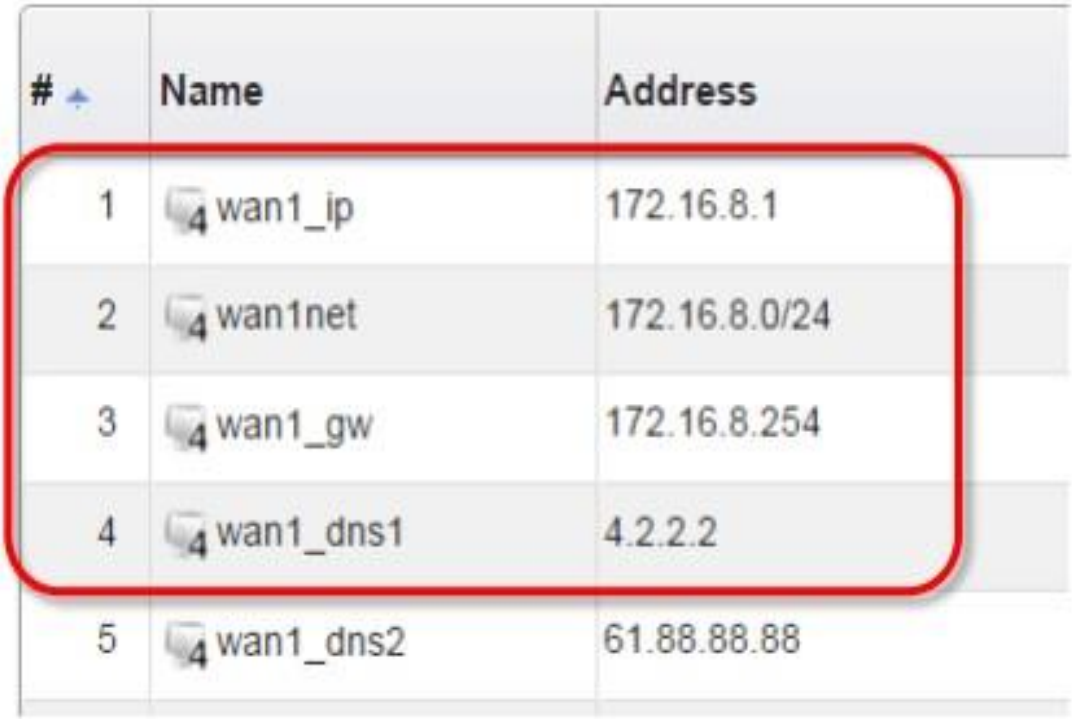
Step 1: Log into the firewall. The default access to LAN is via https://192.168.10.1. Default username is “admin” and password is “admin”.

Step 2: Go to Network > Ethernet > WAN1 and make sure that “DHCP Client” option is not enabled.



Step 3: Go to Objects > Address Book > Interface Addresses.

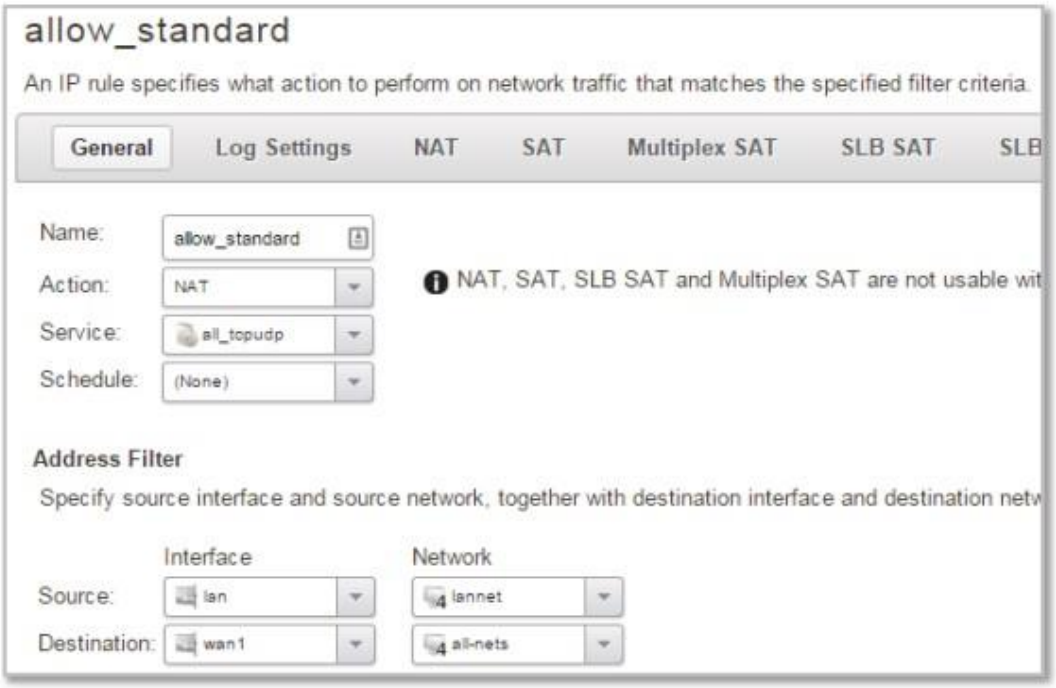
Assign the required IP addresses to “wanip”, “wannet” and “wan_gw”.



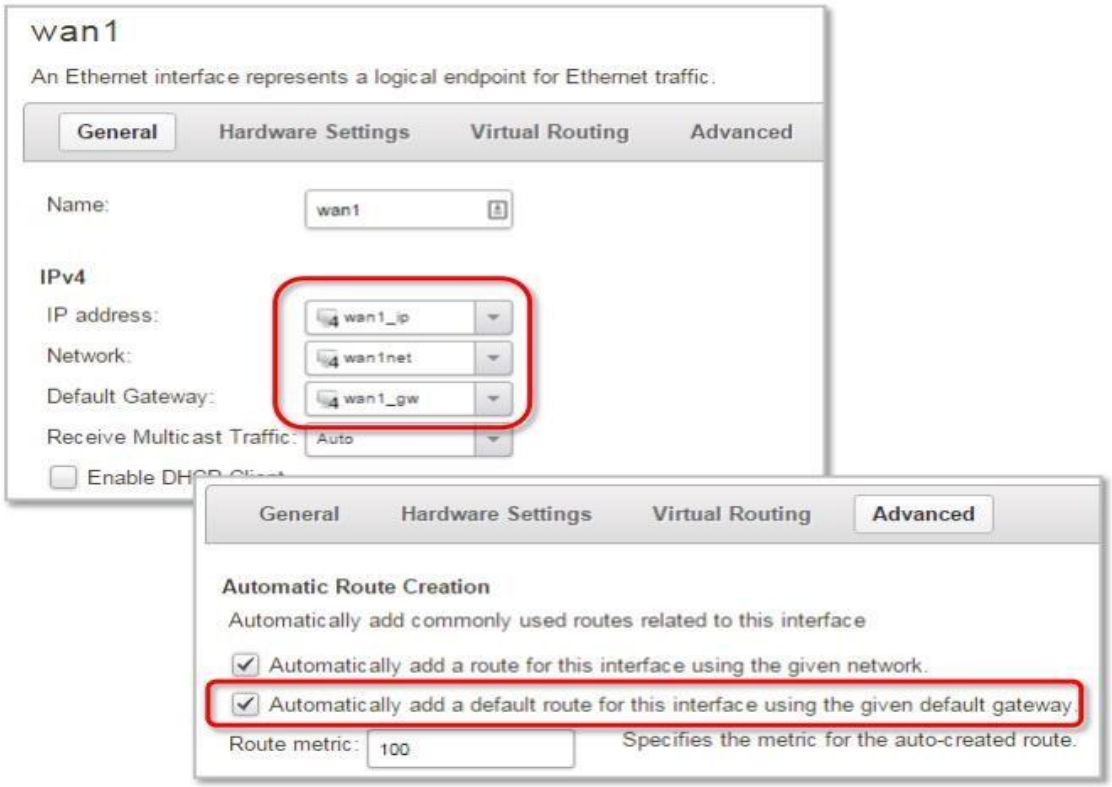
If “wan_gw” is not present - add new “IP4 Address” object.

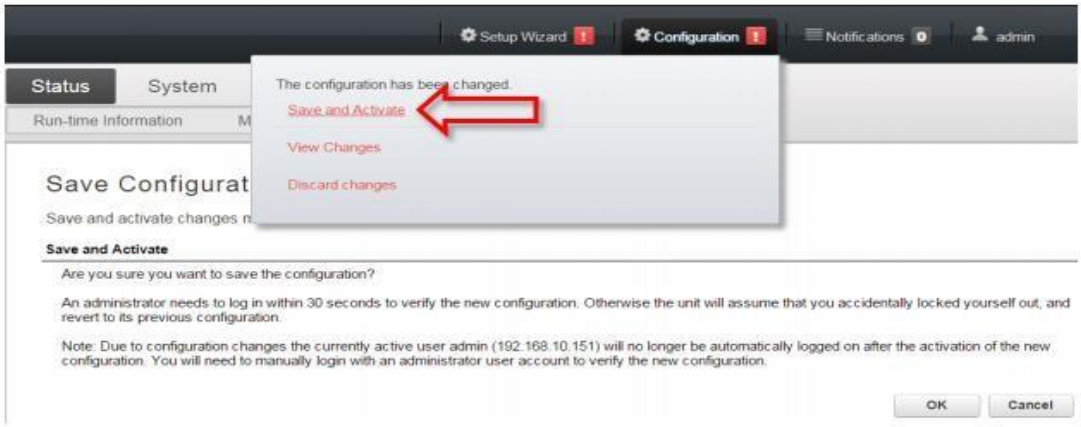
Step 4: Go to Network > Ethernet > WAN.

Verify that WAN has IP Address, Network and Default Gateway assigned to it. Go to Advanced and make sure the “Add default route if default gateway is specified” is enabled. Go to Policies > Main IP Rules > LAN_WAN. You should see the default “Allow Standard” rule that performs Network Address Translation (NAT) for all outgoing traffic. If required, create additional rules to block or allow desired traffic. Choose the necessary Action, Service, Interface and Network for the rules.



Step 5: After the configuration is done, click “Configuration” in main bar and select “Save and Activate”. Then click OK to confirm. Wait for 15 sec. You will be automatically redirected to the firewall’s LAN IP address. **Note**: If you do not re-login into the firewall within 30 sec, the configuration is reverted to its previous state. The validation timeout can be adjusted under System > Remote Management > Advanced Settings.





Practical learning Activity

In group of 2 members, do the following tasks:

- Configure dynamic IP
- Configure Static IP

Checklist

Criteria	Yes	No
✓ Dynamic IP Configured successfully		
✓ Static IP Configured successfully		

Points to Remember (Take home message)

A **dynamic IP address** is an IP address that an ISP lets you use temporarily. If a dynamic address is not in use, it can be automatically assigned to a different device. Dynamic IP addresses are assigned using either DHCP

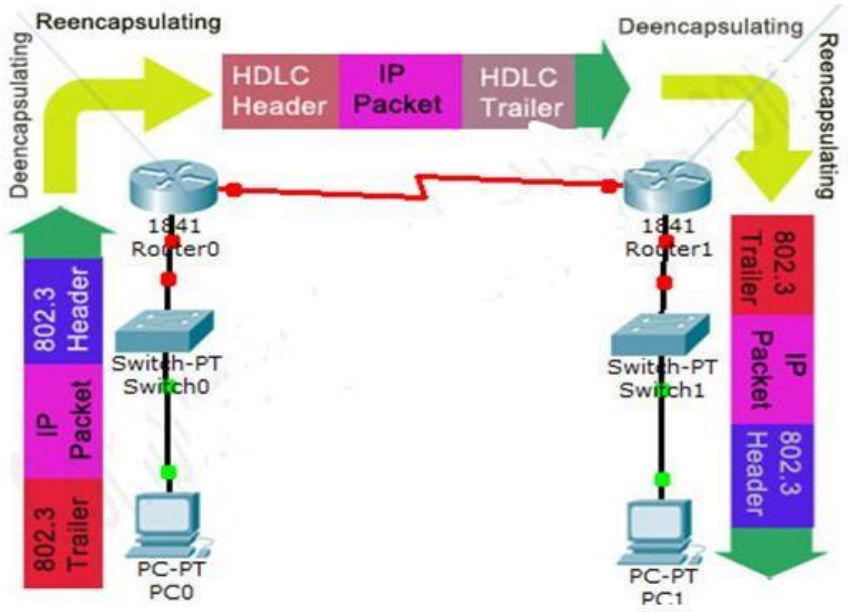
A **static IP address** is an IP address that was manually configured for a device instead of one that was assigned by a DHCP server.

Indicative content 2.2.2: WAN Protocols and Technologies

1) HDLC

HDLC stands for High-level Data Link Control, it is a layer two protocol that provides encapsulation method for serial link. Serial link and Ethernet link both use different encapsulation methods for data transmission. Serial link cannot carry the frame formatted with Ethernet encapsulation and vice versa Ethernet link cannot carry the frame formatted through the Serial encapsulation. Ethernet encapsulation method and protocols are basically specified in LAN technology. Serial protocols and encapsulation methods are primary described in WAN technology. Router is used to connect two different technologies. HDLC is an encapsulation method for serial link.

How HDLC Protocol works



- Suppose PC0 has some data for PC1. So it generated a data packet.
- Since PC1 is not connected with LAN segment, network layer of PC0 will encapsulate data packet with default gateway's IP address.
- Data link layer of PC0 will warp this IP packet in 802.3 header and trailer. Once wrapped, it becomes frame.
- Physical layer of PC0 will put this frame in wire.
- Through switch this frame will be received in Router R0.
- Router will de-encapsulate the frame in packet to find out the Layer 3 destination address.
- Since destination address is connected with serial link, router will forward this frame in serial interface.
- Serial interface will re–encapsulate the frame with serial encapsulation protocol. In our example it is HDLC.
- After re-encapsulation this frame will be forwarded from serial interface.
- This frame will be received in serial interface of Router R1.
- R1 will de-encapsulate the frame in packet to find the Layer 3 destination address.
- Since destination address is connected via FastEthernet, it will forward this packet in FastEthernet interface.
- FastEthernet Interface will re-encapsulate the packet in Ethernet frame.
- After re-encapsulation this frame will be forwarded from FastEthernet interface
- Through switch this frame will be received at PC1.
- PC1 will receive this frame in exactly same format as it was packed by PC0 without knowing how it makes it way to him.

