

INTERNATIONAL SCHOOL OF MANAGEMENT & TECHNOLOGY

**ASSIGNMENT COVER SHEET**

|  |  |  |  |
| --- | --- | --- | --- |
| STUDENT DETAILS | | | |
|  | | | |
| Student ID |  | **Reg No.** |  |
| Family Name | Shrestha | **Given Name** | Bisesh |
| Enrolment Year | 2019 | **Section** | N4 |
| Semester | 3RD | **Email** | bisesh@ismt.edu.np |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| UNIT DETAILS | | | | |
| Unit Title | Business Intelligence | **Unit Code** | Y/615/1682 | |
| Assessor Name | Krishna Parajuli | **Issued Date** |  | |
| Assignment Title | Trijata International (Pvt.) Ltd. Network System | | | |
| Assignment No | **1/1** | **Submission Date** | |  |
| Qualification | BTEC HND IN COMPUTING | **Campus** | | **ISMT** |





**STUDENT ASSESSMENT SUBMISSION AND DECLARATION**

When submitting evidence for assessment, each student must sign a declaration confirming that the work is their own.

|  |  |  |  |
| --- | --- | --- | --- |
| Student Name | Bisesh Shrestha | Assessor Name | Krishna Parajuli |
| Issue Date |  | Submission Date |  |
| Programme | Networking | | |
| Unit Name | Transport Network Design | | |
| Assignment Title | Trijata International (Pvt.) Ltd. Network System | | |

**Plagiarism**

Plagiarism is a particular form of cheating. Plagiarism must be avoided at all costs and students who break the rules, however innocently, may be penalized. It is your responsibility to ensure that you understand correct referencing practices. As a university level student, you are expected to use appropriate references throughout and keep carefully detailed notes of all your sources of materials for material you have used in your work, including any material downloaded from the Internet. Please consult the relevant unit lecturer or your course tutor if you need any further advice.

**Student Declaration**

I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice.



Pearson Education 2018  
Higher Education Qualifications

Contents

[Summary 5](#_Toc94631212)

[Part1 6](#_Toc94631213)

[P1 Examine the network design models and features of scalable networks based on a given set of business needs. 6](#_Toc94631214)

[Introduction 8](#_Toc94631215)

[Network design models 8](#_Toc94631216)

[Hierarchical design 8](#_Toc94631217)

[Core Layer 9](#_Toc94631218)

[Distribution Layer 10](#_Toc94631219)

[Access Layer 11](#_Toc94631220)

[Two-tier hierarchical network model: 12](#_Toc94631221)

[Importance of hierarchical network model 12](#_Toc94631222)

[P2 Discuss LAN redundancy, bandwidth and load related issues and possible solutions with reference to Layer 2 and Layer 3 of the OSI Model. 14](#_Toc94631223)

[LAN Redundancy, Bandwidth, and Load Related Issues: 14](#_Toc94631224)

[Possible solution to layer 2 (Data link layer) and layer 3(Network layer) of OSI model: 15](#_Toc94631225)

[P3 Select LAN devices based on features and requirements, and apply basic configuration commands for network connectivity. 16](#_Toc94631226)

[Selection of LAN devices for network connectivity: 16](#_Toc94631227)

[Switch 17](#_Toc94631228)

[Routers 17](#_Toc94631229)

[Gateways 19](#_Toc94631230)

[Repeater 19](#_Toc94631231)

[Access Point 20](#_Toc94631232)

[Computer 21](#_Toc94631233)

[IP Configuration and Addressing 21](#_Toc94631234)

[Configuration: 21](#_Toc94631235)

[P4 Implement a LAN design with Layer 2 and Layer 3 redundancy using switch and router redundancy protocols. 23](#_Toc94631236)

[EtherChannel: 23](#_Toc94631237)

[Configuration steps: 24](#_Toc94631238)

[Hot Standby Router Protocol (HSRP) 27](#_Toc94631239)

[Configuration 27](#_Toc94631240)

[Conclusion: 31](#_Toc94631241)

[Part2: 32](#_Toc94631242)

[P5 Examine WAN technologies and select the appropriate one for a set of enterprise requirements. 32](#_Toc94631243)

[Presentation slides: 32](#_Toc94631244)

[Summary of above slides: 39](#_Toc94631245)

[Introduction to Wide Area Networks (WAN): 39](#_Toc94631246)

[WAN technology 39](#_Toc94631247)

[Public WAN technology 39](#_Toc94631248)

[Advantages of Public Networks: 40](#_Toc94631249)

[Disadvantages of Public Networks: 40](#_Toc94631250)

[Private WAN technology 41](#_Toc94631251)

[Advantages of Private Networks: 41](#_Toc94631252)

[Disadvantages of Private Networks: 42](#_Toc94631253)

[Selection of WAN technology for my network 42](#_Toc94631254)

[WAN protocol 42](#_Toc94631255)

[P6 Configure WAN protocols as part of an enterprise network solution. 43](#_Toc94631256)

[Configuration with result: 43](#_Toc94631257)

[Result 44](#_Toc94631258)

[Conclusion 44](#_Toc94631259)

[Summary 47](#_Toc94631260)

[P7 Deploy network monitoring tools and troubleshooting methods to establish network baselines and produce network documentation. 47](#_Toc94631261)

[Introduction 47](#_Toc94631262)

[Configuration of monitoring tool: 47](#_Toc94631263)

[Configuration of Network Time Protocol (NTP) 49](#_Toc94631264)

[R1 configuration 50](#_Toc94631265)

[Network Troubleshooting Procedures: 51](#_Toc94631266)

[Ping 51](#_Toc94631267)

[Troubleshoot ntp packets 51](#_Toc94631268)

[P8 Troubleshoot LAN and WAN connectivity issues at different networking layers. 52](#_Toc94631269)

[Troubleshooting LAN connectivity: 52](#_Toc94631270)

[Check cabal for connectivity issue 52](#_Toc94631271)

[Troubleshoot network ID and subnet mask of LAN for connectivity 52](#_Toc94631272)

[PING command for LAN connectivity 53](#_Toc94631273)

[Troubleshoot Loop for LAN connectivity 53](#_Toc94631274)

[Troubleshooting WAN protocol: 54](#_Toc94631275)

[Checking IP address and Routing for troubleshooting WAN connectivity 54](#_Toc94631276)

[“Tracert” command for troubleshooting WAN connectivity 55](#_Toc94631277)

[Checking WAN protocol such as PPP (Point to point protocol) 56](#_Toc94631278)

[Conclusion 61](#_Toc94631279)

# Summary

As per scenario, I am system and network administrator of trijata international (Pvt.) Ltd. located head office at kapan-10 Nepal provides different network services all over the country. Some of the services are listed below:

1. Network design and configuration including LAN, MAN and WAN
2. Configuration of different networking and security devices like switch, routers, AP, firewall IPS, IDS etc.
3. System monitoring, upgrading, maintenance and troubleshooting
4. System and network security solutions
5. Network design and configuration of wired and wireless network

Recently it is going to expand some new branches in Butwal, Pokhara, Surkhet and Nepalgunj. As a system and network administrator of this company I have to design and implement network and have to prepare a report also including the following topics:

1. Switch and router redundancy protocols
2. Bandwidth and load related issues
3. Link aggregation and ether channel issues
4. Scalable network.
5. VPN
6. Network and system security etc.

# Part1

**Prepare a report covering the following topics:**

1. **Examine and produce** an analysis of the network design models and how they contribute to the design of a scalable and reliable network.
2. A detailed **discussion** of LAN redundancy concepts, network features, such as bandwidth and load and their related issues. The **explanations** should contain the **possible solutions provided** at Layer 2 and 3 of the OSI Model

# P1 Examine the network design models and features of scalable networks based on a given set of business needs.

**Report on:**

**Exploring and implementation of LAN design principles and their application in the network design process**

**Prepared by: Bisesh Shrestha**

# Introduction

Within an information system, networking refers to the process of sharing and transmitting data between nodes that share a medium. It is, in essence, the entire process of creating and using computer networks, including software, hardware, and protocols. In general, a network is made up of many devices that communicate with one another. This section discusses several network design paradigms and their responsibilities in ensuring a stable and scalable network. In this section, I'll go through LAN redundancy, bandwidth, and load-related challenges, as well as potential solutions for layer 2 and 3 of the OSI Model.

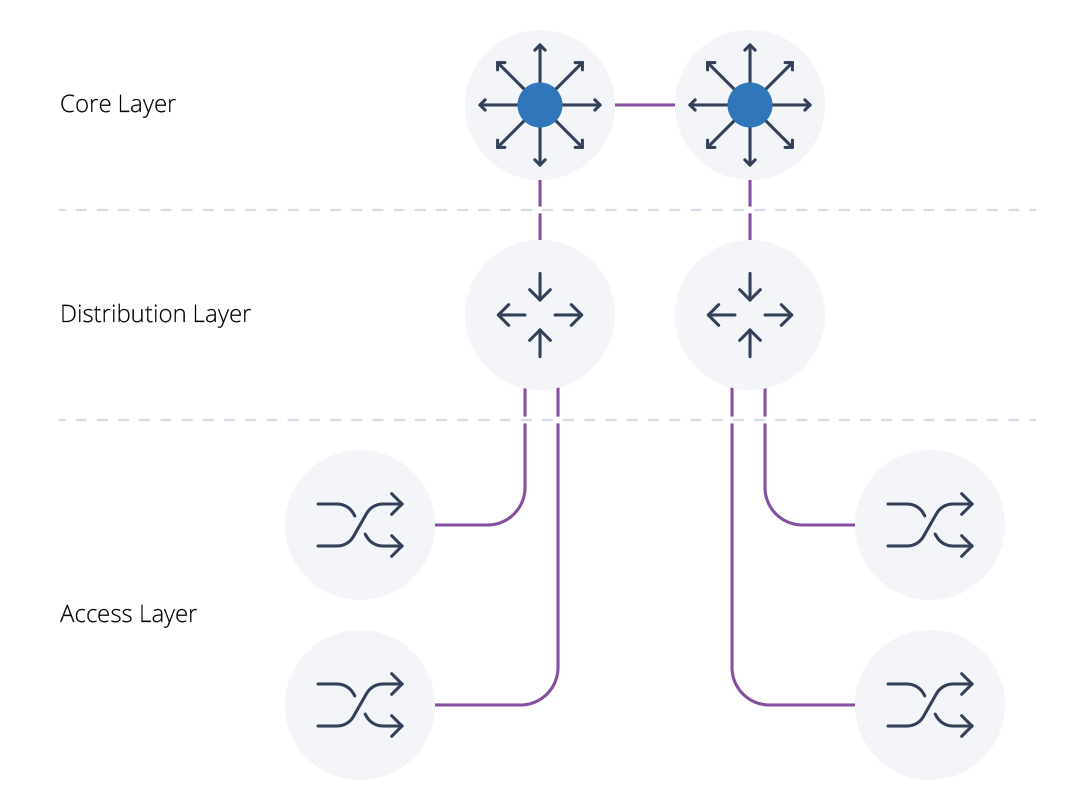
# Network design models

Network sign refers to the system architecture that deals with data transport mechanisms. This includes the analysis stage, in which the requirements are assessed, as well as the implementation stage. Before the execution, the design process is completed, and the subsequent steps are completed.  section of the business network is often designed to be optimized for the quickest functional architecture that operates on high-speed physical infrastructure.

