

Content:-

Part One: Switch Configuration:-

1. Initial Configuration
2. CISCO Discovery Protocol (CDP)
3. Implementing Port Security
4. Implementing and verifying Virtual LANs (VLAN)
5. Implementing Inter-VLAN Routing
6. Implementing VLAN Trunking Protocol (VTP)
7. Verifying Spanning tree Protocols (STP)
8. Ether-Channel Configuration

Part Two: Network administration and troubleshooting:-

9. Password Recovery
10. Backing Up and Restoring Cisco IOS Software and Configurations

Part Three: Router Configuration:-

11. Static (Default) Routing Protocol
12. Routing Information Protocol (RIP) Configuration
13. Open Short Path First (OSPF) Configuration
14. Enhancement Interior Gateway Routing Protocol (EIGRP) Configuration

Part Four: WAN Configuration:-

15. Implementing Leased Line Cable (PPP & HDLC)
16. Frame-relay Configuration

Part Five: IPv6 Address Routing Configuration:-

17. IPv6 Routing Protocol (RIPng)

Part six: Security Configuration:-

18. Implementing and Verifying Access Control List (ACL)
19. Network Address Translation (NAT) Configuration
20. Security Device Manager (SDM)

Part one: Switch Configuration

Router Mode:

Mode	Name
Router>	User mode
Router#	Privileged mode (also known as EXEC-level mode)
Router(config)#	Global configuration mode
Router(config-if)#	Interface mode
Router(config-subif)#	Sub-interface mode
Router(config-line)#	Line mode
Router(config-router)#	Router configuration mode

1. Initial Configuration:-

- Configuring a Router Name

Router(config)#hostname cisco The name can be any word you choose

- Configuring Passwords

Router(config)#enable password cisco Sets enable password

Router(config)#enable secret class Sets enable secret password

- Console

Router(config)#line console 0 Enters console line mode

Router(config-line)#password console Sets console line mode password

Router(config-line)#login Enables password checking at login

- Telnet

Router(config)#line vty 0 4 Enters vty line mode for all five vty

Router(config-line)#password telnet Sets vty password to telnet

Router(config-line)#login Enables password checking at login

- Password Encryption

Router(config)#service password-encryption Applies a weak encryption to Passwords

Router(config)#no service password-encryption Turns off password encryption

- Configuring a Serial Interface

Router(config)#interface s0/0/0 Moves to serial interface 0/0/0 configuration mode

Router(config-if)#description Link to ISP Optional descriptor of the link is locally significant

Router(config-if)#ip address 192.168.10.1 255.255.255.0 Assigns address and subnet mask to interface

Router(config-if)#clock rate 56000 Assigns a clock rate for the interface

Router(config-if)#no shutdown Turns interface on

- Configuring a Fast Ethernet Interface

Router(config)#interface fastethernet 0/0 Moves to Fast Ethernet 0/0 interface configuration mode

Router(config-if)#description Accounting LAN Optional descriptor of the link is locally significant

Router(config-if)#ip address 192.168.20.1 255.255.255.0 Assigns address and subnet mask to interface

Router(config-if)#shutdown Turns interface off

Router(config-if)#no shutdown Turns interface on

Switch(config-if)#duplex auto Enables auto-duplex config

Switch(config-if)#speed auto Enables auto speed configuration

- Creating a Message-of-the-Day Banner

Router(config)#banner motd # Building Power will be interrupted next Tuesday evening from 8 – 10 PM.
#

Router(config)#

is known as a delimiting character. The delimiting character must surround the banner message and can be any character so long as it is not a character used within the body of the message.

- Creating a Login Banner

Router(config)#banner login # Authorized Personnel Only! Please enter your username and password. #

Router(config)#

is known as a delimiting character. The delimiting character must surround the banner message and can be any character so long as it is not a character used within the body of the message.

- Setting the Clock Time Zone

Router(config)#clock timezone EST -5

Sets the time zone for display purposes. Based on coordinated universal time. (Eastern Standard Time is 5 hours behind UTC.)

- Assigning a Local Host Name to an IP Address

Router(config)#ip host London 172.16.1.3

Assigns a host name to the IP address. After this assignment, you can use the host name rather than an IP address when trying to Telnet or ping to that address.

Router#ping London = Router#ping 172.16.1.3

Both commands execute the same objective: sending a ping to address 172.16.1.3

Router(config)#no ip domain-lookup

Router(config)#

Turns off trying to automatically resolve an unrecognized command to a local host name

- The logging synchronous Command

Router(config)#line console 0 Moves to line console configuration mode.

Router(config-line)#logging synchronous

turns on synchronous logging, Information items sent to the console will not interrupt the command you are typing. The command will be moved to a new line.

- The exec-timeout Command

Router(config)#line console 0 Moves to line console configuration mode.

Router(config-line)#exec-timeout 0 0

Sets the time limit when the console automatically logs off. Set to 0 0 (minutes seconds) means the console never logs off.

- Saving Configurations

Router#copy running-config startup-config Saves the running configuration to local NVRAM

Router#write memory Saves the running configuration to local NVRAM

Router#copy running-config tftp Saves the running configuration remotely to a TFTP server

- Erasing Configurations

Router#erase startup-config Deletes the startup configuration file from NVRAM

- Resetting Switch Configuration

Switch#delete flash: vlan.dat Removes the VLAN database from flash memory.

Delete filename [vlan.dat]? Press Enter.

Delete flash: vlan.dat? [Confirm] Reconfirm by pressing Enter

Switch#erase startup-config Erases the file from NVRAM. <Output omitted>

Switch#reload Restarts the switch.

- Setting IP Addresses and Default Gateways

Switch(config)#interface vlan 1 Enters the virtual interface for VLAN 1, the default VLAN on the switch

Switch(config-if)#ip address 172.16.10.2 255.255.255.0

Sets the IP address and netmask to allow for remote access to the switch

Switch(config-if)#exit

Switch(config)#ip default-gateway 172.16.10.1 Allows IP information an exit past the local network

- Managing the MAC Address Table

Switch#show Mac address-table Displays current MAC address forwarding table

Switch#clear Mac address-table Deletes all entries from current MAC address forwarding table

Switch#clear Mac address-table dynamic Deletes only dynamic entries from table

- Configuring Static MAC Addresses

Switch(config)#Mac address-table static aaaa.aaaa.aaaa vlan 1 interface fastethernet 0/1

Sets a permanent address to port fastethernet 0/1 in VLAN 1

- Show Commands

Router#show? Lists all show commands available.

Router#show interfaces Displays statistics for all interfaces.

Router#show interface serial 0/0/0
Displays statistics for a specific interface (in this case, serial 0/0/0).

Router#show ip interface brief
Displays a summary of all interfaces, including status and IP address assigned.

Router#show controllers serial 0/0/0
Displays statistics for interface hardware. Statistics display if the clock rate is set and if the cable is DCE, DTE, or not attached.

Router#show clock Displays time set on device.

Router#show hosts
Displays local host-to-IP address cache. These are the names and addresses of hosts on the network to which you can connect.

Router#show users Displays all users connected to device.

Router#show history Displays the history of commands used at this edit level.

Router#show flash Displays info about flash memory.

Router#show version Displays info about loaded software version.

Router#show arp Displays the Address Resolution Protocol (ARP) table.

Router#show protocols Displays status of configured Layer 3 protocols.

Router#show startup-config Displays the configuration saved in NVRAM.

Router#show running-config Displays the configuration currently running in RAM.

Router(config)#do show running-config
Executes the privileged-level show running-config command while in global configuration mode.

Switch#show flash: Displays information about flash memory (for the 2900/ 2950 series only).

Switch#show Mac-address-table Displays the current MAC address forwarding table.

Switch#show controllers Ethernet-controller Displays information about the Ethernet controller.

Switch#show running-config Displays the current configuration in DRAM.

Switch#show startup-config Displays the current configuration in NVRAM.

Switch#show post Displays whether the switch passed POST.

Switch#show vlan Displays the current VLAN configuration.

Switch#show interfaces

Displays the interface configuration and status of line: up/up, up/down, admin down.

NOTE: This command is unsupported in some Cisco IOS Software releases, such as 12.2(25) FX.

Switch#show interface vlan1 Displays setting of virtual interface VLAN 1, the default VLAN on the switch.

NOTE: This command is unsupported in some Cisco IOS Software releases, such as 12.2(25) FX.

2. CISCO Discovery Protocol (CDP):-

Router#show cdp	<u>Displays global CDP information (such as timers)</u>
Router#show cdp neighbors	<u>Displays information about neighbors</u>
Router#show cdp neighbors detail	<u>Displays more detail about the neighbor device</u>
Router#show cdp entry word	<u>Displays information about the device named word</u>
Router#show cdp entry *	<u>Displays information about all devices</u>
Router#show cdp interface	<u>Displays information about interfaces that have CDP running</u>
Router#show cdp interface x	<u>Displays information about specific interface x running CDP</u>
Router#show cdp traffic	<u>Displays traffic information—packets in/out/version</u>
Router(config)#cdp holdtime x	<u>Changes the length of time to keep CDP packets</u>
Router(config)#cdp timer x	<u>Changes how often CDP updates are sent</u>
Router(config)#cdp run	<u>Enables CDP globally (on by default)</u>
Router(config)#no cdp run	<u>Turns off CDP globally</u>
Router(config-if)#cdp enable	<u>Enables CDP on a specific interface</u>
Router(config-if)#no cdp enable	<u>Turns off CDP on a specific interface</u>
Router#clear cdp counters	<u>Resets traffic counters to 0</u>
Router#clear cdp table	<u>Deletes the CDP table</u>
Router#debug cdp adjacency	<u>Monitors CDP neighbor information</u>
Router#debug cdp events	<u>Monitors all CDP events</u>
Router#debug cdp ip	<u>Monitors CDP events specifically for IP</u>
Router#debug cdp packets	<u>Monitors CDP packet-related information</u>

3. Implementing Switch Port security:-

- Switch Port Security

Switch(config)#interface fastethernet 0/1 Moves to interface configuration mode.

