Troubleshooting, Editing, Port #'s

show ip interface brief (display interface designations, IP address and status)
show ip route (display routing table)
show vlan brief (on switch - show what VLANs exist, names, ports assigned)
show controllers serial x/x/x (see if DCE or DTE connected and if clockrate is present)
show interface trunk (what ports are trunking, native vlan, allowed vlans)
show running-config (display the running configuration - active)
show startup-config (display the starup configuration)
show ip protocol (what routing protocol, which networks, passive interfaces, neighbors)
show cdp interface (display information aboutr the CDP protocol)
show cdp neighbors (see directly connected Cisco devices)
show cdp neighbors detail (includes IP address at other end)
show cdp interface (which interfaces are running CDP)
show interface serial x/x/x (what encapsulation, IP address, counters)
show interface fastethernet x/x switchport (configured mode and operating mode)
show version (which IOS, capability, memory, configuration-register)
show boot (see what the current boot device is)
show run | begin interface (will start listing at the first instance of 'interface')
show ip route connected (show routing table entries for directly connected networks)
show ip route static (show routing table entries for static routes)
show ip route ospf (show routing table entries learned through OSPF)
show ip route eigrp (show routing table entries learned through EIGRP)
show mac-address-table or **show mac address-table** (varies with different IOS)
show flash (display filenames and directories in Flash memory)
show clock (current date/time in this device)
show ipv6 ??? (does the IPv6 version of many IPv4 commands)
show processes (shows active processes running on router)
show process cpu (shows cpu statistics)
show memory (shows memory allocation)
show users (show who is telnetted into this device)
show standby (see if HSRP is active)
ping X.X.X.X (try to reach the destination host at X.X.X.X)
trace X.X.X.X (show the path taken to reach the destination host at X.X.X.X)
R1(config)# **do show ???** (execute show commands from configuration mode)
debug ??? (real-time reporting about processes related to almost any function)
debug all (very dangerous as the router can become consumed by reporting everything)
undebug all (turn off all debugging commands – handy if this is a busy router)

Editing and Navigation Commands

ctrl-a (go to the beginning of the current line)
ctrl-e (go to the end of the current line)
ctrl-p or up-arrow (repeat up to 10 previous commands in the current mode)
ctrl-n or dn-arrow (if you have gone back in command history, this moves forward)
backspace-key (erase the character to the left of the current cursor position)
ctrl-z or **end** (go out to privilege mode)
exit (move back one level in the hierarchical command structure)
ctrl-c (cancel current command or leave Setup mode if you accidentally get into it)
ctrl-shift-6 (stop runaway ping or trace)
do COMMAND (command that otherwise would not work in current configuration mode)
wr (shortcut for 'copy running-config startup-config)
terminal length 0 [zero] (turn off paging – makes output without breaks)
terminal length 24 (normal page breaks in output)
terminal monitor (used with remote access to see output of all commands)
terminal history size [1-256] (change from 10 lines of history)

There are filtering parameters that can be configured after the **show |** command:

- **section** - Shows the entire section that starts with the filtering expression.
- **include** - Includes all output lines that match the filtering expression.
- **exclude** - Excludes all output lines that match the filtering expression.
- **begin** - Shows all the output lines from a certain point, starting with the line that matches the filtering expression

Common Port Numbers and Protocols

File Transfer Protocol (**FTP**)
    FTP Control=TCP port 21
    FTP Data = TCP Port 20
Secure Shell (**SSH**) - TCP Port 22
Telnet - TCP Port 23
Simple Mail Transfer Protocol (**SMTP**) - TCP Port 25
Domain Name System (**DNS**) - TCP/UDP Port 53
Dynamic Host Configuration Protocol (**DHCP**)
    BOOTPS=UDP Port 67 (DHCP request from client to server)
    BOOTPC=UDP Port 68 (DHCP reply from server to client)
Hypertext Transfer Protocol (**HTTP**) - TCP Port 80
Post Office Protocol – incoming mail (**POP**) - TCP Port 110
Network Time Protocol (**NTP**) - UDP Port 123
Simple Network Management Protocol (**SNMP**) - UDP Port 161
Secure Hypertext Transfer Protocol (**HTTPS**) - TCP Port 443

Basic Router / Switch Configuration

To Restore a Switch or Router to Default Configuration

S1# **delete vlan.dat** (hit ‘enter’ to accept defaults) [<u>Note: Only do this on a switch</u>]

S1# **erase startup-config** (hit ‘enter’ to accept defaults [Router or Switch])

S1# **reload** (answer ‘no’ if asked to save current config [Router or Switch])

Router / Switch Basic Configuration

R1# **configure terminal** (enter global configuration mode)

R1(config)# **hostname NAME** (configure the NAME of the Router or Switch)

R1(config)# **security passwords min-length 5** (set minimum password length)

R1(config)# **service password-encryption** (encrypt all passwords – except secret)

R1(config)# **login block-for 60 attempts 3 within 30** (wait 1 min if 3 bad attempts in 30 sec)

R1(config)# **enable secret PASSWORD** (make the privilege level password ‘PASSWORD’)

R1(config)# **no ip domain-lookup** (suppress DNS attempt when a command is mistyped)

R1(config)# **banner motd MESSAGE** (create a MESSAGE that will display when logging in)

R1(config)# **line console 0** [zero] (enter the console connection configuration mode)

R1(config-line)# **password PASSWORD** (make the user level password ‘PASSWORD’)

R1(config-line)# **login** (instruct the router that you want it to check for a password)

R1(config-line)# **logging synchronous** (assists by keeping command entry more orderly)