## Hierarchical design

A hierarchical design divides a network into layers, each of which has a set of functions that define its function within the network. As a result, a network designer may select the best hardware, software, and features for each network layer's specific purpose. In addition, data handling is significantly more efficient. Local traffic stays local in a hierarchical architecture, moving to a higher layer only when it needs to go to another network.

In a hierarchical network architecture, the layers are generally mapped according to the physical structure of the network. However, because they might differ, it's preferable to think of them as logical levels. The most frequent design is three layers, however it is not required. A typical three-layer hierarchical network model consists of:



1. **A core layer**: Your network's backbone is this. It allows for quick communication between network distributions switches.
2. **A distribution layer:** This middle layer manages the border between the other two levels and provides policy-based connectivity. It's also known as the "Workgroup" layer since its where routing and data filtering happen.
3. **A access layer**: It is commonly referred to as the "Workstation" layer since it is where endpoints and local servers connect to the network.

### Core Layer

The network's high-speed switching backbone, known as the core layer, is critical to business communications. The backbone is another name for it. The following properties should be present in the core layer:

* Fast transport
* High reliability
* Redundancy
* Fault tolerance
* Low latency and good manageability
* Avoidance of CPU-intensive packet manipulation caused by security, inspection, quality of service (QoS) classification, or other processes
* Limited and consistent diameter
* QoS

The diameter of a network using routers is the number of router hops from edge to edge. As previously stated, designing for a constant diameter within a hierarchical network is considered best practice. The number of hops between any end station and another end station across the backbone should be the same. The distance between any end station and a backbone server should also be constant. Limiting the width of the internetwork ensures consistent performance and makes troubleshooting easier. Without expanding the width of the core layer, you may add distribution layer routers and client LANs to the hierarchical scheme. The use of a block implementation shields existing end stations from the majority of network expansion's consequences.

### Distribution Layer

The network’s distribution layer is the isolation point between the network’s access and core layers. The distribution layer can have many roles, including implementing the following functions:

* Policy-based connectivity (for example, ensuring that traffic sent from a particular network is forwarded out one interface while all other traffic is forwarded out another interface)
* Redundancy and load balancing
* Aggregation of LAN wiring closets
* Aggregation of WAN connections
* QoS
* Security filtering
* Address or area aggregation or summarization
* Departmental or workgroup access
* Broadcast or multicast domain definition
* Routing between virtual LANs (VLANs)
* Media translations (for example, between Ethernet and Token Ring)
* Redistribution between routing domains (for example, between two different routing protocols)
* Demarcation between static and dynamic routing protocols

You can use several Cisco IOS Software features to implement policy at the distribution layer:

* Filtering by source or destination address
* Filtering on input or output ports
* Hiding internal network numbers by route filtering
* Static routing
* QoS mechanisms, such as priority-based queuing

The distribution layer provides aggregation of routes providing route summarization to the core. In the campus LANs, the distribution layer provides routing between VLANs that also apply security and QoS policies.

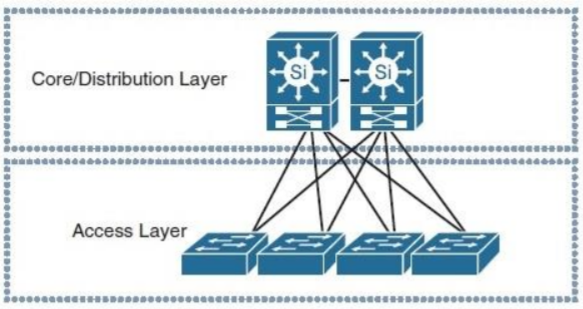
### Access Layer

The access layer provides user access to local segments on the network. The access layer is characterized by switched LAN segments in a campus environment. Micro segmentation using LAN switches provides high bandwidth to workgroups by reducing the number of devices on Ethernet segments. Functions of the access layer include the following:

* Layer 2 switching
* High availability
* Port security
* Broadcast suppression
* QoS classification and marking and trust boundaries
* Rate limiting/policing
* Address Resolution Protocol (ARP) inspection
* Virtual access control lists (VACLs)
* Spanning tree
* Trust classification
* Power over Ethernet (PoE) and auxiliary VLANs for VoIP
* Network Access Control (NAC)
* Auxiliary VLANs

You implement high availability models at the access layer. The section “High Availability Network Services” covers availability models. The LAN switch in the access layer can control access to the port and limit the rate at which traffic is sent to and from the port. You can implement access by identifying the MAC address using ARP, trusting the host, and using access lists.

## Two-tier hierarchical network model:



A two-tier hierarchical network model is one in which the core and distribution layers are merged into a single layer. When the distribution layer and core layer functions are accomplished by a single device, it is referred to as "collapsed core." The reason for this is because a collapsed core reduces network costs while preserving the majority of the three-tier hierarchical network topology. Smaller businesses choose this two-tier hierarchical arrangement because it is more cost effective. The hardware resources that are traditionally distributed over numerous devices between core and distribution will now be spread thin among the hardware within this collapsed layer, which is a downside of this architecture.

## Importance of hierarchical network model

Hierarchical networks offer a wide range of benefits, such as enhanced performance, reliability and scalability, better security, easier management and design, and improved cost-efficiency. Let’s focus a bit on each one below:

* Enhanced performance

A hierarchical network design means data is routed through aggregated switch port links at close to wire rate, instead of being sent through lower performance intermediary switches. The distribution and core layers consist of high-performance switches, which means higher speeds and fewer issues with network bandwidth. Therefore, if the network is designed correctly, data should travel at close to wire-speed between every device on the network for most of its journey within the network.

* Improved reliability

The modular nature of a hierarchical network translates into a more reliable network as a whole, as segments that fail or become degraded can be isolated and routed around. The rest of the network won’t be affected. Availability also increases because it is easier to implement network redundancies. For example, switches in the access layer can be connected to two switches in the distribution layer. If one fails, the other comes into play. Likewise, the distribution switches connect to multiple core switches, providing yet another layer of redundancy. The only redundancy limitation is at the access level, since most end-user devices cannot link to multiple switches simultaneously. However, even if an access switch were to fail, only the devices using that switch would experience an outage and not the entire network.

* Increased scalability

Hierarchical networks are more flexible than their counterparts. Segments and elements can easily be added without significantly disrupting the existing network. Design elements can also be copied and repeated, thanks to the network’s modularity. Consistent design from one module to the next makes it easy for network administrators to plan and implement network expansion, and know the topology is unchanged module to module. Therefore, networks can expand with the organization with little to no downtime.

* Better security

In terms of security, a hierarchical network permits a greater level of control. Access control lists can be more complex and granular, and traffic can be shaped and blocked more effectively. Furthermore, these policies can be applied to a user, a department, or the whole organization, allowing admins to develop network traffic plans tailored to the needs of the enterprise. Since network details aren’t available for most users, intentional or accidental network issues are less of a concern, thereby increasing productivity and improving the network’s performance.

* Easer to manage

Since each network layer is designed for specific and consistent functionality, these networks are easier to manage. For example, should you need to modify the functions of an access layer switch, you can confidently make that same change to all the access layer switches—because they have the same role. It’s also simpler to deploy new switches because you can copy configurations from one device to another without significant changes. Troubleshooting and recovery is also simpler and faster.

* Increased cost efficiency

IT networking equipment is an expensive necessity. However, hierarchical network design can reduce costs because the organization can limit the amount of equipment to only what is needed based on the logical structure of the enterprise. The modular nature of the network means that it can be expanded without significant one-off investments. Adding a new department, for example, can often be done with a single access switch and a few Ethernet cables, rather than needing a new series of routers and switches (many of which will sit underused).

# P2 Discuss LAN redundancy, bandwidth and load related issues and possible solutions with reference to Layer 2 and Layer 3 of the OSI Model.

## LAN Redundancy, Bandwidth, and Load Related Issues:

"Adding additional instances of network devices and lines of communication to help ensure network availability and reduce the risk of failure along the critical data path" is defined as "the process of adding additional instances of network devices and lines of communication to help ensure network availability and decrease the risk of failure along the critical data path". To provide redundancy and mitigate against challenges that may emerge due to bandwidth and load inside a network, network infrastructure has been changed and designs have been established. The word 'bandwidth' refers to the quantity of data that may be transported in a certain length of time from one point to another inside a network. Physical and logical layer 2 loops are caused by duplicated links in a network. Another issue is a broadcast storm, which occurs when switches broadcast multiple frames in a layer 2 loop, using all available bandwidth and rendering the network unusable for actual network traffic, resulting in a denial of service. When switches don't contain the destination MAC address in their MAC table, they send unknown unicast packets into a looped network, causing redundant frames to be sent to the target devices. Layer 3 loops are also caused by redundant LAN networks. In a LAN redundant network with two or more routers, there is also a default gateway issue. Because there are so many devices linked to the network, bandwidth and load balancing are additional difficulty with a LAN redundancy network. When creating a new network, a network designer must consider availability, scalability, resilience, dependability, and Quality of Service (QoS).

