**CNS Assignment 1**

Experiment 1: Basic Network Configuration

**Problem Statement:**

Setup a wired LAN using Layer 2 Switch. It includes preparation of cable, testing of cable using line tester, configuration machine using IP addresses, testing using PING utility & demonstrating the PING packets captured traces using Wireshark Packet Analyzer Tool.

**Requirements:**

* Cat 3, Cat 5, Cat 5e Cat 6a Cables and RJ45 Connectors
* Crimping Tool
* Line Tester
* One server Node with Open Source and Internet Support
* HTTP Server (Apache) with Website pages of your Institute
* Four Client Nodes with Wi-Fi Support
* Wireshark Protocol Analyzer on all nodes
* Layer-II Switch
* IP Address Configuration Chart

**Computer Networks**:   
A computer network can be defined as a collection of computing devices (nodes) interconnected by wires or wireless means and governed by a set of standards(protocols) in order to share data and resources.

**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 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Layer No.** | **OSI Model Layers** | **TCP/IP Model Stages** | **Devices** | **Protocols** | **Services** |
| 1 | Physical | Network Access | Hubs, Repeaters, Cables | Ethernet, USB | Bit transmission |
| 2 | Data Link | Network Access | Switches, Bridges | Ethernet, PPP, Frame Relay, MAC, ARP | Data framing, MAC addressing, Error detection |
| 3 | Network | Internet | Routers | IP (IPv4, IPv6), ICMP, IPSec, ARP | Logical addressing, Routing |
| 4 | Transport | Transport | - | TCP, UDP | End-to-end communication, Flow control, Error correction |
| 5 | Session | Application | - | NetBIOS, PPTP, RPC | Session management, Authentication |
| 6 | Presentation | Application | - | SSL/TLS, FTP, JPEG, MPEG, GIF | Data translation, Encryption/Decryption |
| 7 | Application | Application | - | HTTP, HTTPS, FTP, SMTP, DNS, Telnet, POP3, IMAP, SNMP | Network services to end-users |

**OSI and TCP/IP model layers:**

**Types of cables:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Characteristic | Twisted Pair Cable | Coaxial Cable | Fiber Optic Cable | Ethernet Cable |
| Description | Consists of pairs of insulated copper wires twisted together. | Consists of a central conductor, insulating layer, metallic shield,  and outer  insulating layer. | Uses light to transmit data through strands of glass or plastic. | Typically twisted pair cables but can also include coaxial and fibre optic cables. |
| Types | UTP (Unshielded Twisted Pair), STP (Shielded Twisted Pair) | RG-6, RG-59 | Single mode, multi-mode | Cat5, Cat5e, Cat6, Cat6a, Cat7, Cat8 |
| Installation | Easy to install and maintain | More difficult than twisted pair but easier than fiber optic | More complex and expensive installation | Varies: Twisted pair cables are easy, fibre optic cables are more complex |
| Cost | Low | Moderate | High | Varies: Twisted pair is low; fibre optic is high |
| Use Cases | Telephony, Ethernet networks | Cable TV, Internet, Telecommunications | |  | | --- | | Telecommunications |  |  | | --- | | High-speed data transmission, Backbone networks | | LANs, Data centres, High-speed internet connections |
| Advantages | Cost-effective, Flexible, Easy to install | Higher bandwidth than twisted pair, better shielding | Extremely high bandwidth, Long-distance capabilities | High speed (especially Cat6 and above), Reliable |
| Disadvantages | |  | | --- | |  |  |  | | --- | | Limited bandwidth and distance, Susceptible to interference | | Bulky, Limited distance compared to fibre optic | Expensive, Fragile, Complex installation | Varies: Twisted pair has limited distance and speed; Fiber optic is expensive and fragile |

**Popular Sniffing Tools**

* BetterCAP
* Ettercap
* Wireshark
* Tcpdump
* WinDump
* OmniPeek
* Dsniff
* EtherApe
* MSN Sniffer
* NetWitness
* NextGen

**Features of Wireshark**

* Available for UNIX & Windows
* Capture live packet data from network interface
* Display packets with very detailed protocol information
* Open & Save packet data captured
* Import & Export packet data from & to a lot of other capture programs
* Filter packets, search for packets on many criteria
* Colorize packet display based on filters
* Create various statistics

**Commands used:**

1. ‘ifconfig’ command

The ifconfig (interface configuration) command is used to configure, manage, and query network interface parameters in Unix-based systems, including Linux. It's a powerful tool for network management, allowing users to view and change the configuration of network interfaces.

