CNS Assignment No. 2

WAN Network Configuration

Instructor's Name: Prof. B.P. Masram	**Student's Name: Ayush Chanekar**

Objectives: To learn & understand configuring IP Addresses, related network devices & access points as well as setting up a WAN.

Problem Statement:

Setup a WAN which contains wired as well as wireless LAN by using `packet tracer tool`.
Demonstrate transfer of a packet from LAN 1 (wired LAN) to LAN2 Wireless LAN.

Equipment & Software:

- Cisco Packet Tracer Software.
- Microsoft Windows 8.1, 10, 11 (64bit), Ubuntu 20.04, 22.04 LTS (64bit) or macOS 10.14 or newer
- amd64(x86-64) CPU
- 4GB of free RAM
- 1.4 GB of free disk space

Theory / Background

Comparison between LAN, MAN, WAN:

Characteristic	**LAN**	**MAN**	**WAN**
Definition	Local area network	Metropolitan area network	Wide area network
Coverage	Building/Campus	City/Large campus	Multiple cities/countries
Design and maintenance	Easy	Moderate	Difficult
Speed	High (100 Mbps to 10 Gbps)	Moderate to High (10 Mbps to 1 Gbps)	Variable (1 Mbps to several hundred Mbps)
Propagation delay	Short	Moderate	Long
Technology	Ethernet, Wi-Fi	Ethernet, FDDI, ATM	MPLS, Frame Relay, ATM, VSAT
Cost	Low	Moderate	High
Use Cases	Offices, Schools	Government, Universities	Internet, Corporate Networks
Security	Easier to secure	Moderately challenging	Most challenging
Fault tolerant	More tolerant	Less tolerant	Less tolerant
Congestion	Less	More	More

Wide Area Network (WAN)

A Wide Area Network (WAN) is a network that extends over a large geographical area, often connecting multiple Local Area Networks (LANs). WANs are essential for organizations that need to communicate across different locations, such as branch offices in different cities or countries. Unlike LANs, which are confined to a single location, WANs connect these geographically dispersed networks, enabling data sharing, communication, and resource access across vast distances.

Protocols in Wide Area Networks (WAN)

1. **Transmission Control Protocol/Internet Protocol (TCP/IP)**

TCP/IP is the foundational suite of protocols for communication over the Internet and most WANs. It includes several protocols like:

- **TCP**: Ensures reliable data transmission with error checking and recovery.
- **IP**: Handles the addressing and routing of packets across networks.

2. **Open Shortest Path First (OSPF)**

OSPF is a link-state routing protocol used within an Autonomous System (AS). It operates within a single administrative domain and uses Dijkstra's algorithm to find the shortest path for data transmission.

3. **Border Gateway Protocol (BGP)**

BGP is a path-vector protocol used to manage routing between different ASes on the Internet. It is critical for WANs that span across different networks and need efficient, scalable routing.

4. **Frame Relay**

Frame Relay is a packet-switched WAN protocol that operates at the data link layer. It is used for connecting local area networks (LANs) and transferring data between WAN endpoints using virtual circuits.

5. **Multiprotocol Label Switching (MPLS)**

MPLS is a method of ensuring efficient data packet forwarding in a WAN. It operates between the data link layer and network layer and is known for improving the speed and efficiency of routing.

6. **Point-to-Point Protocol (PPP)**

PPP is a data link layer protocol used to establish a direct connection between two network nodes. It is commonly used for internet connections over serial links and supports authentication, encryption, and compression.

7. **Synchronous Optical Networking (SONET)**

SONET is a standard for transmitting digital data over optical fiber. It is widely used in WANs due to its high-speed capabilities and ability to multiplex multiple streams of data onto a single optical fiber.

8. **Asynchronous Transfer Mode (ATM)**

ATM is a cell-based switching technique that uses fixed-size packets, called cells, to transmit data across a network. It is used in WANs for high-speed data transfer and can handle real-time traffic like voice and video.

9. **Internet Protocol Security (IPsec)**

IPsec is a protocol suite for securing IP communications by authenticating and encrypting each IP packet in a communication session. It is widely used in VPNs for securing data transfer over WANs.

10. **Dynamic Host Configuration Protocol (DHCP)**

DHCP is a network management protocol used to automatically assign IP addresses and other network configuration parameters to devices on a network, making it easier to manage and configure devices in a WAN.

11. **Simple Network Management Protocol (SNMP)**

SNMP is a protocol used for managing devices on IP networks. It is widely used in WANs to monitor and manage network devices like routers, switches, and servers.

12. **File Transfer Protocol (FTP)**

FTP is a standard network protocol used for transferring files from one host to another over a TCP-based network like the Internet. It is commonly used in WANs for the reliable transfer of large files.

