!!! add “no” to the beginning of a command to do the opposite of the command !!!
!!! add “do” to the beginning of a command to force the command !!!
!!! add “?” to the end of a command to list possible syntax !!!
!!! add “brief” to the end of a show command to display shorter information !!!

Essential Commands

enable - put into enable mode
configure terminal - put into configuration mode
---

end - end configuration
write mem - save configuration to memory

do write - saves the configuration
write memory - write configuration to memory
copy running-config starting-config - copy the running configuration to the startup configuration
exit - returns to the previous mode

Basic Router Commands

hostname <*name*> - change name of host/device
enable password <*password*> - set/enable password
enable secret <*password*> - set/enable secret password
security password min-length <#> - set the minimum password length
banner motd #<*message*># - set the message of the day banner
ip default-gateway <*default gateway address*> - set default gateway
line console 0 - Configure physical port connected
login - login to console
---
show interface - displays technical details of interfaces
show ip interface [brief] - displays ip interface status and configuration
show ip route - displays ip routing table
show ipv6 route - displays ipv6 routing table
show ip route connected - displays directly connected networks
show running-config - displays the current configuration

Switching Essentials

duplex full - configure the interface duplex
speed 100 - configure the interface speed
mdix auto - enables feature to adjust to any cable

Interface Commands

interface <*interface*> - put into interface configuration mode
interface range <*interface range*> - put into interface range configuration mode

Ex. f0/1-2

shutdown - shutdown the interface

description <*description*> - add a description

interface vlan <#> - put into interface VLAN configuration mode

IP Address Commands

ip address <*ip address*> <*subnet mask*> - assign ip address

ipv6 unicast-routing - enable ipv6 on a router

ipv6 enable - enable ipv6 on an interface

ipv6 address <*ipv6 address/prefix length*> - assign ipv6 address

VLAN Commands

encapsulation dot1q <#> - use a router interface as a trunk port to a switch

switchport trunk allowed vlan <#>- to specify the list of VLANs allowed on a trunk port

switchport trunk native vlan <#> - specifies the native (untagged) VLAN for the trunk interface

---

vlan <#> - put into VLAN interface configuration mode

name <*name*> - name VLANs

---

in interface configuration:

switchport access vlan <#> - assign the port to a vlan

switchport mode trunk - set interface to trunk mode

---

show vlan - displays VLAN information

show interface trunk - displays trunk interface information

switchport mode dynamic auto - re-enable dynamic trunking protocol

switchport nonegotiate - Will not generate DTP frames

Port Security

switchport mode access - set interface to access mode

switchport port-security - enable port security

switchport port-security maximum <#> - set the maximum number of devices that can access the ports

switchport port-security mac-address sticky - MAC address of a device is dynamically learned

switchport port-security violation restrict - ports are disabled when a violation occurs

---

show port-security interface <*interface*> - displays port-security information

Route Commands

Automatic Route:

- Configured automatically from ip configuration
- Indicated by C (connected) and L (local) in routing table

Static Route:

ip route <*destination address*> <*subnet mask*> <*exit interface* | *next hop address*> [*metric value*] - create a static route

- Indicated by S in routing table

ipv6 route <*destination address/prefix length*> <*exit interface* | *next hop address*> [*link local address*] [*metric valu*e] - create a static route

Static Default Route:

ip route “0.0.0.0” “0.0.0.0” <*interface*> [*metric value*] - create a default route

---

show ip route - displays the routing table

show ipv6 route - displays the ipv6 routing table

RIP Commands

router rip - put into router-rip configuration mode (to configure RIP)

version 2 - use RIPv2

auto-summary - enable the summarization of networks

network <*network address*> [*wildcard mask*] - specify which networks to advertise

passive-interface <*interface*> - disables OSPF and EIGRP route processing

default-information originate - configures OSPF to advertise the default route

Connectivity Commands

Hosts:

ping <*ip address*> - displays the success/failure of packet transmission

tracert <*ip address*> - displays the path of a packet

telnet <*address*> - enables remote control of computers

ipconfig - displays system information

ipv6 config - displays system information

Routers:

traceroute <*ip address*> - displays the path of a packet

SSH Commands

service password-encryption - substitutes text passwords to non-text displayed in the configuration

ip domain-name <*name*> - configures the domain name

crypto key generate rsa - generate RSA keys

username <*username*> secret <*secret*> - create a user with a secret password

line vty <*”0”*> <*# of lines*> - open additional lines

login local - authenticate all incoming virtual terminal sessions via the local username database

transport input <*all* | *none* | *telnet* | *ssh*> - set which protocols are allowed to access the vty lines
no password <*password*> - remove existing vty line password
exec-timeout <minutes> <seconds> - to disable unattended connections

ip ssh version 2
ip ssh time-out <#>
ip ssh authentication-retries <#>

ssh - attempt to log in using SSH
ip ssh authentication-retries <integer> - configure a different number of consecutive SSH retries

login block-for <seconds> attempts <tries> within <seconds> - Disables logins after a specified number of failed login attempts
login quiet-mode access-class <acl-name | acl-number> - maps to an ACL that identifies the permitted hosts
login delay <seconds> - specifies a number of seconds the user must wait between unsuccessful login attempts
login on-success log - logs successful login attempts
login on-failure log - logs unsuccessful login attempts

privilege exec level <level> [command] - configure a privilege level with specific commands