Configure HDLC in Cisco Router

- **HDLC** is the default encapsulation method on Cisco routers. Unless we have changed it with other encapsulation method, there is no need to configure it. It's already configured. Suppose we have changed default encapsulation method with other methods such as PPP. Now we are looking for a way to use HDLC again then we have to go through the following steps:

```
Router>enable

Router# configure terminal

Router(config)#interface serial 0/0/0

Router(config-if) #encapsulation hdlc

Router(config-if)  #end
Router#
```

That's all we need to do. Now HDLC encapsulation is enabled in serial interface Serial 0/0/0.

Verifying HDLC encapsulation

Since HDLC is the default encapsulation method for serial interfaces in Cisco Router, it will not be listed in running configuration. It means we cannot use **show running config** command to verify the HDLC encapsulation. We have to use **show interfaces [*Interface*]** command to view encapsulation type in interface.

Router#show interfaces serial 0/0/0

2) SDLC

The software development life cycle (**SDLC**) is a framework defining tasks performed at each step in the software development process. **SDLC** is a structure followed by a development team within the software organization. It consists of a detailed plan describing how to develop, maintain and replace specific software.

3) PPP

In computer **networking**, Point-to-Point **Protocol** (**PPP**) is a data link layer (layer 2) communications **protocol** between two routers directly without any host or any other **networking** in between. It can provide connection authentication, transmission encryption, and compression.

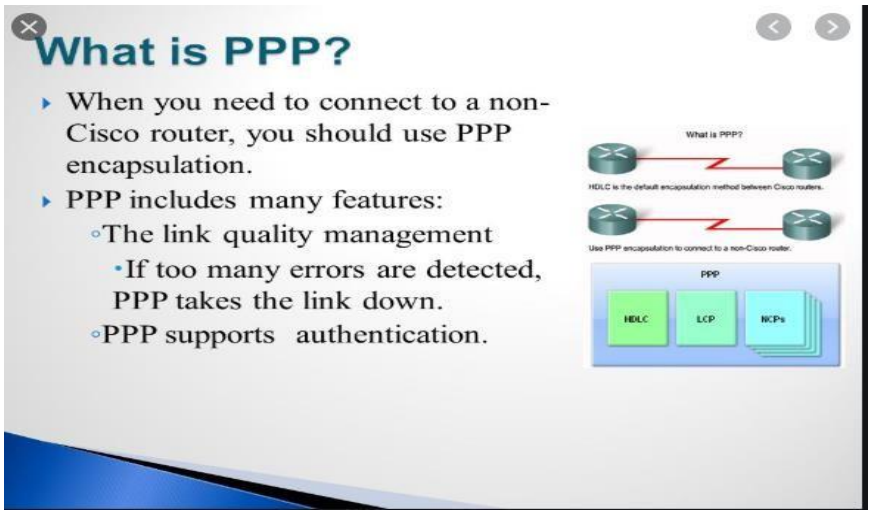


Figure 7 - Features of Point-to-Point Protocol

Configure PPP in Cisco Router

To configure PPP in Cisco router, you need to go through the following steps:

Router>enable

Router# configure terminal

Router(config)#interface serial 0/0/0

Router(config-if)#encapsulation hdlc

Router(config-if) #end
Router#

Verifying PPP encapsulation

Router#show interfaces serial 2/0

Or

Router#show interfaces

4) LAPB

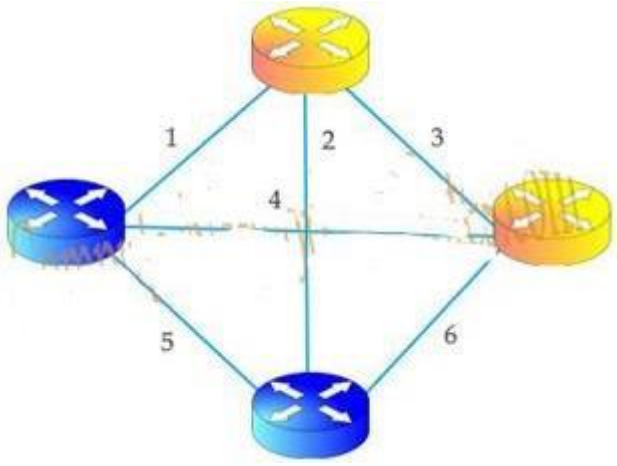
Link Access Procedure, Balanced implements the data link layer as defined in the X.25 protocol suite. LAPB pronounced as LAP bee is a bit-oriented protocol derived from HDLC that ensures that frames are error free and in the correct sequence.

5) Frame-Relay

Frame relay is a packet-switching telecommunication service designed for cost-efficient data transmission for intermittent traffic between local area **networks** (LANs) and between endpoints in wide area **networks** (WANs).

basic concepts of Frame Relay step by step in detail with examples including Frame Relay fundamental, Frame Relay Congestion Control method and Frame Relay Terminology (VC, PVC, SVC, DTE, DCE, DE, Access link, LMI types, LMI status enquiry, DLCI numbers, FECN, BECN, Access rate and CIR).

Frame Relay is one of the most popular WAN service deployed over the past decade. Even though several advanced technologies (such as VPN, ATM) are available today, Frame Relay still rocks and will be in near future due to its features, benefits and lower cost in comparison with other point to point wan services. For example, have look on following figure that illustrates a network with simple point to point leased line connection.



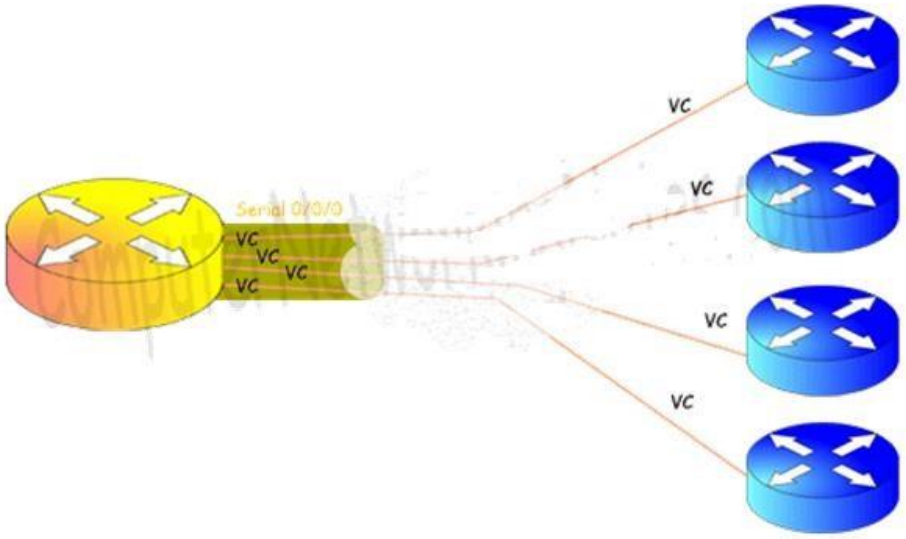
There are four routers in this network. To connect these routers with each other, total six leased lines and three serial interfaces on each router are used. We can use following formula to figure out how many connections are required: -

(N × (N – 1)) / 2 [Here N is the number of routers]

In our example we have four routers so we need (4 x (4-1)) /2 = 6 leased lines.

If we have 100 routers, then we need (100 x (100-1)) /2 = 4950 lease lines and 99 serial interfaces on each router. Forget about low end routers, even a 7700 series router does not have sufficient physical interfaces to handle this requirement.

With Frame Relay implementation, we still need 6 connections to connect all these routers with each other. But instead of physical lines, Frame Relay uses virtual lines to connect all these locations. The biggest benefit of these virtual lines is that we do not need equal physical interfaces on router to connect them. We can connect multiple virtual lines with single interface.



Frame Relay VC, PVC and SVC

In Frame Relay terminology virtual connection lines are known as Virtual Circuits (VCs). There are two types of VCs; PVCs and SVCs.

Differences between Frame Relay PVCs and Frame Relay SVCs

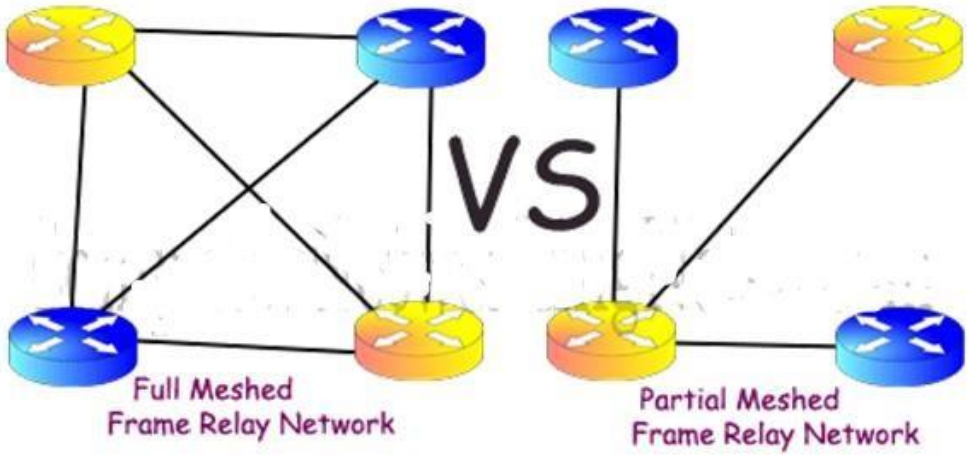
Frame Relay PVCs (Permanent Virtual Circuits)	**Frame Relay SVCs (Switched Virtual Circuits)**
PVC is just like a leased line that is once configured will stay there until we manually reconfigure it.	SVC is just like a telephone connection that is dynamically built whenever we have data to transmit and once transmission is over it will be terminated.
If we have regular data for transmission, then PVC is the best choice.	If we have periodical data for transmission, then SVC is the right choice.

PVCs need a lot of manual configuration.	SVCs need less configuration in comparison with PVCs.
Once PVC is built there is no delay before data transmission.	Since SVC is built each time whenever we send data, therefore a small delay before data transmission is expected.
Whether we use it or not, we have to pay for entire billing cycle.	We need to pay only when we actually use it.

SVC is not tested in any CCNA level exam. So I am not going to include it in rest of the article. After this wherever VC or PVC is referred please take that for PVC only.

Frame Relay Network Type

A frame relay network is considered ***fully meshed*** when all sites (routers) are connected with each other via direct link. When all sites do not have direct link with each other then it would be considered as ***partially meshed*** frame relay network.



Configuration of Frame Relay Step by Step

R1

Router>enable

Router#configure terminal

Router(config)#interface serial 0/0/0

Router(config-if) #encapsulation frame-relay

Router(config-if)#ip address 192.168.1.1 255.255.255.0

Router(config-if) #frame-relay interface-dlci 100

Router(config-if) #frame-relay lmi-type ansi

Router(config-if) #no shutdown

Router(config-if) #exit

Router(config)# exit

Router#

R2

Router>enable

Router#configure terminal

Router(config)#interface serial 0/0/0

Router(config-if) #encapsulation frame-relay

Router(config-if) #ip address 192.168.1.2 255.255.255.0

Router(config-if) #frame-relay interface-dlci 101

Router(config-if) #no shutdown

Router(config-if) #exit

Router(config)#exit

Router#

Let's understand above configuration step by step. As we know, routers allow us to run different WAN services on different interfaces. So our first logical objective is to identify the correct interface. As figure shows interface serial 0/0/0 is assigned for frame relay on both routers. To configure Frame Relay on this interface we need to enter in interface mode. First three commands in above configuration are used for this purpose.

Enable: This command is used to enter in privileged exec mode.

configure terminal: This command is used to enter in global configuration mode.

interface serial 0/0/0: This command is used to enter in interface mode.

In Cisco routers default encapsulation is set to HDLC. We cannot use Frame Relay with default encapsulation. Next command changes this encapsulation.

Router(config-if)#encapsulation frame-relay: This command will change default encapsulation method to Frame Relay.

Next command assigns IP address in interface.

Router(config-if) #ip address 192.168.1.1 255.255.255.0: This command assign IP address in Serial 0/0/0 of R1.

Router(config-if) #ip address 192.168.1.2 255.255.255.0: This command assign IP address in Serial 0/0/0 of R2.

Next command assigns DLCI value in interface.

Router(config-if) #frame-relay interface-dlci 100: This command assigns DLCI value 100 in Serial interface of R1.

Router(config-if) #frame-relay interface-dlci 101: This command assigns DLCI value 101 in Serial interface of R2.

Next command sets LMI option in interface. Until we change LMI option with next command default LMI option is set to Cisco (in Cisco routers).

Router(config-if) #frame-relay lmi-type ansi: This command will change default LMI option to ANSI.

Have you notice? we did not run this command in R2. Since LMI option [Cisco] that we got from provider matches with the default (Cisco) setting, so there is no need to run this command in R2.

By default, all interfaces on router are disabled. We need to enable them before they can communicate with other.

Router(config-if)#no shutdown: This command will enable the Serial interface

6) DSL

Digital subscriber line is a family of technologies that are used to transmit digital data over telephone lines. In telecommunications marketing, the term DSL is widely understood to mean asymmetric digital subscriber line, the most commonly installed DSL technology, for Internet access.

You configure DSL connections in much the same way you configure ISDN or modem connections. DSL connections can be configured as switched or nailed PPP, MP, or MPP, or as Frame Relay-encapsulated connections. You can also use your existing authentication methods, such as RADIUS, to authenticate DSL users, by using PPP protocols in conjunction with PAP or CHAP. You can do this either when the units are first turned on or by setting an inactivity timer.

Any ISDN TA or router (such as an Ascend Pipeline) that supports ISDN BRI (2B1Q) signaling can be connected over an IDSL connection. ADSL and SDSL connections require Ascend DSL Pipe units on the remote end.

DSL connections require the following general configuration on the MAX TNT:

- The DSL port in the line profile
- A Connection profile for the remote device
- For Frame Relay connections, a Frame Relay profile

In addition to standard routing connections, you can configure the following DSL-specific capabilities:

- DSLPipe plug and play
- IDSL voice support

A DSL physical link is always up, but a PPP session can be established and terminated based on data activity, just as it is for ISDN or PSTN calls. Each PPP session initiates negotiations, followed by authentication and accounting. Switched connections can provide per session authentication as well as accounting information typically used for client billing.