R1(config-line)# **exec-timeout 0 0** [zeroes] (no timeout while configuring the router)

R1(config)# **line vty 0 4** [zero 4] (configure the same options as line console above)

S1(config)# **line vty 0 15** [zero 15] (configure the same options in a switch)

R1# **copy running-configuration startup-configuration** (save config in NVRAM)

R1# **wr** (legacy command - Same as copy running-configuration startup-configuration)

R1(config)# ! (remark – makes no configuration changes)

For Switch Management Interface Configuration

S1(config)# **sdm prefer dual-ipv4-and-ipv6 default** (must reload; Allow IPv6 Telnet or SSH)

S1(config)# **interface vlan 1** (create a virtual host on the switch)

S1(config-if)# **description Management interface for this switch** (optional description)

S1(config-if)# **ip address 192.168.100.50 255.255.255.0** (assign an IP address)

S1(config-if)# **ipv6 address 3ffe:b00:c18:1::3/64** (assign IPv6 address – if needed)

S1(config-if)# **no shut** (must turn it on)

S1(config-if)# **exit** (leave interface config and return to global config)

S1(config)# **ip default-gateway 192.168.100.1** (must be on same subnet as Mngt interface)

S1(config)# **enable secret class** (must have an enable password for remote access)

S1(config)# **line vty 0 15** (switches may have 16 VTY connections at once)

S1(config-line)# **password cisco** (must set a login password for telnet to be possible)

S1(config-line)# **login** (tell the VTY ports to ask for password from remote user)

S1(config-line)# **transport input telnet** (allows only telnet for remote config – default)

Configuring IPv4 Router Interface

```
R1(config)# interface INTERFACE-TYPE (enter configuration mode for an interface)
R1(config-if)# ip address ADDRESS SNM (assign the IP Address and subnet mask)
R1(config-if)# description WORDS (document what this interface is used for)
R1(config-if)# bandwidth VALUE (used by the routing protocol for the speed of the link)
R1(config-if)# shutdown (turn the interface off – ‘Administratively down’)
R1(config-if)# no shutdown (turn the interface on)
```

Configuring IPv6 Router Interface

```
R1(config)# ipv6 unicast-routing (activate IPv6 routing – off by default)
R1(config)# interface Gi1/1
R1(config-if)# ipv6 enable (turn on ipv6 in this interface if no other IPv6 configuration)
R1(config-if)# ipv6 address 3ffe:b00:c18:1::3/64 (manually enter complete address)
  -or-
R1(config-if)# ipv6 address 3ffe:b00:c18:1::/64 eui-64 (auto configure host portion)
R1(config-if)# ipv6 address fe80::4 link-local (configure link-local address)
```

Layer-3 Switch Commands

```
S1(config)# ip routing (activate IPv4 routing within the switch)
S1(config)# ipv6 routing (activate IPv6 routing within the switch)
S1(config-if)# no switchport (used to designate that this is a router port, not a switchport)
S1(config-if)# switchport trunk encapsulation dot1q (to configure trunking for dot1Q)
S1(config)# interface vlan 10 (create an SVI to be the default-gateway for VLAN 10)
```

Network Time Protocol (NTP)

```
R1(config)# ntp server 209.165.200.225
R1(config)# clock timezone pst -7
R1# show ntp associations
R1# show ntp status
R1# show clock
```

Syslog Server

```
R1# show logging
R1(config)# logging enable
R1(config)# terminal monitor
R1(config)# logging host ip-address
R1(config)# logging trap level
R1(config)# service timestamps type datetime
R1(config)# logging source-interface Loopback 0
```

VLANS, Trunks, Router-on-a-Stick, VTP

VLAN Creation and Port Assignment

S1(config)# **vlan 10** (create VLAN 10 in the VLAN.DAT database)

S1(config-vlan)# **name Management** (optionally name the VLAN)

S1(config)# **interface fa0/12** (select a port on the switch) --or--

S1(config)# **interface range fa0/12 – 20** (select a range of ports to be configured the same)

S1(config-if)# **switchport mode access** (set the port to Access mode)

S1(config-if)# **switchport access vlan 10** (assign this port(s) to VLAN 10)

Trunk Creation

S1(config)# **interface gi1/1** (select port for trunking)

S1(config-if)# **switchport trunk encapsulation dot1q** (NOTE: on Layer 3 switch only)

S1(config-if)# **switchport mode trunk** (set the port to be in trunk mode)

S1(config-if)# **switchport trunk native vlan 99** (select VLAN 99 to carry native traffic)

S1(config-if)# **switchport trunk allowed vlan 1,10,20,99** (optional – which VLANs are permitted to go across this trunk. Don't forget to include VLAN 1 and the native VLAN)

Router-on-a-Stick Configuration

R1(config)# **interface Fa0/0** (select the main interface)

R1(config-if)# **no ip address** (there should not be any IP Address on the main interface)

R1(config-if)# **interface Fa0/0.10** (create a sub-interface – the number can be anything)

R1(config-if)# **encapsulation dot1q 10** (use 802.1Q trunking; assign to this VLAN #)

R1(config-if)# **ip address 172.16.10.1 255.255.255.0** (the default-gateway IP)

R1(config-if)# **interface Fa0/0.99** (create another sub-interface - this one for native traffic)

R1(config-if)# **encapsulation dot1q 99 native** (802.1Q trunking; VLAN #; and native)

(NOTE: No IP address unless workstations or management interfaces are on this VLAN)

VLAN Trunking Protocol (VTP) Configuration

S1(config)# **vtp mode server** (configure this switch to be in server mode) --or--

S1(config)# **vtp mode client** (configure this switch to be in client mode) ---or--