Switch(config-if)#switchport port-security Enables port security on the interface.

Switch(config-if)#switchport port-security maximum 4
Sets a maximum limit of four MAC addresses that will be allowed on this port.

NOTE: The maximum number of secure MAC addresses that you can configure on a switch is set by the maximum number of available MAC addresses allowed in the system.

Switch(config-if)# switchport port-security mac-address 1234.5678.90ab
Sets a specific secure MAC address 1234.5678.90ab, You can add additional secure MAC addresses up to the maximum value configured.

Switch(config-if)#switchport port-security violation shutdown
Configures port security to shut down the interface if a security violation occurs.

NOTE: In shutdown mode, the port is error disabled, a log entry is made, and manual intervention or error disable recovery must be used to re enable the interface.

Switch(config-if)#switchport port-security violation restrict
Configures port security to restrict mode if a security violation occurs.

NOTE: In restrict mode, frames from a no allowed address are dropped, and a log entry is made. The interface remains operational.

Switch(config-if)#switchport port-security violation protect
Configures port security to protect mode if a security violation occurs.

NOTE: In protect mode, frames from a no allowed address are dropped, but no log entry is made. The interface remains operational.

- Verifying Switch Port Security

Switch#show port-security Displays security information for all interfaces

Switch #show port-security interface fastethernet 0/5
Displays security information for interface fastethernet 0/5

Switch#show port-security address Displays MAC address table security information

Switch#show mac address-table Displays the MAC address table

Switch#clear mac address-table dynamic Deletes all dynamic MAC addresses

Switch#clear mac address-table dynamic address aaaa.bbbb.cccc
Deletes the specified dynamic MAC address

Switch #clear mac address-table dynamic interface fastethernet 0/5
Deletes all dynamic MAC addresses on interface fastethernet 0/5

Switch#clear mac address-table dynamic vlan 10 Deletes all dynamic MAC addresses on VLAN 10

Switch#clear mac address-table notification Clears MAC notification global counters

NOTE: Beginning with Cisco IOS Software Release 12.1(11) EA1, the clear mac address-table command (no hyphen in mac address) replaces the clear mac address- table command (with the hyphen in mac address). The clear mac address- table static command (with the hyphen in mac-address) will become obsolete in a future release.

- Sticky MAC Addresses

Switch(config)#interface fastethernet 0/5 Moves to interface configuration mode.

Switch(config-if)#switchport port-security mac-address sticky
Converts all dynamic port security learned MAC addresses to sticky secure MAC addresses.

Switch(config-if)#switchport port-security mac-address sticky vlan 10 voice
Converts all dynamic port security learned MAC addresses to sticky secure MAC addresses on voice VLAN 10.

NOTE: The voice keyword is available only if a voice VLAN is first configured on a port and if that port is not the access VLAN

4. Implementing Vlan :-

- Creating Static VLANs

- Using VLAN Configuration Mode

Switch(config)#vlan 3 Creates VLAN 3 and enters VLAN configuration mode for further definitions.

Switch(config-vlan)#name Engineering

Assigns a name to the VLAN. The length of the name can be from 1 to 32 characters.

Switch(config-vlan)#exit

Applies changes, increases the revision number by 1, and returns to global configuration mode.

- Using VLAN Database Mode

Switch#vlan database Enters VLAN database mode.

Switch(vlan)#vlan 4 name Sales

Creates VLAN 4 and names it Sales. The length of the name can be from 1 to 32 characters.

Switch (vlan)#vlan 10 Creates VLAN 10 and gives it a name of VLAN0010 as a default.

Switch(vlan)#apply Applies changes to the VLAN database and increases the revision number by 1.

Switch(vlan)#exit

Applies changes to the VLAN database, increases the revision number by 1, and exits VLAN database mode.

- Assigning Ports to VLANs

Switch(config)#interface fastethernet 0/1 Moves to interface configuration mode

Switch(config-if)#switchport mode access Sets the port to access mode

Switch(config-if)#switchport access vlan 10 Assigns this port to VLAN 10

- Using the range Command

Switch(config)#interface range fastethernet 0/1 – 9

Enables you to set the same configuration parameters on multiple ports at the same time.

NOTE: There is a space before and after the hyphen in the interface range command.

Switch(config-if-range)#switchport mode access Sets ports 1–9 as access ports.

Switch(config-if-range)#switchport access vlan 10Assigns ports 1–9 to VLAN 10.

- Verifying VLAN Information

Switch#show vlan Displays VLAN information

Switch#show vlan brief Displays VLAN information in brief

Switch#show vlan id 2 Displays information about VLAN 2 only

Switch#show vlan name marketing Displays information about VLAN named marketing only

Switch#show interfaces vlan x Displays interface characteristics for the specified VLAN

- Erasing VLAN Configurations

Switch#delete flash:vlan.dat Removes the entire VLAN database from flash.

WARNING: Make sure there is no space between the colon (:) and the characters vlan.dat. You can potentially erase the entire contents of the flash with this command if the syntax is not correct. Make sure you read the output from the switch. If you need to cancel, press C-C to escape back to privileged mode: (Switch#)

Switch#delete flash:vlan.dat Delete filename [vlan.dat]?

Delete flash:vlan.dat? [confirm]

Switch#

Switch(config)#interface fastethernet 0/5 Moves to interface configuration mode.

Switch(config-if)#no switchport access vlan 5
Removes port from VLAN 5 and reassigns it to VLAN 1—the default VLAN.

Switch(config-if)#exit Moves to global configuration mode.

Switch(config)#no vlan 5 Removes VLAN 5 from the VLAN database.

Or

Switch#vlan database Enters VLAN database mode.

Switch(vlan)#no vlan 5 Removes VLAN 5 from the VLAN database.

Switch(vlan)#exit Applies changes, increases the revision number by 1, and exits VLAN database mode.

5. Implementing Inter-VLAN Routing:-

Router(config)#interface fastethernet 0/0 Moves to interface configuration mode.

Router(config-if)#duplex full Sets the interface to full duplex.

Router(config-if)#no shutdown Enables the interface.

Router(config-if)#interface fastethernet 0/0.1

Creates sub interface 0/0.1 and moves to sub interface configuration mode.

Router(config-subif)#description Management VLAN 1

(Optional) Sets the locally significant description of the sub interface.

Router(config-subif) #encapsulation dot1q 1 native

Assigns VLAN 1 to this sub interface. VLAN 1 will be the native VLAN. This sub interface will use the 802.1q trunking protocol.

Router(config-subif)#ip address 192.168.1.1 255.255.255.0 Assigns the IP address and netmask.

Router(config-subif)#interface fastethernet 0/0.10

Creates sub interface 0/0.10 and moves to sub interface configuration mode.

Router(config-subif)#description Accounting VLAN 10

(Optional) Sets the locally significant description of the sub interface.

Router(config-subif) #encapsulation dot1q 10

Assigns VLAN 10 to this sub interface. This sub interface will use the 802.1q trunking protocol.

6. Implementing VLAN Trunking Protocol (VTP)

Using Global Configuration Mode

Switch(config)#vtp mode client Changes the switch to VTP client mode.

Switch(config)#vtp mode server Changes the switch to VTP server mode.

Switch(config)#vtp mode transparent Changes the switch to VTP transparent mode.

NOTE: By default, all Catalyst switches are in server mode.

Switch(config)#no vtp mode Returns the switch to the default VTP server mode.

Switch(config)#vtp domain domain-name
Configures the VTP domain name. The name can be from 1 to 32 characters long.

NOTE: All switches operating in VTP server or client mode must have the same domain name to ensure communication.

Switch(config)#vtp password password
Configures a VTP password. In Cisco IOS Software Release 12.3 and later, the password is an ASCII string from 1 to 32 characters long. If you are using a Cisco IOS Software release earlier than 12.3, the password length ranges from 8 to 64 characters long.

NOTE: To communicate with each other, all switches must have the same VTP password set.

Switch(config)#vtp v2-mode
Sets the VTP domain to Version 2. This command is for Cisco IOS Software Release 12.3 and later. If you are using a Cisco IOS Software release earlier than 12.3, the command is vtp version 2.

NOTE: VTP Versions 1 and 2 are not interoperable. All switches must use the same version. The biggest difference between Versions 1 and 2 is that Version 2 has support for Token Ring VLANs.

Switch(config)#vtp pruning Enables VTP pruning.

NOTE: By default, VTP pruning is disabled. You need to enable VTP pruning on only 1 switch in VTP server mode.

Using VLAN Database Mode

Switch#vlan database Enters VLAN database mode.

Switch(vlan)#vtp client Changes the switch to VTP client mode.

Switch(vlan)#vtp server Changes the switch to VTP server mode.

Switch(vlan)#vtp transparent Changes the switch to VTP transparent mode.

NOTE: By default, all Catalyst switches are in server mode.

Switch(vlan)#vtp domain domain-name

Configures the VTP domain name. The name can be from 1 to 32 characters long.

NOTE: All switches operating in VTP server or client mode must have the same domain name to ensure communication.

Switch(vlan)#vtp password password

Configures a VTP password. In Cisco IOS Software Release 12.3 and later, the password is an ASCII string from 1 to 32 characters long. If you are using a Cisco IOS release earlier than 12.3, the password length ranges from 8 to 64 characters long.

NOTE: All switches must have the same VTP password set to communicate with each other.

Switch(vlan)#vtp v2-mode

Sets the VTP domain to Version 2. This command is for Cisco IOS Release 12.3 and later. If you are using a Cisco IOS release earlier than 12.3, the command is vtp version 2.

