Cisco IOS Commands "Cheat Sheet"

1/26/2021

After power-on or reload (reboot):

- New, unconfigured device: no login credentials requested, answer '**n**' to question about configuration, will then be presented with unprivileged console user prompt ">"
- Securely configured device: login credentials asked, will then be presented with unprivileged user prompt ">"

At unprivileged user prompt ">" :

- Limited commands available, type **?** to see them
- Type '**en**' or '**enable**' to go to Exec privileged user mode:
    - New, unconfigured device: no prompt for password asked, goes directly to exec mode privileged user prompt "#"
    - Securely configured device: prompt for Enable password, success passes to exec mode privileged user prompt "#"

At Exec mode privileged user prompt "#" :

- All "**show**" commands are enabled, type **?** to see them, type 1 or more letters of command immediately followed by **?** to filter displayed command list
- Very little configuration is possible in exec mode (older devices may permit VLAN database config here)
- Type '**conf t**' or '**configure terminal**' to go to Global configuration mode ("config" prompt)
- Type '**disable**' to end Exec mode and return to unprivileged user mode
- '**show version**' displays IOS software and hardware info
- '**show ip int br**' (show ip interface brief) is frequently used to show IPaddr, VLAN, and port info
- '**show run**' (show running-config) is frequently used to show many currently active device configuration commands
- '**show vlan**' used to show more VLAN info
- '**show ip route**' is used only on routers to show current routing table entries
- '**show interface <port#>**' (eg, 'show int fa0/0') used to show more detailed info on switch port
- '**vlan database**' used to create Virtual Local Area Network (VLAN) in *older* versions of IOS and *older* versions of Packet Tracer (note: this command is used in Exec mode, *prior* to assigning VLANs in Config mode). If you find that you cannot create VLANs in Config mode, it is likely that the IOS version you're using requires creating them with this command in Exec mode.

At Global Config prompt "(config)" :

- Configuration commands that affects the device "globally" are entered here.
- Type '**?**' to see list of available commands & options at any point, even after a partial command.

- “Show” commands are not directly available in global config mode; however, most “show” commands can be performed by preceding them with ‘**do**’, conveniently eliminating need to drop out of config mode back to exec mode and back.
- Type ‘**end**’ (or keys Ctrl+z) to end config mode and return to Exec mode.
- Typing any command (besides “do” or “?”) in Global config mode typically takes you to a sub-config mode; type ‘**exit**’ (or keys Ctrl+z) when in a sub-config mode to return back to Global config mode.
- ‘**enable secret <password>**’ (eg, ‘enable secret C0nf1dent!al’) sets a password required to enter Exec privileged user mode, where MD5 Hash is calculated and stored in running-config.
- ‘**username <name> secret <password>**’ Adds users and credentials to a table of authorized users, which can be referenced via “local” option in “line” configuration commands. Use of optional ‘secret’ parm causes the password to be hashed using MD5, and the hash value is stored in the table instead of the clear password, improving device security.
- ‘**login local**’ when in console or VTY sub-config mode causes the user to be prompted for username and password that is stored in the user credentials table (see ‘user’ command above).
- ‘**banner motd <delimiter character>**’ (eg, ‘banner motd +’) when in global config mode allows for the creation of a “message of the day” that is displayed upon first connection to the console or virtual teletype terminal user mode, before entering exec mode. The delimiter character can be any ASCII keyboard character, and is used to tell IOS when the banner message text begins and ends (for this reason, a rarely used character is recommended such as the + plus or | vertical bar or % percentage symbol (the delimiter character must not be used within the banner message text, as IOS will truncate the message when it is encountered). Type motd is the most common banner message type used to warn device users against performing unauthorized access, use, or changes to the device, but additional warnings can be set using ‘banner exec’ and/or ‘banner login’.
- **‘hostname <text string for name>’** (eg, ‘hostname SDCswitch1’ changes name of switch to “SDCswitch1”) when in global config mode sets the name of the device to admin user specified text string, for ease in identifying the device in a multiple host device network.
- **‘no ip domain-lookup’** when in global config mode, causes the device to not attempt to contact a DNS server when it does not recognize certain misspelled commands and then wait for a response, which can take minutes during which time the device command line is essentially frozen. This is a convenience option for the administrator user configuring the device. This command is only valid on Cisco routers and Layer 3 switches.
- **‘logging synchronous’** when in *line con 0* sub-config mode, causes the device to not interrupt command entry when the device displays log update information. Default behavior of IOS is to immediately display certain status information to the user (that is being written to the log), which often occurs while the admin user is typing CLI commands and thereby interrupts command input for a moment; this can be irritating, so disabling this behavior is a common practice.