13. **Hypertext Transfer Protocol (HTTP/HTTPS)**

HTTP is the foundation of data communication for the web. HTTPS is the secure version of HTTP, using encryption to protect data in transit, which is crucial in WAN environments.

14. **Voice over Internet Protocol (VoIP)**

VoIP is a protocol used for delivering voice communications and multimedia sessions over IP networks, including the Internet and WANs. It is essential for integrating voice services into WANs.

15. **Virtual Private Network (VPN) Protocols**

VPN protocols like PPTP, L2TP, and SSL/TLS are used to create secure connections over a WAN. They encrypt data and ensure privacy and security for users accessing a WAN remotely.

Layer 3 Routers

Routers operating at Layer 3 of the OSI model (the Network layer) are key components in WAN configurations.
These routers handle the task of forwarding data packets between different networks by analyzing the destination IP addresses. By using routing tables, a Layer 3 router determines the most efficient path to send packets to their intended destination across the WAN.
This routing capability is crucial for managing traffic between distant networks and ensuring that data reaches its endpoint efficiently.

IP Addressing in WANs

IP addressing is a fundamental aspect of configuring WANs. Each interface on a router must be assigned a unique IP address to facilitate communication across the network. WAN configurations often involve the use of both public and private IP addresses.
Public IP addresses are typically used on the WAN side to connect to the broader internet, while private IP addresses are used within the internal LANs. Subnetting may be employed to optimize IP address allocation and enhance network organization.

WAN Link Configuration

WAN links are the connections between routers in a WAN, and they can be physical or logical. These links are established using various technologies, including leased lines, MPLS (Multiprotocol Label Switching), VPNs (Virtual Private Networks), or internet-based connections.
Configuring WAN links involves setting up the interfaces on each router, assigning IP addresses, and enabling the necessary protocols to ensure reliable data transmission between remote sites.

Routing Protocols

Routing protocols are essential in WAN configurations, as they determine how routers communicate with each other to discover and maintain routes.
These protocols ensure that data is forwarded through the most efficient paths across the WAN. Several routing protocols can be used in WAN setups, each with its unique characteristics:

1. OSPF (Open Shortest Path First)

- **Type**: Link-state routing protocol.
- **Function**: OSPF calculates the shortest path for data packets based on the link states within the network. It rapidly adjusts to changes in the network topology, making it suitable for large and complex networks.
- **Usage**: Commonly used in enterprise networks due to its scalability and efficiency.

2. BGP (Border Gateway Protocol)

- **Type**: Path-vector routing protocol.
- **Function**: BGP is the protocol that governs how packets are routed across the internet. It manages the exchange of routing information between different autonomous systems (ASes) and makes routing decisions based on path, network policies, and rule-sets.
- **Usage**: Critical for internet service providers (ISPs) and large organizations that connect to multiple ISPs.

3. EIGRP (Enhanced Interior Gateway Routing Protocol)

- **Type**: Advanced distance-vector routing protocol.
- **Function**: EIGRP combines the best features of link-state and distance-vector protocols. It uses metrics such as bandwidth, delay, load, and reliability to determine the best path for data transmission.
- **Usage**: Primarily used in Cisco networks due to its proprietary nature.