NOTE: VTP Versions 1 and 2 are not interoperable. All switches must use the same version. The biggest difference between Versions 1 and 2 is that Version 2 has support for Token Ring VLANs.

Switch(vlan)#vtp pruning Enables VTP pruning.

NOTE: By default, VTP pruning is disabled. You need to enable VTP pruning on only one switch in VTP server mode.

NOTE: Only VLANs included in the pruning-eligible list can be pruned. VLANs 2 through 1001 are pruning eligible by default on trunk ports. Reserved VLANs and extended-range VLANs cannot be pruned. To change which eligible VLANs can be pruned, use the interface-specific switchport trunk pruning vlan command:

Switch(config-if)#switchport trunk pruning vlan remove 4, 20-30 Removes VLANs 4 and 20 through 30.

Switch(config-if)#switchport trunk pruning vlan except 40-50

All VLANs are added to the pruning list except for 40 through 50.

Switch(vlan)#exit

Applies changes to the VLAN database, increases the revision number by 1, and exits back to privileged mode.

- Verifying VTP

Switch#show vtp status Displays general information about VTP configuration

Switch#show vtp counters Displays the VTP counters for the switch

- Dynamic Trunking Protocol (DTP)

Switch (config)#interface fastethernet 0/1 Moves to interface configuration mode.

Switch(config-if) #switchport mode dynamic desirable
Makes the interface actively attempt to convert the link to a trunk link.

NOTE: With the switchport mode dynamic desirable command set, the interface becomes a trunk link if the neighboring interface is set to trunk, desirable, or auto.

Switch(config-if) #switchport mode dynamic Auto Makes the interface able to convert into a trunk link.

NOTE: With the switchport mode dynamic auto command set, the interface becomes a trunk link if the neighboring interface is set to trunk or desirable.

Switch(config-if) #switchport nonegotiate Prevents the interface from generating DTP frames.

NOTE: Use the switchport mode nonegotiate command only when the interface switchport mode is access or trunk. You must manually configure the neighboring interface to establish a trunk link.

Switch(config-if) #switchport mode trunk
Puts the interface into permanent trunking mode and negotiates to convert the link into a trunk link.

NOTE: With the switchport mode trunk command set, the interface becomes a trunk link even if the neighboring interface is not a trunk link.

- Setting the Encapsulation Type

Switch(config)#interface fastethernet 0/1 Moves to interface configuration mode

Switch(config-if) #switchport mode trunk
Puts the interface into permanent trunking mode and negotiates to convert the link into a trunk link

Switch(config-if) #switchport trunk encapsulation isl Specifies ISL encapsulation on the trunk link

Switch(config-if) #switchport trunk encapsulation dot1q Specifies 802.1q encapsulation on the trunk Link

Switch(config-if) #switchport trunk encapsulation negotiate
Specifies that the interface negotiate with the neighboring interface to become either an ISL or dot1q trunk, depending on the capabilities or configuration of the neighboring interface

TIP: With the switchport trunk encapsulation negotiate command set, the preferred trunking method is ISL.

CAUTION: The 2960 series switch supports only dot1q trunking

7. Verifying Spanning tree Protocols (STP):-

- Enabling Spanning Tree Protocol

Switch(config)#spanning-tree vlan 5 Enables STP on VLAN 5

Switch(config)#no spanning-tree vlan 5 Disables STP on VLAN 5

- Configuring the Root Switch

Switch(config)#spanning-tree vlan 5 root

Modifies the switch priority from the default 32768 to a lower value to allow the switch to become the root switch for VLAN 5.

NOTE: If all other switches have extended system ID support, this switch resets its priority to 24576. If any other switch has a priority set to below 24576 already, this switch sets its own priority to 4096 less than the lowest switch priority. If by doing this the switch would have a priority of less than 1, this command fails.

Switch(config)#spanning-tree vlan 5 root primary

Switch recalculates timers along with priority to allow the switch to become the root switch for VLAN 5.

TIP: The root switch should be a backbone or distribution switch.

Switch(config)#spanning-tree vlan 5 root primary diameter 7

Configures the switch to be the root switch for VLAN 5 and sets the network diameter to 7.

TIP: The diameter keyword is used to define the maximum number of switches between any two end stations. The range is from 2 to 7 switches.

Switch(config)#spanning-tree vlan 5 root primary hello-time 4

Configures the switch to be the root switch for VLAN 5 and sets the hello delay timer to 4 seconds.

TIP: The hello-time keyword sets the hello-delay timer to any amount between 1 and 10 seconds. The default time is 2 seconds.

- Configuring a Secondary Root Switch

Switch(config)#spanning-tree vlan 5 root secondary

Switch recalculates timers along with priority to allow the switch to become the root switch for VLAN 5 should the primary root switch fail.

NOTE: If all other switches have extended system ID support, this switch resets its priority to 28672. Therefore, if the root switch fails, and all other switches are set to the default priority of 32768, this becomes the new root switch. For switches without extended system ID support, the switch priority is changed to 16384.

Switch(config)#spanning-tree vlan 5 root secondary diameter 7

Configures the switch to be the secondary root switch for VLAN 5 and sets the network diameter to 7.

Switch(config)#spanning-tree vlan 5 root secondary hello-time 4

Configures the switch to be the secondary root switch for VLAN 5 and sets the hello-delay timer to 4 seconds.

- Configuring Port Priority

Switch(config)#interface gigabitethernet 0/1

Moves to interface configuration mode.

Switch(config-if)#spanning-tree port-priority 64

Configures the port priority for the interface that is an access port.

Switch(config-if)#spanning-tree vlan 5 port-priority 64

Configures the VLAN port priority for an interface that is a trunk port.

NOTE: Port priority is used to break a tie when 2 switches have equal priorities for determining the root switch. The number can be between 0 and 255. The default port priority is 128. The lower the number, the higher the priority.

- Configuring the Path Cost

Switch(config)#interface gigabitethernet 0/1

Moves to interface configuration mode.

Switch(config-if)#spanning-tree cost 100000

Configures the cost for the interface that is an access port.

Switch(config-if)#spanning-tree vlan 5 cost 1000000

Configures the VLAN cost for an interface that is a trunk port.

NOTE: If a loop occurs, STP uses the path cost when trying to determine which interface to place into the forwarding state. A higher path cost means a lower speed transmission. The range of the cost

keyword is 1 through 200000000. The default is based on the media speed of the interface.

- Configuring the Switch Priority of a VLAN

Switch(config)#spanning-tree vlan 5 priority 12288

Configures the switch priority of VLAN 5 to 12288

NOTE: With the priority keyword, the range is 0 to 61440 in increments of 4096. The default is 32768. The lower the priority, the more likely the switch will be chosen as the root switch. Only the following numbers can be used as a priority value:

CAUTION: Cisco recommends caution when using this command. Cisco further recommends that the spanning-tree vlan x root primary or the spanning-tree vlan x root secondary command be used instead to modify the switch priority.

Switch(config)#interface gigabitethernet 0/1 Moves to interface configuration mode.

Switch(config-if)#spanning-tree cost 100000 Configures the cost for the interface that is an access port.

Switch(config-if)#spanning-tree vlan 5 cost 1000000
Configures the VLAN cost for an interface that is a trunk port.

NOTE: If a loop occurs, STP uses the path cost when trying to determine which interface to place into the forwarding state. A higher path cost means a lower speed transmission. The range of the cost keyword is 1 through 200000000. The default is based on the media speed of the interface.

Switch(config)#spanning-tree vlan 5 priority 12288
Configures the switch priority of VLAN 5 to 12288 { 0 4096 8192 12288 16384 20480 24576 28672 32768 36864 40960 45056 49152 53248 57344 61440 }

- Configuring STP Timers

Switch(config)#spanning-tree vlan 5 hello-time 4
Changes the hello-delay timer to 4 seconds on VLAN 5

Switch(config)#spanning-tree vlan 5 forward-time 20
Changes the forward-delay timer to 20 seconds on VLAN 5

Switch(config)#spanning-tree vlan 5 max-age 25
Changes the maximum-aging timer to 25 seconds on VLAN 5

NOTE: For the hello-time command, the range is 1 to 10 seconds. The default is 2 seconds. For the forward-time command, the range is 4 to 30 seconds. The default is 15 seconds. For the max-age command, the range is 6 to 40 seconds. The default is 20 seconds.

CAUTION: Cisco recommends caution when using this command. Cisco further recommends that the spanning tree vlan x root primary or the spanning-tree vlan x root secondary command be used instead to modify the switch timers.

- Verifying STP

Switch#show spanning-tree Displays STP information

Switch#show spanning-tree active Displays STP information on active interfaces only

Switch#show spanning-tree brief Displays a brief status of the STP

Switch#show spanning-tree detail Displays a detailed summary of interface information

Switch#show spanning-tree interface gigabitethernet 0/1
Displays STP information for interface gigabitethernet 0/1

Switch#show spanning-tree summary Displays a summary of port states

Switch#show spanning-tree summary totals Displays the total lines of the STP section

Switch#show spanning-tree vlan 5 Displays STP information for VLAN 5

- Optional STP Configurations

Port Fast

Switch(config)#interface fastethernet 0/10 Moves to interface configuration mode.

Switch(config-if)#spanning-tree portfast Enables Port Fast on an access port.

Switch(config-if)#spanning-tree portfast trunk Enables Port Fast on a trunk port.

WARNING: Use the portfast command only when connecting a single end station to an access or trunk port. Using this command on a port connected to a switch or hub could prevent spanning tree from detecting loops.

NOTE: If you enable the voice VLAN feature, Port Fast is enabled automatically. If you disable voice VLAN, Port Fast is still enabled. Switch#show spanning-tree interface fastethernet 0/10 portfast Displays Port Fast information on interface fastethernet 0/10.