Bandwidth, latency, and load are three network characteristics that have a significant impact on a network's redundancy. Bandwidth refers to the maximum pace at which data can be sent across a network; delay refers to any stoppage in data transmission over a network; and load refers to the volume of traffic being sent across the network. If a network receives too high bandwidth that it was not planned for, it will slow down, cause delays, and increase the amount of data delivered through the network owing to a backlog. Some of the redundancy principles and protocols listed below might help to prevent these problems. The following is a full explanation of LAN redundancy ideas, network properties like bandwidth and load, and their related concerns, which should include the various solutions given at Layers 2 and 3 of the OSI Model:

## Possible solution to layer 2 (Data link layer) and layer 3(Network layer) of OSI model:

There are a variety of LAN redundancy approaches that may be used in a network, the most basic of which being cabling. This solution consists of several cabled pathways between switches; this provides network availability, resilience, dependability, and QoS by allowing the network to adapt and adopt the other path if one path fails, allowing the network to remain available and resilient. Engineers can also setup and implement EtherChannel if they want to. EtherChannel is a port channel technology that may operate at Layer 2 or Layer 3 of the OSI model. Several connections are combined into a single logical channel rather than being separated. This not only provides for traffic load sharing, but it also allows for increased bandwidth and network robustness.

Spanning Tree Protocol (STP), which is placed at Layer 2 of the OSI model, is another option. STP's primary function is to prevent network loops on layer two devices like as switches, ensuring that the network remains operational and that if one port fails, another becomes active to sustain the network. If a loop forms within a network, it has the potential to bring the entire network down; the STP algorithm creates a logical topology by sending packets known as Bridge Protocol Data Units (BPDUs) out of all ports, and once it has done so, it assigns ports to one of five states: blocking, listening, learning, forwarding, or disabled.

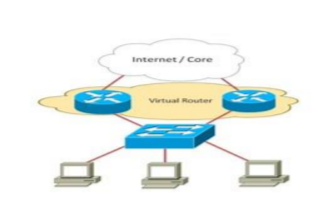
When a port is in the blocking state, it will only listen for BPDUs and ignore any other frames transmitted to it. The goal of this state, and hence the protocol, is to prevent looping pathways from being used. The port's other major state is forwarding, which indicates it will send and receive all frames. The switch can identify whether there are any network changes or failures by sending out BPDUs, which can cause ports to go into one of the other three states. When a port is in the listening state, it will wait for BPDUs to check that no loops exist before delivering the frame; if it is in this condition, it will not populate the MAC address database, which may trigger a network loop. In contrast to the listening state, a port in the learning state will listen to BPDUs, learn the network path, and populate the MAC address table but not forward the frame. The port's final state is disabled, indicating that it will not participate in STP.

Using redundancy protocols placed at Layer 3, we may solve challenges connected to redundancy, bandwidth, and load balancing. Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), and Gateway Load Balancing Protocol (GLBP) are three redundancy protocols that are considered High Availability protocols. The goal of these redundancy protocols is to aid scalable networks. By adopting these protocols, it is possible to balance traffic by permitting a logical redundant gateway link in the event that the primary gateway link fails. All of these protocols are First Hop Redundancy Protocols (FHRPs), which make a collection of physical routers seem to be a single logical router. It makes client setup and connectivity easier when using these protocols due to the configuration of a single default gateway, and the host computer can use standard communication protocols.

**Fig: Active/Standby Redundancy in a layer 2 switched domain**



**Fig: Network with layer 3 redundancy**

****

# P3 Select LAN devices based on features and requirements, and apply basic configuration commands for network connectivity.

## Selection of LAN devices for network connectivity:

Routers and switches are offered in a variety of versions from networking IT suppliers. Different models will provide different characteristics, such as the number of ports available, forwarding rates, and so on. The different routers and switches had to be assessed to determine whether they would be appropriate to fulfill the networks criteria in order to choose the networking equipment that were utilized for the prototype. To make this decision, a number of processes had to be followed to guarantee that the correct switch and router were picked.

### Switch

Switches play a more intelligent function than hubs in most cases. A switch is a multiport device that increases the efficiency of a network. The switch keeps limited routing information about internal network nodes and facilitates connections to systems such as hubs and routers. Switches are commonly used to link LAN strands. In most cases, switches can read the hardware addresses of incoming packets and forward them to the correct destination. Because switches have the capacity to create virtual circuits, they are more efficient than hubs or routers in terms of network efficiency. Switches also increase network security by making it more difficult to investigate virtual circuits with network monitors. A switch may be thought of as a device that combines the greatest features of routers and hubs. In the OSI model, a switch can operate at either the Data Link layer or the Network layer. A multilayer switch is one that can work on both levels, meaning it may be used as a switch and a router. A multilayer switch is a high-capacity device that uses the same routing protocols as routers.

Switches are vulnerable to distributed denial of service (DDoS) assaults, and flood guards are employed to keep malicious traffic from shutting down the switch. Switch port security is critical, therefore disable any unused ports and utilize DHCP snooping, ARP inspection, and MAC address filtering to protect switches.



### Routers

Routers assist in the transmission of packets by charting a path through a sea of interconnected networking devices utilizing various network topologies. Routers are smart devices that retain information about the networks to which they are linked. The majority of routers may be set up to act as packet-filtering firewalls with access control lists (ACLs). Routers are also used to convert LAN framing to WAN framing, in combination with a channel service unit/data service unit (CSU/DSU). Because LANs and WANs utilize distinct network protocols, this is required. Border routers are the name given to such routers. They link a LAN to a WAN from the outside, and they function at the network's perimeter. Internal networks are also divided into two or more subnetworks using routers. Internally, routers may be linked to other routers to create zones that function independently. Routers communicate by keeping track of destinations and local connections in tables. A router stores information about the systems that are linked to it, as well as where requests should be sent if the destination is unknown. Routing and other information is commonly sent by routers using one of three standard protocols: Routing Information Protocol (RIP), Border Gateway Protocol (BGP), or Open Shortest Path First (OSPF) (OSPF).

Routers are your first line of protection, and they must be set to only pass traffic that network administrators have allowed. The routes themselves might be static or dynamic in nature. They can only be manually configured if they are static, and they will remain that way until they are modified. If they're dynamic, they pick up on other routers in the area and utilize that knowledge to create their routing tables.



Routers are multi-purpose devices that link two or more heterogeneous networks together. They're normally reserved for special-purpose computers, having distinct input and output network interfaces for each network connected. Because routers and gateways represent the backbone of huge computer networks such as the internet, they have unique capabilities that allow them to adapt to changing network addressing systems and frame sizes by segmenting large packets into smaller ones that match the new network components. Each router interface has its own Address Resolution Protocol (ARP) module, as well as its own LAN address (network card address) and IP address. The router knows which paths a packet can travel from its source to its destination thanks to a routing table. The routing table evolves dynamically, much like the bridge and switch. The router removes the packet headers and trailers and examines the IP header to determine the source and destination addresses, data type, and arrival time when it receives a packet. It also adds new addresses to the router table that aren't currently there. In the routing table, the IP header and arrival time information are inserted. Routers typically operate at the OSI model's Network layer.

### Gateways

Gateways often operate at the OSI model's Transport and Session levels. There are multiple protocols and standards from various manufacturers at the Transport layer and higher; gateways are used to deal with them. Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) are two networking protocols that are translated by gateways. Gateways connect two or more independent networks, each having its own routing algorithms, protocols, topology, domain name service, and network management processes and rules, as a result of this. All of the duties of routers and more are performed by gateways. In fact, a gateway is a router with additional translation capabilities. A protocol converter is a function that converts data between different network technologies.



### Repeater

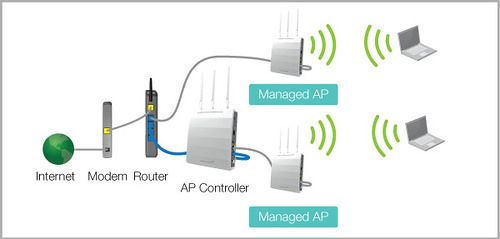
A repeater is a device that receives a signal and enhances it. A repeater is a device that receives a signal and retransmits it at a higher level or power so that it may travel farther distances, such as more than 100 meters for conventional LAN lines. The Physical layer is where repeaters function.



### Access Point

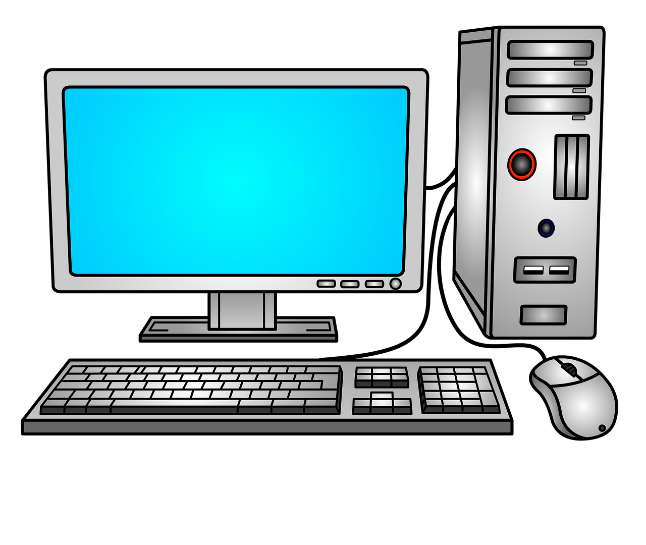
While an access point (AP) can theoretically be a wired or wireless device, it is most usually used to refer to a wireless device. An access point (AP) operates at the Data Link layer of the OSI model, and it can act as a bridge linking a wired network to wireless devices or as a router transmitting data from one access point to another. Wireless access points (WAPs) are devices that combine a transmitter and a receiver (transceiver) to form a wireless LAN (WLAN). Separate network devices with a built-in antenna, transmitter, and adaptor are known as access points. The wireless infrastructure network mode is used by APs to establish a link between WLANs and a wired Ethernet LAN. They also contain many ports, allowing you to expand the network to accommodate more customers. One or more APs may be required to give complete coverage, depending on the size of the network. Additional access points are used to provide access to more wireless clients and to extend the wireless network's range. The distance a client may be from an AP while still receiving an acceptable signal and data processing speed is regulated by each AP's transmission range. The actual distance between the client and the AP is determined by the wireless standard, impediments, and ambient circumstances. High-powered antennas on higher-end APs allow them to expand the range of the wireless transmission.

Many ports may be available on APs, which may be utilized to expand the network's capacity, firewall capabilities, and Dynamic Host Configuration Protocol (DHCP) service. As a result, we have access points that operate as a switch, DHCP server, router, and firewall.