- '**line vty 0-15**' enters sub-config for virtual teletype (TTY) consoles used for remote management access into device. Recommended to use available commands there to secure remote access, eg 'login' to require usernames & passwords, require SSH, etc.
- '**line con 0**' ('**line console 0**') enters sub-config for device console that is displayed either via Console port, Aux port, or VTY ports. Recommended to use available commands there to secure access, eg 'login' to require usernames & passwords.
- '**interface <port number>**' (eg, 'int fa0/1') is frequently used to enter interface sub-configuration mode for a hardware port or VLAN to set IPaddr, mask, VLAN assignment, mode, port speed and more.
- '**switchport mode access**' in interface sub-config mode on a Cisco switch sets the hardware interface port for *access* mode only, recommended for security hardening since default is *dynamic* mode that allows a malicious user to automatically connect in *trunk* mode to facilitate a man-in-the-middle (MITM) exploit.
- '**switchport mode trunk**' in interface sub-config mode on a Cisco switch sets the interface port for *trunk* mode, so that it can be used to support multiple VLANs when connecting to another switch or router port that is also configured as a trunk port.
- **'no shutdown'** when in interface sub-config mode causes the port, or range of ports, to become operational; this is reflected in the pertinent *show ip interface brief* command displaying the protocol for the port(s) as "up".
- '**ip route <outside network IPaddr> <outside subnet mask> <next hop gateway, or outside interface>**' (eg, 'ip route 172.16.0.0 255.255.0.0 192.168.0.1') places a *static* route into the Routing Table of a *router* (or *Layer 3 switch)*, so that the router knows where to fwd TCP/IP packets for outside (non-directly connected) networks
- '**ip route 0.0.0.0 0.0.0.0 <next hop gateway, or interface>**' (eg, 'ip route 0.0.0.0 0.0.0.0 fa0/0') places a "gateway of last resort" route into the Routing Table of a router, essentially setting a default gateway route for all unknown destination networks. Also, see "default gateway" configuration command which is similar.
- '**ip domain-name <name>**' (eg, 'ip domain-name kangas.com') in global config mode assigns a domain name to a router (or certain managed switches), which is required for generating crypto keys for device remote access by SSH and other purposes.
- '**encapsulation dot1q**' sets a switch or router interface to use the open standard 802.1Q trunking protocol when setting up a switch or router to do virtual local area networks VLANs. Both devices connected via trunk mode ports should be set to use this protocol as it offers benefits over the older proprietary Cisco trunking protocol that most Cisco devices default to.
- '**crypto key generate rsa modulus <length>**' (eg, 'crypto key generate rsa modulus 1024') causes IOS to create encryption keys, commonly used for remote device access via SSH and other purposes. The IOS being used must have a license enabling this functionality. Crypto key is required before configuring VTY shells for access via SSH (not required for telnet).

Basic Cisco Router Configuration

First, after entering privileged (exec) user mode, set '*hostname'*, '*enable secret <password>*', '*no ip domain-lookup*', '*motd*', '*logging synchronous*' as you would for a Cisco switch (see previous pages for these commands). Router security is even more important than for a switch.