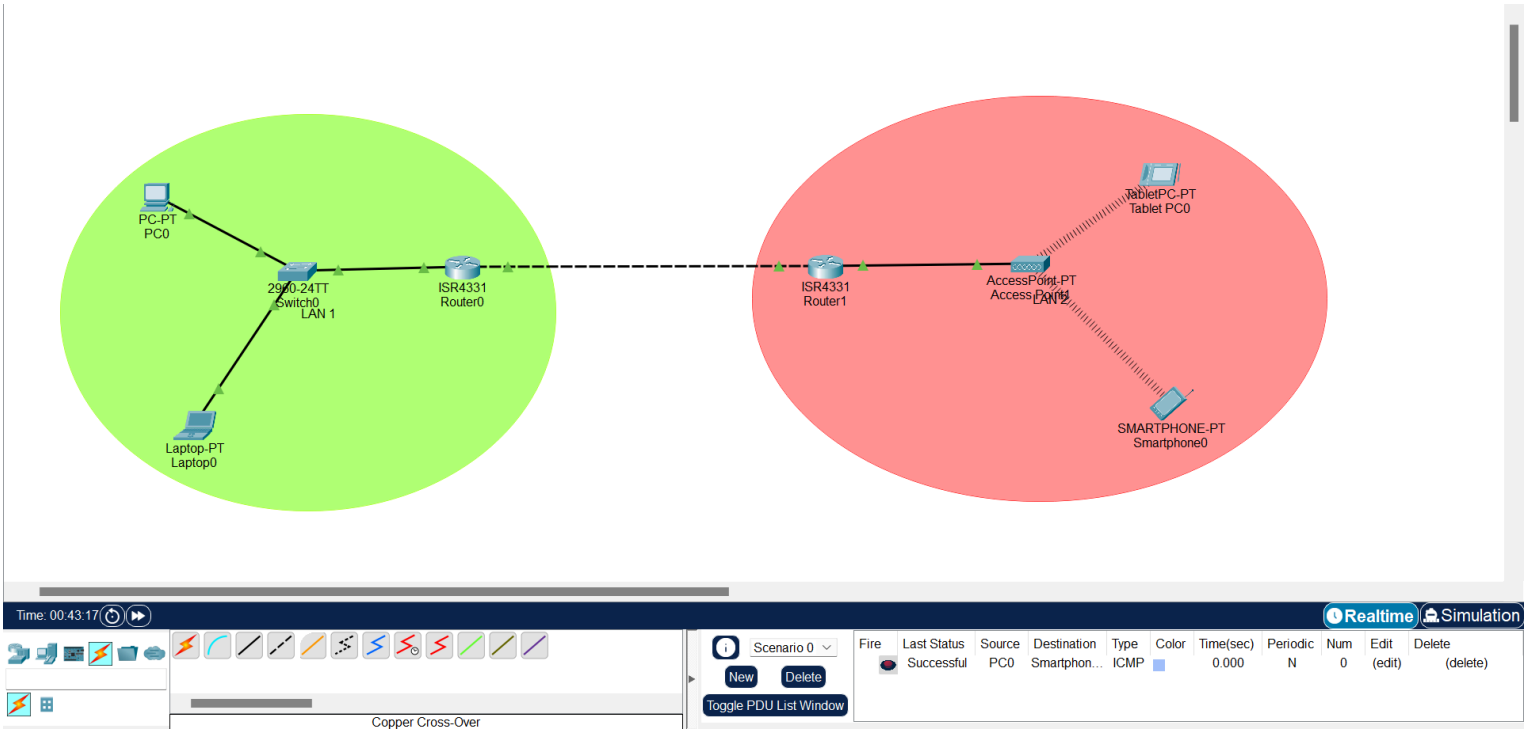
4. RIP (Routing Information Protocol)

- **Type**: Distance-vector routing protocol.
- **Function**: RIP uses hop count as its routing metric to determine the best path to a destination. It is one of the oldest routing protocols and is relatively simple to configure but less efficient in large networks.

- **Usage**: Suitable for smaller networks with simpler configurations.

5. MPLS (Multiprotocol Label Switching)

- **Type**: Data-carrying technique for high-performance telecommunications networks.
- **Function**: MPLS directs data from one network node to the next based on short path labels rather than long network addresses. This reduces the complexity of lookups in a routing table and speeds up the process.
- **Usage**: Often used by service providers to offer efficient and scalable networking solutions.



Observations

1. **Successful LAN Configuration:**
    - Two distinct LAN networks were created using Cisco Packet Tracer.
    - Each LAN was connected to a separate Layer 3 router.
    - The IP addressing scheme was correctly configured for both LANs, ensuring unique IP addresses within each subnet.
2. **Router Configuration:**
    - The routers were configured with appropriate IP addresses on their interfaces, connecting to each LAN.
    - Routing protocols (such as RIP or OSPF) were used to enable communication between the two LANs.
3. **Packet Transmission within LAN:**
    - Packets were successfully transmitted within each LAN.
    - Devices within the same LAN were able to communicate with each other using the configured IP addresses.
    - Ping tests and packet analysis confirmed low latency and no packet loss within the same LAN.
4. **Packet Transmission across LANs:**
    - Packets sent from one LAN to the other successfully traversed the router.
    - Routing tables were accurately updated, allowing for seamless inter-LAN communication.
    - Ping tests showed successful responses from devices in the other LAN, indicating proper router configuration and WAN setup.

Outcomes

1. **Understanding of LAN and WAN Setup:**
    - Gained hands-on experience in setting up and configuring LANs and interconnecting them using routers.
    - Developed a clear understanding of the role of routers in a WAN setup.
2. **Proficiency in Router Configuration:**

- Enhanced skills in configuring routers, including interface setup, IP addressing, and routing protocols.
- Successfully applied theoretical knowledge of routing to practical scenarios.

3. **Troubleshooting and Optimization:**

   - Identified and resolved potential configuration issues during the setup process.
   - Learned how to optimize network performance and ensure reliable communication across the network.

Conclusion

- **We have learnt & understood configuring IP Addresses, related network devices & access points as well as setting up a WAN**
- **We have setup a WAN which contains wired as well as wireless LAN by using `packet tracer tool`.**
- **We have demonstrated the transfer of a packet from LAN 1 (wired LAN) to LAN2 Wireless LAN.**