### Computer

A computer is a system or device that uses software or hardware program instructions to perform functions, computations, and operations. It can take (input) data, process it, and then produce outputs. I gave laptops to each of the department's users while constructing the RRC network at European HQ in Dublin. These machines are given an IP address, which is a unique number. Computers can also connect with computers on other networks using IP addresses. Computers have a MAC address, which is a unique physical location.

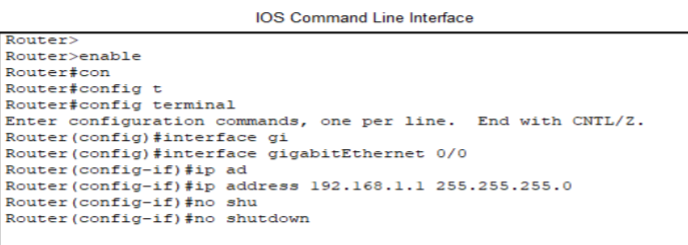


### IP Configuration and Addressing

In the network design of NEC, I have used classless IPv4 and IPV6 for the connection of WAN to LAN. If any difficulties emerge in the future with any NEC branches, we have a remote access service called SSH (Secure Shell) that allows us to operate and monitor each branch from the head office.

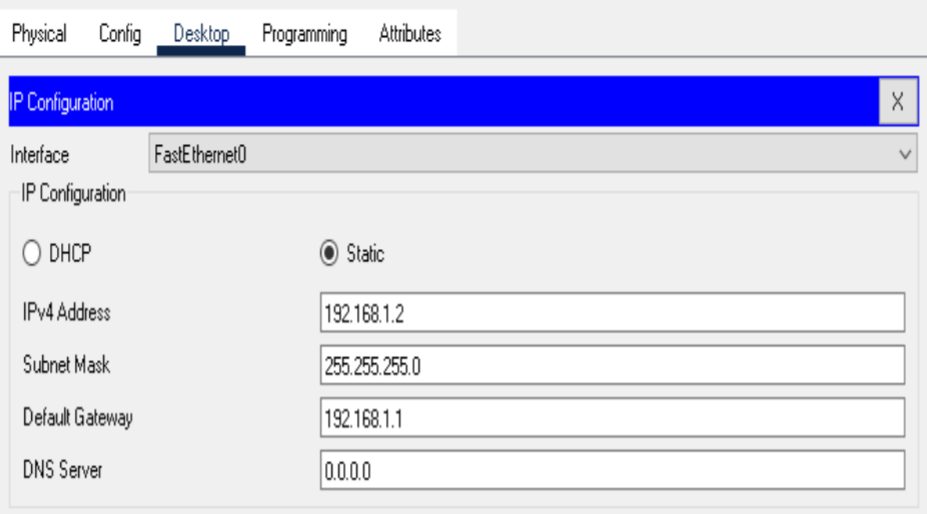
# Configuration:

Step1: I have configured the IP address and subnet mask of Router 1.

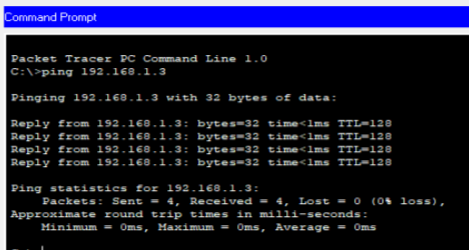


Step2: In each PC, I have established IPv4 address configuration. I've configured a static IPv4 address, subnet mask, and default gateway IP address, as shown in the diagram.

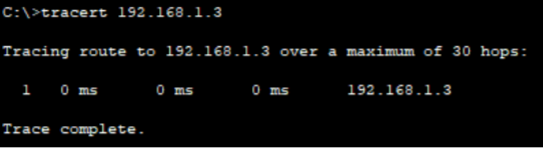
The virtual gateway ip of the LAN is the default gateway ip.



Step3: Ping command: To check the network connectivity of my network I used ping command and the result was positive as seen in the figure.



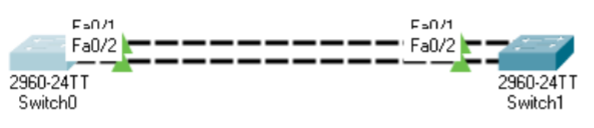
Step4: Tracert: I used tracert command to display the list of routers that a packet must go through.



# P4 Implement a LAN design with Layer 2 and Layer 3 redundancy using switch and router redundancy protocols.

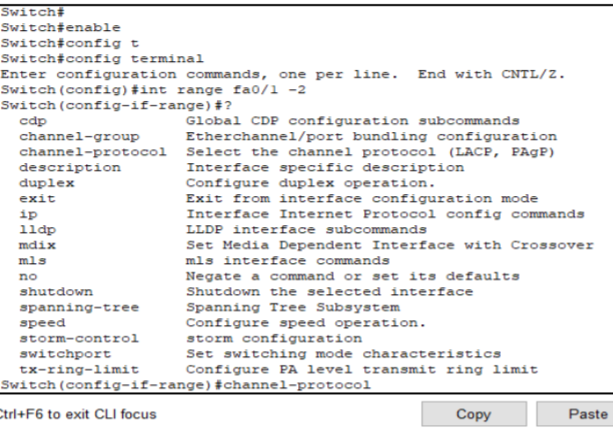
## EtherChannel:

Ether channel is a technique that enables many physical interfaces to be combined into a single logical interface. Link aggregation is another name for it. By aggregating separate switch links, the ether channel boosts bandwidth and offers redundancy. The Ether Channel distributes traffic evenly across all of the bundle's connections. It may be set to either layer 2 or layer 3. STP protocols will regard the grouped links as independent links once EtherChannel is introduced, preventing STP from blocking the supplied ports. The Port Aggregation Protocol (PAgP) and the Link Aggregation Control Protocol are two aggregation protocols that can be used to create EtherChannel (LACP). It helps to make network scalable by implementing these protocols, it means there are alternative paths available if the dedicated path were to fail or become unavailable.



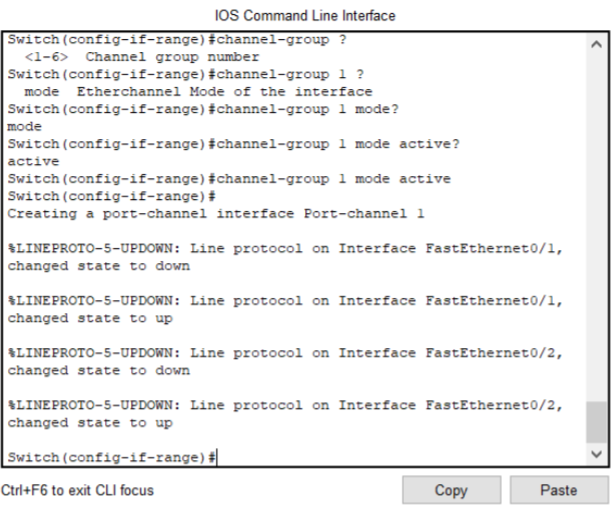
### Configuration steps:

Step1: At first, I clicked on the switch to go to the CLI mode and enabled the CLI and started configuring.

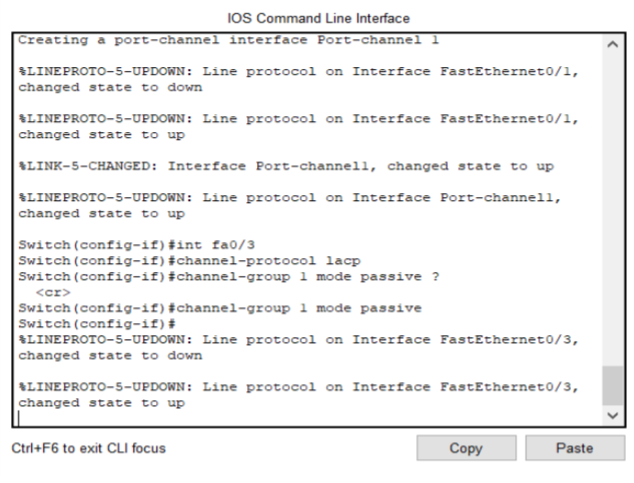


Step2: Then I started configuring channel group number and modes of EtherChannel in both switches.

For switch1

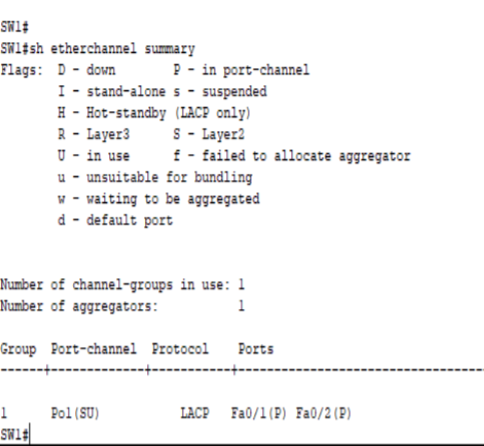


For switch 2

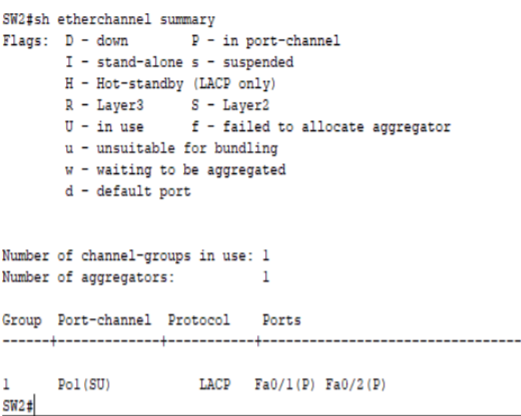


Step3: Here, in sw1 and sw2 we can see the ether channel is configured. It displays the group, port channel, protocol and ports.