1. **'line con 0'** in global config mode enters sub-mode for configuring the administrator console (what you are in right now).
2. **'password <password>'** (eg, 'password CiscoAdmin') while in console line sub-config mode sets a user specified password required for logging into the admin console.
3. **'login'** while in console sub-config mode turns on user challenge for credentials.
4. **'motd-banner'** while in console line sub-config mode enables the display of the MOTD banner (previously configured during global terminal config mode) upon user connection to the line console before login.
5. **'logging synchronous"** while in console line sub-config mode prevents the router from interrupting the user's entry of commands whenever the router enters information into its device log.
6. **'exit'** returns to global config mode (from console line sub-config mode)
7. **'line vty 0 4'** in global config mode enters sub-mode for configuring Virtual TeletYpe admin consoles. VTY consoles are used for administering the router from a remote network location, as opposed to the physical console port on the router. In this case, all available default console line numbers 0 through 4 will be configured simultaneously, which is highly recommended in the initial configuration. If only one console line number is to be configured or changed, specify just that one console line in the command (eg, 'line vty 2').
8. **'password <password>'** (eg, 'password CiscoAdmin') while in console line sub-config mode sets a user specified password required for logging into the consoles.
9. **'login'** while in console line sub-config mode turns on user challenge for credentials.
10. **'transport input ssh'** while in console line sub-config mode sets input connection protocol required to SSH for more secure encrypted communications. Remember, that VTY consoles are accessed from a remote network location, therefore are more vulnerable to attack, so using SSH protocol to connect to them is a best practice.
11. **'motd-banner'** while in console line sub-config mode enables the display of the MOTD banner upon user connection to a line console before login.
12. **'exit'** returns to global config mode (from console line sub-config mode)
13. *LOCAL LAN CONNECTION:* **'interface <port number>'** (eg, 'int gig0/0') while in global config mode, enters sub-config mode for the specified interface port.
14. **'ip addr <IP address> <subnet mask>'** (eg, 'ip addr 192.168.100.1 255.255.255.0') while in interface sub-config mode, assigns a subnetwork gateway IP address to the port. This defines the subnetwork for hosts connected to that port.
15. **'description <text string label>'** (eg, 'description FinanceDept') while in interface sub-config mode causes a descriptive label to be assigned to that particular port, which aids admins

working with a network topology, similar to how a custom hostname helps. Note: this is optional, not required for router operation.

16. **'no shut'** while in interface sub-config mode, turns on the port (by default, the port is shutdown on a new router).
17. **'exit'** returns user to global config mode.
18. *Repeat steps 7-11 for other interfaces in use, including for WAN CONNECTION (if any), or UPSTREAM ROUTER, or OTHER LAN, ETC. Set all other UNused ports to 'shutdown' as a best security practice to help prevent an attacker from using them.*
19. **'ip route <destination subnetwork address> <subnet mask> <next neighbor router hop IP address OR interface port number>'** (eg, 'ip route 192.168.50.0 255.255.255.0 172.16.0.1', OR 'ip route 192.168.50.0 255.255.255.0 gig0/0') while in global config mode enters a *static* route into the routing table, to a tell the router where to forward packets that fall into the specified sub-network address range and that are in a subnetwork not directly connected to this router. Typically, the specified subnetwork is in another area within the organization connected to a different router. "Static" routes are used when *dynamic* router protocol is not in use (default), and typically have the benefits of faster performance and improved security, but are often administrator labor intensive.
20. **'ip route 0.0.0.0 0.0.0.0 <next neighbor router hop IP address OR interface port number>'** (eg, 'ip route 0.0.0.0 0.0.0.0 172.16.0.1' OR 'ip route 0.0.0.0 0.0.0.0 gig0/1') while in global config mode, enters a DEFAULT static route into the routing table. When the router receives a packet it first looks into its routing table for a match, if it does not find a match it then looks to see if there is a default route (specified by IP address 0.0.0.0 and subnet mask 0.0.0.0), but if it does not find a default match it throws the packet away. Use of default routes in a network depends upon network topology and other concerns.
21. **'copy running-config startup-config'** writes the current running configuration, in RAM, to the startup configuration, in non-volatile memory, so that it persists through a reboot or power cycle.