BPDU Guard

Switch(config)#spanning-tree portfast bpduguard default Globally enables BPDU Guard.

Switch(config)#interface range fastethernet 0/1 – 5 Enters interface range configuration mode.

Switch(config-if-range)# spanning-tree portfast Enables Port Fast on all interfaces in the range.

NOTE: By default, BPDU Guard is disabled.

Switch(config)#err disable recovery cause bpduguard
Allows port to re enable itself if the cause of the error is BPDU Guard by setting a recovery timer.

Switch(config)#errdisable recovery interval 400
Sets recovery timer to 400 seconds. The default is 300 seconds. The range is from 30 to 86400 seconds.

Switch#show spanning-tree summary totals Verifies whether BPDU Guard is enabled or disabled.

Switch#show errdisable recovery Displays error disable recovery timer information.

- Changing the Spanning-Tree Mode

Switch(config)#spanning-tree mode mst

Enables MSTP. This command is available only on a switch running the EI software image.

Switch(config)#spanning-tree mode pvst Enables PVST. This is the default setting.

Switch(config)#spanning-tree mode rapid-pvst Enables Rapid PVST+.

- Extended System ID

Switch(config)#spanning-tree extend system-id

Enables extended system ID, also known as MAC address reduction.

NOTE: Catalyst switches running software earlier than Cisco IOS Software Release 12.1(8) EA1 do not support the extended system ID.

Switch#show spanning-tree summary Verifies extended system ID is enabled.

Switch#show running-config Verifies extended system ID is enabled.

- Enabling Rapid Spanning Tree

Switch(config)#spanning-tree mode rapid-pvst Enables Rapid PVST+.

Switch(config)#interface fastethernet 0/1 Moves to interface configuration mode.

Switch(config-if)#spanning-tree link-type point-to-point

Sets the interface to be a point-to-point interface.

NOTE: By setting the link type to point to point, this means that if you connect this port to a remote port, and this port becomes a designated port, the switch negotiates with the remote port and transitions the local port to a forwarding state.

Switch(config-if)#exit

Switch(config)#clear spanning-tree detected-protocols

NOTE: The clear spanning-tree detected-protocols command restarts the protocol-migration process on the switch if any port is connected to a port on a legacy 802.1D switch.

- Troubleshooting Spanning Tree

Switch#debug spanning-tree all	<u>Displays all spanning-tree debugging events</u>
Switch#debug spanning-tree events	<u>Displays spanning-tree debugging topology events</u>
Switch#debug spanning-tree backbone fast	<u>Displays spanning-tree debugging Backbone Fast events</u>
Switch#debug spanning-tree uplinkfast	<u>Displays spanning-tree debugging Uplink Fast event</u>
Switch#debug spanning-tree mst all	<u>Displays all MST debugging events</u>
Switch#debug spanning-tree switch state	<u>Displays spanning-tree port state changes</u>
Switch#debug spanning-tree pvst+	<u>Displays PVST+ events</u>

8. Ether-Channel Configuration:-

- Configuring Layer 2 EtherChannel

Switch(config)#interface range fastethernet 0/1 – 4 Moves to interface range configuration mode.

Switch(config-if-range)#channel-protocol pagp Specifies the pagp protocol to be used in this channel.

Or

Switch(config-if-range)#channel-protocol lacp Specifies the LACP protocol to be used in this channel.

Switch(config-if-range)#channel-group 1 mode {desirable | auto | on | passive | active }
Creates channel group 1 and assigns interfaces 01–04 as part of it. Use whichever mode is necessary, depending on your choice of protocol.

- Verifying EtherChannel

Switch#show running-config Displays list of what is currently running on the device

Switch#show running-config interface fastethernet 0/12
Displays interface fastethernet 0/12 information

Switch#show etherchannel Displays all EtherChannel information

Switch#show etherchannel 1 port-channel Displays port channel information

Switch#show etherchannel summary Displays a summary of EtherChannel information

Switch#show pagp neighbor Shows pagp neighbor information

Switch#clear pagp 1 counters Clears pagp channel group 1 information

Switch#clear lacp 1 counters Clears LACP channel group 1 information

Part Two: Network administration and troubleshooting

9. Password Recovery:-

Step	2500 Series Commands	1700/2600/ISR Series Commands
Step 1: Boot the router and interrupt the boot sequence as soon as text appears on the screen.	Press Ctrl + Break	Press Ctrl + Break
Step 2: Change the configuration register to ignore contents of NVRAM.	> o/r 0x2142	rommon 1>confreg 0x2142
Step 3: Reload the router	> i	rommon 2>reset
Step 4: Enter privileged mode. (Do not enter setup mode.)	Router>enable	Router>enable
Step 5: Copy the startup configuration into the running configuration	Router#copy startup-config running-config	Router#copy startup-config running-config
Step 6: Change the password.	Router (config)#enable secret new	Router (config)#enable secret new
Step 7: Reset the configuration register back to its default value.	Router (config)#config-register 0x2102	Router (config)#config-register 0x2102
Step 8: Save the configuration	Router #copy running-config startup-config	Router #copy running-config startup-config
Step 9: Verify the configuration register.	Router #show version	Router #show version
Step 10: Reload the router	Router #reload	Router #reload

10. Backing Up and Restoring Cisco IOS Software and Configurations

- Boot System Commands

Router(config)#boot system flash image name Loads the Cisco IOS Software with image-name.

Router(config)#boot system tftp image-name 172.16.10.3
Loads the Cisco IOS Software with image-name from a TFTP server.

Router(config)#boot system rom Loads the Cisco IOS Software from ROM.

Router(config)#exit

Router#copy running-config startup-config
Saves the running configuration to NVRAM. The router will execute commands in their order on the next reload.

- Backing Up Configurations to a TFTP Server

Router#copy running-config startup-config
Saves the running configuration from DRAM to NVRAM (locally).

Router#copy running-config tftp Copies the running configuration to the remote TFTP server.

Router#copy startup-config tftp Copies the startup configuration to the remote TFTP server.

Router#copy flash tftp

- Restoring Configurations from a TFTP Server

Router#copy tftp running-config Copies the configuration file from the TFTP server to DRAM.

Router#copy tftp startup-config Copies the configuration file from the TFTP server to NVRAM.

Router#copy tftp flash

Part Three: Router Configuration:

11. Static (Default) Routing Protocol

- Configuring a Static Route on a Router

Router(config)#ip route 172.16.20.0 255.255.255.0 172.16.10.2
172.16.20.0 = destination network. 255.255.255.0 = subnet mask. 172.16.10.2 = next-hop address. Read this to say, "To get to the destination network of 172.16.20.0, with a subnet mask of 255.255.255.0, send all packets to 172.16.10.2."

Router(config)#ip route 172.16.20.0 255.255.255.0 serial 0/0/0
172.16.20.0 = destination network. 255.255.255.0 = subnet mask. Serial 0/0/0 = exit interface. Read this to say, "To get to the destination network of 172.16.20.0, with a subnet mask of 255.255.255.0, send all packets out interface serial 0/0/0."

Router(config)#ip route 172.16.20.0 255.255.255.0 172.16.10.2 200
By default, a static route is assigned an administrative distance (AD) of 1. Administrative distance rates the "trustworthiness" of a route. AD is a number from 0 through 255, where 0 is absolutely trusted and 255 cannot be trusted at all. Therefore, an AD of 1 is an extremely reliable rating, with only an AD of 0 being better. An AD of 0 is assigned to a directly connected route.

- Configuring a Default Route on a Router

Router(config)#ip route 0.0.0.0 0.0.0.0 172.16.10.2
Send all packets destined for networks not in my routing table to 172.16.10.2.

Router(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0
Send all packets destined for networks not in my routing table out my serial 0/0 interface.

- Verifying Static Routes

Router#show ip route

NOTE: The codes to the left of the routes in the table tell you from where the router learned the routes. A static route is described by the letter S.

12. Routing Information Protocol (RIP) Configuration

- The ip classless Command

Router(config)#ip classless

Instructs Cisco IOS Software to forward packets destined for an unknown subnet to the best supernet route

Router(config)#no ip classless Turns off the ip classless Command

NOTE: The ip classless command is enabled by default in Cisco IOS Software Release 11.3 and later

- RIP Routing: Mandatory Commands

Router(config)#router rip Enables RIP as a routing protocol.

Router(config-router)#network w.x.y.z

w.x.y.z is the network number of the directly connected network you want to advertise.

- RIP Routing: Optional Commands

Router(config)#no router rip Turns off the RIP routing process.

Router(config-router)#no network w.x.y.z Removes network w.x.y.z from the RIP routing process.

Router(config-router)#version 2 RIP will now send and receive RIPv2 packets globally.

Router(config-router)#version 1 RIP will now send and receive RIPv1 packets only.

Router(config-if)#ip rip send version 1 The interface will send only RIPv1 packets.

Router(config-if)#ip rip send version 2 The interface will send only RIPv2 packets.

Router(config-if)#ip rip send version 1 2 The interface will send both RIPv1 and RIPv2 packets.

Router(config-if)#ip rip receive version 1 The interface will receive only RIPv1 packets.

Router(config-if)#ip rip receive version 2 The interface will receive only RIPv2 packets.

Router(config-if)#ip rip receive version 1 2 The interface will receive both RIPv1 and RIPv2 packets.

Router(config-router)#no auto-summary

RIPv2 summarizes networks at the classful boundary. This command turns auto summarization Off

Router(config-router)#passive-interface s0/0/0 RIP updates will not be sent out this interface.

Router(config-router)#neighbor a.b.c.d

Defines a specific neighbor with which to exchange information.