S1(config)# **vtp mode transparent** (configure this switch in transparent mode - Suggested)

S1(config)# **vtp domain NAME** (change the VTP domain name of this switch to NAME)

S1(config)# **vtp password PASSWORD** (change the VTP password for this switch)

S1(config)# **vtp pruning** (activate VTP pruning – Not supported in Packet Tracer)

S1(config)# **vtp version 2** (change the VTP version to 2)

S1# **show vtp status** (see VTP mode, revision, version, domain name, pruning mode, etc)

S1# **show vtp password** (only way to see the VTP password – does not show in status)

Etherchannel (PortChannel)

To configure a Layer 2 (trunking) Etherchannel:

```
S1(config)# interface range fa0/1 – 4 (group of physical interfaces)
S1(config-if)# switchport trunk encapsulation dot1q (NOTE: on Layer 3 switch only)
S1(config-if)# switchport mode trunk (set to trunk mode)
S1(config-if)# switchport trunk native vlan 777 (set native VLAN)
S1(config-if)# channel-protocol lacp (optional - set this interface to LACP portchannel)  -or-
S1(config-if)# channel-protocol pagp (optional - set this interface to PAgP portchannel)
S1(config-if)# channel-group 3 mode [see choices below]
                        passive     (enable LACP only if a LACP device is detected)
                        active      (enable LACP unconditionally)
                        auto        (enable PAgP only if a PAgP device is detected)
                        desirable   (enable PAgP unconditionally)
                        on          (enable Etherchannel – only use with ‘on’ at the other end)
S1(config)# interface port-channel 3 (configure the virtual interface from 1 to 6)
S1(config-if)# switchport mode trunk (set to trunk mode)
S1(config-if)# switchport trunk native vlan 777 (set native VLAN the same as the physical)
S1(config-if)# no shutdown (turn on the virtual interface)
```

To configure a Layer 3 Etherchannel:

```
SW1(config)# interface range fa0/1 – 2
SW1(config-if)#  no switchport
SW1(config-if)#  channel-group 1 mode {active, passive, on}
SW1(config)# interface port-channel 1
SW1(config-if)# no switchport
SW1(config-if)# ip address x.x.x.x m.m.m.m
```

(The other end is configured the same)

EtherChannel uses a load-balancing algorithm based on selected type or criteria:

- Source IP Address (src-ip)
- Destination IP Address (dst-ip)
- Both Source and Destination IP (src-dst-ip) – default L3 type
- Source MAC address (src-mac) – default L2 type
- Destination MAC address (dst-mac)
- Both Source and Destination MAC (src-dst-mac)
- Source TCP/UDP port number (src-port)
- Destination TCP/UDP port number (dst-port)
- Both Source and Destination port number (src-dst-port)

```
SW1(config)# port-channel load-balance TYPE
```

Spanning Tree Protocol (STP), HSRP

Spanning Tree

S1(config)# **spanning-tree mode pvst** (configure for PVST – Default)

S1(config)# **spanning-tree mode rapid-pvst** (configure this switch for rapid PVST)

S1(config)# **spanning-tree vlan 10,20 root primary** (make root bridge for these VLANs)

S1(config)# **spanning-tree vlan 10 root secondary** (make secondary root bridge for VLAN)

S1(config)# **spanning-tree vlan 10 priority 8192** (set the BID priority to 8192 in this VLAN)

S1(config)# **spanning-tree portfast default** (default Portfast on all interfaces in this switch)

S1(config)# **spanning-tree portfast bpduguard default** (global BPDU configuration)

S1(config)# **interface range fa0/10 – 20** (must be configured as Access ports for Portfast)

S1(config-if)# **spanning-tree portfast** (set interfaces for Portfast)

S1(config-if)# **spanning-tree bpduguard enable** (disables interface if it receives a BPDU)

S1(config)# **interface fa0/1** (select a port to set STP port priority)

S1(config-if)# **spanning-tree vlan 10 port-priority 16** (set port priority to 16; default is 128)

S1# **show spanning-tree** (see spanning-tree status on a VLAN-by-VLAN basis)

S1# **show spanning-tree vlan 10** (see detail spanning-tree information for VLAN 10)

S1# **show spanning-tree summary** (among other things, see if this is the root bridge)

S1# **show spanning-tree blockedports** (see which ports are in STP blocking status)

S1# **show spanning-tree root** (see which BID is root on a VLAN-by-VLAN basis)

Hot Standby Routing Protocol (HSRP) for IPv4

R1(config)# **interface fastethernet 0/1**

R1(config-if)# **standby version 2** (most recent version)

R1(config-if)# **standby 1 10.10.10.1** (activate HSRP and virtual default gateway address)

R1(config-if)# **standby 1 priority 150** (default 100; higher is better)

R1(config-if)# **standby 1 preempt** (trigger re-selection of active router)

R1# **show standby**

R1# **show standby brief**

Hot Standby Routing Protocol (HSRP) for IPv6

R1(config)# **interface fastethernet 0/1**

R1(config-if)# **standby version 2** (use the same version at each end)

R1(config-if)# **standby GROUP# ipv6 autoconfig** (create virtual IPv6 Link-Local address)

R1(config-if)# **standby GROUP# ipv6 2001:CAFE:ACAD:4::1/64** (set virtual shared IP)

R1(config-if)# **standby GROUP# priority NUMBER**

Set a higher priority (default 100) to make this router the primary in HSRP

R1(config-if)# **standby GROUP# preempt** (trigger re-selection of active router)

Preempt will make this router the active one if it had been down and comes back up

R1# **show standby** (verify the configuration)