Basic Cisco Switch Configuration, including Security

First, after entering privileged (exec) user mode, set '*hostname'*, '*enable secret <password>*', '*motd'*, '*logging synchronous*' (and '*no ip domain-lookup*' if it is a Layer3 switch), as you would for a Cisco router (see previous pages for these commands). Switch security is important to defeat a number of targeted attacks.

1. **'line con 0'** in global config mode enters sub-mode for configuring the administrator console (what you are in right now).
2. **'exec-timeout <number of minutes>'** (eg, 'exec-timeout 5') while in console sub-config mode sets a time value after which the user is logged out when there is no activity for the specified number of minutes. This is a best practice security step to prevent the privileged/exec console session from never timing out and leaving it open for an unauthorized user who may follow along after the authorized administrator user.
3. **'logging synchronous'** while in console sub-config mode prevents the switch from interrupting user entry of commands during those instances when the switch is entering information into its device log.
4. **'login'** while in console sub-config mode turns on user challenge for credentials.
5. **'motd-banner'** while in console line sub-config mode enables the display of the MOTD banner upon user connection to a line console before login.
6. **'exit'** returns to global config mode (from console line sub-config mode)
7. **'line vty 0 4'** in global config mode enters sub-mode for configuring Virtual TeletYpe admin consoles. VTY consoles are used for administering the router from a remote network location, as opposed to the physical console port on the router. In this case, all available default console line numbers 0 through 4 will be configured simultaneously, which is highly recommended in the initial configuration. If only one console line number is to be configured or changed, specify just that one console line in the command (eg, 'line vty 2').
8. **'secret <password>'** (eg, 'password CiscoAdmin') while in console line sub-config mode sets a user specified password required for logging into the consoles.
9. **'login'** while in console line sub-config mode turns on user challenge for credentials.
10. **'transport input ssh'** while in console line sub-config mode sets input connection protocol required to SSH for more secure encrypted communications. Remember, that VTY consoles are accessed from a remote network location, therefore are more vulnerable to attack, so using SSH protocol to connect to them is a best practice.
11. **'motd-banner'** while in console line sub-config mode enables the display of the MOTD banner upon user connection to a line console before login.
12. **'exit'** returns to global config mode (from console line sub-config mode)
13. **'interface range <starting interface port ID> , <ending interface port ID>'** (eg, 'int fa0/0 , fa0/23' to select all switchports beginning at fa0/0 through fa0/23) while in global config mode selects sub-config mode for all specified switchports simultaneously.
14. **'switchport mode access'** while in interface sub-config mode sets the specified port(s) to Access Mode only (disables using them for Trunks and other modes).