Router(config-router)#no ip split-horizon Turns off split horizon (on by default).

Router(config-router)#ip split-horizon re enables split horizon.

Router(config-router)#timers basic 30 90 180 270 360 Changes timers in RIP:

30 = Update timer (in seconds)

90 = Invalid timer (in seconds)

180 = Hold-down timer (in seconds)

270 = Flush timer (in seconds)

360 = Sleep time (in milliseconds)

Router(config-router)#maximum-paths x

Limits the number of paths for load balancing to x (4 = default, 6 = maximum).

Router(config-router)#default-information originate Generates a default route into RIP.

- Troubleshooting RIP Issues

Router#debug ip rip Displays all RIP activity in real time

Router#show ip rip database Displays contents of the RIP Database

13. Open Short Path First (OSPF) Configuration

- Configuring OSPF: Mandatory Commands

Router(config)#router ospf 123

Starts OSPF process 123. The process ID is any positive integer value between 1 and 65,535. The process ID is not related to the OSPF area. The process ID merely distinguishes one process from another within the device.

Router(config-router)#network 172.16.10.0 0.0.0.255 area 0

OSPF advertises interfaces, not networks. Uses the wildcard mask to determine which interfaces to advertise. Read this line to say "Any interface with an address of 172.16.10.x is to be put into area 0."

NOTE: The process ID number of one router does not have to match the process ID of any other router. Unlike Enhanced Interior Gateway Routing Protocol (EIGRP), matching this number across all routers does not ensure that network adjacencies will form.

Router(config-router)#log-adjacency- changes detail

Configures the router to send a syslog message when there is a change of state between OSPF neighbors.

TIP: Although the log-adjacency changes command is on by default, only up/down events are reported unless you use the detail keyword.

Router(config-router)#network 172.16.10.1 0.0.0.0 area 0

Read this line to say "Any interface with an exact address of 172.16.10.1 is to be put into area 0."

Router(config-router)#network 172.16.10.0 0.0.255.255 area 0

Read this line to say "Any interface with an address of 172.16.x.x is to be put into area 0."

Router(config-router)#network 0.0.0.0 255.255.255.255 area 0

Read this line to say "Any interface with any address is to be put into area 0."

- Configuring OSPF: Optional Commands

Loopback Interfaces

Router(config)#interface loopback 0

Creates a virtual interface named loopback 0, and then moves the router to interface configuration mode.

Router(config-if)#ip address 192.168.100.1 255.255.255.255

Assigns the IP address to the interface.

NOTE: Loopback interfaces are always "up and up" and do not go down unless manually shut down. This makes loopback interfaces great for use as OSPF router IDs.

Router ID

Router(config)#router ospf 1

Starts OSPF process 1.

Router(config-router)#router-id 10.1.1.1

Sets the router ID to 10.1.1.1. If this command is used on an OSPF router process that is already active (has neighbors), the new router ID is used at the next reload or at a manual OSPF process restart.

Router(config-router)#no router-id 10.1.1.1

Removes the static router ID from the configuration. If this command is used on an OSPF router process that is already active (has neighbors), the old router ID behavior is used at the next reload or at a manual OSPF process restart.

DR/BDR Elections

Router(config)#interface serial 0/0

Changes the router to interface configuration mode.

Router(config-if)#ip ospf priority 50

Changes the OSPF interface priority to 50.

NOTE: The assigned priority can be between 0 and 255. A priority of 0 makes the router ineligible to become a designated router (DR) or backup designated router BDR. The highest priority wins the election. A priority of 255 guarantees a tie in the election. If all routers have the same priority, regardless of the priority number, they tie. Ties are broken by the highest router ID.

Modifying Cost Metrics

Router(config)#interface serial 0/0

Changes the router to interface configuration mode.

Router(config-if)#bandwidth 128

If you change the bandwidth, OSPF recalculates the cost of the link.

Or

Router(config-if)#ip ospf cost 1564

Changes the cost to a value of 1564.

NOTE: The cost of a link is determined by dividing the reference bandwidth by the interface bandwidth. The bandwidth of the interface is a number between 1 and 10,000,000. The unit of measurement is kilobits. The cost is a number between 1 and 65,535. The cost has no unit of measurement—it is just a number.

Authentication: Simple

Router(config)#router ospf 1

Starts OSPF process 1.

Router(config-router)#area 0 authentication

Enables simple authentication; password will be sent in clear text.

Router(config-router)#exit

Returns to global configuration mode.

Router(config)#interface fastethernet 0/0

Moves to interface configuration mode.

Router(config-if)#ip ospf authentication-key NEW

Sets key (password) to NEW.

NOTE: The password can be any continuous string of characters that can be entered from the keyboard, up to 8 bytes in length. To be able to exchange OSPF information, all neighboring routers on the same network must have the same password.

Authentication: Using MD5 Encryption

Router(config)#router ospf 1 Starts OSPF process 1.

Router(config-router)#area 0 authentication message-digest
Enables authentication with MD5 password encryption.

Router(config-router)#exit Returns to global configuration mode.

Router(config)#interface fastethernet 0/0 Moves to interface configuration mode.

Router(config-if)#ip ospf message-digest-key 1 md5
NEW 1 is the key-id. This value must be the same as that of your neighboring router. md5 indicates that the MD5 hash algorithm will be used. NEW is the key (password) and must be the same as that of your neighboring router.

NOTE: If the service password encryption command is not used when implementing OSPF MD5 authentication, the MD5 secret is stored as plain text in NVRAM.

Timers

Router(config-if)#ip ospf hello-interval timer 20 Changes the Hello Interval timer to 20 seconds.

Router(config-if)#ip ospf dead-interval 80 Changes the Dead Interval timer to 80 seconds.

NOTE: Hello and Dead Interval timers must match for routers to become neighbors.

Propagating a Default Route

Router(config)#ip route 0.0.0.0 0.0.0.0 s0/0 Creates a default route.

Router(config)#router ospf 1 Starts OSPF process 1.

Router(config-router)#default-information originate
Sets the default route to be propagated to all OSPF routers.

Router(config-router)#default-information originate always
The always option propagates a default “quad-zero” route even if one is not configured on this router.

NOTE: The default-information originate command or the default-information originate always command is usually only to be configured on your “entrance” or “gateway” router, the router that connects your network to the outside world—the Autonomous System Boundary Router (ASBR).

- Verifying OSPF Configuration

Router#show ip protocol	<u>Displays parameters for all protocols running on the router</u>
Router#show ip route	<u>Displays a complete IP routing table</u>
Router#show ip ospf	<u>Displays basic information about OSPF routing processes</u>
Router#show ip ospf interface	<u>Displays OSPF info as it relates to all interfaces</u>
Router#show ip ospf interface fastethernet 0/0	<u>Displays OSPF information for interface fastethernet 0/0</u>
Router#show ip ospf border-routers	<u>Displays border and boundary router information</u>
Router#show ip ospf neighbor	<u>Lists all OSPF neighbors and their states</u>
Router#show ip ospf neighbor detail	<u>Displays a detailed list of neighbors</u>
Router#show ip ospf database	<u>Displays contents of the OSPF database</u>
Router#show ip ospf database nssa-external	<u>Displays NSSA external link states</u>

- Troubleshooting OSPF

Router#clear ip route *	<u>Clears entire routing table, forcing it to rebuild</u>
Router#clear ip route a.b.c.d	<u>Clears specific route to network a.b.c.d</u>
Router#clear ip ospf counters	<u>Resets OSPF counters</u>
Router#clear ip ospf process	<u>Resets entire OSPF process, forcing OSPF to re-create neighbors, database, and routing table</u>
Router#debug ip ospf events	<u>Displays all OSPF events</u>
Router#debug ip ospf adjacency	<u>Displays various OSPF states and DR/ BDR election between adjacent routers</u>
Router#debug ip ospf packets	<u>Displays OPSF packets</u>

14. Enhancement Interior Gateway Routing Protocol (EIGRP) Configuration:-

- Configuring EIGRP

Router(config)#router eigrp 100

Turns on the EIGRP process. 100 is the autonomous system number, which can be a number between 1 and 65,535. All routers in the same autonomous system must use the same autonomous system number.

Router(config-router)#network 10.0.0.0 Specifies which network to advertise in EIGRP.

Router(config-if)#bandwidth x

Sets the bandwidth of this interface to x kilobits to allow EIGRP to make a better metric calculation.

TIP: The bandwidth command is used for metric calculations only. It does not change interface performance.

Router(config-router)#no network 10.0.0.0 Removes the network from the EIGRP process.

Router(config)#no router eigrp 100 Disables routing process 100.

Router(config-router)#network 10.0.0.0 0.255.255.255

Identifies which interfaces or networks to include in EIGRP. Interfaces must be configured with addresses that fall within the wildcard mask range of the network statement. A network mask can also be used here.

Router(config-router)#metric weights tos k1 k2 k3 k4 k5

Changes the default k values used in metric calculation. These are the default values: tos=0, k1=1, k2=0, k3=1, k4=0, k5=0

TIP: For two routers to form a neighbor relationship in EIGRP, the k values must match.

CAUTION: Unless you are very familiar with what is occurring in your network, it is recommended that you do not change the k values.

- EIGRP Auto-Summarization

Router(config-router)#auto-summary Enables auto-summarization for the EIGRP process.

NOTE: The default behavior of auto summarized changed from enabled to disabled was introduced in Cisco IOS Software Release 12.2(8)T.

Router(config-router)#no auto-summary Turns off the auto-summarization feature.

NOTE: The behavior of the auto-summary command is disabled by default, beginning in Cisco IOS Software Release 12.2(8)T. This means that Cisco IOS Software will now send sub prefix routing information across classful network boundaries.

Router(config)#interface fastethernet 0/0 Enters interface configuration mode.