Security Practices

R1(config)# **service password-encryption** (encrypt all passwords (except ‘secret’)

R1(config)# **security password min-length 8** (set minimum 8 character passwords)

R1(config)# **login block-for 120 attempts 3 within 60** (block for 2 minutes if more than 3 failed logins within 60 seconds)

SSH Configuration

Router(config)# **hostname R1** (must change the name of the device from the default)

R1(config)# **username Bob password Let-me-in!** (configure a local user and password)

R1(config)# **ip domain-name ANYTHING.COM** (must set for crypto-key generation)

R1(config)# **crypto key generate rsa** (make an encryption key - typically 1024 bits)

R1(config)# **ip ssh version 2** (configure for SSH version 2)

R1(config)# **line vty 0 4** (change parameters for remote access)

R1(config-line)# **login local** (select to authenticate against usernames in this device)

R1(config-line)# **transport input ssh** (only allow SSH for remote management)

R1(config-line)# **ip ssh timeout** ***seconds*** (default is 120 seconds)

R1(config-line)# i**p ssh authentication-retries** ***number*** (retries can be 1-5)

Port Security Configuration on a Switch

S1(config)# **interface fa0/1** or **interface range fa0/1 – 15, gi1/1**

S1(config-if)# **switchport mode access** (must change from dynamic to access mode)

S1(config-if)# **switchport port-security** (must do to activate port-security)

S1(config-if)# **switchport port-security maximum 25** (allow 25 MAC addresses)

S1(config-if)# **switchport port-security aging time 10** (timeout in 10 minutes)

S1(config-if)# **switchport port-security aging static** (aging for manually entered addresses)

S1(config-if)# **switchport port-security aging type absolute** (delete at specified time)

S1(config-if)# **switchport port-security aging type inactivity** (delete if inactive for time)

S1(config-if)# **switchport port-security mac-address [MAC Address]**

S1(config-if)# **switchport port-security mac-address sticky** (memorize MAC addresses)

S1(config-if)# **switchport port-security violation restrict** (send SNMP message) --or--

S1(config-if)# **switchport port-security violation protect** (only stop excess MACs) –or--

S1(config-if)# **switchport port-security violation shutdown** (shutdown interface - default)

S1(config-if)# **switchport nonegotiate** (disable DTP on this interface)

S1(config-if)# **switchport protected** (does not allow traffic to/from other protected ports)

S1(config-if)# **spanning-tree bpduguard enable** (disables interface if it receives a BPDU)

S1(config-if)# **shutdown** then **no shutdown** (restore individual interface if it has shutdown)

S1(config)# **errdisable recovery cause all** (automatically recovery after 300 seconds)

S1(config)# **errdisable recovery cause psecure_violation** (recover after 300 seconds)

S1(config)# **errdisable recovery interval 150** (change time limit to 150 seconds)

S1# **show port-security interface fa0/12** (show security configuration for an interface)
S1# **show port-security address IP-ADDRESS** (show security associated with this address)

IP DHCP Snooping and Dynamic Arp Inspection (DAI)

S1(config)# **ip dhcp snooping** (global activation of DHCP snooping)
S1(config)# **ip dhcp snooping vlan 1,10,120-123** (enable DHCP snooping on VLANs)
S1(config)# **ip arp inspection vlan 1,10,120-123** (enable dynamic ARP inspection)
S1(config)# **ip arp inspection validate src-mac** (drop packet if the source MAC is bad)
S1(config)# **ip arp inspection validate dst-mac** (drop packet if the destination MAC is bad)
S1(config)# **ip arp inspection validate ip** (drop packet if unexpected IP address is there)
S1(config-if)# **ip dhcp snooping limit rate 5** (How many DHCP requests/sec permitted)
S1(config-if)# **ip dhcp snooping trust** (allow DHCP server replies on a specific interface)
S1(config-if)# **ip arp inspection trust** (disable DAI on trusted port – like to the router)
S1# **show ip dhcp snooping**

Enable/Disable Cisco Discovery Protocol (CDP)

R1(config)# **cdp run** (activate CDP globally in the router – on by default)
R1(config)# **no cdp run** (disable CDP within the entire router)
R1(config-if)# **no cdp enable** (stop CDP updates leaving through this specific interface)

Enable/Disable Link-Layer Discovery Protocol (LLDP)

R1(config)# **lldp run** (global activation of LLDP)
R1(config)# **no lldp run** (disable LLDP globally)
R1(config-if)# **lldp transmit** (enable LLDP transmit on an interface)
R1(config-if)# **lldp receive** (enable LLDP receive on an interface)
R1# **show lldp**
R1# **show lldp neighbors**
R1# **show lldp neighbors detail**

Routing (IPv4 OSPF, Static Routes)

Configuring IPv4 OSPF(v2)

R1(config)# **interface loopback 10** (optionally create a virtual interface for OSPF router ID)

R1(config)# **router ospf 1** (configure an OSPF routing process)

R1(config-router)# **router-id 2.2.2.2** (optionally configure the OSPF Router ID - Suggested)

R1(config-router)# **network 172.16.45.0 0.0.0.255 area 0** (include directly connected networks that match this parameter)

-or-

R1(config-router)# **network 192.168.25.1 0.0.0.0 area 0** (specify the interface IP address)

-or-

R1(config-if)# **ip ospf 10 area 0** (associate OSPF at an interface instead of network statement in ‘router ospf 1’)

R1(config-router)# **default-information originate** (propagate the quad-0 default route)

R1(config-router)# **redistribute static** (propagate classful static routes configured on this router to other OSPF routers)

