Unit 1

Network Management Techniques & Cisco IOS

Basic Commands

1. **IPCONFIG:** This is a command-line application which displays all the current TCP/IP (Transmission Control Protocol/Internet Protocol) network configuration. Give us information about IP address, subnet mask, default gateway etc.
2. **ipconfig/all** : This command is use to access the detail of layer two that is Datalink layer which uses MAC address.
3. **Nslookup**: The nslookup command stands for "name server lookup." It helps you find the domain name associated with an IP address or the IP address associated with a domain name.
4. **Ping**: This command is used to check whether the ip address is reachable from the host system or not.
5. **Tracert**: This command is used to trace the route means the path taken by the packet while travelling from source to destination.
6. **Netstat**: The netstat command generates displays that show network status and protocol statistics. You can display the status of TCP and UDP endpoints in table format, routing table information, and interface information. netstat displays various types of network data depending on the command line option selected.

Configuring Cisco Router

Commands

1. Enable (privilege mode)
2. Configer terminal
3. Int f0/0 (Interface in which you want to assign the IP)
4. Ip address 192.168.1.2 255.255.255.0 (assign the IP and subnet mask)
5. no shutdown (on the device)

Virtual LAN

A VLAN (Virtual Local Area Network) is a logical grouping of devices within a network, even if they are not physically connected on the same network switch. VLANs enable network administrators to segment their network into smaller, isolated broadcast domains, improving network efficiency, security, and management.

VLAN is created on the Layer 2 switch to reduce the size of the broadcast domain. It is one of the technologies used to improve network performance by the separating of large broadcast domains into smaller ones.

There are 5 main types of VLANs depending on the type of network they carry:

1. **Default VLAN –** When the switch initially starts up, all switch ports become a member of the default VLAN (generally all switches have default VLAN named as **VLAN 1**), which makes them all part of the same broadcast domain. Using default VLAN allows any network device connected to any of the switch port to connect with other devices on other switch ports. One unique feature of Default VLAN is that it can't be renamed or delete.
2. **Data VLAN –** Data VLAN is used to divide the whole network into 2 groups. One group of users and other group of devices. This VLAN also known as a user VLAN, the data VLAN is used only for user-generated data. This VLAN carrying data only. It is not used for carrying management traffic or voice.
3. **Voice VLAN –** Voice VLAN is configured to carry voice traffic. Voice VLANs are mostly given high transmission priority over other types of network traffic. To ensure voice over IP (VoIP) quality (delay of less than 150 milliseconds (ms) across the network), we must have separate voice VLAN as this will preserve bandwidth for other applications.
4. **Management VLAN –** A management VLAN is configured to access the management capabilities of a switch (traffic like system logging, monitoring). VLAN 1 is the management VLAN by default (VLAN 1 would be a bad choice for the management VLAN). Any of a switch VLAN could be define as the management VLAN if admin has not configured a unique VLAN to serve as the management VLAN. This VLAN ensures that bandwidth for management will be available even when user traffic is high.
5. **Native VLAN –** This VLAN identifies traffic coming from each end of a trunk link. A native VLAN is allocated only to an 802.1Q trunk port. The 802.1Q trunk port places untagged traffic (traffic that does not come from any VLAN) on the native VLAN. It is best to configure the native VLAN as an unused VLAN.

Document a Network

Documenting a network involves creating a comprehensive record of the network's design, settings, and equipment. Here's a basic outline on how you can approach this task:

Network Diagram: Create a visual representation of your network. This should include all devices (routers, switches, servers, workstations, printers, etc.), their connections, and the IP addresses assigned to them.

Inventory of Equipment: Make a list of all network devices, including their make, model, and any other relevant details. This can also include software versions if applicable.

IP Addressing Scheme: Document your network's IP addressing scheme. This should include details about DHCP ranges, static IP addresses, and subnet masks.

Network Settings: Record important network settings such as DNS servers, gateway addresses, and VLAN configurations.

Security Measures: Document the security measures in place. This can include firewall rules, VPN configurations, and access control lists.

The goal of network documentation is to provide a clear understanding of the network's design and operation. It should be detailed enough that another network

professional could use it to understand and troubleshoot the network Document a Network.

Monitor traffic load

Monitoring traffic load in Cisco devices can be done using various methods. Here are some of the ways you can monitor traffic loads.

- **Command-Line Interface (CLI):** The Cisco IOS Command-Line Interface (CLI) provides several commands to monitor traffic on router interfaces. The show interface [interface_name] command is commonly used1.
- **Show Controllers Utilization Command**: Use the show controllers [interface-id] utilization command in EXEC mode to display bandwidth utilization on the switch or specific ports2.
- **NetFlow IP Top-Talkers**: Use the netflow ip top-talkers command to see the IP protocols utilization1.
- Show Interface Summary Command: Use the show interface summary or show interface [interface_name] summary command to see average statistics for "load-interval" which is by default 5 minutes3.
- **Cisco Security Packet Analyzer**: This tool provides several dashboards and tools to help you monitor and analyze your network traffic data

Use Diagnoses tools

Network diagnostic tools are software applications and utilities that help network administrators and technicians identify and resolve network issues12. These tools are designed to:

- **Analyse network performance**: They monitor the network's speed and latency, helping to identify any performance issues.
- **Identify problems**: These tools can detect issues such as slow speeds, network connection problems, packet loss on overloaded network devices, or missing information in your routing table and other system databases.
- **Provide insights into the functioning of the network**: They give you details about the network like latency values and the hostname of the device

Wireshark is the one of the best network diagnostic tools and troubleshooting software.

Set-up a TFTP server to back-up IOS images.

Network traffic monitoring is an essential part of any network administration toolkit. It can help to prevent problems from occurring and can also be used to troubleshoot existing issues.

As a network administrator, you should always have a backup for worse conditions. One of the common worse conditions that can occur is the IOS image of a device being deleted. This condition gets worse if there is no backup of the IOS image present.

So to ignore conditions like these, a backup should be a must and here we will take a Cisco IOS image backup on the TFTP server.

Trivial File Transfer Protocol (TFTP)
TFTP is a simple file transfer protocol that is either used to put or get a file from a remote host. It uses UDP port number 69.
But TFTP is used where no authentication and control are required. Also, it takes less overhead. While on the other hand, it is less interactive than FTP. Therefore, according to the need, FTP or TFTP is used.

Setting up a TFTP server to back up IOS images in Cisco involves several steps. Here's a general guide:

- **Set Up a TFTP Server**: First, you need to set up a TFTP server. There are several free TFTP software available like Tftpd64 and 3Com Daemon1. Make sure the TFTP server is running and accessible from the Cisco device2.
- **Connect the Cisco Device to the TFTP Server**: Connect your Cisco router or switch directly or through another network device to the TFTP server1.
- **Configure IP Addresses**: Configure IP addresses on both the router and the TFTP server to ensure they can communicate with each other1.
- **Check the Flash**: Use the show flash command on your Cisco device to make sure you have enough space for the backup3.
- **Transfer the IOS Image**: Place the IOS image in the root folder of the TFTP server on your computer3. Then, use the copy flash: tftp: command on your Cisco device to start the backup process. You will be prompted to enter the IP address of the TFTP server and the name of the IOS image file3.
- **Verify the Backup**: After the backup process is complete, verify the IOS image on the TFTP server to ensure the backup was successful