For switch1

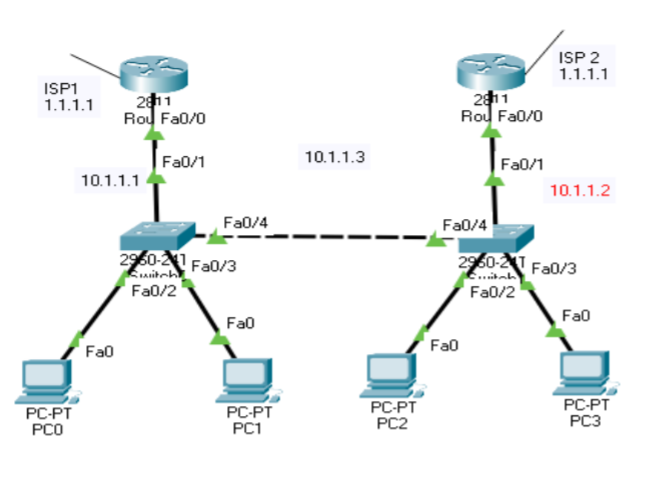


For switch2:



## Hot Standby Router Protocol (HSRP)

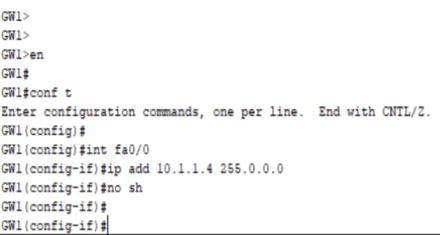
The Cisco proprietary technology Hot Standby Router Protocol (HSRP) allows many routers or multilayer switches to appear as a single gateway IP address. It ensures that the layer 3 functions in our networks are redundant. Multiple physical routers or multilayer switches are combined into a single virtual router via HSRP. This implies that all of the routers in the HSRP group have the same virtual IP address and virtual MAC address. As a result, if a router fails or the router's link breaks, a second physical device is ready to react to the identical default gateway address information. As a result, there is no loss of connectivity, and problems may be resolved without having to deal with requests from customers who are experiencing network outages. Another example of how these protocols facilitate scalable networks is HSRP's support for IPv6. Due to the brief time it takes the network to identify the issue, re-converge, and pick a new path, the network would not be harmed if the network engineer elected to add another service or device to the network with these protocols set. As a result, it contributes to the network's scalability.



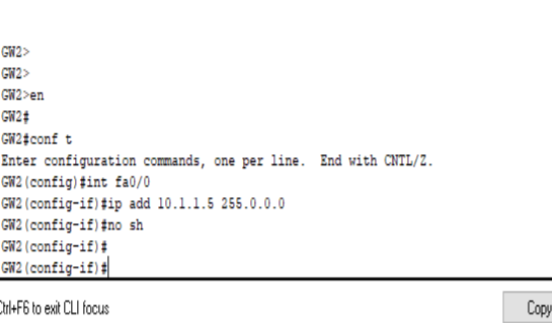
### Configuration

Step1: very 1st step, I added the IP address on both routers respectively.

For router1

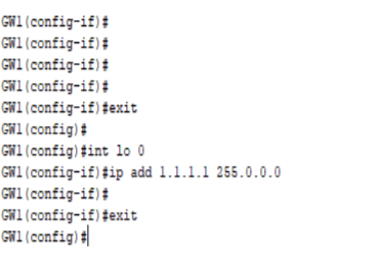


For router 2:

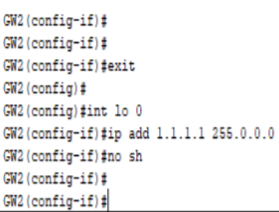


Step2: Then I created loopback address on both router 1 and router 2 respectively

For router1:

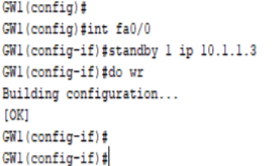


For router2:



Step3: I configured standby in router on both routers. The Router did not become the active router but will keep sending Hello message. If the active router fails it will take over.

For router1

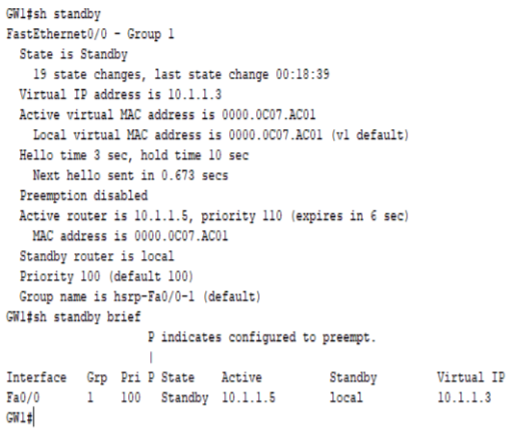


For router 2

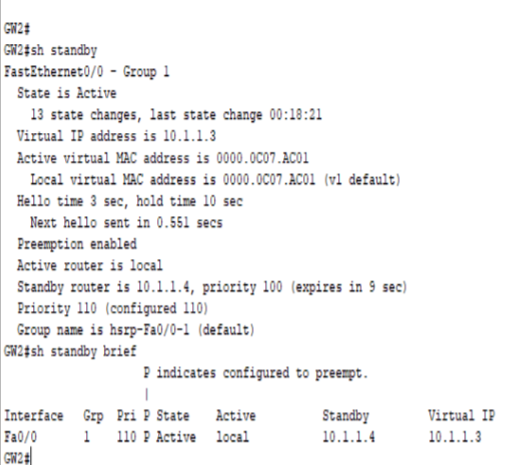


Step4: Here is the final outcome of the HSRP configuration.

Outcome of router 1



Outcome of router 2



# Conclusion:

In the end, this part of the report represents the design and prototype of the network designed for Trijata International (Pvt.) Ltd.  Along with the detailed documentation of several redundancy protocols. The NSP architecture depicts the connection between branches as well as the use of Layer 2 and Layer 3 redundancy protocols including STP, OSPF, and Ether-Channel. With this protocol's detailed report.

# Part2:

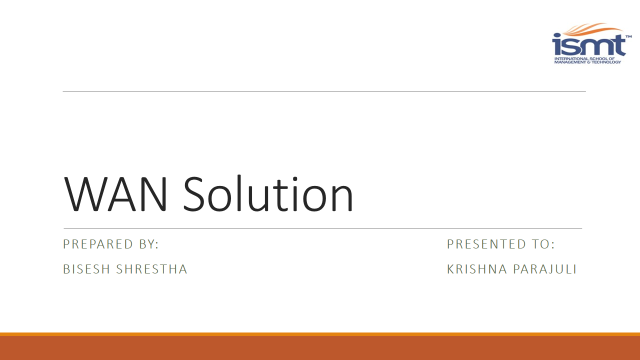
1. **Produce presentation** slides which show an appropriate WAN solution to a set of organizational requirements. The presentation includes”

* Examine WAN technologies and select the appropriate one for a set of enterprise requirements and analyze the benefits and drawbacks of private and public WAN technologies.
* Configure WAN protocols as part of an enterprise network solution.

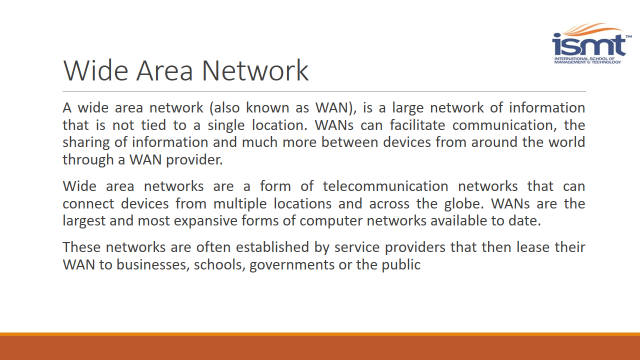
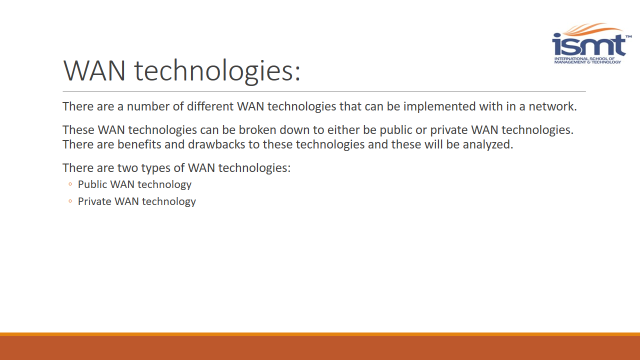
1. **Produce technical report** which includes
   * Deploy network monitoring tools and troubleshooting methods to establish

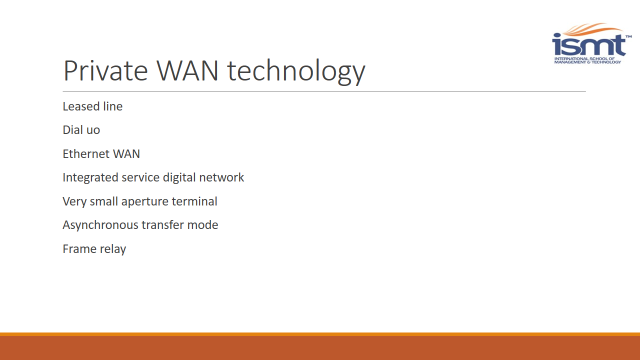
# P5 Examine WAN technologies and select the appropriate one for a set of enterprise requirements.

