CISCO

Sunday, March 17, 2024 8:05 PM

- Correctly configure zones (they could be configured incorrectly)
- Make sure zones have correct traffic rules (follow flow control)

DHCP commands

Security commands

Monitoring and logging commands

Command Modes

Cisco IOS has several command modes that fall into further categories such as operational and configuration. Each mode serves a slightly unique purpose. For instance, Setup Mode provides the user with an interactive menu guide the user to create an initial configuration file for the device.

The key most common modes are the following:

User exec mode — This mode is the mode you land in when you first log onto a Cisco device. It provides limited access to commands and configuration settings. For instance, this mode enables you to view status using certain show commands but does not enable you to view or edit configurations.

Privileged exec mode — This mode provides access to all commands, enabling more detailed examination and control of the device's operation and configuration.

Global Configuration mode: Global configuration commands apply to features that affect the device as a whole. While Exec and Privileged Exec are read-only modes, Global Configuration mode gives the user writable access to modify the active configuration file. To use Global Configuration mode, you first need to enter Privileged EXEC Mode and then execute the configure terminal command although numerous shortcuts are accepted such as config t. Global Configuration mode can be further divided into the following command modes, which permit you to configure different components:

- Interface configuration mode
- Subinterface configuration mode
- Router configuration mode
- Line configuration mode

Mode Control Commands

Command	Description
enable	Moves a user from user exec mode into Privileged EXEC mode. Privileged exec mode is indicated by the # symbol in the command prompt.
configure terminal	Logs the user into Global Configuration mode
interface *fastethernet/number*	Enters interface configuration mode for the specified fast ethernet interface

Basic Configuration Commands List

reload	Reboots the Cisco switch or router
hostname *name*	Sets a host name to the current Cisco network device
copy *from-location to-location*	Copies files from one file location to another
copy running-config startup-config	Replaces the startup config with the active config when the Cisco network device initializes

copy startup-config running-config	Merges the startup config with the currently active config in RAM
write erase **erase startup-config**	Deletes the startup config
ip address *ip-address mask*	Assigns the specified IP address and subnet mask
shutdown **no shutdown**	Shuts the interface down (shutdown) or brings it up (no shutdown)
ip default-gateway *ip_address*	Sets the default gateway on the Cisco device
show running-config	Displays the current configuration of

show running-config	Displays the current configuration of the device
show startup-config	Displays the saved configuration stored in the device's NVRAM, which will be loaded when the device starts up
description *string*	Assigns the specified description to an interface
show running-config interface *interface slot/number*	Displays the running configuration for the specified interface
show ip interface *[type number]*	Displays the status of a network interface as well as a detailed listing of its IP configurations and related characteristics.
ip name-server *serverip-1 serverip-2*	Sets the IP address of or more DNS servers that the device can use to resolve hostnames to IP addresses.

Troubleshooting Cisco Commands List

ping *{hostname | system-address} [source source-address]*	Used to diagnose basic network connectivity
speed *{10 | 100 | 1000 | auto}*	Either configures the transmission speed of a network interface to the specified value in megabits per second (Mbps), or enables automatic speed detection for the port
duplex *{auto | full | half}*	Sets duplex to half, full or auto
cdp run **no cdp run**	Enables or disables Cisco Discovery Protocol (CDP) for the device
show mac address-table	Displays the MAC address table
show cdp	Shows whether CDP is enabled globally
show cdp neighbors*[detail]*	Lists summary (or detailed) information about each neighbor connected to the device
show interfaces	Displays detailed information about

show interfaces	Displays detailed information about interface status, settings and counters
show interface status	Displays the interface line status
show interfaces switchport	Displays many configuration settings and current operational status, including VLAN trunking details

show interfaces trunk	Lists information about the currently operational trunks and the VLANs supported by those trunks
show vlan **show vlan brief**	Lists each VLAN and all interfaces assigned to that VLAN but does not include trunks
show vtp status	Lists the current VLAN Trunk Protocol (VTP) status, including the current mode

Routing and VLAN Commands

show ip route	Displays the current state of the IP routing of all known routes that are either statically configured or learned dynamically through a routing protocol
ip route *network-number network-mask {ip-address | interface}*	Sets a static route in the IP routing table
router rip	Enables a Routing Information Protocol (RIP) routing process, which places you in router configuration mode
network *ip-address*	Associates a network with a RIP routing process
version 2	Configures the software to receive and send only RIP version 2 packets
no auto-summary	Disables automatic summarization

default-information originate	Generates a default route into RIP

passive-interface *interface*	Sets the specified interface to passive RIP mode, which means RIP routing updates are accepted by, but not sent out of, the interface
show ip rip database	Displays the contents of the RIP routing database
ip nat *[inside | outside]*	Configure Network Address Translation (NAT), which allows private IP addresses on a local network to be translated into public IP addresses before being sent over the internet
ip nat inside source *{list{access-list-number | access-list-name}} interface type number[overload]*	Establishes dynamic source translation. Use of the "list" keyword enables you to use an ACL to identify the traffic that will be subject to NAT. The "overload" option enables the router to use one global address for many local addresses.
ip nat inside source static *local-ip global-ip*	Establishes a static translation between an inside local address and an inside global address
vlan	Creates a VLAN and enters VLAN configuration mode for further definitions
switchport access vlan	Sets the VLAN that the interface belongs to.
switchport trunk encapsulation dot1q	Specifies 802.1Q encapsulation on the trunk link.

