2024

CCNA COMMANDS

CISCO CERTIFIED NETWORK ASSOCIATE

WRITTEN BY MAHTAB PUZESHI

CONTENTS

BASIC

Command	Purpose
#enable	Enter global configuration mode.
#configure terminal	To execute any command.
#hostname SW-01	Configure the NAME of the Router or Switch.
#username admin secret admin	Set username and password .
#enable secret admin	Make the privilege level password.
#service password-encryption	Encrypt all passwords .
#line console 0	Enter the console connection configuration mode.
#login	Instruct the router that you want it to check for a password.
#password admin	Set password for Line Console .
# line vty 0 15	To enable telnet connectivity on the Cisco devices.
# copy running-config startup-config	To Save configuration.
# wr	Same as copy running-configuration startup-configuration.

Interface

Command	Purpose
#interface fastethernet 0/1	To select a port for configuration.
#interface range fastethernet 0/1-6	To select a range of ports for configuration.
#switchport mode access	To set the port to Access mode.
#no shutdown	To enable the port.
#description MNG	To set description for interface.
#speed 10 / auto	To configure the speed of interface.
#duplex auto / full / half	To prevent a duplex mismatch
#ip address 192.168.1.1 255.255.255.0	To assign an IP address & Subnet Mask for interface .
#switchport access vlan 10	To access the port to VLAN10.
#show interfaces status	Display the status of interfaces.
#show ip interface brief	Display interfaces IP address and status.
#show interface fastethernet 0/1	Display the detail and status of the selected port.
#show cdp interface	Shows which interfaces are running CDP.
#interface Loopback 0	Loopback interface acts as a place holder for the static IP add
#ip address 10.108.1.1 255.255.255.0	To set an IP address for loopback .

SSH

Secure Shell is a Secure Method for Remote Access as it includes Authentication and Encryption.

Command	Purpose
#hostname SW-1	Must change the hostname of the device from the default.
#username admin secret admin	Configure a local user and password.
#line vty 0 15	Change parameters for remote access.
#login local	To tell the VTY ports to ask for password from remote user.
#privilege level 15	Default Privilege Levels allows full access to all commands.
#ip ssh version 2	Configures the Switch to run SSH Version 2.
#transport input ssh	This will restrict SSH into this device.
#transport output ssh	This will allow SSH to be initiated from this device.
#ip domain-name cisco.local	Configure a host domain .
#crypto key generate rsa	Make an encryption key - select 1024 bits.
#banner motd "welcome"	Display a MESSAGE when you login .

Port Security on Switch

To Stop or Prevent Unauthorized Users to Access the LAN .

Command	Purpose
#interface fastethernet 0/1	Select the interface to configure.
# switchport mode access	Change from dynamic to access mode.
# switchport port-security	To activate port-security.
# switchport port-security maximum 25	Only 25 MAC addresses are allowed .
#switchport port-security mac-address sticky	To memorize MAC addresses.
#switchport port-security violation protect | restrict | shutdown	To choose the violation response.
#spanning-tree bpduguard enable	To disable interface if receives BPDU.
# no cdp run	No one can see what devices are connected.
#ip dhcp snooping	Prevents unauthorized DHCP servers offering IP addresses to DHCP clients.

VLAN

Virtual LAN - Segmentation of a Network helps to Increase Security, Reliability, and Efficiency of a Network.

Command	Purpose
#vlan 10	To create a VLAN.
#name IT	To name the VLAN.
# interface fastethernet 0/1	Select a port .
# switchport mode access	To change the mode from dynamic to access .
#switchport access vlan 10	To access the interface to VLAN 10.
#show vlan brief	Shows what VLANs exist , name , interface assigned .

VTP

VLAN Trunking Protocol - When you configure a new VLAN on a VTP server, the VLAN will distribute through all switches in the domain .

Command	Purpose
#vtp domain CSO	The name of the VTP domain.
#vtp password admin	The password for the VTP administrative domain.
#vtp version 3	The VTP version.
#vtp mode server | client | transparent	Choose the VTP mode.
#show vtp status	Displays information about the VTP configuration on device.

Trunk

A Trunk port is a port that is Assigned to carry Traffic for all the VLANs that are Accessible by a Specific Switch , a process known as Trunking . There are two methods of Encapsulation: IEEE 802.1Q & ISL .

