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.

What is subnet Mask?

A subnet Mask is generated by setting all the network bits 1 and host bits 0.

What is Default Gateway?

Default gateway of the system is the IP address of the first router it is hitting.

Above are the Layer 3 means Network layer information we are accessing. Network Layer uses IP addresses.

1. **ipconfig/all** : This command is use to access the detail of layer two that is Datalink layer which uses physical address or MAC address.
2. **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.
3. **Ping**: This command is used to check whether the ip address is reachable from the host system or not.
4. **Tracert**: This command is used to trace the route means the path taken by the packet while travelling from source to destination.
5. **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.

Routing

Routing involves determining the best path for data packets to travel from the source to the destination across a network.

Types of routing

1. **Static Routing**: In static routing, network administrators manually configure the routing table on each router. Routes do not change unless an administrator manually updates the routing table. It's simple to configure but lacks flexibility in dynamic network environments.
2. **Dynamic Routing**: Dynamic routing protocols automate the process of updating routing tables based on network changes. Routers exchange routing information with neighbouring routers to dynamically learn about network topology and choose the best paths. Examples of dynamic routing protocols include RIP (Routing Information Protocol), OSPF (Open Shortest Path First), and BGP (Border Gateway Protocol).

Static Routing Vs Dynamic Routing

Feature	Static Routing	Dynamic Routing
Configuration	Manually configured by network admins.	Automatically updated by routing protocols.
Route Updates	Routes remain fixed until manually changed.	Routes are dynamically updated based on network changes.
Scalability	Less scalable, requires manual updates for changes.	More scalable, adapts to network changes without manual intervention.
Complexity	Simple configuration but less adaptable.	More complex configuration but highly adaptable to network changes.
Convergence Time	Faster convergence as routes don't change dynamically.	Slower convergence as routes need time to update in response to network changes.

Routing Information Protocol

RIP stands for Routing Information Protocol. It's one of the oldest distance vector routing protocols used in computer networks. RIP operates based on the Bellman-Ford algorithm and is primarily designed for small to medium-sized networks.

RIP uses several timers to control various aspects of its operation:

1. **Route Update Timer (Update Interval)**: This timer determines how frequently routers send routing updates to their neighboring routers. By default, the

update interval is 30 seconds. Routers exchange their entire routing tables with neighboring routers during these updates.
2. **Route Timeout Timer**: This timer specifies the maximum time a router waits without receiving updates about a particular route before considering the route invalid. By default, the timeout period is set to 180 seconds (6 times the update interval).
3. **Route Flush Timer**: After a route is deemed invalid due to expiration of the timeout timer, the flush timer specifies how long the router waits before removing the route from its routing table. By default, the flush timer is set to 240 seconds.
4. **Holddown Timer**: The holddown timer is activated when a router receives a route advertisement with a higher metric for a previously known route. During the holddown period, the router maintains the existing route in its table and refrains from accepting any new route updates for that destination. This helps prevent routing loops. The default holddown period is 180 seconds.

These timers help RIP routers maintain accurate and up-to-date routing information while also preventing routing loops and minimizing the impact of temporary network fluctuations.

Feature	RIP Version 1	RIP Version 2
Classful/Classless	Classful	Classless
Subnet Mask	Not included	Included
Authentication	Not supported	Supported
Addressing	Broadcast	Broadcast or Multicast
Route Tagging	Not supported	Supported
Next Hop	Not supported	Supported
Backward Compatibility	N/A	Supported

Zinin's Routing Principle

Zinin's routing principles, as described in Alex Zinin's book "Cisco IP Routing", are fundamental concepts that help understand, configure, and troubleshoot routing issues. They are as follows:

Principle 1: Every router makes its decision alone, based on the information it has in its own routing table.

Principle 2: The fact that one router has certain information in its routing table does not mean that other routers have the same information.

Principle 3: Routing information about a path from one network to another does not provide routing information about the reverse, or return, path.

These principles highlight the autonomous nature of routers and the importance of complete and accurate routing information for effective network communication.