From the service provider perspective, a DSL connection is handled exactly like an ISDN or PSTN call. The MAX TNT checks the Answer-Defaults profile, applies authentication methods, and establishes the PPP session. After some inactivity PPP session is dropped, again generating accounting information. DSL Pipe units initiate all switched ADSL and SDSL connections and the MAX TNT handles them as regular incoming PPP calls. Note that Frame Relay connections must be nailed.

You configure the DSL Pipe for a switched connection in a similar way to other Pipeline switched connections, with the following important differences:

Set the Chan Usage parameter in the Configure profile to Switch/Unused (for ADSL or SDSL connections) or Switch/Switch (for IDSL connections)

Set the Dial # parameter in the Configure profile to the DSL port number, which in the case of a single DSL Pipe is always 1.

To configure a switched connection on the MAX TNT for an incoming connection from a DSL Pipe, you must set the Call-Type parameter to Off in the Connection profile for the DSL Pipe.

For example:

admin> **read connection dslpipe-1**

CONNECTION/dslpipe-1 read
admin> **set telco call-type =**
off admin> **write**
CONNECTION/dslpipe-1 read

For more information about configuring switched connections on the MAX TNT, see the *MAX TNT Network Configuration Guide*.

Configuring nailed connections

In a nailed connection, the MAX TNT and the remote unit always assume the connection is up and do not attempt to verify the line is operational.

A nailed connection does not record accounting or authentication information after the session is established and therefore cannot be used to bill for DSL service as if it were a call on an ISDN network or the PSTN.

Nailed connections are typically used for Frame Relay connections, but PPP can also be used. Voice calls are not supported over a nailed connection.

You specify whether a ADSL or SDSL connection is nailed by:

- Specifying a nailed group number in the ADSL or SDSL profile
- Setting Call-Type to FT1 in the Connection profile for the nailed connection

You specify whether an IDSL connection is nailed by:

- Specifying a nailed group number in the IDSL profile
- Setting Channel-Usage to Nailed-64-Channel in the IDSL profile
- Setting Call-Type to FT1 in the Connection profile for the nailed connection

You configure the DSL Pipe for a nailed connection in a similar way to other
Pipeline nailed connections:

- In the Configure profile, set Chan Usage to Leased/Unused
- In the Connection profile for the MAX TNT, set Call Type to Nailed in the Telco Options submenu
- In the Connection profile for the MAX TNT, specify a Group number in the Telco Options submenu

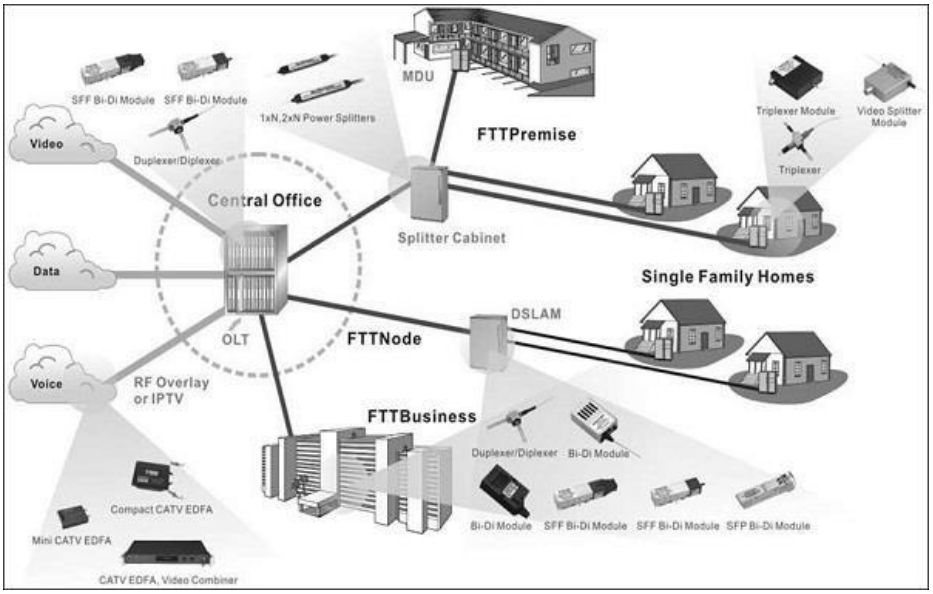
DSL configurations, includes:

- An IDSL Frame Relay connection
- An ADSL nailed PPP connection
- An SDSL Frame Relay configuration using interface-based routing
- An SDSL Frame Relay configuration using system-based routing

7) FTTH

Fiber to the home (**FTTH**), also called "fiber to the premises" (FTTP), is the installation and use of optical fiber from a central point directly to individual buildings such as residences, apartment buildings and businesses to provide unprecedented highspeed Internet access.

Fiber to the Home or simply **FTTH** is a technology that uses optical fiber directly from the central point to the residential premises (as shown in the following image). It provides uninterrupted high-speed internet service. Here, “H” includes both home and small business.

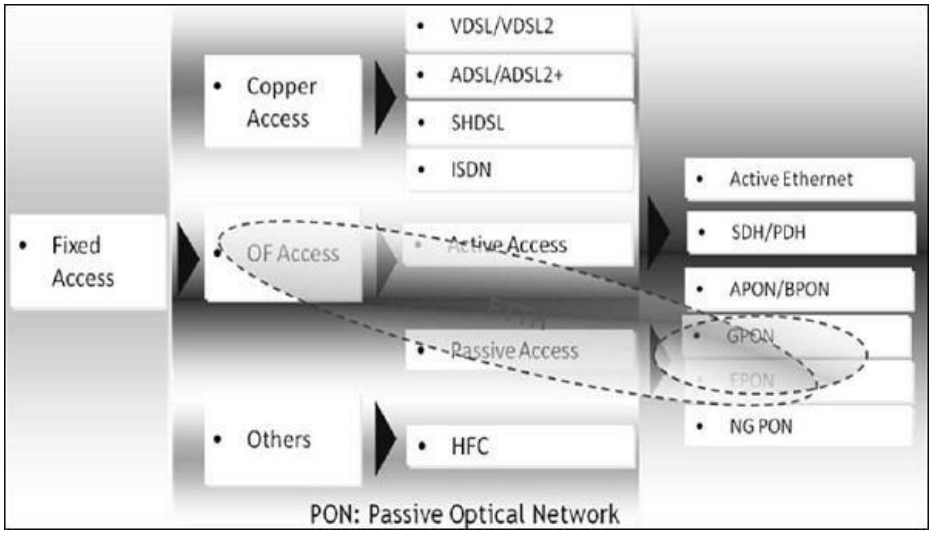


FTTH is the ultimate fiber access solution where each subscriber is connected to an optical fiber. The deployment options discussed in this tutorial are based on a complete optical fiber path from the **Optical Line Termination** (OLT) right to the subscriber premises. This choice facilitates high bandwidth services and content to each customer and ensures maximum bandwidth for future demands of new services. Therefore, Hybrid options involving 'part' fiber and 'part' copper infrastructure networks are not included.

As an access to the home over fiber, Fiber to The Home (FTTH) scenario is mainly for the single family unit (SFU), providing a comparatively small number of ports, including the following types — POTS, 10/100/1000 BASE-T, and RF (18dBmV).

Optical Fiber Method can be deployed in two ways: Active Method and Passive Method. The current mass FTTH deployment is based on the passive method. Hence, let's discuss the Passive Method in detail.

Passive Method − The two typical technologies used in this method are **Ethernet Passive Optical Network** (EPON) & **Gigabit-capable Passive Optical Networks** (GPON). Refer the following image.



- **Very high bit rate digital subscriber loop** (VDSL) supports a maximum bit rate of 55 bps. VDSL2 has better QoS and better SNR.
- ADSL (asymmetric digital subscriber line) supports a maximum bit rate of 8Mbps, however ADSL2 can go up to 12Mbps.
- SHDSL stands for **symmetric high bit rate digital subscriber line**. The larger the diameter of the telephone, the longer the distance it could reach. The transmission rate depends on the diameter of the telephone wire.
- **Integrated service digital network** (ISDN) is based on circuit-switched network.

Why FTTH?

Fiber offers a number of advantages over the previous technologies (Copper). The most important ones are as follows:

- Enormous information carrying capacity
- Easily upgradeable
- Easy to install
- Allows fully symmetric services
- Reduces operations and maintenance costs
- Covers very long distances
- Strong, flexible, and reliable
- Allows small diameter and lightweight cables
- Safe and secure
- Immune to electromagnetic interference (EMI)
- Lower cost

8) FTTP

Fiber To The Premises (FTTP) is a fiber optic cable delivery medium that provides Internet access directly to a user or groups of users from an Internet service provider (ISP).

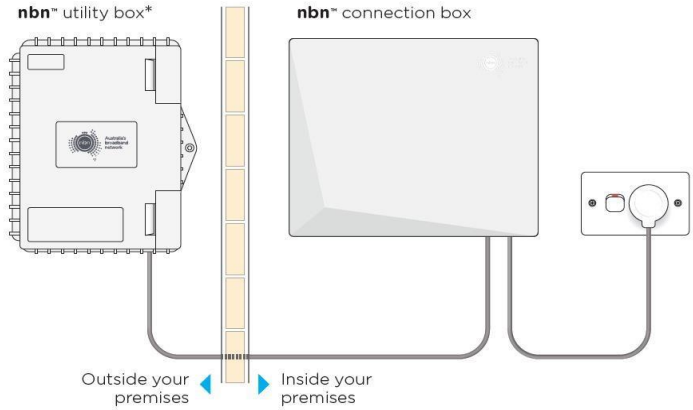
Fibre to the Premises means that the fibre broadband internet connection from the local exchange is connected to the router in your home, which is much faster than the old copper telephone line used by many other broadband services.

The result is you can enjoy very high speeds of 1Gbps (gigabits per second) or more. Though FTTP can also deliver lower speeds, which is useful if very fast fibre is beyond your budget, or not required, but might be something you'll use later.

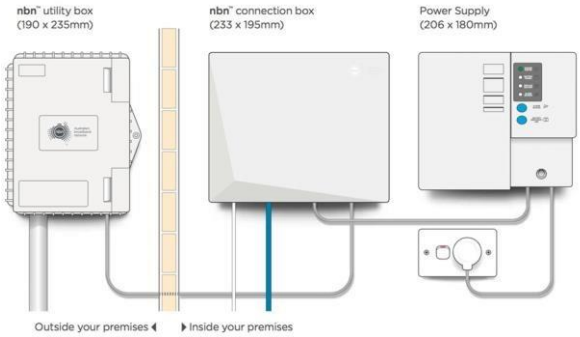
Setting Up Fibre to the Premises (FTTP)

Step 1: locate the nbn™ FTTP Network Termination Device (NTD)

Find the indoor nbn™ FTTP Network Termination Device (NTD) in your home. This will usually be installed in a garage but may be located in an odd location such as a wardrobe, cupboard or underneath a staircase. Ensure you check your entire home for the NTD including any unusual places that you may not expect.



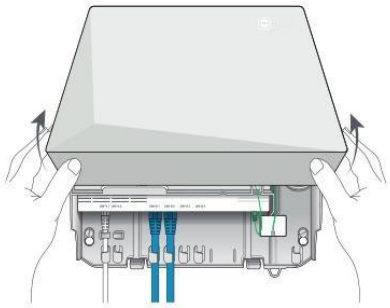
The nbn™ Network Termination Device (NTD) may be installed without a battery backup unit (as shown above) or with an optional battery backup unit. The image below shows the nbn™ Network Termination Device (NTD) installed alongside a battery backup unit. Please note that the battery backup adds little value to an nbn™ FTTP service. If your power is cut, your nbn™ NTD unit will continue to run for a limited time on the battery backup, but your wireless modem/router will not be powered, and any associated services such as a VoIP phone service will also stop working.



Step2: plug in your BYO modem/router to the nbn™ FTTP Network Termination Device (NTD)

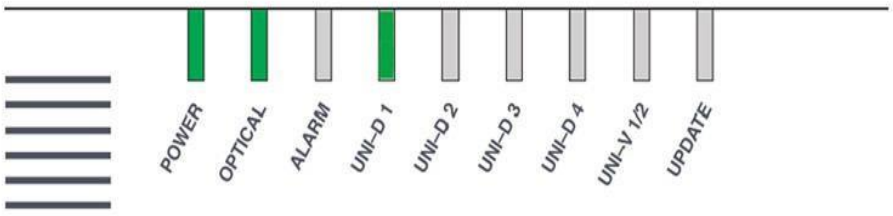
You will need to plug your modem/router into your nbn™ FTTP Network Termination Device (NTD) to connect your Internet service. First, remove the cover on the NTD to access the ports

on the bottom. Press the two clips on either side and lift the cover at an angle (as shown below) to remove it.



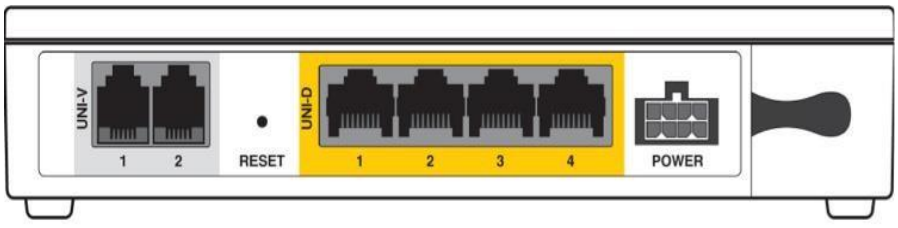
Ensure that the included power cable from the power port on the back of the FTTP Network Termination Device (NTD) is plugged in and secure. Plug the other end of the power cable into a power wall outlet in your home and switch the powerpoint on.

After a few minutes, you should notice the POWER and OPTICAL lights on the front of the NTD turn solid green. If you have a battery backup unit installed, the ALARM button may also be green. If the optical light on your nbn™ FTTP NTD remains red or is off, please contact our support team for further troubleshooting.



Now, take your modem/router's power supply cable and use it to connect your modem/router's power port to an electrical outlet. Switch the powerpoint on.

Take your Ethernet cable (this is typically blue, yellow, grey or white) and plug one end into the required yellow port marked UNI-D on the back of the nbn™ FTTP Network Termination Device (NTD). The active UNI-D port would have been sent to you via email and SMS – in many cases, this is usually UNI-D 1 but may be another number such as UNI-D 2, UNI-D 3 or UNI-D 4.