Command	Purpose
#interface Gigabitethernet 0/1	Select a port to configure.
#switchport trunk encapsulation dot1q	To use IEEE 802.1Q encapsulation on frames.
#switchport mode trunk	To convert the link into a trunk link.
#switchport nonegotiate	To Prevents the interface from generating DTP frames.
#swithport trunk native vlan 99	To carry untagged traffic.
#switchport trunk allowed vlan all|none|vlan-list	Define which VLANs allowed on the trunk.
#show interface trunk	Shows the ports that are trunk .

Etherchannel

EtherChannel provides Incremental Trunk Speeds between Fast Ethernet, Gigabit Ethernet, and 10 Gigabit Ethernet . EtherChannel combines multiple Fast Ethernet up to 800Mbps _ Gigabit Ethernet up to 8Gbps _ and 10 Gigabit Ethernet up to 80Gbps.

Command	Purpose
#interface portchannel 10	Creates the port channel interface.
#switchport mode trunk	To convert the link into Trunk .
#interface range fastethernet 0/1-4	Select a range of interface to configure.
#switchport mode trunk	To convert the links into Trunk .
#channel-group 10 mode active | passive | on | desirable	Specifies the mode : **PAgP** supports only the **auto** and **desirable** **LACP** supports only the **active** and **passive**
#channel-protocol lacp | pagp	Choose the EtherChannel protocol.
#show etherchannel summary	Display brief information of all port-channels.

SVI

Switch Virtual Interface created on a specific VLAN can be used as a Default Gateway for the VLAN .

Command	Purpose
#interface vlan 10	The valid VLAN interface.
#no shutdown	To enable the vlan.
#ip address 192.168.10.1 255.255.255.0	Assign an IP address as default gateway on vlan 10 .

IVR

Inter VLAN Routing Enables Routers or Layer 3 Switches to Route Traffic between VLANs.

Command	Purpose
Router#interface GigabitEthernet 0/0.10	To create a sub-interface for VLAN 10.
Router#encapsulation dot1Q 10	Use 802.1Q trunking.
Router #ip address 10.0.10.1 255.255.255.0	Assign the default gateway ip address of vlan 10 .
#show ip interface brief	To see the subinterfaces with IP addresses .

DHCP

Dynamic Host Configuration Protocol will Automates the process of Allocating IP addresses .

Command	Purpose
# interface Vlan 10	Select a valid vlan interface .
# ip address 192.168.10.1 255.255.255.0	To set the default gateway of vlan 10 .
# no shutdown	To enable the vlan .
#ip dhcp excluded-address 192.168.10.0 192.168.1.10	Set excluded IP Addresses .
#ip dhcp pool VLAN-10	To create a DHCP pool , also will change the mode to DHCP pool configuration mode.
#network 192.168.10.0 255.255.255.0	Set the Network with SM .
#default-router 192.168.10.1	To set default gateway for vlan 10 .
#dns-server 192.168.10.2	To Set a primary DNS server for the clients.
#show ip dhcp binding	Displays the IP DHCP server lease entry.

DHCP Relay Agent

DHCP Relay Agent provides a way for DHCP clients to Communicate with DHCP Servers when None are available on its Local Subnet.

Command	Purpose
#interface FastEthernet 0/1	The interface that connect to server.
#description DHCP	To set description for the port.
#switchport trunk encapsulation dot1q	To use IEEE 802.1Q encapsulation on the frames.
#switchport mode trunk	To convert the link into trunk .
# ip dhcp snooping trust	Configure the interface as a trusted interface.
#interface vlan 100	The DHCP Vlan.
#ip address 192.168.100.2 255.255.255.0	To set gateway for dhcp vlan.
#ip helper-address 192.168.100.1	Now set ip helper-address on Vlan so clients could receive IP add .

server (physical)	
IP address	192.168.100.1
Subnet mask	255.255.255.0
Default gateway	192.168.100.2
DNS Server	8.8.8.8
DHCP Services	
ServerPool-10	ON
Default gateway	192.168.10.1
DNS Server	8.8.8.8
Start IP address	192.168.10.10

Spanning Tree Protocol

Spanning Tree Protocol (STP) is a Layer 2 Network Protocol used to Prevent Loop within a Network Topology.