15. **'switchport port-security maximum <max number of mac addresses>'** (eg, 'switchport port-security max 1' allows only a single MAC address) while in interface sub-config mode sets a maximum number of MAC address that will be accepted for the specified port(s) being configured.
16. **'switchport port-security mac-address sticky'** while in interface sub-config mode sets the selected port(s) to remembering/persisting (by writing into the *running-configuration* memory) the MAC address(es) that are connected to it, thereafter refusing any other MAC addresses beyond the maximum number allowed.
17. **'switchport port-security violation restrict'** while in interface sub-config mode sets what happens when a port-security violation occurs, in this case "restrict" causes the port to discard traffic, increment the violation counter, make a log entry of the violation, and send an SNMP trap message if configured, for the specified port(s) being configured.
18. **'switchport port-security aging type inactivity'** while in interface sub-config mode sets inactivity of the selected port(s) as the trigger for starting the aging clock.
19. **'switchport port-security aging time <integer number of minutes>'** (eg, 'switchport port-security aging time 5') while in interface sub-config mode, sets the amount of time minutes, for the specified port(s) being configured.
20. **'snmp enable traps port-security trap-rate 5'** while in ? config model sets a Simple Networking Management Protocol (SNMP) trap for alerting a SNMP server when the switch port security function has been violated.
21. **'switchport port-security'** while in interface sub-config mode turns on port security feature for the port(s) being configured (recommended *after* configuring port security per above).
22. **'exit'** to return to Global Config mode ("config" prompt).
23. **'ip dhcp snooping'** while in global config mode enables DHCP Snooping function. This sets all ports to "untrusted" for DHCP server offers/acknowledgements, which disables their use by a DHCP server.
24. **'ip dhcp snooping database flash:/<filename>**' (eg, 'ip dhcp snooping database flash:/snoop.db' creates the file "snoop.db") while in dhcp snooping sub-config mode, creates a port information table file that persists in local flash storage (not in RAM in this case). The specified table file stores each switch port number along with its client IP address, its VLAN number if assigned, its MAC address, and the current time, whenever a client/host makes a DHCP request on a port.
25. **'interface <switch port number>'** (eg, 'interface fa0/0' enters sub-config for fast ethernet port 0/0) while in global config mode enters the configuration of the specified switch port number to be used as a *trusted* port for connecting to a trusted DHCP server. Frequently, the DHCP server is built into a router device that is being connected, but may alternatively be in a server computer being directly connected to the trusted switch port.
26. **'description <user specified text label>'** (eg, 'description Trunk to DHCP server') while in switch port interface sub-config mode, assigns a text label to that port for easier human administration identification. Use a label specific to the device being connected, in the example it is a server computer running the DHCP server, but if it is instead a router than it's best to label the port with the router name.

27. **'ip dhcp snooping trust'** while in switch port interface sub-config mode, allows the port to be *trusted* for DHCP traffic, particularly DHCPOFFER and DHCPACK traffic.
28. **'ip dhcp snooping limit rate <number of packets per second>'** (eg, 'ip dhcp snooping limit rate 10' sets limit of 10 packets per second) while in interface sub-config mode. The rate limit should be configured for maximum expected number of DHCP packets per second for the device being connected to the trusted DHCP port; this will depend upon what type of device is being connected to the trusted port, the number of client host devices connected to all the untrusted switch ports, the number of DHCP servers within a large subnet, whether interconnected routed subnets are using a common DHCP server, time of the workday (traffic surges at the beginning of the work day), and perhaps other factors. The Rate Limit value may need to be adjusted in practice; a good starting point is to specify a Rate Limit of "10" for a directly connected router, a Rate Limit of "20" for a directly connected DHCP server computer.
29. **'exit'** to return to Global Config mode ("config" prompt).
30. **'ip dhcp relay information trust'** while in global config mode ("config" prompt) allows a Cisco router to be used as a DHCP server when 'ip snooping' is enabled in the router. It enhances a trust relationship between the switch and router to resist rogue DHCP attacks.
31. **'exit'** to return to privileged exec admin mode.
32. **'show ip dhcp snooping'** displays DHCP Snooping configuration info; used to check accurate/complete configuration.
33. **'show ip dhcp snooping binding'** displays the snooping database file information for connected host port bindings.
34. **'copy running-config startup-config'** writes the current running configuration, in RAM, to the startup configuration, in non-volatile memory, so that it persists through a reboot or power cycle.