Plug the other end of this Ethernet cable into the WAN port on your modem/router. This may also be labelled as INTERNET, WAN/LAN or FIBRE. The Ethernet cable is larger than a

telephone cable. DO NOT use the telephone cable to plug in your modem/router to the nbn™ FTTP Network Termination Device (NTD).

Step 4: Connect and configure your BYO modem/router

Your BYO modem/router will need to be configured with your new MATE nbn™ details to work.

1. First, ensure the supplied yellow Ethernet cable with your modem/router (this is usually yellow, blue, grey or white) is plugged from the required yellow UNI-D port on your nbn™ FTTP Network Termination Device (NTD), into the WAN port on the back of your modem/router. This WAN port may also be labelled as INTERNET, LAN/WAN or FIBRE depending on the make and model of your modem.
2. You will now need to connect your BYO modem/router to your device. You'll need a computer, laptop, tablet or smartphone that is connected to your BYO modem/router via Ethernet or Wi-Fi.
3. Once you have connected your device to your BYO modem/router, open the web browser on your connected device and type in your modem/router's default gateway/admin IP address in the address bar. This will be printed on the bottom or back of your modem/router depending on the make and model. Some of the most common addresses are 192.168.1.1, 192.168.20.1, 10.1.1.1 and 10.0.0.138. The IP gateway address for your modem/router will typically be printed on the bottom or back of your device.
4. Once you have accessed the gateway of your modem/router, you may see a login page. If there's a username or login field, the default username will almost always be **admin** (it may even already be filled in). The default password is typically **admin** or **password**.

If you can't log in with these settings, please check the manufacturer's website for your BYO modem/router's default login settings. If your BYO modem/router is secondhand or you have used it previously, it may have custom login details set. If you need to, you can factory reset the modem/router to return it to the default settings.

5. From here, it gets a little tricky to offer general advice for all BYO modem/routers. The layout of modem/router settings pages can vary greatly for each different device depending on the make and model. If you get stuck or it is not clear where you should change your internet settings, you need to check the manufacturer's website for support information. Ideally, your modem/router will have a Setup Wizard or Quick Setup section that will run automatically the first time you log in to the settings, or there'll be a fairly obvious button to launch it.
6. The Setup Wizard or Internet Settings section should run you through entering the required connection settings, step by step. The most important settings are the following:

Encapsulation or Connection Type – **MUST BE SET TO PPPOE**

Connection Mode/Access Type/Service Type – **ETHERNET WAN/RESIDENTIAL GATEWAY/WIRELESS ROUTER MODE**

This will then allow you to enter your username (sometimes called Login) and password which are supplied in your MATE welcome email, titled “You’re nearly there mate!”

7. After completing the Setup Wizard or Internet Settings section and saving your settings, give the modem/router some time. Some modem/routers reboot automatically after every new configuration, while others simply need a few minutes to apply the settings.

Take a look at the lights on your modem router. Most should now be green, blue, purple or another “positive” colour. Many modem routers have lights that flash to indicate connection activity, so you shouldn’t be concerned if any lights are flashing unless the manufacturer’s support information specifically advises that flashing lights indicate a problem.

8. Hop on one of your computers or Wi-Fi devices and try to visit a website. If it works, your MATE nbn™ internet is up and running! If you have issues connecting, please contact our support team for further troubleshooting.

9) L2TP

In computer networking, Layer 2 Tunnelling Protocol (**L2TP**) is a tunnelling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself.

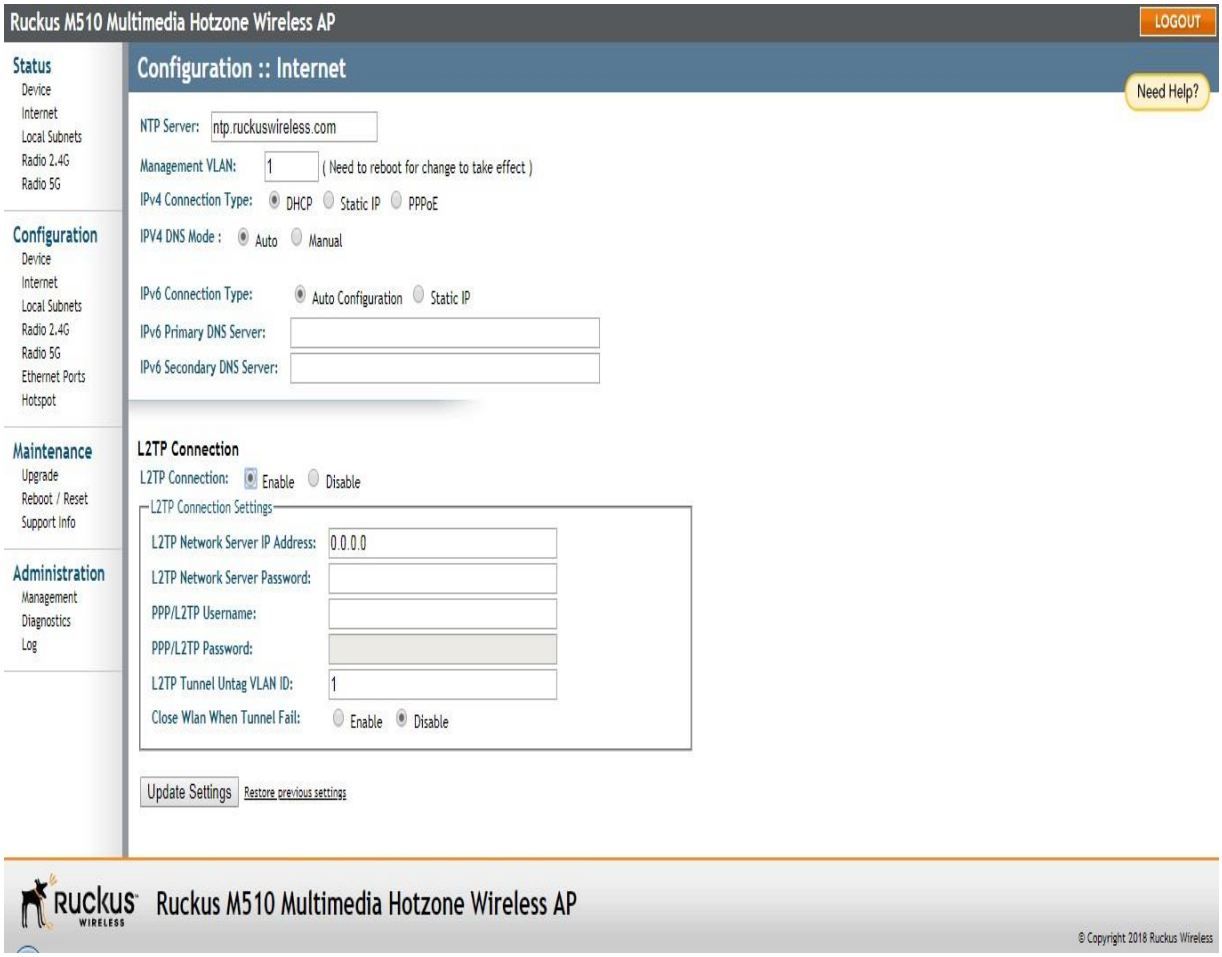
Configuring L2TP Connection Settings

Use the following procedure to configure Layer 2 Tunnelling Protocol settings.

You can implement transparent bridging by using L2TP (Layer 2 Tunnelling Protocol) tunnelling. By tunnelling traffic from an AP to a centralized data center, access controllers with policy enforcement software can apply rules and services. In a typical WLAN implementation, these rules include a captive portal to authenticate users' credentials. In the case of L2TP, the Ruckus AP functions as a remote bridge, forwarding traffic on to PPP sessions over the L2TP tunnel. This implementation ensures that you have complete visibility into MAC addresses of users, as individual Wi-Fi clients are essentially placed

(bridged) onto the ISP's core network.

1. Go to **Configuration > Internet**.
2. Under **L2TP Connection**, click **Enable**.



1. In **L2TP Network Server IP Address**, type the IP address of the L2TP network server (LNS) to which the device connects.
2. In **L2TP Network Server Password**, type the L2TP server password.
3. If your network requires PPP authentication, configure the following fields under L2TP/PPP Authentication:
   - **Username**: Type your PPP user name.
   - **Password**: Type the password for the account.
   - **L2TP Tunnel Untag VLAN ID**: Enter the Untag VLAN ID for the L2TP tunnel.
4. In **Close WLAN When Tunnel Fail**, select **Enable** if you want to disable the WLAN when the tunnel connection is lost. This prevents clients from remaining connected to the WLAN but without Internet connectivity.
5. Click **Update Settings** to save your settings.
6. ATM and LAPB configuration

10) PPTP

PPTP stands for Point-to-Point Tunneling Protocol, and it's a VPN protocol that was introduced back in 1995, though it was in development ten years prior to that date. PPTP improved on the previous PPP standard which lacked the tunneling feature. What started out as a protocol

implement in Windows systems quickly became a widespread VPN protocol available on numerous platforms

11) ATM

An automated teller machine (**ATM**) is an electronic telecommunications device that enables customers of financial institutions to perform financial transactions, such as cash withdrawals, deposits, transfer funds, or obtaining account information, at any time and without the need for direct interaction with bank staff.

Practical learning Activity

Group of two members, do the following task:

a. Configure the following WAN Protocols
   - HDLC
   - SDLC
   - PPP
   - LAPB
   - Frame-Relay
   - DSL
   - FTTH
   - FTTP
   - L2TP
   - PPTP
   - ATM

Checklist

Criteria	Yes	No
✓ HDLC is configured correctly		
✓ SDLC is configured correctly		
✓ PPP is configured correctly		
✓ LAPB is configured correctly		
✓ Frame-Relay is configured correctly		
✓ DSL is configured correctly		
✓ FTTH is configured correctly		
✓ FTTP is configured correctly		
✓ L2TP is configured correctly		
✓ PPTP is configured correctly		
✓ ATM is configured correctly		

Points to Remember (Take home message)

WAN Protocols and technologies: HDLC, SDLC, PPP, LAPB, Frame-Relay, DSL, FTTH, FTTP, L2TP, PPTP.

Indicative content 2.2.3: Testing WAN

- **Testing WAN connections**

When testing WAN connections, consider the following:

- **Bandwidth** — The data transfer capacity, or speed of transmission, of a digital communications system as measured in bits-per-second (bps).
- **Latency** — The time that is required for a request to travel from one point on a network to another point.
- **Network congestion** - The condition of a network when the current load approaches or exceeds the available resources and bandwidth that are designed to handle that load at a particular location in the network. Packet loss and delays are associated with congestion.

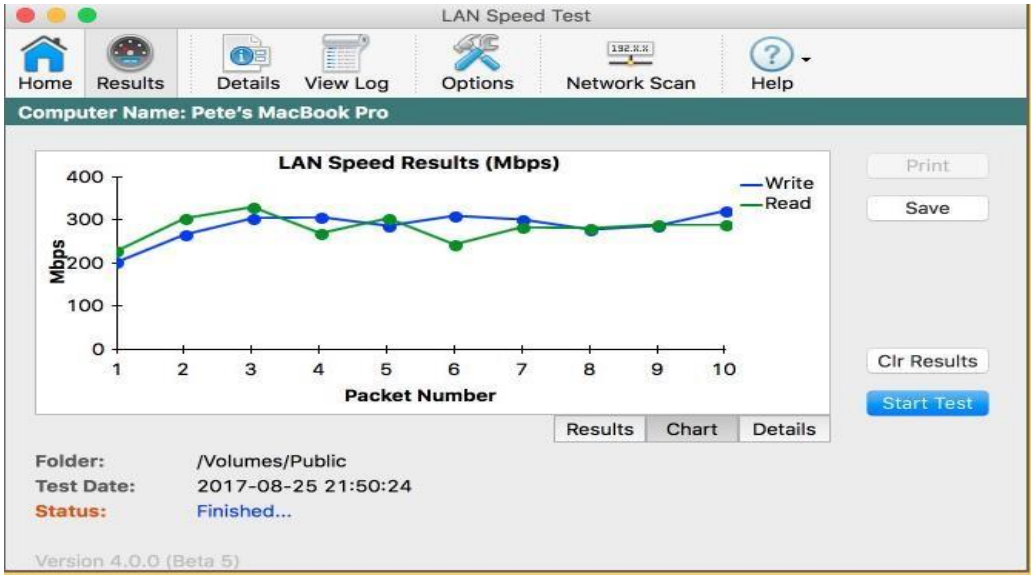
The simplest method to test performance over WAN connections is to have a user at a remote location connect to a SharePoint site and perform several user actions. For example, you can host an online meeting, talk the user through the actions, and count the number of seconds for actions to be completed. Or, you can connect to a computer remotely and perform the tasks.

- **Testing WAN speed**

There are different WAN Testing tools. One of them is LAN Speed Test. Despite its name **LAN Speed Test** from TotuSoft can very well be used to test WAN connections. The tool was designed to be a simple but powerful tool for measuring file transfer, hard drive, USB Drive, and network speeds. To test a WAN connection, all you have to do is pick a destination on the site where you want to test the WAN connection. Next, the tool will build a file in memory and transfer it both ways— avoiding the misleading effects of Windows or Mac file caching— while keeping track of the time it takes. It then does all the calculations for you.

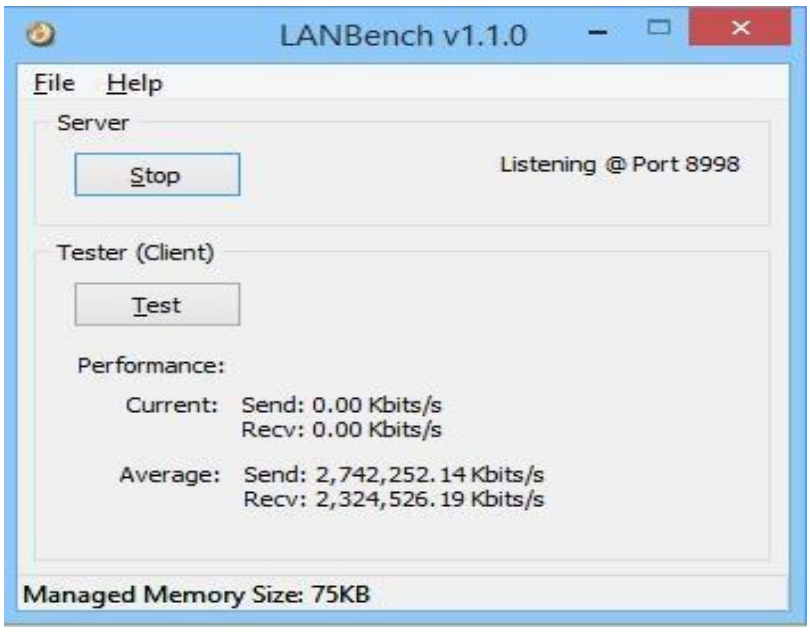
Here are free network benchmarking tools that can be used to test your network speed between computers to make sure the network is running at the speeds you expect.