Command	Purpose
#spanning-tree mode stp ∣ rstp	To select which Spanning Tree Protocol (STP) protocol to run.
#spanning-tree vlan 10,20 root primary ∣ secondary	To set these vlans as primary .
#spanning-tree vlan 10 priority 100	The low value will have higher priority.
# spanning-tree hello-time 5	How often the device broadcasts Hello messages to other devices.
# spanning-tree guard root	So it cannot be selected as the root port even if it receives superior STP BPDUs.
#spanning-tree portfast	To be a "designated port" immediately without going through the normal listening and learning states.
#spannnig-tree bpdugaurd enable	To shutdown an interface when it receives a BPDU, will reduce the risk of attacks on the network.
#show switch spanning-tree	To see the STP configuration.

ROUTING

To Managing Data Traffic in Router .

Types	Command
Static route	172.16.0.0 255.255.0.0 gigabitethernet 0/1
Next Hop	172.16.0.0 255.255.0.0 10.10.10.1
Default route	0.0.0.0 0.0.0.0 10.10.10.1

Routing Protocols

EIGRP

Enhanced Interior Gateway Routing Protocol Enables Routers to Exchange Information more Efficiently than Earlier Network Protocols .

Command	Purpose
#router eigrp 100	Assign an ID to EIGRP.
#network 172.16.10.0 0.0.0.3	Define the interfaces + Wildcard mask.
#network 10.10.40.0 0.0.0.255	Define the interfaces + Wildcard mask.
#no auto-summary	EIGRP auto-summary will only create summary routes for directly connected networks, not for routes you learn from other EIGRP routers.
#redistribute eigrp 200 metric 1000000 100 255 1 1500	To exchange routing information between different routing protocols – Eigrp metric { bandwidth | delay | reliability | load | MTU }
# show ip route	To display the Ipv4 routing table .
#show ip eigrp topology	To view all available routes for each destination.
#show ip route eigrp	To list all routes added in the routing table by EIGRP.
#show ip eigrp neighbors	To see the routers which became neighbors.

OSPF

Open Shortest Path First - Can Recalculate the Routes in a Short Amount of Time .

Command	Purpose
#router ospf 1	Enables OSPF configuration mode.
#network 192.168.10.0 0.0.0.255 area 0	To define network and area .
# ip ospf cost 1562	To set an absolute OSPF cost for a link .
# ip ospf hello-interval seconds	Change hello timer from default 10 seconds.
# ip ospf dead-interval seconds	Change dead timer from default 40 seconds
#show ip ospf interface	Displays OSPF-related interface information.
#show ip ospf neighbor	Displays OSPF neighbors information .

RIP

Routing Information Protocol is a Distance Vector Protocol that uses Hop Count as its Primary Metric.

Command	Purpose
#router rip	Enable RIP routing mode .
#network 192.168.10.0	To define the interfeces network which are connecte
#version 2	Enable RIP routing protocol version 2.
#no auto-summary	To disable automatically summarize networks .
# show rip database	Displays information about routes in the Routing Information Base.
#show rip neighbors	Displays information about all RIP route gateways.

ACL

Access Control List is an Ordered Set of Rules that you can use to Filter Traffic .

Standard-ACL

Command	Purpose
#access-list 1 permit host 192.168.146.0	Access-list standard (1-99) - To allow access for this host .
#access-list 1 deny 11.0.0.0 0.0.0.255	To deny access for this host .
#ip access-group 1 out | in	Set this on incoming | outgoing interfaces .

Extended-ACL

Command	Purpose
#access-list 100 permit ip 10.0.0.1 0.0.0.0 host 192.168.0.1	To allow all access to host 192.168.0.1.
#access-list 100 deny ip 10.0.0.2 0.0.0.0 host 192.168.0.1	To deny all access to host 192.168.0.1.
#interface fastethernet 0/0	Select the port.
#ip access-group 100 in	Set this on incoming | outgoing interfaces .
#ip access-list extended 100	Access list extended (100-199) .
#permit tcp 10.0.0.2 0.0.0.3 host 192.168.0.1 eq 80	To allow access only for website 192.168.0.1 .
# permit tcp any any eq 80	To allow web access for all.
#permit ip any any	Full access for all.
#deny udp 172.16.10.0 0.0.0.255 host 192.168.0.1 eq 53	To deny DNS .
#deny icmp 10.10.10.0 0.0.0.3 host 192.168.0.1	To deny ICMP .

NAT

Network Address Translation

Static NAT is used to do a One-To-One Mapping between an Inside address and an Outside address.