EIGRP Commands

router eigrp <#> - enable EIGRP routing process
network <*network address*> [*wildcard mask*] - specify which networks to advertise
passive-interface <*interface*> - disables OSPF and EIGRP route processing
auto-summary - enable the summarization of networks

---

show ip eigrp neighbors - determine when neighbors become active and inactive
show ip protocols - verify that the routing protocol configuration is being processed correctly

Access List Commands

access-list <#>... - create a standard/extended access list
ip access-list standard <*name*> … - create a named access list
<*permit* | *deny*> … - specify access

in interface configuration:
ip access-group <# | *name*> <*out* | *in*> - add an access-list to an interface

in vty lines:
access-class <#> <*in* | *out*> - apply ACL to the VTY lines

---

show access-list - display currently configured ACLs

DHCP Commands

ip dhcp excluded-address <*first address*> <*last address*> - exclude addresses from the DHCP address pool

ip dhcp pool <*name*> - put into DHCP pool configuration mode

network <*network address*> [*subnet mask*] - specify which networks to advertise

default-router <*address*> - set the default gateway

dns-server <*address*> - set the DNS server

in interface configuration:

ip helper-address <*address*> - set router as a DHCP relay agent

ip address dhcp - enable the DHCP client on an interface

---

show ip dhcp binding - display DHCP bindings

NAT Commands

ip nat <*inside* | *outside*> <*"source"*> <*"static"*> … - create a static NAT translation

in interface configuration:

ip nat <*inside* | *outside*> - configure interface to be inside/outside interfaces for NAT

ip nat pool [dynamic] [name]<*first address*> <*last address*> <*"netmask"*> <*netmask*> - create a NAT pool

ip nat <*inside* | *outside*> <*"source"*> <*"list"*> <# | *name*> <*"pool"*> <*"dynamic"*>

---

show ip nat translation - display active Network Address Translations

show ip nat statistics - display NAT statistics

CDP Commands

in interface configuration:

cdp ena - enable Cisco Discovery Protocol (CDP) on an interface

cdp run - enable the CDP

---

show cdp - display global CDP information

show cdp neighbors [detail] - displays detailed information about neighboring devices discovered using CDP

NTP Commands

ntp server <*address*> - specify an NTP server

ntp update-calendar

ntp authenticate - enables authentication with an NTP server

ntp trusted-key - specifies an authentication key ID to be a trusted key

ntp authentication-key 1 md5 <key> - sets a key to authenticate with an NTP server

show clock

service timestamps log datetime msec - timestamp log messages
logging host <address> - specify syslog server
show logging

Syslog & NTP Commands

logging <*address*> - send log events to the Syslog server
interface loopback 0 - configure a loopback interface
clock set <*hr:min:sec*> <*month*> <*day*> <*year*> - manually set the clock
service timestamps log datetime msec - send timestamps with logs to Syslog server
ip ips notify log -

Backup Commands

copy tftp running-configuration - transfer configuration from the TFTP server
Address or name of remote host [ ]? _____
Source filename [ ]? _____
Destination filename [running-config]? _____
copy flash tftp: - copy the IOS in flash to the TFTP Server
Source filename [ ]? _____
Address or name of remote host [ ]? _____
boot system flash <*filename*> - load the image on the next reload

STP Commands

spanning-tree mode <*mode*> - changes the STP mode
spanning-tree vlan <*VLANs*> root primary - configure switch to be the primary root for VLANs
spanning-tree portfast - causes a port to enter the spanning tree forwarding state immediately
---
show spanning-tree - display spanning tree configurations

VTP Commands

vtp mode server - set switch as a VTP server
vtp domain ccna - set CCNA as the VTP domain name
vtp password <*password*> - set VTP password
vtp mode <*client* | *transparent*> - set device mode
---
show vtp status - display VTP information
show vtp password - display the VTP password

Role-Based Views

aaa new-model - enable AAA
aaa authentication login default local - to specify that the local database be used for authentication

enable [view [view-name]] - log in as the root view to configure and edit views
parser view [view-name] - Create a view
aaa authorization exec default local - to configure command authorization
ip scp server enable - enable SCP server-side functionality

line console 0 - configure console login
login authentication default - configure AAA authentication for the console login to use the default method list
line vty 0 4
transport input ssh
login authentication <name>

Secure Cisco IOS Image and Configuration Files

secure boot-image - to secure the IOS image and enable Cisco IOS image resilience
secure boot-config - to take a snapshot of the router running configuration and securely archive it in persistent storage
no service password-recovery - mitigate potential security breach

ASA Basic Configuration

Key config-key password-encryption - change the master passphrase
nameif - names the interface
security-level - sets the security level
telnet timeout - alters the default exec timeout
aaa authentication telnet console LOCAL - configures Telnet to refer to the local database
clear configure telnet - removes the telnet connection from the configuration

DHCP Server

dhcpd address - Creates a DHCP address pool
dhcpd dns - specifies the IP addresses of the DNS server
dhcpd lease - changes the lease length granted to the client
dhcpd domain - specifies the domain name assigned to the client
dhcpd enable - enables the DHCP server service on the interface

OSPF Configuration

router ospf 1 - Enables OSPF routing and enters router configuration mode
area 0 authentication message-digest - Configure OSPF MD 5 authentication for all the routers in area 0
Ip ospf message-digest-key 1 md5 <key> - In interface configuration mode, configure the MD5 key