- **LAN Speed Test (Lite).**



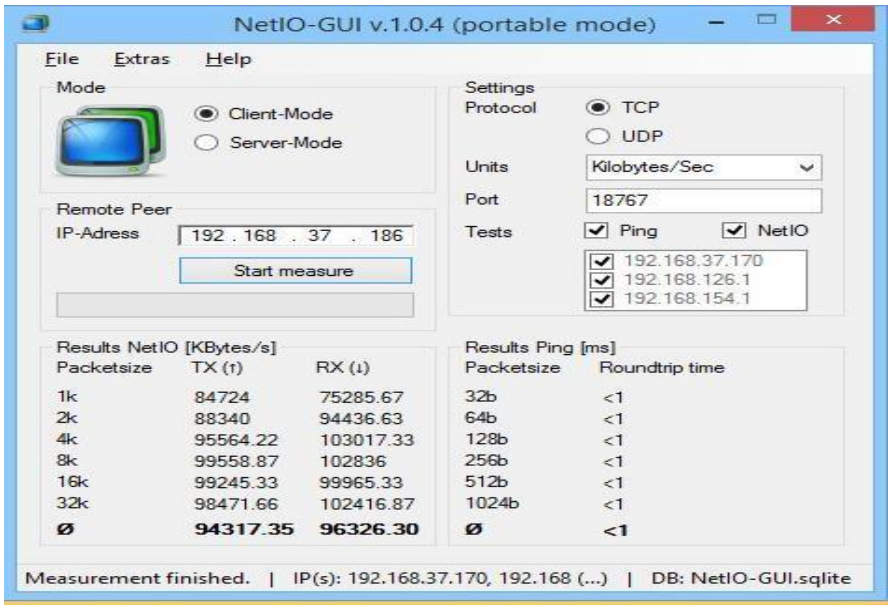
LAN Speed Test was designed from the ground up to be a simple but powerful tool for measuring file transfer, hard drive, USB Drive, and Local Area Network (LAN) speeds (wired & wireless). First, you pick a folder to test to. This folder can be on a local drive or USB drive, etc. to test the drive speed, or a shared folder on your network to test your network speed.

- **LANBench**



LANBench is a simple LAN / TCP Network benchmark utility. It is designed for testing network performance between two computers and is based on Winsock 2.2. LANBench tests TCP performance only and is designed for minimal CPU usage so that the pure performance of your network could be fully tested.

❖ **NetIO-GUI**



NetIO-GUI is a Windows frontend for the multiplatform command line utility 'netio'. It measures ICMP respond times and network transfer rates for different packet sizes and protocols. All results are stored in a SQLite database file and can easily be compared. NetIOGUI is preferred to rate the quality of peer-to-peer connections like VPN.

There are **other WAN Testing tools,** such as **HELIOS LanTest**, and **Tamosoft Throughput Test** works on both windows and macOS, **NetStress** and **PassMark Advanced Network Test** work on Windows, and **iperf** works on MacOS and Linux.

Theoretical learning Activity

In group of 2-3 members, discuss on the following task:

a. Testing WAN
   - Testing WAN connections
   - Testing WAN speed

Points to Remember (Take home message)

When testing WAN connections, consider the following:

- Bandwidth
- Latency
- Network congestion

Three network benchmarking tools that can be used to test your network speed.

- LAN Speed Test (Lite).
- LANBench
- NetIO-GUI

Learning outcome 2.2 formative assessment

Written assessment

1. Enlarge the following network protocols
   a. LAPB
   b. GPON
   c. VDSL
   d. FTTP
   e. L2TP
2. Enumerate the things to consider while testing WAN connections.
3. Suggest three network benchmarking tools that can be used to test your network speed.

ANSWERS:

1. Enlarge the following network protocols
   a. LAPB: Link Access Procedure, Balanced
   b. GPON: Gigabit-capable Passive Optical Networks
   c. **VDSL:** Very high bit rate digital subscriber loop
   d. FTTP: Fiber to The Premises
   e. L2TP: Layer 2 Tunnelling Protocol
2. The things to consider while testing WAN connections.
   - **Bandwidth**
   - **Latency**
   - **Network congestion**
3. Three network benchmarking tools that can be used to test your network speed.
   - **LAN Speed Test (Lite).**
   - **LANBench**
   - **NetIO-GUI**

Practical assessment

Integrated situation

Design the network of three WAN Links, and three LANs. Configure the routing protocol of your choice. The IP address will be assigned to the client devices dynamically and statically. Configure Frame-Relay to encapsulate the packet transferred across WAN link.

Checklist

Criteria	**Yes**	**No**
✓ Dynamic IP Configured successfully		
✓ Static IP Configured successfully		
✓ Frame-Relay is configured correctly		

Learning outcome 2.3 Configure and Verify a site to site VPN

Duration: 9hrs

Learning outcome 2.3 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Classify correctly VPN Network
2. Configure VPN network properly
3. Verify properly VPN Network

Resources

Equipment	Tools	Materials
Computer	Handout notes	Internet Bundles
Projector	Simulator	Video aid
Black/White board	Books	Chalks
Switch	Console cable	Marker Pens
Router	Reference books	Cables
Modem(CSU/DSU)	Networking Tool Kit	
Communication Server		

Advance preparation:

- Sample videos representing VPN Network

Indicative content 2.3.1: Configuration of VPN

There are different methods to configure a VPN. Each device has its own steps differ from another:

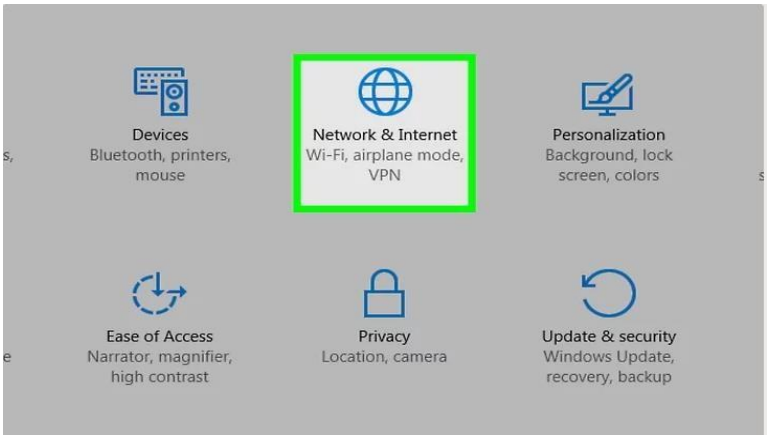
- Setting up a VPN App
- Adding a VPN Connection on Windows
- Adding a VPN Connection on Mac
- Adding a VPN Connection on iPhone
- Adding a VPN Connection on Android

Adding a VPN Connection on Windows 10.

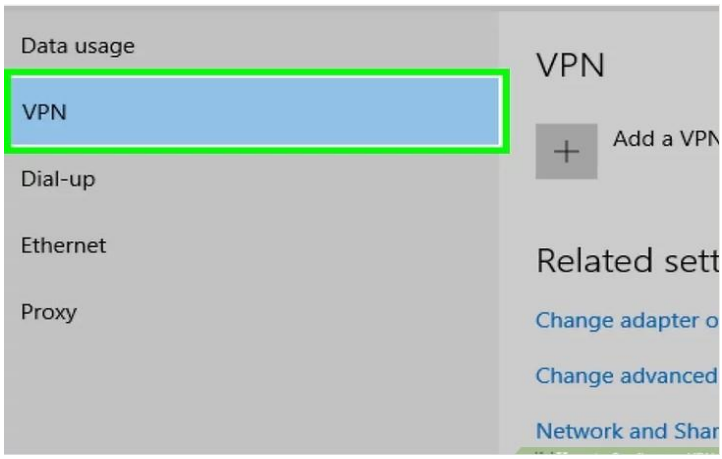
Step 1. Open Start Click the Windows logo in the bottom-left corner of the screen.

Step 2. **Open Settings** Click the gear-shaped icon in the lower-left side of the Start window.

Step 3. Click **Network & Internet.** It's in the middle of the Settings window

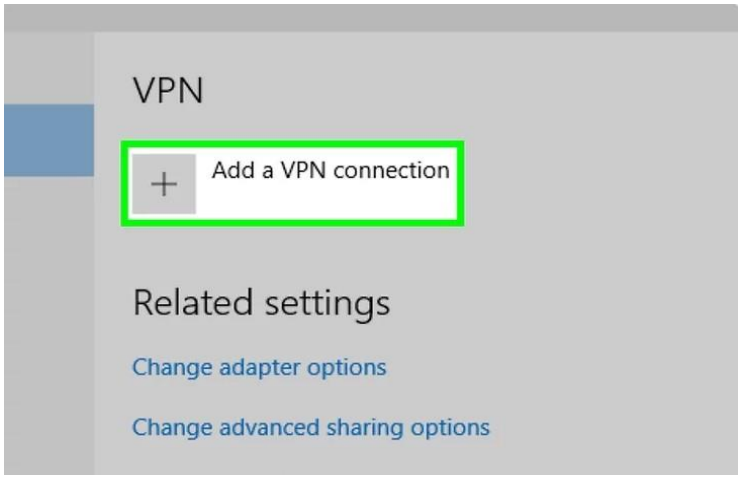


Step 4. Click **VPN.** This tab is on the left side of the Network & Internet menu



Step 5. Click **+ Add a VPN Connection.** It's at the top of the page. A VPN form will open.

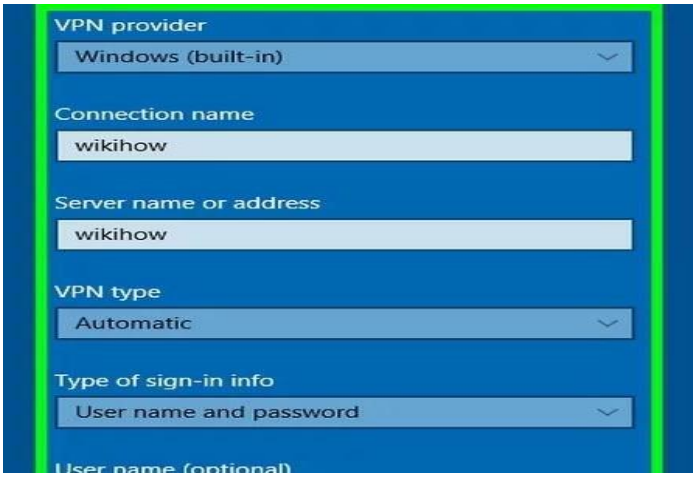
If you want to edit an existing VPN configuration, click the name of the VPN you want to configure, click **Advanced options**, and click **Edit** in the middle of the page



Step 6. Configure your VPN's information. Enter or update any of the following information:

- *VPN provider* — Click this drop-down box, then click the name of the VPN you want to use.

- *Connection name* — Add the name of the VPN on your computer.
- *Server name or address* — Enter or change the VPN's server address.
- *VPN type* — Enter or change the connection type.
- *Type of sign-in info* — Select a new type of sign-in (e.g., **Password**) if necessary.
- *User name (optional)* — If necessary, change the username that you use to sign into the VPN.
- *Password (optional)* — If necessary, change the password that you use to sign into the VPN.



Step 7. Click **Save.** It's at the bottom of the page. Doing so will save your changes to the VPN and apply them.

Practical learning Activity

In group of two members, do the following task:

a. Add VPN network to your computer with the following criteria:
   i. Connection Name will be VPNL5NET
   ii. Server address 172.16.0.1
   iii. Set username as VPNTEST and password as V1p@n;3#

Checklist

Criteria	Yes	No
✓ VPN created successfully		
✓ The name of VPN set correctly		
✓ Sever address configured correctly		
✓ Username and Password Set correctly		

Points to Remember (Take home message)

There are different methods to configure a VPN. Each device has its own steps differ from another:

- Setting up a VPN App
- Adding a VPN Connection on Windows
- Adding a VPN Connection on Mac
- Adding a VPN Connection on iPhone
- Adding a VPN Connection on Android

Indicative content 2.3.2: Classifications of VPN

1. **Deployment classification**

- **Site to Site VPN**
  - A **site-to-site VPN** connection lets branch offices use the internet as a conduit for accessing the main office's intranet. How Stuff Works. A **site-to-site VPN** allows offices in multiple fixed locations to establish secure connections with each other over a public network such as the internet.
  - Remote access VPN allows a user to connect to a private network and access its services and resources remotely. The connection between the user and the private network happens through the Internet and the connection is secure and private.
  - Remote Access VPN is useful for business users as well as home users.
  - A corporate employee, while traveling, uses a VPN to connect to his/her company's private network and remotely access files and resources on the private network.
  - Home users, or private users of VPN, primarily use VPN services to bypass regional restrictions on the Internet and access blocked websites. Users conscious of Internet security also use VPN services to enhance their Internet security and privacy.
- **Remote Access VPN**
  - A **remote-access VPN** connection allows an individual user to connect to a private network from a **remote** location using a laptop or desktop computer connected to the internet.
  - A Site-to-Site VPN is also called as Router-to-Router VPN and is mostly used in the corporates.
  - Companies, with offices in different geographical locations, use Site-to-site VPN to connect the network of one office location to the network at another office location.
  - When multiple offices of the same company are connected using Site-to-Site VPN type, it is called as Intranet based VPN.

- When companies use Site-to-site VPN type to connect to the office of another company, it is called as Extranet based VPN.
- Basically, Site-to-site VPN create a virtual bridge between the networks at geographically distant offices and connect them through the Internet and maintain a secure and private communication between the networks.

2. Classification based on OSI layers

- **Layer 4/7 VPN – WebVPN:**

Layer 4-7. The two **layers** in a network packet that identify its content (for details about **layers**, see TCP/IP and OSI model). The bottom **layers** 1, 2 and 3 are the protocols that move a network packet from source to destination. Layers 4 and 7 identify the application that created the packets as well as the specifics of the request. For example, inspecting layer 4 can identify HTTP traffic (Web traffic), but inspecting layer 7 can determine what the HTTP request is for.