Brodar Gateway Protocol

- **Inter-Autonomous System Configuration**: BGP's main role is to provide communication between different autonomous systems.
- **Path Information**: BGP advertisements include path information, along with the reachable destination and next destination pair.
- **Policy Support**: BGP can implement policies that can be configured by the administrator.
- **Runs Over TCP**: BGP runs over Transmission Control Protocol (TCP), which provides reliable delivery of BGP updates.
- **Supports CIDR**: BGP supports Classless Inter-Domain Routing (CIDR), which allows for efficient allocation of IP addresses.

Enhanced Interior Gateway Routing Protocol

- **Advanced Distance Vector Routing Protocol**: EIGRP is an advanced distance vector routing protocol that finds the best path between any two-layer 3 devices to deliver the packet.
- **Classless Routing Protocol**: EIGRP is a classless routing protocol that supports Variable Length Subnet Mask (VLSM).
- **Fast Convergence**: EIGRP converges quickly, which means it is able to quickly establish the best path for data transmission.
- **Supports Multiple Network Layer Protocols**: EIGRP supports multiple network layer protocols such as IPv4, IPv6 etc.
- **Uses Multicast for Routing Updates**: EIGRP uses the multicast address of 224.0.0.10 for routing updates

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.
6. **Port-based VLAN:** In a port-based VLAN, each port on an organization switch is relegated to a particular VLAN. All traffic on that port is then naturally appointed to the VLAN related with that port.
7. **Tagged VLAN:** A Tagged VLAN is utilized to help different VLANs on a solitary actual port. In this kind of VLAN, every parcel is labeled with a VLAN ID, which recognizes the VLAN to which it has a place. This permits different VLANs to be persisted in a solitary actual port.
8. **Protocol-based VLAN**: A protocol-based VLAN utilizes Layer 3 convention data to dole out bundles to a VLAN. For instance, all traffic for a particular convention, like IPX, could be relegated to a particular VLAN. This kind of VLAN is less ordinarily utilized contrasted with port-based and labeled VLANs.

Commands for configuring the VLANs

1. config t
2. hostname sw1
3. vlan 10
4. name salse
5. vlan 20
6. name marketing

Now vlan has been created now to see the vlan type (show vlan)

1. Now to assign the ports type

int range f0/1-3

switchport access vlan 10

1. Same for vlan 20

Int range f0/4-6

Switchport access vlan 20

What Is Network Traffic Monitoring?

Network Traffic Monitoring is the process of gathering, analyzing, and reporting on network traffic data to troubleshoot network problems, optimize performance, or better understand overall network activity.

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.

Configuration –

Here is a simple topology in which there is a router (for which we will take IOS backup) and a TFTP server. The router has IP address 10.1.1.1/24 and the TFTP server has IP address 10.1.1.2/24.

We see an IOS image file in flash (.bin file) by command:

```
router#show flash
```

Now, we will copy this file to our Tftp server by command:

```
router#copy flash: tftp:
Source filename[]? c1841-advipservicesk9-mz.124-15.T1.bin
Address or name of remote host []? 10.1.1.2
Destination filename [c1841-advipservicesk9-mz.124-15.T1.bin]? routerios
```

- **Source filename** – It is the name of the IOS image file. here, it is named c1841-advipservicesk9-mz.124-15.T1.bin (shown in flash).
- **Address or name of remote host** – It is the IP address of the TFTP server. In our scenario, it is 10.1.1.2.
- **Destination filename** – It is the name of the destination file that will be put in the TFTP server. Here, we have named it routerIOS.

The file has been copied to the TFTP server.

Now to copy the IOS file from the TFTP server we will use the command:

```
rommon 1>tftpdnld
```

Now, as soon as we type this command, we see the parameters which we have to enter next.

```
ROMMON 2>IP_ADDRESS=10.1.1.1
ROMMON 3>IP_SUBNET_MASK=255.255.255.0
ROMMON 4>DEFAULT_GATEWAY=10.1.1.2
ROMMON 5>TFTP_SERVER=10.1.1.2
ROMMON 6>TFTP_FILE=routerios
```

After we have entered these commands, we will again enter the command tftpdnld.