Command	Purpose
#ip nat inside source static 10.0.0.0 255.255.255.0 100.1.1.1	**10.0.0.0 will translate to ip public 100.1.1.1**
#interface fastethernet 0/1	**Incoming port**
#ip nat inside	
#interface fastethernet 0/2	**Outgoing port**
#ip nat outside	

Dynamic NAT is used when you have a Pool of Public IP addresses that you want to Assign to your Internal Hosts Dynamically.

Command	Purpose
#interface fastethernet 0/0	
#ip nat inside	Incoming interface .
#interface fastethernet 0/1	
#ip nat outside	Outgoing interface .
#access-list 1 permit 10.0.0.0 0.0.0.255	Define the network that have access .
#ip nat pool STUDY 5.5.5.1 5.5.5.11 netmask 255.255.255.0	Define a pool of public ip address .
#ip nat inside source list 1 pool STUDY	Dynamic NAT command.
#show ip nat translations	To show NAT table.

Overload NAT | PAT also known as Port Address Translation, is a technique used in computer networking.

It Allows for Multiple Devices on a Private Network to Access the Internet using a Single Public IP Address.

Command	Purpose
#access list 1 permit 192.168.0.0 0.255.255.255	Define the network that have access .
#ip nat pool STUDY 20.20.20.2 20.20.20.2 netmask 255.255.255.252	Define a pool which include single ip public .
#ip nat inside source list 1 pool STUDY overload	PAT Command.
#interface fastethernet 0/1	
#ip nat inside	Incoming port.
#interface fastethernet 0/2	
#ip nat outside	Outgoing port.

HSRP Configuration

Hot Standby Router Protocol is Cisco's Standard Method of providing High network Availability by providing First-hop Redundancy for IP hosts .

Command	Purpose
# interface gigabitethernet 0/1	Enter the interface which you want to enable HSRP.
# standby 10 ip 172.167.10.10	Create the HSRP group using its number and virtual IP address.
#standby 10 priority 120	Assigning priority helps select the active and standby - The highest number represents the highest priority.
#standby preempt	If preemption is enabled , the switch with the highest priority becomes the designated active .
#standby 10 delay 300	To postpone taking over the active role for the shown number of seconds.
# standby 1 timers 5 15	Configure the time between hello packets and the time before other switche declare the active switch to be down.
# show standby	To see if HSRP is active.
#show standby brief	To see HSRP details.

Troubleshoot

Command	Purpose
#ping 172.16.10.10	To reach the destination host.
#traceroute 172.16.10.10	Shows the path taken to reach the destination host .
#show process cpu	Shows cpu statistics .
#show arp	Display the arp cache.
#show users	Displays the users currently logged on.
#show reload	Reboots the device.
#clrear crypto session	Debug crypto isakmp.
#ip routing	Activate IPv4 routing within the switch.
#show running-config	Display the running configuration – active.
#show startup-config	Display the startup configuration.
#**show ip route connected**	Show routing table entries for directly connected networks.
# **show version**	Display the software version that the switch runs.
#show inventory	To display the product inventory listing of all Cisco products installed in the networking device.
# show module	Display status and information for all modules.
#show clock	Display the clock.
#show cdp neighbors	Show directly connected cisco devices.
#show mac-address table	Display switch mac address table.
#show standby	See if HSRP is active.

Common Port Numbers and Protocols

Protocol	Port
File Transfer Protocol (**FTP**)	FTP Control=TCP port **21** FTP Data = TCP Port **20**
Secure Shell (**SSH**)	TCP Port **22**
Telnet	TCP Port **23**
Simple Mail Transfer Protocol (**SMTP**)	TCP Port **25**
Dynamic Host Configuration Protocol (**DHCP**)	UDP Port **67** (request from client to server) UDP Port **68** (reply from server to client)
Hypertext Transfer Protocol (**HTTP**)	TCP Port **80**
Secure Hypertext Transfer Protocol (**HTTPS**)	TCP Port **443**
Post Office Protocol – incoming mail (**POP**)	TCP Port **110**
Network Time Protocol (**NTP**)	UDP Port **123**
Simple Network Management Protocol (**SNMP**)	UDP Port **161**
Domain Name System name resolver **(DNS)**	TCP, UDP Port **53**
Trivial File Transfer Protocol**(TFTP)**	UDP Port **69**
Internet Message Access Protocol **(IMAP)**	TCP, UDP Port **143**
Remote Desktop Protocol **(RDP)**	TCP port **3389**