R1(config-router)# **redistribute static subnets** (propagate classless static routes configured on this router to other OSPF routers)

R1(config-router)# **passive-interface default** (no routing updates out any interface)

R1(config-router)# **no passive-interface fastethernet 0/1** (allow certain interfaces)

R1(config-router)# **passive-interface fastethernet 0/1** (do not send OSPF routing updates out this interface)

R1(config-router)# **auto-cost reference-bandwidth ???** (optionally change the reference bandwidth in terms of Mbits per second 1-4294967; must be the same on all routers)

R1(config-if)# **ip ospf cost 1562** (optionally configure an absolute OSPF cost for a link – this example same as bandwidth 64)

R1(config-if)# **ip ospf hello-interval seconds** (change hello timer from default 10 seconds)

R1(config-if)# **ip ospf dead-interval seconds** (change dead timer from default 40 seconds)

R1(config-if)# **ip ospf priority {0 - 255}** (for OSPF DR/BDR election, default=1, ineligible=0)

R1# **show ip ospf neighbor** (display OSPF neighbor adjacencies – State should be ‘FULL’ or ‘2WAY’)

R1# **show ip protocols** (includes the OSPF Router ID of this router)

R1# **clear ip ospf process** (re-calculate OSPF Router ID based on current parameters)

R1# **show ip ospf** (display OSPF process and router IDs, as well as area information)

R1# **show ip ospf interface serial 0/0/0** (see DR/BDR information, hello and dead intervals)

Configuring IPv4 Static Routes

R1(config)# **ip route 0.0.0.0 0.0.0.0 serial0/0** (default-route goes out serial 0/0)

R1(config)# **ip route 0.0.0.0 0.0.0.0 50.77.4.13** (default-route goes to next-hop 50.77.4.13)

R1(config)# **ip route 0.0.0.0 0.0.0.0 serial0/0 150** (default-route goes out serial 0/0. An optional parameter is added to set the administrative distance to 150)

R1(config)# **ip route 47.151.2.0 255.255.255.0 172.24.2.11** (to get to network 47.151.2.0/24, go to next-hop address of 172.24.2.11)

R1(config)# **ip route 47.151.2.0 255.255.255.0 serial0/1** (to get to network 47.151.2.0/24, go out interface serial 0/1)

R1(config)# **ip route 47.151.2.0 255.255.255.0 fastethernet0/0 192.168.12.2** (to get to network 47.151.2.0/24, go to the next-hop 192.168.12.2 out Fastethernet0/0; on Ethernet both are needed – makes a fully specified static route)

R1(config)# **ip route 47.151.2.1 255.255.255.255 serial0/1** (Configure a static host route)

Configuring IPv64 Static Routes

IPv6 static routes start with ‘ipv6 route’ and substitute IPv6 addresses/prefix lengths for the IPv4 addresses and subnet masks.

Access Control Lists

Standard Access Lists

-Standard access lists only evaluate the source IP field. They can use the 'host' and 'any' keywords, or apply wildcard masks. They do not use port numbers.

**Named Standard Access List :

```
R-1(config)# ip access-list standard NAME (name the list)
R-1(config-std-nacl)# deny host 192.168.20.5 log (deny a specific host / log matches)
R-1(config-std-nacl)# permit 192.168.20.0  0.0.0.255 (permit subnet 192.168.20.0)
R-1(config-std-nacl)# deny any (deny all other IP addresses)
```

**Numbered IP Standard Access List:

```
R-1(config)# access-list 25 deny host 192.168.20.5 (deny specific host)
R-1(config)# access-list 25 permit 192.168.20.0  0.0.0.255 (permit entire subnet)
R-1(config)# access-list 25 deny any (deny all other IP addresses)
R-1# show access-list (see access lists on this router and # of 'matches' per line)
R-1# show access-list NAME (see a specific access list and # of 'matches' per line)
```

Extended Access Lists

Action (required)	Protocol (required)	Source IP (required)	Compare (optional)	Port/Protocol (optional)	Dest IP (required)	Compare (optional)	Port/Protocol (optional)
permit	IP	IP address & Wildcard mask	eq	23 – telnet	IP address & Wildcard mask	eq	23 – telnet
deny	TCP		gt	80 – http		gt	80 – http
remark	UDP	any	lt	443 – https	any	lt	443 – https
	ICMP	host X.X.X.X	neq	echo (ping)	host X.X.X.X	neq	echo (ping)
	OSPF		range	echo-reply		range	echo-reply
	EIGRP						
	Etc…						

The protocol field must match the destination port / protocol - if they are used (example: TCP=Telnet, ICMP=Ping, UDP=DNS).

**Named Extended Access List:

```
R-1(config)# ip access-list extended NAME (name the list)
```

Example: Deny an individual host to an entire subnet for Telnet and also log matches:

```
R-1(config-ext-nacl)# deny tcp host 192.168.20.10  172.16.0.0  0.0.255.255 eq 23 log
```

Example: Permit an entire subnet to go anywhere:

```
R-1(config-ext-nacl)# permit ip 192.168.20.0  0.0.0.255  any
```

Example: Deny everything:

```
R-1(config-ext-nacl)# deny ip any any (this is applied by default if not configured)
```

Applying Access Lists

```
R-1(config)# interface fastethernet 0/0
R-1(config-if)# ip access-group NAME in (evaluate packets coming in to the router)
R-1(config-if)# ip access-group NAME out (evaluate packets leaving the router)
R-1(config)# line vty 0 4
```

R-1(config-line)# **access-class NAME in** (evaluate packets for telnet or SSH)