- **Layer 3 VPN – IPSec**:

Layer 3 VPN (L3VPN) is a type of **VPN** mode that is built and delivered on OSI **layer 3** networking technologies. The entire communication from the core **VPN** infrastructure is forwarded using **layer 3** virtual routing and forwarding techniques. **Layer 3 VPN** is also known as virtual private routed network (VPRN).

- **Layer 2 VPN - L2TP, PPTP:**

Layer Two Tunnelling Protocol (**L2TP**) is an extension of the Point-to-Point Tunnelling Protocol (**PPTP**) used by an Internet service provider (ISP) to enable the operation of a virtual private network (**VPN**) over the Internet.

3. Classification based on trust level

- **Intranet VPN**

An **intranet VPN** links enterprise customer headquarters, remote offices, and branch offices to an internal network over a shared infrastructure using dedicated connections. **Intranet VPNs** differ from extranet **VPNs** in that they only allow access to the enterprise customer's employees.

- **Extranet VPN**

Extranet VPNs link customers, suppliers, partners, or communities of interest to a corporate intranet over a shared infrastructure using dedicated connections. In this example, the **VPN** is often an alternative to fax, snail mail, or EDI. The **extranet VPN** facilitates e-commerce.

- **Remote VPN**

A **remote**-access **VPN** connection allows an individual user to connect to a private network from a **remote** location using a laptop or desktop computer connected to the internet. ... Those users can access the secure resources on that network as if they were directly plugged in to the network's servers.

4. Customer point of view classifications:

Small companies taking the **customers**' **point of view** are **customer**-focused. That means they keep the **customer** in mind when developing their products and services. Marketers also make it easier or more convenient for **customers** to order

5. Traditional VPN:

Traditional VPN solution uses a local **VPN** router to connect through the internet, with a secure **VPN** tunnel to a second remote **VPN** router or software client (Fig. ... There is no cloud server between the two devices with either method of connection: **VPN** router to **VPN** router, or **VPN** router to **VPN** software.

The following protocols are used in traditional VPN:

- **Frame-relay (L2 VPN):**

The **Frame Relay** over L2TPv3 feature enables **Frame Relay** switching over **Layer 2 Tunnel** Protocol Version 3 (L2TPv3).

- **ATM VPN (L2 VPN):**

A L2 VPN is a method that Internet service providers use to segregate their network for their customers, to allow them to transmit data over an IP network. Implementing a **Layer 2 VPN** on a router is similar to implementing a **VPN** using a **Layer 2** technology such as Asynchronous Transfer Mode (**ATM**)

6. <u>CPE based VPN</u>

CPE-**Based** IP **VPN** is an IP **VPN** that initiates IPSec tunneling and encryption at the edge of the customer's network for dedicated locations and on the remote user's PC for remote access users.It uses the following protocols on layer 2-3.

- **L2TP and PPTP (Layer 2 VPN**

The Point-to-Point Tunneling Protocol is an obsolete method for implementing virtual private networks. PPTP has many well-known security issues. PPTP uses a TCP control channel and a Generic Routing Encapsulation tunnel to encapsulate PPP packets.

- **IPSec VPN (Layer 3 VPN)**

Internet Protocol Security is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks.

7. <u>Provider Provisioned VPN</u>

Provider Provisioned Virtual Private Networks (PPVPNs) are enterprise-level **VPNs** mainly used by businesses to allow staff secure remote access to their corporate network. PPVPNs

are also used to securely connect physically separate sites and networks with each other across the Internet. They use the following protocol on layer 2-3.

- **BGP/MPLS (L2/L3 VPN):**

Border Gateway Protocol (BGP) is the routing protocol for the Internet. Much like the post office processing mail, **BGP** picks the most effecient routes for delivering Internet traffic. ... Border Gateway Protocol (**BGP**) is the postal service of the Internet.

And **Multiprotocol Label Switching (MPLS):** It is a mechanism for routing traffic within a telecommunications network, as data travels from one network node to the next. **MPLS** can provide applications including VPNs (Virtual Private Networks), traffic engineering (TE) and Quality of Service (QoS).

8. Session based VPN:

In a **session**-level **VPN**, the end-to-end TCP connection can be split into two connections, one over the wireline network and one over the wireless network. ... IP **VPNs** on the other hand, do not allow for split TCP solutions since encryption is carried out at the network layer, making TCP optimizations infeasible. The protocol we use is:

- SSLVPN/WebVPN (L4/L7 VPN)

An **SSL VPN** is a type of virtual private network that uses the Secure Sockets Layer protocol -- or, more often, its successor, the Transport Layer Security (TLS) protocol -- in standard web browsers to provide secure, remote-access VPN capability. SSL VPN is often called Web VPN.

 **Theoretical learning Activity**

In group of 2-3 members, discuss on the following task:

a. Site to Site VPN Vs Remote Access VPN
b. Intranet VPN Vs Extranet VPN
c. Traditional VPN

 **Points to Remember (Take home message)**

- **Deployment classification**
- Site to Site VPN
- Remote Access VPN
- **Classification based on OSI layers**
- Layer 4/7 VPN -WebVPN
- Layer 3 VPN - IPSec
- Layer 2 VPN - L2TP, PPTP

- **Classification based on trust level**
- Intranet VPN
- Extranet VPN
- Remote VPN
- **Traditional VPN**
- Frame-relay (L2 VPN)
- ATM VPN (L2 VPN)
- **CPE based VPN**
- L2TP and PPTP (Layer 2 VPN)
- IPSec VPN (Layer 3 VPN)

Indicative content 2.2.3: VPN Verfication

1. **How to check if VPN is working**

How do you know whether your VPN is doing its job? You may think your VPN is working even while it leaks your identity and location. Leaks (= accidentally lose or admit contents, especially liquid or gas, through a hole or crack.) can be hard to spot, so use these tips to see if your VPN is really protecting you.

The most common VPN leaks

There are many reasons why your VPN might not be providing 100% security and exposing your private information. Here are the most common ways that your VPN could be leaking:

- **IP leak**

Your IP address says a lot about you, like your location or the websites you visit. A VPN protects you from snoopers trying to access this information, so if your original IP leaks it defeats the purpose of using a VPN. This usually happens due to two internet protocols, IPv4 and IPv6 and their incompatibility.

- **DNS leak**

Sometimes your IP might stay hidden while your DNS address secretly reveals your location. The DNS server changes plain text URLs into numerical IP addresses. If you're not using a VPN, this process is handled by your ISP and their servers, which can see who visited what websites. If your DNS leaks, then anyone snooping on your traffic will be able to access this information too. It could even lead to a DNS hijacking attack.

- **WebRTC leak**

Web Real-Time Communication (WebRTC) is built into most popular browsers (i.e., Firefox, Opera, Chrome, and Brave). It enables real-time communications such as voice and video chat, but it also presents another vulnerability for VPN users.

Some websites can take advantage of WebRTC by inserting a few lines of code to see past your VPN and discover your original IP. This is very useful for websites that provide or block content based on your geo-location.

It's possible to prevent these leaks, but first, you have to identify them. You can do so by running some basic tests that anyone can do. **WebRTC is a free, open-source project that provides web browsers and mobile applications with real-time communication via simple application programming interfaces.**

How to check for IP and/or DNS leaks

- You need to find out your original IP address given by your ISP.
- Make a note of your real IP address.
- Turn on your VPN and go back to the test website.
- It should now show a different IP address and the country you connected your VPN to. If the results show your original IP address, then, unfortunately, your VPN is leaking.
- Sometimes IPLeak tests fail to detect DNS leaks, which can also reveal your identity. So it's advisable to check it on DNSLeakTest.
- If your VPN is on, DNSLeakTest should show the location you've chosen and your new IP.
- Select Extended Test to dig even deeper. This test might take a few minutes.
- If the results now show your new IP address and your chosen country, you are safe. Your VPN isn't leaking.

What to do if your IP and/or DNS is leaking

The easiest way is to change your VPN provider to one that has dedicated DNS Servers or offers DNS leak protection, like NordVPN. Or you could manually turn IPv6 off on your device. However, this might require some technical know-how.

How to check for WebRTC leaks (Web Real-Time Communication**)**

- If you haven't already, find out your original IP address on the IPLeak website. Make a note of it.
- Connect to your VPN and refresh the webpage (or go to its alternative dedicated to WebRTC Testing). It should now show your new IP address and new location based on the country you've chosen.
- Under 'Your IP addresses – WebRTC detection' you should see a private IP that should be different from your original public IP address. Note that the website showing your private IP (usually begins with 10.xxx or 192.xxx or sometimes an alpha-numeric IPv6) doesn't mean that your WebRTC is leaking.

What to do if your WebRTC is leaking

This time, changing your VPN or tinkering with your settings won't help. However, you can:

- Use a browser that doesn't have WebRTC. You can find the full list of browsers that exclude it on Wikipedia.
- Disable WebRTC by following these tips.
- Install browser extensions:

Eg: on Chrome: Install WebRTC Network Limiter.

My VPN is still not working

However, checking for various leaks might not be enough. There are other reasons why it might seem that your VPN isn't working, for example:

- **Your browsing speed has dropped.** This might happen for several reasons. For example, you've chosen a server which is on the other side of the world, the server is overloaded, or your ISP is throttling bandwidth. However, you can check your VPN speed and increase it with a few simple tricks.
- **Your ISP or your country is blocking VPN usage**. In some countries, especially with online censorship, VPN usage can be blocked or considered illegal. In China, for example, only government-approved VPNs are legal.
- **Your VPN connection has dropped**. Most VPNs offer an automatic kill switch (including NordVPN), which means that if your VPN connection drops, it will terminate your internet connection (application-level kill switches will only terminate individual programs). The kill switch makes sure that you don't access the internet outside of the encrypted VPN tunnel and that your personal information isn't exposed if the connection drops. If your VPN connection dropped and activated your system-level kill switch, you will not be able to access the internet until you connect back to a VPN server.
- **VPN malware**. Technology experts would never recommend using a free VPN. Not only do most contain annoying ads, some actually contain malware. If you are using a free VPN, you might already be exposing more personal information than you wanted to.
- **You've been hacked**. You might think that your VPN isn't working because someone has broken into it. In reality, it's pretty difficult to do so. It's more likely that you've visited a malicious website or fell for a phishing attack and someone has taken control of your device. Unfortunately, if someone hacks you, a VPN can't do much to protect you.

2. **Test the VPN tunnel**

To verify that your **VPN tunnel** is working properly, it is necessary to ping the IP address of a computer on the remote network. By pinging the remote network, you send data packets to the remote network and the remote network replies that it has received the data packets.

3. **Test network connectivity**

Ping is a **network** administration utility or tool used to **test connectivity** on an Internet Protocol (IP) **network**. It also measures the latency or delay between two computers. To **test network connectivity** with ping: Open the Command Prompt or Terminal.

4. **Test application connectivity**

Before sending requests to Universal API, a ping request is recommended to ensure that there is proper network **connectivity** and **application** operability.

5. **Verify that you can access a file server on the private network**

There are many ways to make files available over the Internet. The real challenge here is finding a secure, easy-to-use solution.

We recommend TeamViewer as the ideal solution for remotely accessing a PC, whether you're accessing your own PC or performing remote tech support. TeamViewer is most often used to
remotely access a PC's desktop. However, it also has a remote file transfer feature you might not have noticed. Just select the File transfer option when connecting to a remote PC.Another way is to already have an SSH server running on your local network, you can use SSH tunneling to access local network resources rather than setting up a VPN.

6. **Test and Verify IKE Configuration**

IKEv2 stands for Internet key exchange version two, and **IPSec** refers to the Internet protocol security suite. ... **IKEv2/IPSec** uses a Diffie–Hellman key exchange, has no known vulnerabilities, allows Perfect Forward Secrecy, and supports fast VPN connections.

Practical learning Activity

In group of 2-3 members, perform the following task:

a. VPN Verification
b. Test the VPN tunnel
c. Test network connectivity
d. Test application connectivity
e. Verify that you can access a file server on the private network
f. Test and Verify IKE Configuration

Checklist

Criteria	**Yes**	**No**
✓ VPN verified		
✓ VPN Tunnel tested		
✓ Network connectivity tested		
✓ Application connectivity tested		
✓ access of a file server on the private network verified		
✓ IKE Configuration verified and tested		

Points to Remember (Take home message)

While testing VPN, you need to perform the following test:

- VPN Verification
- Test the VPN tunnel
- Test network connectivity
- Test application connectivity
- Verify that you can access a file server on the private network
- Test and Verify IKE Configuration

Learning outcome 2.3 formative assessment

Written assessment

Answer the following statements by **True** if the statement is correct, or **False** if the statement is incorrect.

a. A corporate employee, while traveling, uses a VPN to connect to his/her company's private network and remotely access files and resources on the private network. ……
b. A **remote-access VPN** allows offices in multiple fixed locations to establish secure connections with each other over a public network such as the internet. ……
c. A **site-to-site VPN** connection allows an individual user to connect to a private network from a **remote** location using a laptop or desktop computer connected to the internet. ……
d. Adding a VPN Connection on Windows is the same as Adding a VPN Connection on Mac ……
e. An **intranet VPN** links enterprise customer headquarters, remote offices, and branch offices to an internal network over a shared infrastructure using dedicated connections ……
f. Before sending requests to Universal API, an ipconfig/all is recommended to ensure that there is proper network **connectivity** and **application** operability. ……
g. Extra VPN solution uses a local **VPN** router to connect through the internet, with a secure **VPN** tunnel to a second remote **VPN** router or software client. ……
h. PPTP uses a TCP control channel and a Generic Routing Encapsulation tunnel to encapsulate PPP packets. ……

ANSWERS:

a. **True**
b. **False**
c. **False**
d. **False**

e. **True**
f. **False**
g. **False**
h. **True**

Practical assessment

Individually, perform the following tasks:

- Configure VPN
- Test the VPN tunnel
- Test network connectivity
- Test application connectivity
- Verify that you can access a file server on the private network
- Test and Verify IKE Configuration

Checklist:

Criteria	**Yes**	**No**
✓ VPN created successfully		
✓ The name of VPN set correctly		
✓ Sever address configured correctly		
✓ Username and Password Set correctly		
✓ VPN verified		
✓ VPN Tunnel tested		
✓ Network connectivity tested		
✓ Application connectivity tested		
✓ access of a file server on the private network verified		
✓ IKE Configuration verified and tested		

Learning outcome 2.4 Troubleshoot WAN Network

Duration: 4hrs

Learning outcome 2.4 objectives:

By the end of the learning outcome, the trainees will be able to:

1. List correctly the steps for troubleshooting WAN Network.
2. Apply correctly the steps of Troubleshooting WAN Network.