switchport access	Configures a specific Ethernet port on a switch to operate in access mode to accommodate an end device such as a computer, server or printer. The port must then be assigned to a single VLAN.
vlan vlan-id *[name vlan-name]*	Configures a specific VLAN name (1 to 32 characters)
switchport mode *{ access | trunk }*	Configures the VLAN membership mode of a port. The access port is set to access unconditionally and operates as a non-trunking, single VLAN interface that sends and receives non-encapsulated (non-

	tagged) frames. An access port can be assigned to only one VLAN. The trunk port sends and receives encapsulated (tagged) frames that identify the VLAN of origination. A trunk is a point-to-point link between two switches or between a switch and a router.
switchport trunk *{encapsulation { dot1q }*	Sets the trunk characteristics when the interface is in trunking mode. In this mode, the switch supports simultaneous tagged and untagged traffic on a port.
encapsulation dot1q vlan-id	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance
show spanning-tree	Provides detailed information about the Spanning Tree protocol for all VLANs

DHCP Commands

ip address dhcp	Acquires an IP address on an interface via DHCP
ip dhcp pool name	Used to configure a DHCP address pool on a DHCP server and enter DHCP pool configuration mode
domain-name *domain*	Specifies the domain name for a DHCP client
network *network-number [mask]*	Configures the network number and mask for a DHCP address pool primary or secondary subnet on a Cisco IOS DHCP server
ip dhcp excluded-address *ip-address [last-ip-address]*	Specifies IP addresses that a DHCP server should not assign to DHCP clients
ip helper-address *address*	Enables forwarding of UDP broadcasts, including BOOTP, received on an interface

default-router *address[address2 ... address8]*	Specifies the default routers for a DHCP client

Security Commands

password *pass-value*	Lists the password that is required if the login command (with no other parameters) is configured
username *name* **password** *pass-value*	Defines one of possibly multiple user names and associated passwords used for user authentication. It is used when the **login local** line configuration command has been used
enable password *pass-value*	Defines the password required when using the **enable** command
enable secret *pass-value*	Sets the password required for any user to enter enable mode
service password-encryption	Directs the Cisco IOS software to encrypt the passwords, CHAP secrets and similar data saved in its configuration file
ip domain-name *name*	Configures a DNS domain name
crypto key generate rsa	Creates and stores (in a hidden location in flash memory) the keys that are required by SSH
transport input *{telnet | ssh}*	Defines whether Telnet or SSH access is allowed into this switch. Both values can be specified in a single command to allow both Telnet and SSH access (default settings)
access-list *access-list-number {deny | permit} source [source-wildcard] [log]*	Defines a standard IP access list
access-class	Restricts incoming and outgoing connections between a particular

	VTY (into a basic Cisco device) and

	the addresses in an access list
ip access-list *{standard | extended} {access-list-name | access-list-number}*	Defines an IP access list by name or number
permit source *[source-wildcard]*	Allows a packet to pass a named IP ACL. To remove a permit condition from an ACL, use the "no" form of this command.
deny source *[source-wildcard]*	Used to set conditions in a named IP ACL that will deny packets. To remove a deny condition from an ACL, use the "no" form of this command.
ntp peer *<ip-address>*	Configures the software clock to synchronize a peer or to be synchronized by a peer
switchport port-security	Enables port security on the interface
switchport port-security maximum maximum	Sets the maximum number of secure MAC addresses on the port
switchport port-security mac-address *{mac-addr | {sticky [mac-addr]}}*	Adds a MAC address to the list of secure MAC addresses. The "sticky" option configures the MAC addresses as sticky on the interface
switchport port-security violation *{shutdown | restrict | protect}*	Sets the action to be taken when a security violation is detected
show port security *[interface interface-id]*	Displays information about security options configured on the interface

Monitoring and Logging Commands

logging *ip address*	Configures the IP address of the host that will receive the system logging (syslog) messages
logging trap level	Used to limit messages that are logged to the syslog servers based on severity. Specify the number or name of the desired severity level at which messages should be logged
show logging	Displays the state of system logging

show logging	Displays the state of system logging (syslog) and the contents of the standard system logging buffer
terminal monitor	Sends a copy of all syslog messages, including debug messages, to the Telnet or SSH user who issues this command