DHCP and NAT

Configuring DHCP for IPv4

R1(config)# **service dhcp** or **no service dhcp** (enable / disable DHCP service – default on)

R1(config-if)# **ip address dhcp** (obtain an IP address automatically – usually from ISP)

R-1(config)# **ip dhcp excluded 172.16.2.1 172.16.2.7** (excluded IP range)

R-1(config)# **ip dhcp pool LAN-2** (name this DHCP pool)

R-1(dhcp-config)# **network 172.16.2.0 255.255.255.128** -or- **/25** (entire network range)

R-1(dhcp-config)# **default-router 172.16.2.1** (address on router port – can have up to 8)

R-1(dhcp-config)# **dns-server 140.198.8.14** (DNS server – can have up to 8)

R-1(dhcp-config)# **domain-name MCC.COM** (optional domain name)

R-1(dhcp-config)# **lease-time 5** (optional - change to 5 day lease, 1 day is default)

!

R-3(config)# **interface fastethernet 0/1** (interface for network with DHCP clients)

R-3(config-if)# **ip helper-address 192.168.15.2** (address where DHCP server is)

!

R-1# **show ip dhcp binding** (see what IP addresses are assigned & MAC addresses)

DOS-PROMPT>**ipconfig /release** (remove dynamically assigned IP information on PC)

DOS-PROMPT>**ipconfig /renew** (get new IP address from DHCP server)

Configuring IPv6 Stateless Address Auto-Configuration (SLAAC) with DNS

R1(config)# **ipv6 unicast routing** (make sure IPv6 is activated)

R1(config)# **ipv6 dhcp pool LAN-F-STATELESS** (create pool for addresses and DNS)

R1(config-dhcpv6)# **dns-server 2001:345:ACAD:F::5** (IPv6 DNS server address)

R1(config-dhcpv6)# **domain-name cisco.com** (optional domain name)

R1(config)# **interface g1/1**

R1(config-if)# **ipv6 dhcp server LAN-F-STATELESS** (look to this DHCP pool)

R1(config-if)# **ipv6 nd other-config-flag** (include the information from the DHCP pool)

Configuring DHCP for IPv6 Stateful Address Auto-configuration

R1(config)# **ipv6 unicast routing** (make sure IPv6 is activated)

R1(config)# **ipv6 dhcp pool LAN-10-STATEFUL** (create pool for addresses and DNS)

R1(config-dhcpv6)# **address prefix 2001:D7B:CAFÉ:10::/64 lifetime infinite infinite**

R1(config-dhcpv6)# **dns-server 2001:345:ACAD:F::5** (IPv6 DNS server address)

R1(config-dhcpv6)# **domain-name cisco.com** (optional domain name)

R1(config)# **interface g1/1**

R1(config-if)# **ipv6 dhcp server LAN-10-STATEFUL** (look to this DHCP pool)

R1(config-if)# **ipv6 nd prefix default no-autoconfig** (don’t use SLAAC)

R1(config-if)# **ipv6 nd managed-config-flag** (enable IPv6 Neighbor Discovery)

R-3(config)# **interface fastethernet 0/1** (interface for network with DHCP clients)

IPv6 DHCP – Other Configuration Options

R1(config-if)# **ipv6 address dhcp** for router to get IP if using stateless configuration

R1(config-if)# **ipv6 address autoconfigure** for router to get IP using statefull configuration

R1(config-if)# **ipv6 dhcp relay destination aaaa:bbbb:cccc:dddd::10**

R1(config-if)# **ipv6 dhcp relay destination fe80::10 G0/0** (if destination is LLA)

R1# **show ipv6 dhcp pool**

R1# **show ipv6 dhcp binding**

Configure NAT for IPv4

-For both static and dynamic NAT, designate interfaces as inside or outside:

R-1(config)# **interface fa0/0** (typically designate all interfaces except the outside one)

R-1(config-if)# **ip nat inside** (designate this as an inside interface)

R-1(config)# **interface serial 0/0/0** (typically there is only one outside interface)

R-1(config-if)# **ip nat outside** (designate this as an outside interface)

!

-Static NAT requires only one statement. The IP addresses are inside / outside:

R-1(config)# **ip nat inside source static 192.168.10.22 73.2.34.137**

!

-Dynamic NAT may use a pool of 'outside addresses'. If you do not use a pool, you will have to use the address on the outside interface. You can use 'netmask':

R-1(config)# **ip nat pool POOL-NAME 73.2.34.138 73.2.34.143 netmask 255.255.255.248**

-or- You may choose to use 'prefix-length':

R-1(config)# **ip nat pool POOL-NAME 73.2.34.138 73.2.34.143 prefix-length 29**

!

-Dynamic NAT requires an ACL to define which internal addresses can be NATted:

R-1(config)# **ip access-list standard NAT-ELIGIBLE**

R-1(config-std-nacl)# **permit 192.168.10.0 0.0.0.255** (include all subnets)

R-1(config-std-nacl)# **deny any**

!