Router(config-if)#ip summary-address eigrp 100 10.10.0.0 255.255.0.0 75

Enables manual summarization for EIGRP autonomous system 100 on this specific interface for the given address and mask. An administrative distance of 75 is assigned to this summary route.

NOTE: The administrative-distance argument is optional in this command. Without it, an administrative distance of 5 is automatically applied to the summary route.

- Load Balancing: variance

Router(config)#router eigrp 100 Creates routing process 100

Router(config-router)#network 10.0.0.0 Specifies which network to advertise in EIGRP

Router(config-router)#variance n

Instructs the router to include routes with a metric less than or equal to n times the minimum metric route for that destination, where n is the number specified by the variance command

NOTE: If a path is not a feasible successor, it is not used in load balancing.

NOTE: EIGRP supports up to six unequal-cost paths

- Bandwidth Use

Router(config)#interface serial 0/0 Enters interface configuration mode.

Router(config-if)#bandwidth 256

Sets the bandwidth of this interface to 256 kilobits to allow EIGRP to make a better metric calculation.

Router(config-if)#ip bandwidth-percent eigrp 50 100

Configures the percentage of bandwidth that may be used by EIGRP on an interface. 50 is the EIGRP autonomous system number. 100 is the percentage value. $100\% * 256 = 256$ kbps.

- Authentication

Router(config)#interface serial 0/0 Enters interface configuration mode.

Router(config-if)#ip authentication mode eigrp 100 md5

Enables Message Digest 5 algorithm (MD5) authentication in EIGRP packets over the interface.

Router(config-if)#ip authentication key-chain eigrp 100 CISCO

Enables authentication of EIGRP packets. CISCO is the name of the key chain.

Router(config-if)#exit Returns to global configuration mode.

Router(config)#key chain CISCO

Identifies a key chain. The name must match the name configured in interface configuration mode above.

Router(config-keychain)#key 1 Identifies the key number.

NOTE: The range of keys is from 0 to 2147483647. The key identification numbers do not need to be consecutive. At least 1 key must be defined on a key chain.

Router(config-keychain-key)#key-string Shakespeare Identifies the key string.

NOTE: The string can contain from 1 to 80 uppercase and lowercase alphanumeric characters, except that the first character cannot be a number.

Router(config-keychain-key)#accept-lifetime start-time {infinite | end-time | duration seconds}
Optionally specifies the period during which the key can be received.

NOTE: The default start time and the earliest acceptable date is January 1, 1993. The default end time is an infinite period.

Router(config-keychain-key)#send-lifetime start-time {infinite | endtime | duration seconds}
Optionally specifies the period during which the key can be sent.

NOTE: The default start time and the earliest acceptable date is January 1, 1993. The default end time is an infinite period.

- Verifying EIGRP

Router#show ip eigrp neighbors Displays the neighbor table.

Router#show ip eigrp neighbors detail Displays a detailed neighbor table.

TIP: The show ip eigrp neighbors detail command verifies whether a neighbor is configured as a stub router.

Router#show ip eigrp interfaces Shows information for each interface.

Router#show ip eigrp interfaces serial 0/0 Shows information for a specific interface.

Router#show ip eigrp interfaces 100 Shows information for interfaces running process 100.

Router#show ip eigrp topology Displays the topology table.

TIP: The show ip eigrp topology command shows you where your feasible successors are.

Router#show ip eigrp traffic Shows the number and type of packets sent and received.

Router#show ip route eigrp Shows a routing table with only EIGRP Entries

- Troubleshooting EIGRP

Router#debug eigrp fsm Displays events/actions related to EIGRP feasible successor metrics (FSM)

Router#debug eigrp packet Displays events/actions related to EIGRP packets

Router#debug eigrp neighbor Displays events/actions related to your EIGRP neighbors

Router#debug ip eigrp neighbor Displays events/actions related to your EIGRP neighbors

Router#debug ip eigrp notifications Displays EIGRP event notifications

Part Four: WAN Configuration:-

15. Implementing Leased Line Cable (PPP & HDLC)

- Configuring HDLC Encapsulation on a Serial Line

Router#configure terminal Moves to global configuration mode

Router(config)#interface serial 0/0/0 Moves to interface configuration mode

Router(config-if)#encapsulation hdlc

NOTE: HDLC is the default encapsulation for synchronous serial links on Cisco routers. You would only use the encapsulation hdlc command to return the link to its default state.

- Configuring PPP on a Serial Line (Mandatory Commands)

Router#configure terminal Moves to global configuration mode

Router(config)#interface serial 0/0/0 Moves to interface configuration mode

Router(config-if)#encapsulation ppp Changes encapsulation from default HDLC to PPP

- Configuring PPP on a Serial Line (Optional Commands): Compression

Router(config-if)#compress predictor Enables the predictor compression algorithm

Router(config-if)#compress stac Enables the stac compression algorithm

- Configuring PPP on a Serial Line (Optional Commands): Link Quality

Router(config-if)#ppp quality x

Ensures the link has a quality of x percent. Otherwise, the link will shut down.

- Configuring PPP on a Serial Line (Optional Commands): Multilink

Router(config-if)#ppp multilink Enables load balancing across multiple Links

- Configuring PPP on a Serial Line (Optional Commands):

Authentication

Router(config)#username R2 password cisco

Sets a username of R2 and a password of cisco for authentication from the other side of the PPP serial link. This is used by the local router to authenticate the PPP peer.

Router(config)#interface serial 0/0/0 Moves to interface configuration mode.

Router(config-if)#ppp authentication pap

Turns on Password Authentication Protocol (PAP) authentication only.

Router(config-if)#ppp authentication chap

Turns on Challenge Handshake Authentication Protocol (CHAP) authentication only.

Router(config-if)#ppp authentication pap chap

Defines that the link will use PAP authentication, but will try CHAP if PAP fails or is rejected by other side.

Router(config-if)#ppp authentication chap pap

Defines that the link will use CHAP authentication, but will try PAP if CHAP fails or is rejected by other side.

Router(config-if)#ppp pap sent username R2 password cisco

This command must be set if using PAP in Cisco IOS Software Release 11.1 or later.

- Verifying or Troubleshooting a Serial Link/PPP Encapsulation

Router#show interfaces serial x Lists information for serial interface x

Router#show controllers serial x

Tells you what type of cable (DCE/DTE) is plugged into your interface and whether a clock rate has been set

Router#debug serial interface Displays whether serial keepalive counters are incrementing

Router#debug ppp Displays any traffic related to PPP

Router#debug ppp packet Displays PPP packets that are being sent and received

Router#debug ppp negotiation Displays PPP packets related to the negotiation of the PPP link

Router#debug ppp error Displays PPP error packets

Router#debug ppp authentication Displays PPP packets related to the authentication of the PPP link

Router#debug ppp compression

Displays PPP packets related to the compression of packets across the link

16. Frame-relay Configuration

- Setting the Frame Relay Encapsulation Type

Router(config)#interface serial 0/0/0

Router(config-if)#encapsulation frame-relay

Turns on Frame Relay encapsulation with the default encapsulation type of cisco.

Or

Router(config-if)#encapsulation frame-relay ietf

Turns on Frame Relay encapsulation with the encapsulation type of ietf (RFC 1490). Use the ietf encapsulation method if connecting to a non-Cisco router.

- Setting the Frame Relay Encapsulation LMI Type

Router(config-if)#frame-relay lmi-type {ansi | cisco | q933a}

Depending on the option you select, this command sets the LMI type to the ANSI standard, the Cisco standard, or the ITU-T Q.933 Annex A standard.

- Setting the Frame Relay DLCI Number

Router(config-if)#frame-relay interface-dlci 110

Sets the DLCI number of 110 on the local interface and enters Frame Relay DLCI configuration mode

Router(config-fr-dlci)#exit Returns to interface configuration mode

Router(config-if)#exit Returns to global configuration mode

- Configuring a Frame Relay map Statement

Router(config-if)#frame-relay map ip 192.168.100.1 110 broadcast

Maps the remote IP address (192.168.100.1) to the local DLCI number (110). The optional broadcast keyword specifies that broadcasts across IP should be forwarded to this address. This is necessary when using dynamic routing protocols.

Router(config-if)#no frame-relay inverse arp Turns off Inverse ARP.

- Configuring Frame Relay Using Sub interfaces

Router(config)#interface serial 0/0/0

Router(config-if)#encapsulation frame-relay ietf

Sets the Frame Relay encapsulation type for all sub interfaces on this interface

Router(config-if)#frame-relay lmi-type ansi Sets the LMI type for all sub interfaces on this interface

Router(config-if)#no ip address Ensures there is no IP address set to this interface

Router(config-if)#no shutdown Enables the interface

Router(config-if)#interface serial 0/0/0.102 point-to-point
Creates a point-to-point sub interface numbered 102

Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Assigns an IP address and netmask to the sub interface

Router(config-subif)#frame-relay interface-dlci 102 Assigns a DLCI to the sub interface

Router(config-subif)#interface serial 0/0/0.103 point-to-point
Creates a point-to-point sub interface numbered 103

Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Assigns an IP address and netmask to the sub interface

Router(config-subif)#frame-relay interface-dlci 103 Assigns a DLCI to the sub interface

Router(config-subif)#exit Returns to interface configuration mode

Router(config-if)#exit Returns to global configuration mode

NOTE: There are two types of sub interfaces:

- Point-to-point, where a single PVC connects one router to another and each sub interface is in its own IP subnet.
- Multipoint, where the router is the middle point of a group of routers. All other routers connect to each other through this router, and all routers are in the same subnet.

NOTE: Use the no ip split-horizon command to turn off split-horizon commands on multipoint interfaces so that remote sites can see each other.