This command displays all active network interfaces and their configurations, such as IP addresses, netmask, and broadcast addresses.

1. ‘sudo wireshark’ Command

wireshark is a powerful network protocol analyser that allows users to capture and interactively browse the traffic running on a computer network. Running it with sudo (superuser do) grants the necessary permissions to capture packets on network interfaces.

* **sudo**: This prefix runs the command with superuser privileges. Capturing network packets usually requires elevated permissions.
* **wireshark**: Launches the Wireshark GUI.

When you run sudo wireshark, the application starts with root privileges, enabling it to capture network packets on all available interfaces. It provides a graphical interface to:

* Start and stop packet captures.
* Apply filters to capture only specific types of traffic.
* Analyze packet details to troubleshoot network issues, investigate security incidents, or study protocol behaviour.

**Types of Connectors:**

* RJ45 (Registered Jack 45): An eight-pin connector commonly used for Ethernet networking.
* RJ11 (Registered Jack 11): A four or six-pin connector commonly used for telephone connections.
* RJ14 (Registered Jack 14): A six-pin connector similar to RJ11 but used for two telephone lines.
* RJ21 (Registered Jack 21): A 50-pin connector often referred to as a "telco" connector.
* BNC (Bayonet Neill–Concelman): A quick connect/disconnect RF connector.
* USB (Universal Serial Bus): A standard connector for peripheral devices.
* HDMI (High-Definition Multimedia Interface): A connector for transmitting audio and video signals.
* Thunderbolt: A high-speed interface developed by Intel and Apple.

**PING command (Packet Internet Groper):**

The ping command is a network utility used to test the reachability of a host on an Internet Protocol (IP) network. It is also used to measure the round-trip time for messages sent from the originating host to a destination computer.

‘ping’ uses the ICMP protocol’s mandatory ECHO\_REQUEST datagram to elicit an ICMP ECHO\_RESPONSE from a host or gateway. ECHO\_REQUEST datagrams (‘’ping’’) have an IP and ICMP header, followed by a ‘struct timeval’ and then an arbitrary number of “pad” bytes used to fill out the packet.

* -c count: Send count number of packets and then stop.
* -i interval: Wait interval seconds between sending each packet. The default is one second.
* -s packetsize: Specify the number of data bytes to be sent. The default is 56, which translates into 64 ICMP data bytes when combined with the 8 bytes of ICMP header data.
* -t ttl: Set the Time To Live (TTL) value for the packets.
* -W timeout: Time to wait for a response, in seconds.

**Switch vs Router vs Bridge vs Hub**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Switch | Router | Bridge | Hub |
| Layer | Data Link (Layer 2) | Network (Layer 3) | Data Link (Layer 2) | Physical (layer 1) |
| Function | Connects devices within a LAN, forwards data based on MAC addresses | Connects multiple networks, routes data between them based on IP addresses | Connects 2 or more network segments, filters traffic based on MAC addresses | Connects multiple Ethernet devices, broadcasts data to all ports |
| Addressing | MAC addresses | IP addresses | MAC addresses | None |
| Traffic isolation | Yes | Yes | Yes | No |
| Plug and play | Yes | No | Yes | Yes |
| Optimal routing | No | Yes | No | No |
| Cut through | Yes | No | No | Yes |

**Troubleshooting:**

When a ping is made from machine A to machine B which are connected through a switch through the wireshark sniffing tool and

Case 1: The IP of machine B isn’t correctly mentioned while pinging through A then the wireshark on machine A shows ‘Destination Host Unreachable’ error message.

Case 2: The wireshark on machine B is closed during the process then the wireshark on machine A shows ‘Destination Host Unreachable’ error message.

Case 3: The machine B is shut down in between the process then the wireshark on machine A shows ‘Destination Host Unreachable’ error message.

Case 4: The class of IPs of the machines aren’t same then the wireshark on machine A shows ‘Network Unreachable’ error message.

**Graphic Symbols in Cisco Packet Tracer:**

1. Bridge
2. Switch
3. Router
4. Access switch
5. Personal computer
6. Web server
7. VLAN
8. Ethernet
9. Serial line
10. Hub

Q) Assume a network with ‘n’ devices. Calculate how many links required to setup a network with the following topologies

|  |  |
| --- | --- |
| **Topologies** | **Number of links** |
| Ring | n |
| Bus | n |
| Mesh | = |
| Star | n |

**LAN Setup:**

A diagram of a computer network

Description automatically generated