# Presentation slides:

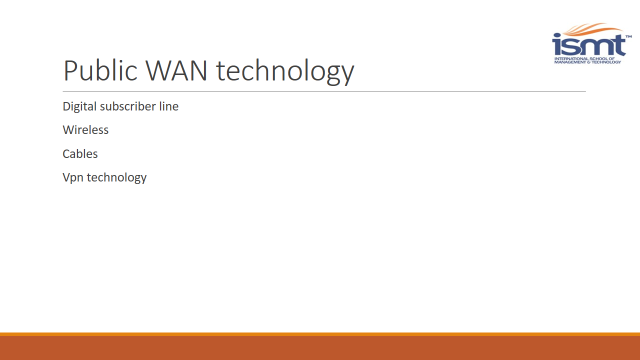


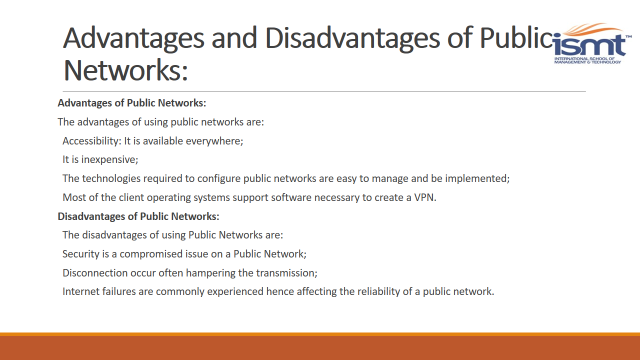


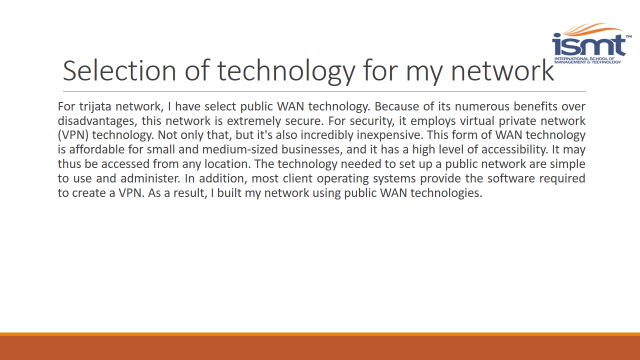
 

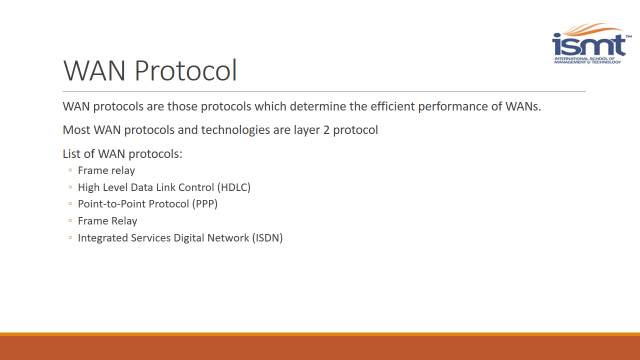


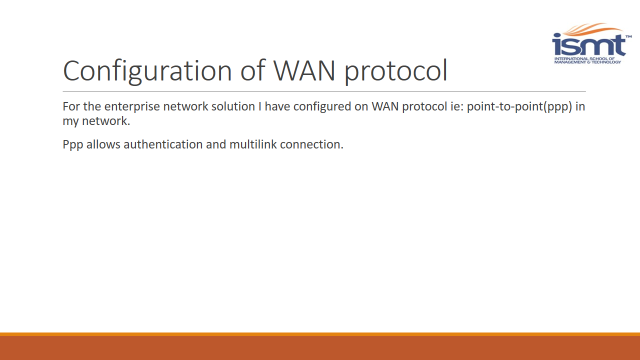


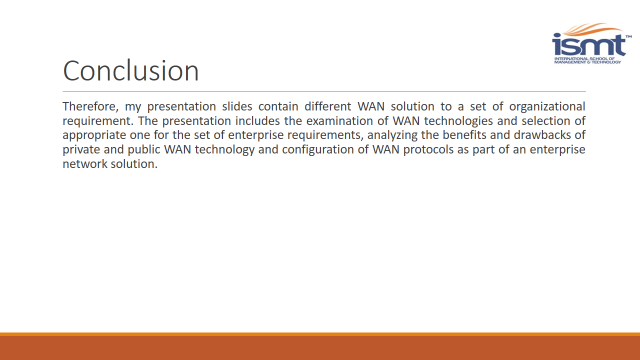












## Summary of above slides:

### Introduction to Wide Area Networks (WAN):

A wide area network (WAN) is a type of telecommunication network that may link devices from all over the world. Larger firms or organizations utilize them to ease data interchange, and corporations with operations in several regions have adopted WANs in a range of industries. WANs can be point-to-point, which involves a direct link between two locations, or packet-switched, which involves data being sent in packets through shared circuits.

WAN technology:

There are several distinct WAN technologies that may be used in a network. There are two types of WAN technology: public and private WAN technologies. These technologies have advantages and disadvantages, which will be discussed. WAN technologies are divided into two categories. There are two types of WAN technology: public and private WAN technology.

### Public WAN technology

Public WAN technology refers to the infrastructure that allows service providers to deliver Internet access via broadband services such as DSL, cable, and satellite. Small offices and telecommuting employees usually utilize broadband connections to connect to a corporate location through the Internet. VPNs should be used to safeguard data transiting between corporate sites over public WAN infrastructure.

The following are some examples of public WAN technology:

* DSL (Digital Subscriber Line)

DSL is an always-on connection technology that transports high-bandwidth data and delivers IP services to customers over existing twisted-pair telephone lines.

Using a DSL access multiplexer (DSLAM) at the provider's point of presence, numerous DSL subscriber lines are multiplexed into a single, high-capacity link (POP). There are many different types of DSLs, as well as standards and upcoming standards. For company IT teams to assist home employees, DSL has become a popular solution. Although there are security dangers in this procedure, they may be mitigated using security measures.

* Wireless technology

Wireless technology sends and receives data through an unlicensed radio spectrum. Anyone with a wireless network and wireless technology in his or her device has access to the unlicensed spectrum. The requirement to be within the local transmission range (usually less than 100 feet) of a wireless router or wireless modem with a wired connection to the Internet has been one constraint of wireless access. As a result, new developments in broadband technology are altering the landscape. Multiple Wi-Fi, WiMAX, and satellite internet are examples of change.

* Cables

In metropolitan areas, coaxial cable is commonly utilized to distribute television signals. Several cable television companies provide network connectivity. This connection provides more bandwidth than the traditional telephone local loop. Cable modems (CMs) offer a constant connection and are easy to set up. A cable television subscriber connects a PC or LAN router to the cable modem, which converts digital signals into broadband frequencies for transmission via a cable television network.

* VPN (Virtual Private Network) technology

When a teleworker or a distant office worker utilizes a broadband service to connect to the business WAN over the Internet, security problems arise. Broadband providers offer VPN connections to a network device that accepts VPN connections, which is often placed at the corporate site, to solve security issues. VPNs are divided into two categories. Site-to-site VPN and remote access VPN are the two options.

### Advantages of Public Networks:

The advantages of using public networks are:

* Accessibility: It is available everywhere;
* It is inexpensive;
* The technologies required to configure public networks are easy to manage and be implemented;
* Most of the client operating systems support software necessary to create a VPN.

### Disadvantages of Public Networks:

* The disadvantages of using Public Networks are:
* Security is a compromised issue on a Public Network;
* Disconnection occur often hampering the transmission;
* Internet failures are commonly experienced hence affecting the reliability of a public network.

### Private WAN technology

A service provider may offer dedicated point-to-point leased lines, circuit-switched links such as PSTN or ISDN, and packet-switched links such as Ethernet WAN, ATM, or Frame Relay as part of their private WAN technology.

The following are some examples of private WAN technology:

* **Leased line**

The term "leased line" refers to the fact that an organization pays a service provider a monthly lease charge to utilize the line. Leased lines come in a variety of capacities and are normally charged according to the desired bandwidth and the distance between the two connected places.

* Dial up

When no alternative WAN technology is available, dialup WAN connection may be necessary. For example, to provide limited capacity and dedicated switched connections, a remote site might employ modems and analog dialed telephone lines. These relatively slow dialup connections are sufficient for exchanging sales statistics, pricing, regular reports, and email for small firms.

* WAN Ethernet

Ethernet has become a viable WAN access option because to updated Ethernet standards that use fiber-optic lines. Metropolitan Ethernet (MetroE), Ethernet over MPLS (EoMPLS), and Virtual Private LAN Service are all names for the Ethernet WAN service (VPLS). The advantages of employing an ethernet WAN include lower costs and administration, simple connection with existing networks, and increased corporate productivity.

* Relay frame

Frame Relay is a no-broadcast multi-access (NBMA) Layer 2 WAN technology that is used to connect business LANs. Using permanent virtual circuits, a single router interface may connect to several sites (PVCs). PVCs are created by Frame Relay and are identifiable by a data-link connection identifier (DLCI). PVCs and DLCIs allow bidirectional communication from one DTE to another.

### Advantages of Private Networks:

The advantages of using Public Networks are:

* Security is never an issue with these systems;
* It offers a complete managed solution to the communication needs of a company.

### Disadvantages of Private Networks:

The disadvantages of using Private Networks are:

* It is a costly affair as compared to the PSTN which is made available at a very nominal rate.
* Requires more administrative control than the public networks.
* Specialized staff is required to manage the network which further adds to the costs.
* As the network grows so does the complexity of the same.

## Selection of WAN technology for my network

I chose public WAN technology for the Trijata International (Pvt.) Ltd. Service providers use broadband services such as DSL, cable, and satellite access to deliver Internet access using public WAN technologies. Small offices and telecommuting employees usually utilize broadband connections to connect to a corporate location through the Internet. VPNs should be used to safeguard data transiting between corporate sites over public WAN infrastructure. VPN technology, Digital Subscriber Line (DSL), cables, wireless, and other forms are included.

A virtual private network (VPN) is an encrypted link between two private networks that is established over a public network, such as the Internet. Instead of utilizing a dedicated Layer 2 connection, such as a leased line, a VPN employs VPN tunnels, which are virtual connections that are routed across the Internet from the company's private network to the remote site or employee host. Similarly, DSL is an always-on connection technology that transports high-bandwidth data and delivers IP services to customers over existing twisted-pair telephone lines. A DSL access multiplexer (DSLAM) at the provider site, referred to as the point of presence, multiplexes multiple DSL subscriber lines into a single, high-capacity link (POP). Furthermore, wireless technology sends and receives data through an unlicensed radio spectrum. Because of its numerous advantages over disadvantages, I believe this technology is acceptable and appropriate for the Trijata International (Pvt.) Ltd. In terms of security, this network is excellent. For security, it makes use of VPN technology. Not only that, but it's also incredibly inexpensive. This form of WAN technology is affordable for small and medium-sized businesses, and it has a high level of accessibility.

It may thus be accessed from any location. The technology needed to establish public networks are simple to use and administer. In addition, most client operating systems include the software required to set up a VPN. As a result, I used public WAN technology for my Trijata International (Pvt.) Ltd.

## WAN protocol

WAN protocols are those protocols which determine the efficient performance of WANs. Most WAN protocols and technologies are layer 2 protocols (data link layer). List of WAN protocols:

* Frame relay
* ISDN (Integrated Services Digital Network
* LABP (Link Access Procedure Balanced)
* HDLC (High-level Data Link Control)
* SDLC (Synchronous Data link Control)
* PPP (Point-to-Point Protocol)

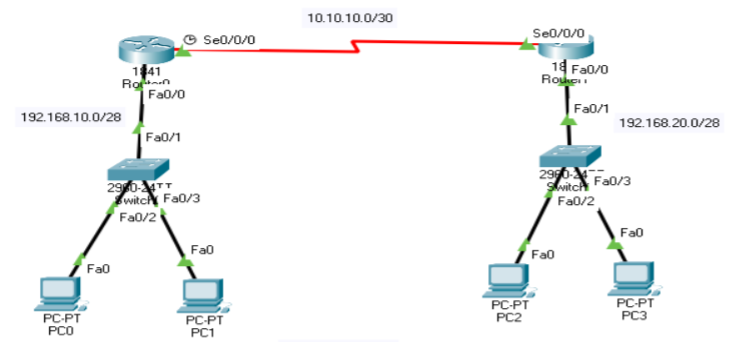
# P6 Configure WAN protocols as part of an enterprise network solution.