-Dynamic NAT can use the pool for outside addresses:

R-1(config)# **ip nat inside source list NAT-ELIGIBLE pool POOL-NAME**

-or- Dynamic NAT can use the pool with overload to share outside addresses:

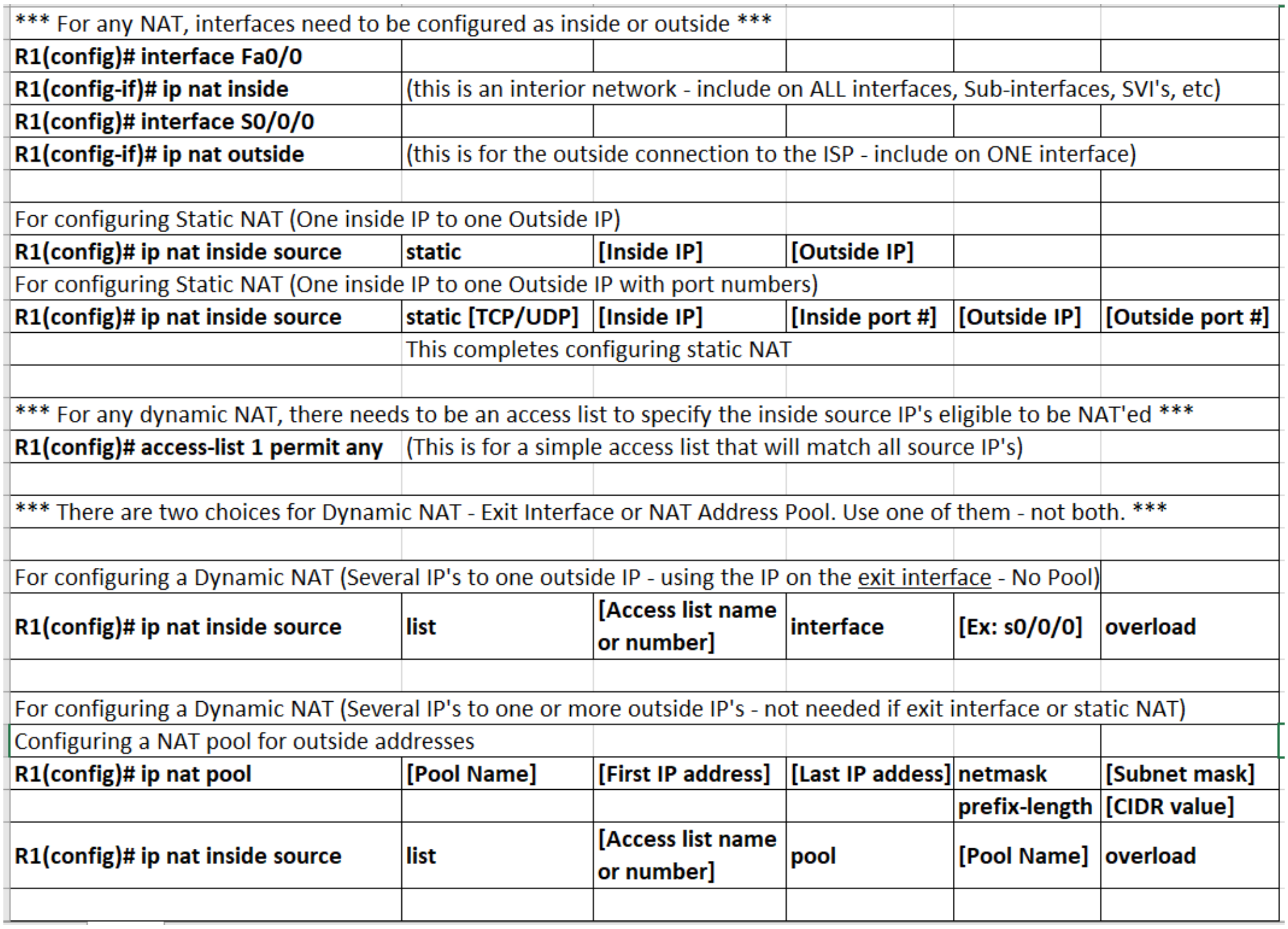
R-1(config)# **ip nat inside source list NAT-ELIGIBLE pool POOL-NAME overload**

-or- Dynamic NAT can use the exit interface – almost always will use overload:

R-1(config)# **ip nat inside source list NAT-ELIGIBLE interface serial 0/0/0 overload**

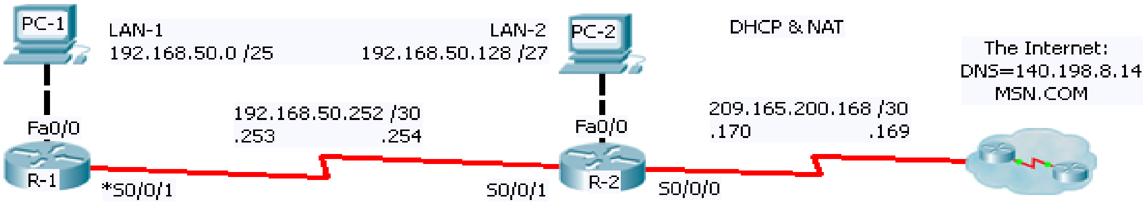
R-1# **show ip nat translations** (current translations- dynamic and static)

R-1# **show ip nat statistics** (see # of active translations, role of interfaces, etc)



