Checking a router

1. Check version of cisco on machine

* show version

2. Check all commands placed onto router

* show run
  + - make sure that service password encryption is set
    - make sure hostname is set
    - make sure that enable secret is set
    - make sure domain name is set
    - make sure username is set
    - make sure passwords are encrypted (ex. password 7 1P312A910I)
    - make sure “no ip http server” is set
    - make sure that a default route is set (ex. ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/1)
    - make sure created access lists are on
    - make sure telnet is disabled and ssh is enabled (“login local” and “transport input ssh should be set” on line vty 0 4)

3. Check ip addresses (machines that you are directly connected to)

* show ip int OR show ip int brief
  + - make sure ip addresses correlate to what your ip allocations/network

4. Check all possible routes for network traffic

* show ip route
  + - make sure that a default route is set
    - make sure that any routing protocols (ex. ospf) are within the designated network (ex: no network 0.0.0.0 255.255.255.255 area 0)
    - make sure routes are not going to an unknown address

5. Check neighbor machines (machines that you are directly connected to)

* show cdp neighbor
  + - make sure no unknown neighbors are there

6. Check all access lists on router

* show ip access-lists
  + make sure no unwanted traffic is going in or out of network

7. Check hosts

* sh hosts
  + make sure that the hosts designated have the correct ips and hostnames
* delete any hosts that should not be designated a hostname

8. Check Logging configuration and log messages

* show logging (shows logging configuration
* show logging message (shows list of log messages)

9. Ping loopback

* should get replies

10. Ping devices within network

* should get replies

11. Ping devices outside of network

* \*replies depend

Configuring a router

* Passwords
* service password-encryption (sets encryption to password)
* enable secret <cisco> (set password to cisco)
* Configure a hostname
  + hostname <name>
* Configure domain name and ip for domain name server (DNS)
  + ip domain name <name> (sets domain name)
  + ip name-server <server ip> (sets ip for domain name)
* Configure to no ip domain look ups
* no ip domain-lookup
* Configure an Interface and its ip address
* int <g0/0> (configure int g0/0)
* ip address <#.#.#.#.> (set ip address for interface)
* no shutdown (Turns interface on)
* Configure a Vlan Interface and its ip address
  + int <g0/0.1> (configure int g0/0.1)
  + ip address <#.#.#.#.> (set ip address for interface)
  + no shutdown (Turns interface on)
* Configure OSPF
* router <ospf 1>(starts ospf process 1)
* network <172.16.10.0> <0.0.0.255> <area 0> ( Any interface with an address of 172.16.10.0~255 is to be put in area 0 )
* Configure ip route
* int <g0/0>
* ip route <0.0.0.0> <0.0.0.0> (route traffic from a certain src ip to a specific destination)
* Set SSH and turn off telnet
* username <Roland> password <tower> (creates username/password for SSH connection)
* ip domain-name <name> (creates a host domain name for the router)
* crypto key generate rsa (enable ssh server for local and remote authentication on router and generates RSA key pair)
* ip ssh version 2 (enables ssh version 2 on device)
* line vty 0 4 (move to vty config mode)
* login local ( enable password checking)
* transport input ssh (limits remote connectivity to ssh)
* Apply Standard Access Lists
* access-list <10> <permit> <172.16.0.0> <0.0.255.255>(All packets with source ip of 172.16.x.x. will be permitted to come through)
* int <g0/0> (move to interface)
* ip access-group <10> <in> (takes access list 10’s lines and applies to packets going into interface)
* Apply Extended Access Lists
* access-list <110> <permit> <tcp> <172.16.0.0> <0.0.0.255> <192.168.100.0> <0.0.0.255> <eq 80> ( HTTP packets (port 80) with a source ip address of 172.16.0.x will be permitted to travel to the destination address 192.168.100.x).
* Enable Logging
  + logging enable
* Turn off ip http server
  + no ip http server