CCNA 200-301 v1.1	**Network Device Management**
Basic Cisco Commands	
enable	Enter Privileged EXEC mode
configure terminal	Enter Global Configuration mode
hostname [name]	Set the device's hostname
enable password	Require a password to enter privileged mode Store the password in the configuration file using a reversible encryption method (type 7 encryption)
enable secret	Store the enable password in the configuration file using the more secure MD5 hash (type 5 encryption) Overrides any existing enable password If both an enable password and enable secret are configured on the device, the user must enter the secret
service password-encryption	Encrypt all passwords in the device's configuration file using a type 7 encryption method
clock	Set the device clock
banner motd	Set a message of the day that displays as the user logs in
banner login	Set a banner the user sees as before they log in Warn people against unauthorized use
exit	Exit from the current mode to the previous mode
end	Exit from current mode directly to privileged EXEC
copy running-config startup-config write memory	Save the running configuration to NVRAM
reload	Reboot the device
logout	Terminate your session and log out of the device
Basic Show Commands	
show version	Display the system hardware and software version
show running-config	Display the current configuration in RAM
show startup-config	Display the configuration stored in NVRAM
show ip interface	Display interface IP information
show ip interface brief	Display a brief summary of IP addresses and interface statuses
show interface	Display all statistics of an interface
show mac address-table	Display the contents of a switch's mac table
show ip route	Display a router's route table
show ip arp	Display a device's arp cache
?	Display online help

Interface Configuration Commands	
interface [type] [number]	Enter interface configuration mode
ip address [ip address] [subnet mask]	Assign an IP address to a Layer 3 interface
description [text]	Add a description to an interface
no shutdown	Enable the interface (bring it up)
shutdown	Disable the interface (bring it down)
Local User Creation Commands	
username <name> privilege 1 secret <password>	Create a local user account Log in as unprivileged user
username <name> privilege 15 secret <password>	Create a local user account Log in as a privileged user
Telnet Commands	
line vty 0 4 line vty 0 15	Enter vty configuration mode for the desired number of vty telnet sessions (5, or 16)
login local	Username and password is checked against the local database
transport input telnet	Allow telnet connections
telnet <target device IP>	Start a telnet session from another Cisco device
CTRL+6+SHIFT, x	Toggle away from the telnet session back to your local CLI
ENTER	Resume your telnet session
exit	End a telnet session
show session	Shows your active outbound telnet sessions to other devices
show users	Shows active inbound telnet sessions to this device Shows username, telnet and SSH incoming connections
SSH Commands	
hostname	Configure a hostname for the device
ip domain-name <domain name>	Provide the device domain name
crypto key generate rsa	When prompted, choose between 360 – 4096 bit key length
ip ssh version 2	Set the SSH version
username <user> privilege 15 secret <password>	Create a local user with a secret password who will have admin privilege in the session
line vty 0 15	Enter vty configuration mode for 16 vty lines
transport input ssh	Enable SSH only
transport input ssh telnet	Enable SSH and if that fails, permit telnet
login local	Require local authentication for the user
ip ssh time-out 60	The user must successfully authenticate in 60 seconds
ip ssh authentication-retries 3	The user can retry authentication 3 times before the session is terminated and they must start over

SSH Connection Commands	
ssh -l <username> <destination IP>	Start an SSH connection from one Cisco device to another
CTRL+SHIFT+6, x	Toggle back to your local CLI
ENTER	Resume your SSH session
exit logout	End your SSH session
show ssh	View active SSH sessions in our out of this device
show users	Shows active inbound SSH sessions to this device Shows username, SSH and telnet incoming connections
CDP Commands	
cdp run	Enable CDP globally
no cdp run	Disable CDP globally
cdp enable	Enable CDP on a specific interface
no cdp enable	Disable CDP on a specific interface
cdp receive	Only receive CDP packets on an interface, don't transmit any out
Show CDP Commands	
show cdp	Displays general CDP information on the device
show cdp interface	Displays the status of CDP on each device interface
show cdp neighbors	Quick overview of connected devices, including their capabilities, platform, and the interfaces
show cdp neighbors detail	Provides detailed information of connected devices including IP address and software version
show cdp entry	Detailed information about a specific CDP neighbor
show cdp traffic	Provides statistics on CDP traffic
LLDP Commands	
lldp run	Enable LLDP globally
no lldp run	Disable LLDP globally
lldp reinit <seconds>	If LLDP configuration changes, wait x seconds before reinitializing the LLDP process Helps avoid network instability caused by frequent or rapid changes
lldp transmit	Enable sending LLDP on a specific interface
no lldp transmit	Disable sending LLDP on a specific interface
lldp receive	Enable receiving LLDP on a specific interface
no lldp receive	Disable receiving LLDP on a specific interface
Show LLDP Commands	
show lldp	View global LLDP statistics
show lldp neighbors	View LLDP neighbors incl. name, ports, MAC address
show lldp neighbors detail	Provides detailed information about the neighbor including system capabilities and IP address

Basic Troubleshooting Commands	
show version	Provides detailed information about the device's software and hardware including the IOS version, image file, device model, uptime, memory, and configuration register
show interface	View Layer 2 status of an interface
show ip interface	Display detailed interface IP information
show ip interface brief	Display status of all interfaces in table format
ping [destination]	Test Layer 3 connectivity to a remote host (ICMP echo, echo reply)
ping	Advanced ping Specify source, datagram size, repeat count, timeout and more
traceroute [destination]	Trace the path to a remote host Manipulates the TTL of a UDP packet to collect ICMP expired in transit messages from hops along the path
show controller	View Layer 1 status of an interface