Resources

Equipment	Tools	Materials
Computer	Handout notes	Internet Bundles
Projector	Simulator	Video aid
Black/White board	Books	Chalks
Switch	Console cable	Marker Pens
Router	Reference books	Cables
Modem(CSU/DSU)	Networking Tool Kit	
Communication Server		

Advance preparation:

- Sample videos of troubleshooting WAN Network

Indicative content 2.4.1: Steps for troubleshooting WAN Network

Steps for troubleshooting WAN Networks

- **Use monitoring tools**

Monitoring tools are used to continuously keep track of the status of the system in **use**, in order to have the earliest warning of failures, defects or problems and to improve them. There are **monitoring tools** for servers, networks, databases, security, performance, website and internet usage, and applications.

Network monitoring systems make use of applications to **monitor** the **network** traffic, such as the video stream **monitoring**, Voice over Internet Protocol (VoIP) **monitoring** and mail server (POP3 server) **monitoring**.

- **Monitoring WAN links**

The **WAN monitoring** feature in OpManager monitors the availability of all your **WAN links**, the Round Trip Time (RTT) and the traffic details. Detailed **WAN** performance dashboard reports are provided and you can quickly navigate the dashboard to see the root cause of poor **WAN** availability.

- **Monitoring WAN latency**

Latency. The time it takes in milliseconds for a data packet to travel across the **WAN** link. High **latency** means data travels more slowly across the **network**, which can affect business users. Typically, high **latency** is caused by **network** congestion over the **WAN** link.

- **Check the settings and configurations of the WAN**

WAN settings let you control how Google Wifi connects to the Internet. The type of **WAN** connection you have is generally determined by your Internet Service Provider. In **WAN settings**, you can choose from one of the **WAN** types below and **configure** their respective **settings**: DHCP or Static IP.

- **Restore the configuration of WAN devices to its factory default settings**

If WAN device cannot be accessed from the web interface, the **configuration** can be **restored to factory defaults** by using the **Reset** button. This kind of **reset** clears all **configuration settings**.

- **Troubleshooting of IP configurations issues**

The first step in the **troubleshooting** process is to check the TCP/**IP configuration**. The easiest way to do this is to open a Command Prompt window and enter the IPCONFIG /ALL command. Windows will then display the **configuration** results.

- **Troubleshooting of WAN protocols issues**

If the wide area network connection is working the way it should, you could still have problems with the configuration of the protocols that are going over that wide area network. A good example of this is split horizon. This is a configuration you would set in the dynamic routing protocols that you're using across this wide area network link. This is ideally designed to prevent any type of routing loop on the network.

- **Troubleshooting of WAN connectivity issues**

Easy-to-Do Ways to Troubleshoot Network Connection:

1. Check Your Settings. First, check your Wi-Fi settings.
2. Check Your Access Points. Check your WAN (wide area network) and LAN (local area network) connections.
3. Go Around Obstacles.
4. Restart the Router.
5. Check the Wi-Fi Name and Password.
6. Check DHCP Settings.
7. Update Windows.
8. Open Windows Network Diagnostics.

If you feel that there is some type of hardware problem, the wide area network provider can loopback one of the connections, usually at the interface inside of your environment, and they can test to see what the experience is like sending traffic to your location and having it loopback to the provider. They can then see if they're receiving the same information back and determine if that line is working well or not. Then you can start troubleshooting even further to determine is the problem with an interface inside of our building or cables between the wide area network point of presence and our equipment inside of our location?

- **Troubleshooting of WAN performance issues**

1. **Troubleshoot slow network problems with network traffic analysis**

One of the vaguest issues to land on any Network Administrators desk is users complaining that the network is slow. In most cases, the network is not to blame, instead the user is experiencing issues with a slow application or website. However, more than often it is the responsibility of Network Administrators to troubleshoot slow network issues and prove that it is not the network

2. **Check overall traffic volumes.**

If the user complaints are coming from a remote office, I would check traffic volumes on the link first. We covered this topic in a previous post which looks at ways for generating reports on WAN bandwidth utilization. If the complaints are coming from users on the local LAN, then I would focus on all network activity.

3. **Find out what are the top applications consuming bandwidth.**

Next up, I would check for the most active applications. For most networks, activity like file sharing, web or database activity ranks highest during business hours. If you see something like backup running during the day or large data replications between servers, it can be the source of network slowdowns.

4. **Check for network broadcast issues.**

A broadcast storm can slow down a network within seconds. All it takes is for one rogue device to send out a few hundred megabytes of broadcast data and suddenly your LAN will be saturated with broadcast packets. A quick way to look for this activity is to filter on network packets which have ff:ff:ff:ff:ff:ff as a destination MAC address.

5. **Watch out for excessive connection rates.**

Firewalls and layer 3 devices such as routers, can struggle if connection rates increase significantly on a network. If clients start disconnecting from web sites or services hosted on the other side of routers, it is worth checking this metric.

Theoretical learning Activity

In group of 2-3 members, discuss on the following task:

a. List the steps to go through while troubleshooting WAN Networks.

Points to Remember (Take home message)

Steps for troubleshooting WAN Networks

- Use monitoring tools
- Monitoring WAN links
- Monitoring WAN latency
- Check the settings and configurations of the WAN
- Restore the configuration of WAN devices to its factory default settings
- Troubleshooting of IP configurations issues
- Troubleshooting of WAN protocols issues
- Troubleshooting of WAN connectivity issues
- Troubleshooting of WAN performance issues

Learning outcome 2.4 formative assessment

Written assessment

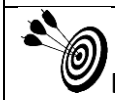
1. Enumerate the steps of troubleshooting WAN Networks.
2. Mention the activities to be done while troubleshooting WAN Performance issues.

ANSWERS:

1. The steps of troubleshooting WAN Networks.
- Use monitoring tools
- Monitoring WAN links
- Monitoring WAN latency
- Check the settings and configurations of the WAN
- Restore the configuration of WAN devices to its factory default settings
- Troubleshooting of IP configurations issues
- Troubleshooting of WAN protocols issues
- Troubleshooting of WAN connectivity issues
- Troubleshooting of WAN performance issues
2. The activities to be done while troubleshooting WAN Performance issues.
- Troubleshoot slow network problems with network traffic analysis
- Check overall traffic volumes.
- Find out what are the top applications consuming bandwidth.
- Check for network broadcast issues.
- Watch out for excessive connection rates.

Learning outcome 2.5 Configure and Verify an ADSL Connection

Duration: 5hrs



Learning outcome 2.5 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Install correctly DSL Network
2. Identify correctly the properties supplied by TCP/IP
3. Verify and troubleshoot DSL Network

Resources

Equipment	Tools	Materials
Computer	Books	Internet
Projector	Handout notes	Video aid
Switch	Reference books	Cables
Router	Simulator	Phone Jack (RJ11)
Modem (CSU/DSU)		
Communication Server		

Advance preparation:

- Sample videos that represent configuration and verification of ADSL Connection.

Indicative content 2.5.1: Installation and verficaion of DSL modem.

- **Hardware Installation for external DSL modem**
  - Connect one end of the DSL modem to the phone jack (RJ11)
  - Connect the other end of the DSL modem to a NIC installed in the computer
  - RJ45 type of connection is often required
  - Connect the power supply to the DSL modem
- **Provide supplied TCP/IP properties**
  - One static IP address
  - Subnet mask
  - Gateway IP address
  - Primary DNS server IP address
  - Secondary DNS server IP address
- **DSL Network Installation**

DSL is a wired transmission that uses traditional copper telephone lines already **installed** to homes and businesses. When you **connect** to the Internet, you might **connect** through a regular modem, through a local-area network **connection** in your office, through a cable modem or through a digital subscriber line (**DSL**) **connection**. **DSL** is a very high-speed **connection** that uses the same wires as a regular telephone line.

First install the Network Interface Card (NIC)

- Adapter
- Protocol (TCP/IP)
- Services (If required)
- Configure the protocol with the settings provided by the ISP

- **Installing on a Computer Already Connected to a LAN**
  - If the computer already is connected to a LAN, an additional NIC need to be installed
  - The second NIC is connected to the DSL modem
  - The TCP/IP protocol will be installed on the additional NIC and configured based on the values provided by the ISP
- **Verification and troubleshooting**
  - Problem with Modem Powering ON
  - Problem with the LAN LED
  - Problem with LAN Interface
  - Problem with the DSL LED
  - Problem with the WAN Interface
  - Problem with the Login Password
  - Problem with WEB Configuration
  - Problem with Internet Browsing
  - Problem with the Wi-Fi Connectivity

Theoretical learning Activity

In group of 2-3 members, discuss on the following task:

a. List the properties provide supplied by TCP/IP
b. Mention the possible problems that may occur in DSL connection

Points to Remember (Take home message)

DSL is a wired transmission that uses traditional copper telephone lines already **installed** to homes and businesses. When you **connect** to the Internet, you might **connect** through a regular modem, through a local-area network **connection** in your office, through a cable modem or through a digital subscriber line (**DSL**) **connection**. **DSL** is a very high-speed **connection** that uses the same wires as a regular telephone line.

Learning outcome 2.5 formative assessment

Written assessment

1. List the properties provide supplied by TCP/IP
2. Mention the possible problems that may occur in DSL connection

ANSWERS:

1. The properties provide supplied by TCP/IP
    - One static IP address
    - Subnet mask
    - Gateway IP address
    - Primary DNS server IP address
    - Secondary DNS server IP address
2. Problems that may occur in DSL connection
    - Problem with Modem Powering ON
    - Problem with the LAN LED
    - Problem with LAN Interface
    - Problem with the DSL LED
    - Problem with the WAN Interface
    - Problem with the Login Password
    - Problem with WEB Configuration
    - Problem with Internet Browsing
    - Problem with the Wi-Fi Connectivity

LEARNING UNIT 3: DOCUMENT THE WORK DONE

STRUCTURE OF LEARNING UNIT

Learning outcomes:

3.1. Accurate documentation and submission of review process

3.2. Documentation of all logs issues and action taken for future reference

Learning outcome 3.1 Accurate documentation and submission of review process

Duration: 15hrs

Learning outcome 3.1 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Define correctly the term technical journal.
2. Define correctly the term network diagram.
3. Identify correctly the importance of network diagram.
4. Identify correctly configuration backups.

Resources

Equipment	Tools	Materials
Routers Switches Computer	Books Handout notes Console cable Serial to USB adapter Simulator	Internet Cables

Advance preparation:

- Two or more samples of technical journal

Indicative content 3.1.1: Technical Journal

❖ **Technical journal**

Technical journal is a multidisciplinary **journal** in the field of engineering science and technology that offers platform for researchers, engineers and scientists to publish their original and to date research of high scientific value. ... The **journal** is being published electronically as well as in print form.

- **Network diagram**

A **network diagram** is a visual representation of a computer or telecommunications **network**. It shows the components that make up a **network** and how they interact, including routers, devices, hubs, firewalls, etc.

Importance and benefits of network diagrams

- **Network Diagrams** aid in planning, organizing and controlling. Since all project activities are shown in sequence with **relevant** interrelationships, the **network diagram** of a project will help the project manager and team during planning and organizing.
- **Network Diagrams help justify your time estimate for the project**. Since network diagram of a project shows how activities are interrelated with each other from the beginning of the project till the end, it will be very beneficial for calculating the overall project duration. After the critical path of the project is determined, activities on the critical path will give us the total duration of the project respectively.
- **Network diagrams show interdependencies of activities**. Since interdependencies of activities are visible in the network diagram, it will be easier to see which activity can start after which one, which activity depends on each other, predecessors and successors of each activity etc.
- **Network Diagrams show workflow of the project activities**. So the project team will know the sequence of activities. At a certain point in the project, it will be easier to see in the network diagram what has been accomplished and the remaining activities and their interdependencies with each other.
- **Network diagrams identify opportunities to compress the schedule**. You may need to shorten the duration of the remaining activities in a project. This can be because your project is behind schedule and in order to complete the project on time, you need to compress the schedule. In this case, since network diagrams show the order of the activities and durations, it will be easier to focus on how to compress the remaining activities in the project.
- **Network diagrams show project progress**. Since it shows the order of activities in a project and total path from the beginning of the project till the end, it is a good instrument for showing the project progress.

So these 6 benefits of using a network diagram show that, in Time management, estimating the project duration, knowing the interdependencies between the activities, being able to see the workflow are really important. Furthermore, a network diagram can help the project team and the project manager to see the opportunities to shorten the duration of the project and also see the progress in general.

Here is our list of the best network diagram, mapping and topology tools:

- SolarWinds Network Topology Mapper
- Paessler PRTG Network Mapping Tools
- ConceptDraw Pro
- Lucidchart
- Intermapper
- CADE
- Dia
- eDraw
- LanFlow
- NetProbe
- Network Notepad
- Microsoft Visio
- Ipswitch WhatsUp Gold
- GoVisual Diagram Editor

- **Configuration backup**

Configuration backup is the process of extracting configuration settings from a system and writing it to disk. You must back up your application data by using the appropriate backup methods. To enable routine maintenance, the configuration settings for each system are stored on each node.

- **IOS**

IOS (iPhone Operating System) is a mobile operating system created and developed by Apple Inc. exclusively for its hardware. It is the operating system that presently powers many of the company's mobile devices, including the iPhone, and iPod Touch.

- **Configurations**

A configuration of a system refers to the arrangement of each of its functional units, according to their nature, number and chief characteristics.

 **Theoretical learning Activity**

In group of 2-3 members, discuss on the following task:

1. Define the following terms:
   a. Technical journal
   b. Network diagram
2. Identify the importance of network diagram.

Points to Remember (Take home message)

Importance and benefits of network diagrams

- Network Diagrams aid in planning, organizing and controlling.
- Network Diagrams help justify your time estimate for the project.
- Network diagrams show interdependencies of activities.
- Network Diagrams show workflow of the project activities.
- Network diagrams identify opportunities to compress the schedule
- Network diagrams show project progress.

Learning outcome 3.1 formative assessment

Written assessment

Answer the following statements by **True** if the statement is correct, or **False** if the statement is incorrect.