In my Trijata International (Pvt.) Ltd, I have setup one WAN protocol, Point-to-Point Protocol (PPP), for the corporate network solution (NEC). There are several reasons for implementing this protocol. The point-to-point protocol is a widely used industrial standard. PPP can be used to construct point-to-point links across various vendors' equipment since many versions of HDLC are private.

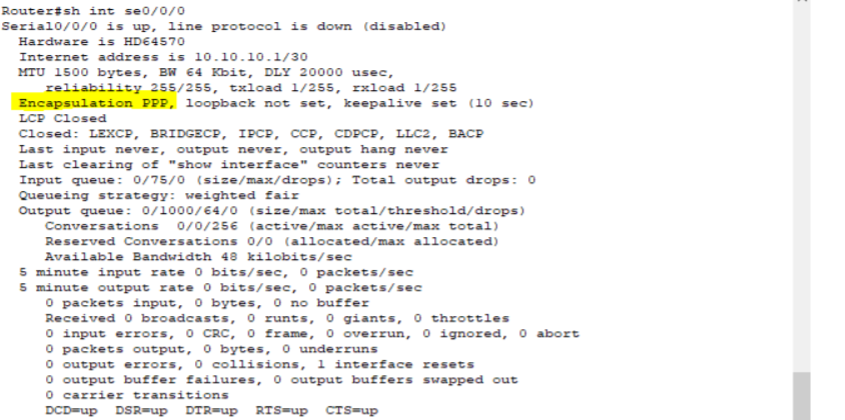
The Network layer protocol is identified by a Network Control Protocol field in the Data Link header.

Authentication, multilink connections, transmission encryption, and data compression are all possible with PPP.

## Configuration with result:



## Result



# Conclusion

As a result, different WAN solutions to a set of organizational needs are included in my presentation slides. Examining WAN technologies and selecting the most appropriate one for a set of company needs, comparing the benefits and downsides of private and public WAN technology, and configuring WAN protocols as part of an enterprise network solution are all covered in this presentation.

**Report on:**

**Deployment of network monitoring tools and troubleshooting methods**

**Prepared by: Bisesh Shrestha**

**Content**:

* Summary
* Introduction
* Network monitoring tools
* Troubleshooting methods
* Troubleshooting LAN and WAN connectivity issues at different networking layer
* Effective documentation of troubleshooting methods and steps
* Evaluation of troubleshooting method
* Effectiveness of troubleshooting method in solving enterprise-wide networking issues.
* Conclusion

## Summary

This report includes the deployment of network monitoring tools in the network for monitoring network devices such as routers, switches, and servers, as well as various types of troubleshooting methods for troubleshooting different types of networks such as LANs and WANs. Wan networks are made up of many LAN networks. Various sorts of troubleshooting techniques are used to troubleshoot the LAN, such as the ping method for connection, and the "show running-configuration" command in the privileged mode of the switch for displaying all the running configuration in the switch. Similarly, several sorts of troubleshooting methods are used to troubleshoot the wan, such as the ping method, tracert method, search method, and so on.

# P7 Deploy network monitoring tools and troubleshooting methods to establish network baselines and produce network documentation.

## Introduction

"Network monitoring may be characterized as a vital IT process in which all networking components such as routers, switches, firewalls, servers, and virtual machines are continually monitored for fault and performance in order to maintain and enhance their availability (manageengine.com, 2014)." Network monitoring should be proactive, which is one of the most critical aspects. We can simply find out about network device performance difficulties thanks to network monitoring, and it also eliminates network downtime and failures. Network monitoring technologies, such as Nagios XI, Wireshark, Network Time Protocol (NTP), NetFlow, and basic Network Management Protocol, are used to monitor the network (SNMP). The process of evaluating and resolving network issues is known as troubleshooting. In addition, network troubleshooting entails creating a network baseline, using methodical troubleshooting approaches, and obtaining data. I'll go through a few different sorts of troubleshooting approaches in the section below.

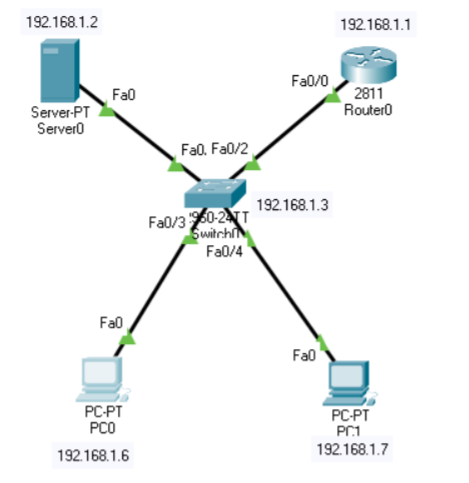
## Configuration of monitoring tool:

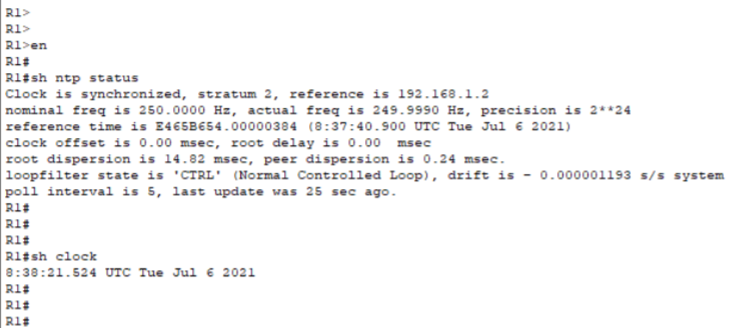
I used network time protocol as a monitoring tool (NTP). It's used to keep track of time. It's also utilized to allow network devices to synchronize their clocks with the central source clock. For network equipment such as routers, switches, servers, and firewalls, NTP is critical. It ensures that logging data and timestamps reflect the correct time and date. To function, NTP uses a hierarchical system of time sources and a client-server architecture. It uses an NTP source that ranges from stratum 0 to stratum 15.

Stratum 0 is an atomic clock that is not utilized in CISCO routers or switches, but stratum 1 through 15 are legitimate levels that are used in CISCO routers and switches. Furthermore, stratum 16 denotes that NTP is not synced. The internal clock of a CISCO router or switch has a default stratum level of 8. The Network Time Protocol is used to timestamp Syslog messages (NTP). NTP may be protected with an MD5-based authentication scheme. Authentication is required for all NTP packets that can update the clock.



## Configuration of Network Time Protocol (NTP)





## R1 configuration



SW1 configuration

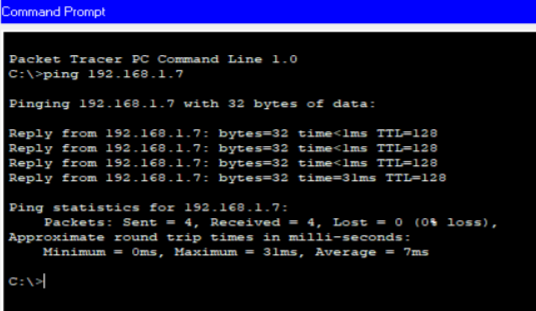


## Network Troubleshooting Procedures:

Network troubleshooting methods are critical for a network administrator. PING, TRACERT/TRACRROUTE, IPCONFIG/IFCONFIG, NSLOOKUP, and NETSTAT are some of the troubleshooting solutions available. A network manager may quickly diagnose the network using these troubleshooting methods. These are the troubleshooting strategies that I would take if I encountered an issue while utilizing a networking monitoring program. The following are a few of them:

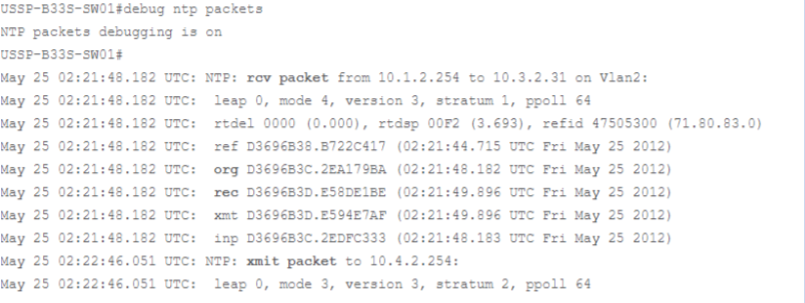
Ping:

The ping technique is a standard troubleshooting approach used by network administrators to determine whether or not there is a connection between network devices. This method is used to perform a basic connection test between the requesting host and the destination host. This is performed by using the Internet Control Message Protocol (ICMP), which allows you to send an echo packet to a target host and listen for a response from that host. Simply put, if the asking host receives a response from the destination host, this host is accessible. This strategy is often used to get a rudimentary picture of where a networking problem can exist. For e.g., while configuring NTP monitoring tool, if there occurs any problem while configuring, at first, I would check problem by doing ping. If source network is pinging the destination network, then there is no any problem or if there is problem while pining, there must be problem during configuration.



## Troubleshoot ntp packets

NTP does not work on received packets in the case below. Despite receiving NTP packets (as evidenced by debug ip packets), the NTP process does nothing with them. Because the NTP process must produce the packet, a debug ntp packets output is provided for any NTP packets that are sent out. The problem only affects received NTP packets that aren't handled.



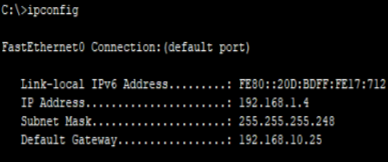
# P8 Troubleshoot LAN and WAN connectivity issues at different networking layers.

Basically, when troubleshooting the LAN and WAN connectivity, such network troubleshooting is done with the help of OSI (Open Systems Interconnection) model layer. There are seven layers in OSI model layer. Layer seven is application layer, layer six is presentation layer, layer five is session layer, layer four is transport layer, layer three is network layer, layer two is data link layer and layer one is physical layer. So, using theses networking layers, I have troubleshot LAN and WAN connectivity.