- Verifying Frame Relay

Router#show frame-relay map Displays IP/DLCI map entries

Router#show frame-relay pvc Displays the status of all PVCs configured

Router#show frame-relay lmi Displays LMI statistics

Router#clear frame-relay counters Clears and resets all Frame Relay counters

Router#clear frame-relay inarp Clears all Inverse ARP entries from the map table

- Troubleshooting Frame Relay

Router#debug frame-relay lmi

Used to help determine whether a router and Frame Relay switch are exchanging LMI packets properly

Part Five: IPv6 Address Routing Configuration:

17. IPv6 Routing Protocol (RIPng)

- Assigning IPv6 Addresses to Interfaces

Router(config)#ipv6 unicast-routing

Enables the forwarding of IPv6 unicast datagrams globally on the router.

Router(config)#interface fastethernet 0/0 Moves to interface configuration mode.

Router(config-if)#ipv6 enable

Automatically configures an IPv6 link-local address on the interface and enables IPv6 processing on the interface.

NOTE: The link-local address that the ipv6 enable command configures can be used only to communicate with nodes on the same link.

Router(config-if)#ipv6 address 3000::1/64

Configures a global IPv6 address on the interface and enables IPv6 processing on the interface.

Router(config-if)#ipv6 address 2001:db8:0:1::/64 eui-64

Configures a global IPv6 address with an interface identifier in the low-order 64 bits of the IPv6 address.

Router(config-if)#ipv6 address fe80::260:3eff:fe47:1530/64 linklocal

Configures a specific link-local IPv6 address on the interface instead of the one that is automatically configured when IPv6 is enabled on the interface.

Router(config-if)#ipv6 unnumbered type/number

Specifies an unnumbered interface and enables IPv6 processing on the interface. The global IPv6 address of the interface specified by type/number will be used as the source address.

- IPv6 and RIPng

Router(config)#interface serial 0/0 Moves to interface configuration mode.

Router(config-if)#ipv6 rip tower enable

Creates the RIPng process named tower and enables RIPng on the interface.

NOTE: Unlike RIPv1 and RIPv2, where you needed to create the RIP routing process with the router rip command and then use the network command to specify the interfaces on which to run RIP, the RIPng process is created automatically when RIPng is enabled on an interface with the ipv6 rip name enable command.

NOTE: Cisco IOS Software automatically creates an entry in the configuration for the RIPng routing process when it is enabled on an interface.

NOTE: The ipv6 router rip processname command is still needed when configuring optional features of RIPng.

Router(config)#ipv6 router rip tower

Creates the RIPng process named tower if it has not already been created, and moves to router configuration mode

Router(config-router)#maximum-paths 2

Defines the maximum number of equal cost routes that RIPng can support.

NOTE: The number of paths that can be used is a number from 1 to 64. The default is 4.

- Static Routes in IPv6

Router(config)#ipv6 route 2001:db8:c18:3::/64 2001:db8:c18:2::2/64

Creates a static route configured to send all packets to a next-hop address of 2001:db8:c18:2::2

Router(config)#ipv6 route 2001:db8:c18:3::/64 fastethernet 0/0

Creates a directly attached static route configured to send packets out interface fastethernet 0/0

Router(config)#ipv6 route 2001:db8:c18:3::/64 fastethernet 0/0 2001:db8:c18:2::2

Creates a fully specified static route on a broadcast interface

- Verifying and Troubleshooting IPv6

CAUTION: Using the debug command may severely affect router performance and might even cause the router to reboot. Always exercise caution when using the debug command. Do not leave debug on. Use it long enough to gather needed information, and then disable debugging with the un debug all command.

TIP: Send your debug output to a syslog server to ensure you have a copy of it in case your router is overloaded and needs to reboot. Router#clear ipv6 rip Deletes routes from the IPv6 RIP routing table and, if installed, routes in the IPv6 routing table

Router#clear ipv6 route * Deletes all routes from the IPv6 routing table

NOTE: Clearing all routes from the routing table will cause high CPU utilization rates as the routing table is rebuilt.

Router#clear ipv6 route 2001:db8:c18:3::/64 Clears this specific route from the IPv6 routing table.

Router#clear ipv6 traffic Resets IPv6 traffic counters.

Router#debug ipv6 packet Displays debug messages for IPv6 packets.

Router#debug ipv6 rip Displays debug messages for IPv6 RIP routing transactions.

Router#debug ipv6 routing

Displays debug messages for IPv6 routing table updates and route cache updates.

Router#show ipv6 interface Displays the status of interfaces configured for IPv6.

Router#show ipv6 interface brief Displays a summarized status of interfaces configured for IPv6.

Router#show ipv6 neighbors Displays IPv6 neighbor discovery cache information.

Router#show ipv6 protocols
Displays the parameters and current state of the active IPv6 routing protocol processes.

Router#show ipv6 rip Displays information about the current IPv6 RIP process.

Router#show ipv6 route Displays the current IPv6 routing table.

Router#show ipv6 route summary Displays a summarized form of the current IPv6 routing table.

Router#show ipv6 routers Displays IPv6 router advertisement information received from other routers.

Router#show ipv6 static Displays only static IPv6 routes installed in the routing table.

Router#show ipv6 static 2001:db8:5555:0/16
Displays only static route information about the specific address given.

Router#show ipv6 static interface serial 0/0
Displays only static route information with the specified interface as the outgoing interface.

Router#show ipv6 static detail Displays a more detailed entry for IPv6 static routes.

Router#show ipv6 traffic Displays statistics about IPv6 traffic.

Router#show ipv6 tunnel Displays IPv6 tunnel information.

Part six: Security Configuration:

18. Implementing and Verifying Access Control List (ACL)

- Creating Standard ACLs

Router(config)#access-list 10 permit 172.16.0.0 0.0.255.255

Read this line to say, "All packets with a source IP address of 172.16.x.x will be permitted to continue through the internetwork."

Router(config)#access-list 10 deny host 172.17.0.1

Read this line to say, "All packets with a source IP address of 172.17.0.1 will be dropped and discarded."

Router(config)#access-list 10 permit any

Read this line to say, "All packets with any source IP address will be permitted to continue through the internetwork."

- Applying Standard ACLs to an Interface

Router(config)#interface fastethernet 0/0

Moves to interface configuration mode.

Router(config-if)#ip access-group 10 in

Takes all access list lines that are defined as being part of group 10 and applies them in an inbound manner. Packets going into the router from fastethernet 0/0 will be checked.

TIP: Access lists can be applied in either an inbound direction (keyword in) or in an outbound direction (keyword out).

TIP: Apply a standard ACL as close as possible to the destination network or device.

- Verifying ACLs

Router#show ip interface

Displays any ACLs applied to that interface

Router#show access-lists

Displays the contents of all ACLs on the router

Router#show access-list access-list-number

Displays the contents of the ACL by the number specified

Router#show access-list name

Displays the contents of the ACL by the name specified

Router#show run

Displays all ACLs and interface assignments

- Removing ACLs

Router(config)#no access-list 10

Removes all ACLs numbered 10

- Creating Extended ACLs

Router(config)#access-list 110 permit tcp 172.16.0.0 0.0.0.255 192.168.100.0 0.0.0.255 eq 80

Read this line to say, "HTTP packets with a source IP address of 172.16.0.x will be permitted to travel to the destination address 192.168.100.x."

Router(config)#access-list 110 deny tcp any 192.168.100.7 0.0.0.0 eq 23

Read this line to say, "Telnet packets with any source IP address will be dropped if they are addressed to specific host 192.168.100.7."

- Applying Extended ACLs to an Interface

Router(config)#interface fastethernet 0/0

Router(config-if)#ip access-group 110 out

Moves to interface configuration mode and takes all access list lines that are defined as being part of group 110 and applies them in an outbound manner. Packets going out fastethernet 0/0 will be checked.

TIP: Access lists can be applied in either an inbound direction (keyword in) or in an outbound direction (keyword out).

TIP: Only one access list can be applied per interface, per direction.

TIP: Apply an extended ACL as close as possible to the source network or device.

- The established Keyword (Optional)

Router(config)#access-list 110 permit tcp 172.16.0.0 0.0.0.255 192.168.100.0 0.0.0.255 eq 80 established

Indicates an established Connection

NOTE: A match will now occur only if the TCP datagram has the ACK or the RST bit set.

TIP: The established keyword will work only for TCP, not UDP.

- Creating Named ACLs

Router(config)#ip access-list extended CISCO

Creates an extended named ACL called CISCO and moves to named ACL configuration mode.

Router(config-ext-nacl)#permit tcp any host 131.108.101.99 eq smtp

Permits mail packets from any source to reach host 131.108.101.99.

Router(config-ext-nacl)#permit udp any host 131.108.101.99 eq domain

Permits Domain Name System (DNS) packets from any source to reach host 131.108.101.99.

Router(config-ext-nacl)#deny ip any any log

Denies all other packets from going anywhere. If any packets do get denied, this logs the results for you to look at later.

Router(config-ext-nacl)#exit

Returns to global configuration mode.

Router(config)#interface fastethernet 0/0

Router(config-if)#ip access-group CISCO out

Moves to interface configuration mode and applies this ACL to the fastethernet interface 0/0 in an outbound direction.

- Using Sequence Numbers in Named ACLs

Router(config)#ip access-list extended serveraccess2

Creates an extended named ACL called serveraccess2.

Router(config-ext-nacl)#10 permit tcp any host 131.108.101.99 eq smtp

Uses a sequence number 10 for this line.

Router(config-ext-nacl)#20 permit udp any host 131.108.101.99 eq domain

Sequence number 20 will be applied after line 10.

Router(config-ext-nacl)#30 deny ip any any log Sequence number 30 will be applied after line 20

Router(config-ext-nacl)#exit Returns to global configuration mode.