1. A configuration of a system refers to the arrangement of each of its functional units, according to their nature, number and chief characteristics. ……
2. A **network diagram** is a visual representation of a computer or telecommunications **network**. ……
3. IOS, CADE and DIA are **network diagram, mapping and topology tools.** ……
4. Network diagram can help the project team and the project manager to see the opportunities to shorten the duration of the project and also see the progress in general. ……
5. **Network Diagrams** aid only in planning, organizing. ……
6. **Network diagrams show dependencies of activities.** ……
7. **Technical journal** offers a platform for researchers, engineers and scientists to publish their original and to date research of high scientific value. ……
8. **Technical journal** shows the components that make up a **network** and how they interact, including routers, devices, hubs, firewalls. ……
9. The process of extracting configuration settings from a system and writing it to disk is called Configuration backup. ……

ANSWERS:

1. True, 2. True, 3. False, 4. True, 5. False, 6. False, 7. True, 8. False, 9. True

Learning outcome 3.2 Documentation of all logs issues and cation taken for future reference

Duration: 10hrs

Learning outcome 3.2 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Define correctly the term report.
2. List correctly the advantages of writing report.
3. Identify correctly logs issues

Resources

Equipment	Tools	Materials
PC	Books Handout notes	Internet

Advance preparation:

- Two or more samples of reports.

Indicative content 3.2.1: Report

- **Report**

A report is a document that presents information in an organized format for a specific audience and purpose. Although summaries of reports may be delivered orally, complete reports are almost always in the form of written documents.

What are the main advantages of report writing?

1. **Report gives consolidated and updated information.**

A report provides consolidated, factual and an up-to-date information about a particular matter or subject. Information in the report is well organized and can be used for future planning and decision making.

2. **Report as a means of internal communication.**

A report acts as an effective means of communication within the organization. It provides feedback to employees. It is prepared for the information and guidance of others connected with the matter/ problem.

3. **Report facilitates decision making and planning**

Report provide reliable data which can be used in the planning and decision making process. It acts as a treasure house of reliable information for long term planning and decision making.

4. **Report discloses unknown information**

Reports provide information, which may not be known previously. The committee members collect data, draw conclusions and provide information which will be new to all concerned parties. Even new business opportunities are visible through unknown information available in the reports.

4. **Report gives Information to employees**

Reports are available to managers and departments for internal use. They are widely used by the departments for guidance. Report provide a feedback to employees and are useful for their self-improvement.

5. **Report gives reliable permanent information**

The information provided by a report is a permanent addition to the information available to the office. We have census reports (prepared since last 100 years) which are used even today for reference purpose.

6. **Report facilitates framing of personnel policies**

Certain reports relating to employees are useful while preparing personnel policies such as promotion policy, training policy and welfare facilities to employees.

7. **Report gives information to shareholders**

Some company reports are prepared every year for the benefit of shareholders. Annual report for example, is prepared and sent to all shareholders before the AGM. It gives information about the progress of the company.

8. **Report gives information to the Registrar**

Annual report and annual accounts are sent to the Registrar every year for information. Such reports enable the government to keep supervision on the companies.

9. **Report solves current problems**

Reports are useful to managers while dealing with current problems faced by the company. They provide guidance while dealing with complicated problems.

10. **Report helps directors to take prompt decisions**

Company reports relate to internal working of the company and are extremely useful to directors in decision making and policy framing. Reports give reliable, updated and useful information in a compact form.

- **Logs issues**

An issue log is a documentation element of software project management that contains a list of ongoing and closed issues of the project. While issue logs can be viewed as a way to track errors in the project, the role it plays often extends further.

What are the benefits of keeping a log of all transactions that occur on your network and reviewing them?

From a security point of view, the purpose of a **log** is to act as a red flag when something bad is happening. **Reviewing logs** regularly could help identify malicious attacks on **your** system. Given the large of amount of **log** data generated by systems, **it** is impractical to **review all** of **these logs** manually each day.

- **Solution implementation**

Solution Implementation involves the identification, adaptation, and **implementation** of new and enhanced future-proof business and technical scenarios. It is designed to separate technical installation from business innovation and uses SAP **Solution** Manager to **implement** innovation within the system landscape.

- **Description of materials used**

Here you describe all **materials** and equipment to be **used**, whether or not shown on.
In this part of report, there is a list of the Equipment, materials and tools.
This part also, it contains the details or description of each material used during implementing connections to remote site.

Theoretical learning Activity

In group of 2-3 members, Discuss about the following task:

1. Define correctly the term report.
2. List correctly the advantages of writing report.
3. Identify correctly logs issues

Points to Remember (Take home message)

The main advantages of report writing:

- Report gives consolidated and updated information.
- Report as a means of internal communication.
- Report facilitates decision making and planning
- Report discloses unknown information
- Report gives Information to employees
- Report gives reliable permanent information
- Report facilitates framing of personnel policies
- Report gives information to shareholders
- Report gives information to the Registrar
- Report solves current problems
- Report helps directors to take prompt decisions

Learning outcome 3.2 formative assessment

Written assessment

Answer the following statements by **True** if the statement is correct, or **False** if the statement is incorrect.

1. A report is a document that presents information in an organized format for a specific audience and purpose. ……
2. A report is prepared for the information and guidance of others connected with the matter/ problem. ……
3. A report provides consolidated, factual and an up-to-date information about a particular matter or subject. ……
4. An issue log is a documentation element of software project management that contains a list of ongoing and closed issues of the project. ……
5. Report provide negative feedback to employees and are not necessary for their self-improvement. ……
6. Reports are useful to managers while dealing with current problems faced by themselves. ……
7. Reports provide information, which are known previously. ……
8. Reviewing logs regularly could help identify malicious attacks on the other's system. ……

ANSWERS:

1. True
2. True
3. True
4. True
5. False
6. False
7. False
8. False

SUMMATIVE ASSESSMENT

Integrated situation	Resources
Company ABC has two locations; one is in NYARUGENGE District and the other in MUHANGA District. Enabling all team members from the two locations to collaborate on the same data set, file sharing and centralized storage is a problem. The company wants the two locations to be able to communicate with one another without using the Internet. As the network administrator, you are requested to choose a WAN technology that connects these two LANs together, basing your decision on the performance and the cost of the technology. Given Public IP address 10.10.10.5/25, a DNS server 2.4.2.4, you are also requested to install and configure the appropriate devices and equipment so that the two remote offices can communicate by sharing resources. The above works are intended to be done in 3 hours.	✓ Routers ✓ Switches ✓ CPE ✓ Computer ✓ Cables ✓ Simulator (Packet tracer) ✓ Console cable ✓ Serial to USB adapter ✓ Modem(CSU/DSU) ✓ Communication Server ✓ Phone Jack (RJ11) ✓ Networking toolkit

Checklist

Assessment Criteria		Indicator	Score	
			Yes	No
1. Quality of Process	1.1. Analyze network requirements is done	Network architectures		
		Network applications		
		Network protocols		
	1.2. Analyze Enterprise facilities, existing WIFI &WIRED networks and sites is done	Network Analysis		
		Physical Design		
		Logical Design		
		Wired network technologies		
		Wireless network technologies		
		Networks devices		
	1.3 Identify Security requirements is done	Requirements for Secure Remote Access		
	1.4 Selection of WAN technology, hardware and software components is done	LAN technologies		
		MAN technologies		
		WAN technologies		
		Network hardware and software specifications		
	1.5 Appropriate identification of tools, equipment and materials used in Remote is done	Remote connection tools		
		Equipment		
		Resources		
		Network design principles		

	1.6 Systematic design and interpretation of network blueprint is done	Network design Tools		
	1.7 Configure and verify a serial WAN configuration is done	WAN Devices		
		WAN connections types		
		Physical Parameters for WAN Connections		
	1.8 Configure and verify WAN Protocols is done	Configuration of IP parameters		
		Testing WAN		
		WAN protocols and technologies		
	1.9 Configure and verify a site to site VPN is done	Configuration of VPN based		
	1.10 Monitor WAN using monitoring software is done	Monitoring WAN links		
		Monitoring WAN latency		
		Troubleshooting WAN issues		
	1.11 Restore the configuration of WAN devices to its factory default settings	Troubleshooting of the web-based configuration page issues		
		Troubleshooting of IP configurations issues		
		Troubleshooting of WAN protocols issues		
		Troubleshooting of WAN connectivity issues		
		Troubleshooting of WAN performance issues		
	1.12 Configure and verify an ADSL connection is done	Hardware Installation for external DSL modem		
		Provide supplied TCP/IP properties		
		DSL Network Installation		
	1.13 Installing on a Computer Already Connected to a LAN	Verification and troubleshooting		
	1.14 Accurate documentation and submission of review process is done	Backup configuration		
	1.15 Documentation of all logs issues and action taken for future reference is done	Produce a report		
		Appropriate personnel		
	2.1 The Routers and Switches are secured	Username and Passwords are set		
		Log in Banners		

2. Quality of product	**2.2 WAN are Communicate**	Easy addition of users		
	2.3 remote site is well done	Two location communicate		
	2.4 remote is accessible	WAN remote/connected		
3. Relevance	**3.1 Time is respected**	Time required (4hrs)		
	3.2 Materials and equipment are well used	No wasted materials		
	3.3 The report is produced	Report format		
		Report content		

REFERENCES

- ICTNEW5001-TVET CERTIFICATE V in Networking REQF Level 5 CURRICULUM
- Jennifer H. (February, 2023). What Is a Peer-to-Peer (P2P) Network? (With Examples). Retrieved from URL: https://www.indeed.com/career-advice/career-development/what-is-a-peer-to-peer-network, Accessed on April 10, 2023
- Konstantin. (n.d). What's the difference between peer-to-peer (P2P) networks and client-server? Retrieved from URL: https://www.resilio.com/blog/whats-the-difference-between-peer-to-peer-and-client-server. Accessed on April 10, 2023
- Benjamin P. (December, 2017). **Network Applications.** Retrieved from URL: https://silo.tips/download/network-applications, Accessed on April 10, 2023
- Jon W. (August , 2022). What is Fibre Channel Protocol? Retrieved from URL: https://www.cbtnuggets.com/blog/technology/networking/what-is-fibre-channel-protocol, Accessed on April 10, 2023
- Oracle. (n.d). Introducing the TCP/IP Protocol Suite. Retrieved from URL: https://docs.oracle.com/cd/E18752_01/html/816-4554/ipov-6.html, Accessed on April 10, 2023
- Jomile N. (Dec 2022). The best VPN protocols. Retrieved from URL: https://nordvpn.com/blog/protocols/#:~:text=A%20VPN%20protocol%20is%20a,device%20a%20new%20IP%20address. Accessed on April 10, 2023
- Katie T. (n.d). ADSL (Asymmetric Digital Subscriber Line). Retrieved from URL: https://www.techtarget.com/searchnetworking/definition/ADSL#:~:text=ADSL%20(Asymmetric%20Digital%20Subscriber%20Line)%20is%20a%20technology%20that%20facilitates,%2C%20always%2Don%20broadband%20connections. Accessed on April 10, 2023
- Jennifer E. (n.d). 9 steps for wireless network planning and design. Retrieved from URL: https://www.techtarget.com/searchnetworking/feature/How-to-tackle-wireless-network-planning-in-9-steps, Accessed on April 10, 2023
- Docplayer (n.d). 7 Key Requirements for Secure Remote Access. Retrieved from URL: https://docplayer.net/8357604-7-key-requirements-for-secure-remote-access.html, Accessed on April 10, 2023
- Cisco P. (Nov 30, 2017). WAN Concepts. Retrieved from URL: https://www.ciscopress.com/articles/article.asp?p=2832405&seqNum=5, Accessed on April 10, 2023
- Cisco P. (Nov 30, 2002). VPNs and VPN Technologies. Retrieved from URL: https://www.ciscopress.com/articles/article.asp?p=24833, Accessed on April 10, 2023
- Mary B. (April 8, 2023). Telnet vs SSH – Difference Between Them. Retrieved from URL: https://www.guru99.com/telnet-vs-ssh.html, Accessed on April 12, 2023
- Colmac L. (n.d). IP network design, part 1: Fundamental principles. Retrieved from URL:
- https://www.techtarget.com/searchnetworking/tip/IP-network-design-part-1-Fundamental-principles, Accessed on April 12, 2023

- Tim K. (June, 2018). 14 Best Network Diagram, Mapping and Topology Tools. Retrieved from URL: https://www.itprc.com/best-network-diagram-mapping-and-topology-tools/, Accessed on April 12, 2023
- Chiradeep B. (August, 2022). Packet-Switched Network vs. Circuit-Switched Network: Understanding the 15 Key Differences. Retrieved from URL: https://www.spiceworks.com/tech/networking/articles/packet-switched-vs-circuit-switched-network/, Accessed on April 12, 2023
- Katie T. (n.d). customer premises equipment (CPE). Retrieved from URL: https://www.techtarget.com/searchnetworking/definition/customer-premises-equipment, Accessed on April 12, 2023
- How to configure Dynamic IP or Static IP on the TP-Link Wi-Fi router to work with a Cable/Fiber modem or a community network (new designed blue UI). (June 2022). Retrieved from URL: https://www.tp-link.com/latam/support/faq/714/, Accessed on April 12, 2023
- Configure Cisco router as DHCP server. (n.d). Retrieved from URL: https://study-ccna.com/configure-cisco-router-as-dhcp-server/, Accessed on April 13, 2023
- Chapter: Configuring the Cisco IOS DHCP Relay Agent. (2023). Retrieved from URL: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-sy/dhcp-15-sy-book/dhcp-relay-agent.html, Accessed on April 13, 2023
- Chapter: Basic Router Configuration. (2023). Retrieved from URL: https://www.cisco.com/c/en/us/td/docs/routers/access/800M/software/800MSCG/routconf.html, Accessed on April 13, 2023
- Cisco Systems, I. (July, 2022). Cisco Online Privacy Statement. Retrieved from URL: *https://www.cisco.com/c/en/us/about/legal/privacy-full.html,* Accessed on April 10, 2023
- Cisco Systems, I. (February, 2017). Cisco 800M Series ISR Software Configuration Guide. Retrieved from URL: https://www.cisco.com/c/en/us/td/docs/routers/access/800M/software/800MSCG/routconf.html, Accessed on April 10, 2023
- *Alessandro M.* (2021). WAN Connections and Technologies Explained. Retrieved from URL: https://www.ictshore.com/free-ccna-course/wan-connections/, Accessed on April 10, 2023