Creating VLANS (Virtual Local Area Networks) on a Cisco Switch

While in global config mode (config prompt) on a Cisco switch device:

1. **'interface vlan <ID number>'** (eg, 'interface vlan 2') when in global config mode causes creation of a VLAN ID (it is recommended to NOT use VLAN 1 for security reasons, as VLAN 1 is the default native VLAN management interface for all VLANs including sub-VLANs)
2. **'name <text string label>'** OR **'description <text string label'** (eg, 'description Finance VLAN') when in VLAN interface sub-config mode (config-if prompt), causes a custom admin user defined label to be assigned to the VLAN for easier identification of the purpose later. Command for this ('name' vs 'description') depends upon IOS version and switch model)
3. **'exit'** causes system to drop back to global config mode (config prompt).
4. **'interface range <starting port ID#> , <ending port ID3>'** (eg, 'interface range fa0/2 , fa0/12'), causes a range of switch ports to be grouped into a following sub-config mode (easy way to perform VLAN assignment to multiple switch ports).
5. **'switchport mode access'** when in interface sub-config mode (config-if prompt) causes the ports to be set to access type mode only (changes them from dynamic mode), recommended for security hardening since default is *dynamic* mode that allows a malicious user to automatically connect in *trunk* mode to facilitate a man-in-the-middle (MITM) exploit.
6. **'switchport access vlan <ID number>'** (eg, 'switchport access vlan 2') causes the current port or range of ports to be assigned to the designated VLAN number.
7. **'no shutdown'** causes the port, or range of ports, to become active/operational (this is shown later in the *show ip interface brief* command as the protocol status "up").
8. **'exit'** causes return to global config mode ('no shutdown' is default for a Cisco switch, so that range of ports should now be up and operating in access mode and assigned to their assigned VLAN)
9. **'do show vlan'** while in global config mode shows the status of VLANs and port assignments
10. Repeat all preceding steps for additional VLANs (each VLAN with a unique VLAN ID number) and their switch port assignments (do not assign same port ID number on the same switch to more than one VLAN ID).

OSI Layer 2 frame communications takes place only between those ports assigned to the same VLAN within the switch device, and cannot communicate with ports on a different VLAN within the switch device.

Connecting switches with VLAN Trunking

Multiple switches can be connected via a "trunk" and configured to allow ports on other switches to be assigned to the same VLAN(s), in which case the ports assigned to the same VLAN on the first switch can communicate with the ports assigned to the same VLAN on the second switch, third, and so on.

While in global config mode (config prompt) on a Cisco switch device:

1. **'interface <port ID number>'** (eg, 'interface fa0/1') causes system to go to sub-config mode for the specified port interface.
2. **'switchport mode trunk'** when in interface sub-config mode (config-if prompt) causes the port to be set to trunk type mode only.
3. **'description <text string label>'** (eg, 'description VLAN Trunk') when in interface sub-config mode (config-if prompt) applies a custom admin user descriptive label to the port for easier identification later among the device's multiple ports.
4. '**switchport trunk encapsulation dot1q'** when in interface sub-config mode (config-if prompt) causes the trunk port to use the 802.1q trunking protocol. Note: older IOS and switch models do not support 802.1Q trunking protocol, thus this command option may not be available; in that case, you are limited to the proprietary Cisco InterSwitch Linking (ISL) protocol that is the default trunking protocol.
5. **'exit'** to drop back into global config mode (config prompt)
6. **' do show vlan'** do confirm status of vlan configuration.

Configuring Cisco Router for Connecting Layer 2 Switch Trunks for IP networking

Switches often cannot support OSI Layer 3 IP address networking and routing for their Layer 2 host connections and VLANs, therefore a router device is required for VLANs. The router must be configured with a compatible trunk port(s) for connection to the switch(es), VLANs setup as different subnetworks in the router, and the method of VLAN tagging configured. Here are instructions for configuring a Cisco *Router* to support Cisco switch VLANs.