Router(config)#interface fastethernet 0/0 Moves to interface configuration mode.

Router(config-if)#ip access-group serveraccess2 out Applies this ACL in an outbound direction.

Router(config-if)#exit Returns to global configuration mode.

Router(config)#ip access-list extended serveraccess2

Moves to named ACL configuration mode for the ACL serveraccess2.

Router(config-ext-nacl)#25 permit tcp any host 131.108.101.99 eq ftp

Sequence number 25 places this line after line 20 and before line 30.

Router(config-ext-nacl)#exit Returns to global configuration mode.

TIP: Sequence numbers are used to allow for easier editing of your ACLs. The preceding example used numbers 10, 20, and 30 in the ACL lines. If you had needed to add another line to this ACL, it would have previously been added after the last line—line 30. If you had needed a line to go closer to the top, you would have had to remove the entire ACL and then reapply it with the lines in the correct order. Now you can enter in a new line with a sequence number, placing it in the correct location.

- Removing Specific Lines in Named ACLs Using Sequence Numbers

Router(config)#ip access-list extended serveraccess2

Moves to named ACL configuration mode for the ACL serveraccess2

Router(config-ext-nacl)#no 20 Removes line 20 from the list

Router(config-ext-nacl)#exit Returns to global configuration mode

Sequence Number Tips

- Sequence numbers start at 10 and increment by 10 for each line.
- If you forget to add a sequence number, the line is added to the end of the list.
- Sequence numbers are changed on a router reload to reflect the increment by 10 policy (tip 1). If your ACL has numbers 10, 20, 30, 32, 40, 50, and 60 in it, on reload these numbers become 10, 20, 30, 40, 50, 60, and 70.

- Including Comments About Entries in ACLs

Router(config)#access-list 10 remark only Jones has access

The remark command allows you to include a comment (limited to 100 characters).

Router(config)#access-list 10 permit 172.16.100.119

Read this line to say, "Host 172.16.100.119 will be permitted through the internetwork."

Router(config)#ip access-list extended NEW

Creates a named ACL called NEW and moves to named ACL configuration mode.

Router(config-ext-nacl)#remark do not let Smith have telnet

The remark command allows you to include a comment (limited to 100 characters).

Router(config-ext-nacl)#deny tcp host 172.16.100.153 any eq telnet

Read this line to say, "Deny this specific host Telnet access to anywhere in the internetwork."

TIP: You can use the remark command in any of the IP numbered standard, IP numbered extended, or named IP ACLs.

TIP: You can use the remark command either before or after a permit or deny statement. Therefore, be consistent in your place

- Restricting Virtual Terminal Access

Router(config)#access-list 2 permit host 172.16.10.2

Permits host 172.16.10.2 to Telnet into this router based on where this ACL is applied.

Router(config)#access-list 2 permit 172.16.20.0 0.0.0.255

Permits anyone from the 172.16.20.x address range to Telnet into this router based on where this ACL is applied. The implicit deny statement restricts anyone else from being permitted to Telnet.

Router(config)#line vty 0 4 Moves to vty line configuration mode.

Router(config-line)#access-class 2 in

Applies this ACL to all 5 vty virtual interfaces in an inbound direction.

TIP: When restricting access through Telnet, use the access-class command rather than the access group command, which is used when applying an ACL to a physical interface.

19. Network Address Translation (NAT) Configuration

- Configuring Static NAT: One Private to One Permanent Public Address Translation

Step 1: Create a static mapping on your router that will perform NAT.

Router(config)#ip nat inside source static 172.16.10.5 64.64.64.65

Permanently translates the inside address of 172.16.10.5 to a public address of 64.64.64.65. Use the command for each of the private IP addresses you want to statically map to a public address.

Step 2: Define which interfaces are inside (contain the private addresses).

Router(config)#interface fastethernet 0/0 Moves to interface configuration mode.

Router(config-if)#ip nat inside You can have more than one inside interface on a router.

Step 3: Define the outside interface (the interface leading to the public network).

Router(config-if)#interface serial 0/0/0 Moves to interface configuration mode.

Router(config-if)#ip nat outside Defines which interface is the outside interface for NAT.

CAUTION: Make sure that you have in your router configurations a way for packets to travel back to your NAT router. Include a static route on the ISP router advertising your NAT pool and how to travel back to your internal network. Without this in place, a packet can leave your network with a public address, but it will not be able to return if your ISP router does not know where the pool of public addresses exists in the network. You should be advertising the pool of public addresses, not your private addresses.

- Configuring Dynamic NAT: One Private to One Public Address Translation

Step 1: Define a pool of usable public IP addresses on your router that will perform NAT.

Router(config)#ip nat pool CISCO 64.64.64.70 64.64.64.126 netmask 255.255.255.128

Defines the following: The name of the pool is CISCO. (The name of the pool can be anything.) The start of the pool is 64.64.64.70. The end of the pool is 64.64.64.126. The subnet mask is 255.255.255.128.

Step 2: Create an access control list (ACL) that will identify which private IP addresses will be translated.

Router(config)#access-list 1 permit 172.16.10.0 0.0.0.255

Step 3: Link the ACL to the pool of addresses (create the translation).

Router(config)#ip nat inside source list 1 pool CISCO

Defines the following: The source of the private addresses is from ACL 1. The pool of available public addresses is named CISCO.

Step 4: Define which interfaces are inside (contain the private addresses).

Router(config)#interface fastethernet 0/0 Moves to interface configuration mode.

Router(config-if)#ip nat inside

You can have more than one inside interface on a router. Addresses from each inside interface are then allowed to be translated into a public address.

Step 5: Define the outside interface (the interface leading to the public network).

Router(config)#interface serial 0/0/0

Router(config-if)#ip nat outside

- Configuring PAT: Many Private to One Public Address Translation

Step 1: Define a pool of usable public IP addresses on your router that will perform NAT (optional).

Router(config)#ip nat pool CISCO 64.64.64.70 64.64.64.70 netmask 255.255.255.128

Defines the following: The name of the pool is CISCO. (The name of the pool can be anything.) The start of the pool is 64.64.64.70. The end of the pool is 64.64.64.70. The subnet mask is 255.255.255.128.

Step 2: Create an ACL that will identify which private IP addresses will be translated.

Router(config)#access-list 1 permit 172.16.10.0 0.0.0.255

Step 3 (Option 1): Link the ACL to the outside public interface (create the translation).

Router(config)#ip nat inside source list 1 interface serial 0/0/0 overload

The source of the private addresses is from ACL 1. The public address to be translated into is the one assigned to serial 0/0/0. The overload keyword states that port numbers will be used to handle many translations.

Step 3 (Option 2): Link the ACL to the pool of addresses (create the translation).

Router(config)#ip nat inside source list 1 pool CISCO overload

The source of the private addresses is from ACL 1. The pool of the available addresses is named CISCO. The overload keyword states that port numbers will be used to handle many translations.

Step 4: Define which interfaces are inside (contain the private addresses).

Router(config)#interface fastethernet 0/0 Moves to interface configuration mode.

Router(config-if)#ip nat inside You can have more than one inside interface on a router.

Step 5: Define the outside interface (the interface leading to the public network).

Router(config)#interface serial 0/0/0 Moves to interface configuration mode.

Router(config-if)#ip nat outside Defines which interface is the outside interface for NAT.

- Verifying NAT and PAT Configurations

Router#show ip nat translations Displays the translation table

Router#show ip nat statistics Displays NAT statistics

Router#clear ip nat translations inside a.b.c.d outside e.f.g.h
Clears a specific translation from the table before it times out

Router#clear ip nat translations* Clears the entire translation table before entries time out

- Troubleshooting NAT and PAT Configurations

Router#debug ip nat
Displays information about every packet that is translated. Be careful with this command. The router's CPU might not be able to handle this amount of output and might therefore hang the system.

Router#debug ip nat detailed Displays greater detail about packets being translated.

20. Security Device Manager (SDM)

NOTE: Cisco recommends that you use the Cisco Router and Security Device Manager (SDM) to configure your router. However, Cisco also realizes that most implementations of a router with SDM will be to use the command line interface (CLI) for initial configuration; then, after the routers have been added to the network, all future configuration will take place using SDM.

The screenshot displays the Cisco Router and Security Device Manager (SDM) web interface. The title bar indicates the connection to 192.168.100.1. The interface includes a menu bar (File, Edit, View, Tools, Help) and a toolbar with icons for Home, Configure, Monitor, Refresh, Save, Search, and Help. The main content area is divided into two primary sections: 'About Your Router' and 'Configuration Overview'.

About Your Router

Host Name: 2821

Hardware (More...)

- Model Type: Cisco 2821
- Available / Total Memory(MB): 196/256 MB
- Total Flash Capacity: 61 MB

Software (More...)

- IOS Version: 12.4(10a)
- SDM Version: 2.3.1

Feature Availability: IP ☒ Firewall ☒ VPN ☒ IPS ☒ NAC ☒

Configuration Overview (View Running Config)

Interfaces and Connections (Up (1), Down (13))

Total Supported LAN:	3	Total Supported WAN:	2(Serial Sync/Async)
Configured LAN Interface:	1	Total WAN Connections:	1(HDLC)
DHCP Server:	Not Configured	No. of DHCP Clients:	0
DHCP Pool:	Not Configured		

Interface	Type	IP/Mask	Description
GigabitEthernet0/0	GigabitEthernet	192.168.100.1/24	
GigabitEthernet0/1	GigabitEthernet	no ip address	

Routing

- No. of Static Route: 0
- Dynamic Routing Protocols: None

- Resetting the Router to Factory Defaults Using SDM

Starting at the SDM home page, to reset the router back to factory defaults, first click the Configure button at the top of the SDM screen, and then click Additional Tasks on the left side of the screen under the Tasks column