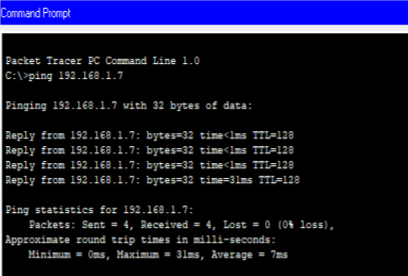
## Troubleshooting LAN connectivity:

Check cabal for connectivity issue: The physical layer of the OSI model layer is where cable connection is found. When a network problem arises, first inspect the cable to determine whether the problem is caused by the cable or not. We utilized straight through cable for connections between separate devices and crossover cable for connections between the same devices. For example, when connecting a router to a switch, use straight through cable; similarly, when connecting a switch to an end device, such as a user's computer, use straight through cable; nevertheless, when connecting a switch to another switch, use crossover cable. Check to see whether the cable is damaged as well.

Troubleshoot network ID and subnet mask of LAN for connectivity: The network ID and subnet mask of the LAN devices must match for communication within the LAN. I've used the command line to get the network id and subnet mask in this case. To run this command, open a command prompt (CMD) and type "IPCONFIG" followed by enter. This command displays the device's IP address and subnet mask. IPCONFIG is a TCP/IP tool that shows each network interface card's current TCP/IP setup parameters (NIC). As a result, the IPCONFIG command belongs to the OSI model layers 3 and 4. The output of the IPCONFIG command is shown in the diagram below:

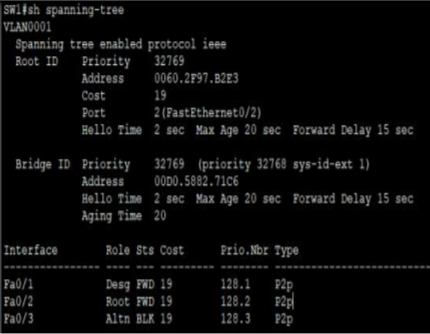


PING command for LAN connectivity: To use ping, type "ping 192.168.1.7" into the command line (cmd). The ping technique is part of the network layer. We normally use the PING function to see if there is a connection between the devices. The ping technique is one of the most frequent troubleshooting methods used by network administrators to determine whether or not there is a connection between network devices. This method is used to perform a basic connection test between the requesting host and the destination host. Using the Internet Control Message Protocol (ICMP), which can send an echo packet to a destination host and a mechanism to listen for a response from that host, this is accomplished.



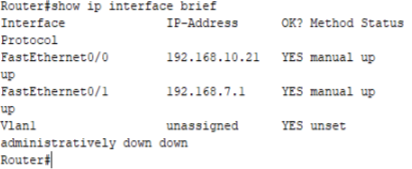
Troubleshoot Loop for LAN connectivity: It falls under the layer 2 of the OSI model for loop troubleshooting. When we employ switches in a local area network, we run the risk of creating a loop. A LAN loop can bring the entire network down. Using the Spanning Tree protocol, we can escape a loop (STP). If there are redundant network links, Spanning Tree is used to eliminate loops in the LAN and to choose the quickest network links. In the data link layer 2, the spanning tree protocol only serves as a routing mechanism.

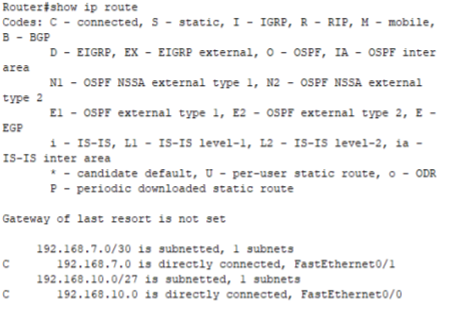
As a result, in order to eliminate the LAN loop, we must enable the spanning tree protocol in the layer 2 device switch.



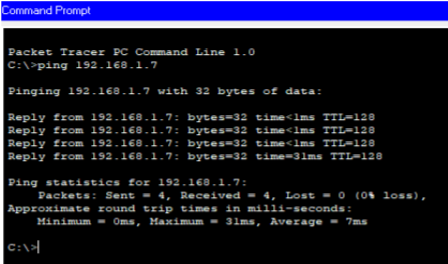
## Troubleshooting WAN protocol:

Checking IP address and Routing for troubleshooting WAN connectivity: In a WAN device such as a router, we assign IP addresses and employ routing protocol. Layer 3 devices are routers. We must assign IP address and routing protocol in the WAN device for packets to move within the WAN network, however if packets do not transfer inside the WAN network, we must check whether an IP address has been allocated to the WAN device. We must also verify whether the routing protocol is enabled in the WAN device, in addition to the IP address. To verify an IP address, use the "display ip interface short" command from the privileged mode of a layer three device known as a router.

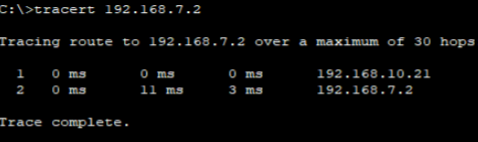




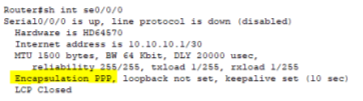
“Ping” command for troubleshooting WAN connectivity: Ping” command is a network layer utility and helps us to find out and troubleshoot whether the network is reachable or not. With the help of ping command, we can also know the status of the WAN device. If the ping command show successful output or no packet loss result, then we can reach in that network. But if there is breakage in cable and port down then Ping does not show the successful result. It shows the result by displaying packet loss. Figure below shows the result output while pinging FTPS server’s IP address from the user’s PC.



“Tracert” command for troubleshooting WAN connectivity: The Tracert command tool is part of the OSI model layer 3. The tracert command shows the path packets follow to get to the host. It will tell you how many hops it takes to get to the host and how long each hop takes. This helps us to troubleshoot the WAN network's accessible routes. The output of the tracert command is shown in the diagram below.



Checking WAN protocol such as PPP (Point to point protocol):The Point-to-Point Protocol (PPP) is a data link layer (layer 2) communication protocol that connects two routers directly without the use of a host or other networking. It will enable connection authentication, transmission encryption, and compression. We can only use a serial cable on a serial port to run the PPP protocol; we can't use a fast Ethernet or giga Ethernet cable. To test or debug PPP settings in the WAN device router, we must use the "display running-configuration" command from the router's privileged mode. This command displays the PPP configuration that is configured in the router's particular port. The outcome of debugging PPP protocol settings in WAN device "router" is shown in the diagram below:



|  |  |  |  |
| --- | --- | --- | --- |
| Test No | Expected result | Actual result | Evidence |
| 1 | I expect to see all of the connections from R1, R2 and R3 to be active, and the cables to be connected as specified in the addressing table | Using the command “show ip int brief” within all routers, it showed that all the interfaces except g0/1 on R2 were disabled. | To fix this, I went into each interface across all routers and used the command “no shut” to activate all the interfaces; this is shown in above figure. |
| 2 | I expect to see the clock rates on all the DCE interfaces to be configured at “64000”. | To show the clock rate, the command “show controllers s0/0/1” was inputted. The output of the command is shown in | To fix this, I went into int s0/0/1 as this was the interface that had the wrong configuration and as shown below in Figure above, I configured it to have the same clock rate as the other two DCE interfaces. |
| 3 | All serial interfaces should be configured to use PPP as the encapsulation n type. | To view whether the expected result was the case, the command “sh int s0/0/0” was inputted. As shown in Figure, the output of this command showed the interfaces to have HSRP as the encapsulation type. | To fix this issue, I entered the interfaces that were configured with the wrong configuration type and entered “encapsulation ppp”, this made the encapsulation type ppp. Shown in figure below is the change of encapsulation type once the above command was inputted.  **Examine encapsulation type**    **encapsulation type fixed** |
| 4 | Examine and set CHAP usernames and passwords – I expect to see each router to be configured with the correct CHAP usernames and passwords. | Examine and set CHAP usernames and passwords – I expect to see each router to be configured with the correct CHAP usernames and passwords. | As shown in Figure below, when the debug command was used, it showed that the interfaces on which PPP was meant to be configured were closed/misconfigured. |
| 5 | Verify IP addressing - I expect the IP addressing to match the IP addressing table above. | To view the IP addresses configured on the devices, I used to the command “sh ip int brief”. This showed that across the routers, some were misconfigured | Shown in Figure above is the addressing table on R2. This showed that whilst the serial interfaces were configured correctly, the gigabit Ethernet interface was not. |
| 6 | Verify full connectivity – I expect to be successful in being able to trace route a path from PC1 and PC3 to the webserver | When the commands “ping” and “tracert” were used, they were successful in reaching the webserver. | As shown below in Figure below, pinging was successful to each device. The PCs were able to ping the webserver and the webserver was able to ping the PCs.    Shown in Figure below is the trace route output which shows the path the PC take to reach the webserver. |

Conclusion:

To conclude this part, we firstly, presented the appropriated WAN solution by examining WAN technologies and also, analyzed the benefits of public and private WAN technologies. And, the network monitoring tools are evaluated along with the troubleshooting methods to create the network baselines

References

<https://www.ciscopress.com/articles/article.asp?p=2698000>

<https://www.auvik.com/franklyit/blog/hierarchical-network-design/>

<https://blog.netwrix.com/2019/01/08/network-devices-explained/>

<https://www.comptia.org/content/guides/what-is-a-wide-area-network>

<http://www.vce-download.net/study-guide/comptia-networkplus-6.1-differences-between-public-and-private-wan.html>

<https://www.pluralsight.com/blog/it-ops/wan-protocol>

<https://www.networkcomputing.com/data-centers/campus-network-design-models> <https://www.manageengine.com/network-monitoring/basics-of-network-monitoring.html>

<https://networkdirection.net/articles/network-theory/hierarchicalnetworkmodel/>

<https://www.researchgate.net/publication/4230253_An_Evaluation_of_the_Virtual_Router_Redundancy_Protocol_Extension_with_Load_Balancing/>

<https://searchsecurity.techtarget.com/answer/Arethere-security-benefits-to-using-a-site-to-site-VPN>

<https://www.vxchnge.com/blog/networkredundancy-explained>

<https://ccnacompletecourse.blogspot.com/2019/11/hierarchical-network-design.html>