While in global configuration mode (config prompt) in a Cisco **ROUTER**:

1. **'interface <port ID number>'** (eg, 'interface g0/1') go into sub-config mode for the physical interface port to be used for the trunk.
2. **'no ip address'** removes any prior IP address that may be assigned to this port.
3. **'no shutdown'** turns the port on.
4. **'interface <port ID number>.<sub-interface number>'** (note decimal between port ID number and sub-interface number) (eg, 'int fa0/0.1) causes the single physical port to have a logical sub-interface ID assigned.
5. **'encapsulation dot1q <vlan ID number>'** (eg, 'encapsulation dot1q 10' assigns that sub-interface to a specific VLAN ID while also setting the proper encapsulation 802.1q protocol.
6. **'ip address <ip address> <subnet mask>'** (eg. 'ip ad 192.168.1.1 255.255.255.0') assigns a gateway address for the specified VLAN ID number.
7. **'exit'** drops back to global config mode level
8. *Repeat for all other VLAN IDs configured in the attached switch(s)*
9. **'interface vlan <vlan ID number>'** (eg, 'interface vlan 10') causes system to go to sub-config mode for the specified vlan interface.
10. **'no shutdown'**
11. **'exit'** drops back to global config mode level.
12. *Repeat for all other VLAN IDs configured in the attached switch(s)*

13. **'do show run'** to confirm that VLAN IDs have IP addresses assigned and are not shutdown.
14. **'do show vlan-switch'** to confirm VLAN configuration with switch(s).
15. **'do show interfaces trunk'** to confirm trunk status (note: this command may not be available on all versions of IOS).
16. **'switchport trunk vlan allowed add <vlan ID number>'** (eg, 'switchport trunk vlan allowed add 10') restricts only the specified VLAN ID number using the trunk, a security measure. There are other options available, eg 'all' 'remove' 'none' 'except', refer to IOS ? and online info.
17. *Repeat for each VLAN ID number allowed on the trunk port.*

Configuring Cisco Router for DHCP Service

Some computer networks do not have a Dynamic Host Control Protocol (DHCP) server already in the network. Sometimes such networks have all devices manually configured with *static IP addresses*, which are assigned by a network administrator, and are not often changed. This is often an administrative burden particularly as devices come and go in the network, require the administrator to develop, maintain, and keep handy a table of assignments. Also, as a sub-network grows the number of available host IP addresses can be depleted even if some reserved addresses are not currently in use by a connected host, forcing more administrative configuration changes. The solution to such problems is DHCP, which responds to requests from hosts for IP addresses and assigns them from a pool of available host addresses, restoring unused IP addresses back to the pool as hosts disconnect. If there is no DHCP server available to provide this *dynamic IP address* service for the network, a Cisco router can be configured to provide DHCP service. (NOTE: Configure all host devices connected to a DHCP server's network for DHCP, not static, IP addressing.)

***First*,** make sure that the interface ports for connected networks have been assigned IP addresses and are not shutdown (see previous pages for those commands).

While in global configuration mode (config prompt) in a Cisco **ROUTER**:

1. **'ip dhcp pool <name>'** (eg, 'ip dhcp pool marketing-dept') go into sub-config mode for configuring a custom named pool of DHCP pool of addresses.
2. **'network <IPv4 subnetwork address> <subnet mask>'** (eg. 'network 192.168.0.0 255.255.255.0') specify the sub-network address and mask for this pool.
3. **'dns-server <IP address>'** (eg, 'dns-server 8.8.8.8') set the IP address of the DNS server to be used by hosts on this sub-network.
4. **'default-router <IP address>'** (eg, 'default-router 192.168.0.1') specify what IP address that connected hosts should use for their default gateway.
5. **'exit'** drop back to global configuration mode.
6. **'ip dhcp excluded-address <IP address range>'** (eg, 'excluded-address 192.168.0.0 192.168.0.1') this sets one of more IP addresses that are not to be issued by the DHCP service to hosts; typically, this would be a interface address for the router's gateway port interface for a connected sub-network, or a VLAN interface address, or a range of IP addresses that are static.

On some Cisco routers, this command must be repeated for all individual addresses to be excluded from the pool.

7. **‘do show run’** check your work in the running configuration
8. **‘exit’** to privileged exec mode
9. **‘ ip dhcp binding’** to view that the dhcp service is working properly and to see the IP addresses provided to connected hosts.