*** For any NAT, interfaces need to be configured as inside or outside ***					
R1(config)# interface Fa0/0					
R1(config-if)# ip nat inside	(this is an interior network - include on ALL interfaces, Sub-interfaces, SVI's, etc)				
R1(config)# interface S0/0/0					
R1(config-if)# ip nat outside	(this is for the outside connection to the ISP - include on ONE interface)				
For configuring Static NAT (One inside IP to one Outside IP)					
R1(config)# ip nat inside source	**static**	**[Inside IP]**	**[Outside IP]**		
For configuring Static NAT (One inside IP to one Outside IP with port numbers)					
R1(config)# ip nat inside source	**static [TCP/UDP]**	**[Inside IP]**	**[Inside port #]**	**[Outside IP]**	**[Outside port #]**
	This completes configuring static NAT				
*** For any dynamic NAT, there needs to be an access list to specify the inside source IP's eligible to be NAT'ed ***					
R1(config)# access-list 1 permit any	(This is for a simple access list that will match all source IP's)				
*** There are two choices for Dynamic NAT - Exit Interface or NAT Address Pool. Use one of them - not both. ***					
For configuring a Dynamic NAT (Several IP's to one outside IP - using the IP on the exit interface - No Pool)					
R1(config)# ip nat inside source	**list**	**[Access list name or number]**	**interface**	**[Ex: s0/0/0]**	**overload**
For configuring a Dynamic NAT (Several IP's to one or more outside IP's - not needed if exit interface or static NAT)					
Configuring a NAT pool for outside addresses					
R1(config)# ip nat pool	**[Pool Name]**	**[First IP address]**	**[Last IP addess]**	**netmask**	**[Subnet mask]**
				prefix-length	**[CIDR value]**
R1(config)# ip nat inside source	**list**	**[Access list name or number]**	**pool**	**[Pool Name]**	**overload**

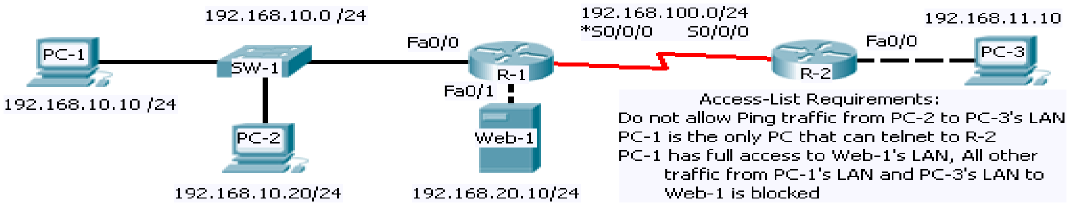
DHCP & NAT Configuration:



```
R-1
!
ip dhcp excluded-address 192.168.50.1 192.168.50.7
ip dhcp excluded-address 192.168.50.129 192.168.50.131
!
ip dhcp pool LAN-1
 network 192.168.50.0 255.255.255.128
 default-router 192.168.50.1
 dns-server 140.198.8.14
!
ip dhcp pool LAN-2
 network 192.168.50.128 255.255.255.224
 default-router 192.168.50.129
 dns-server 140.198.8.14
```

```
R-2
!
interface FastEthernet0/0
 ip address 192.168.50.129 255.255.255.224
 ip helper-address 192.168.50.253
 ip nat inside
!
interface Serial0/0/0
 ip address 209.165.200.170 255.255.255.252
 ip nat outside
!
interface Serial0/0/1
 ip address 192.168.50.254 255.255.255.252
 ip nat inside
!
ip nat inside source list INSIDE-ADDRESSES interface
                                   Serial0/0/0 overload
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
!
ip access-list standard INSIDE-ADDRESSES
 permit 192.168.50.0  0.0.0.127
 permit 192.168.50.128  0.0.0.31
 permit 192.168.50.252  0.0.0.3
 deny any
```

ACLs – (Access Control Lists):

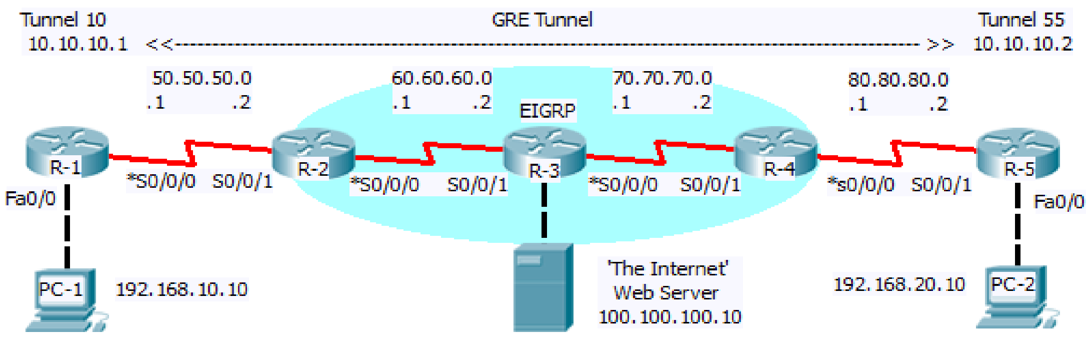


Access-List Requirements:
Do not allow Ping traffic from PC-2 to PC-3's LAN
PC-1 is the only PC that can telnet to R-2
PC-1 has full access to Web-1's LAN, All other traffic from PC-1's LAN and PC-3's LAN to Web-1 is blocked

```
R1
!
interface FastEthernet 0/0
 ip access-group NO-PING-PC2-TO-PC3-LAN in
!
ip access-list extended NO-PING-PC2-TO-PC3-LAN
 remark Deny Ping from PC-2 to PC-3's LAN
  deny icmp host 192.168.10.20  192.168.11.0  0.0.0.255  echo
 remark Permit all other traffic
  permit ip any any
!
!
interface FastEthernet 0/1
 ip access-group RESTRICT-WEB1-TRAFFIC out
!
ip access-list standard RESTRICT-WEB1-TRAFFIC
 remark Permit PC-1
  permit host 192.168.10.10
 remark Deny all PC-1 and PC-3 LAN traffic
  deny 192.168.10.0  0.0.1.255
 remark Allow all other traffic
  permit any
!
```

```
R2
!
access-list 10 remark Only allow PC-1
access-list 10 permit host 192.168.10.10
access-list 10 remark Deny all others
access-list 10 deny any
!
line vty 0-4
 access-class 10 in
!
```

VPN GRE Tunnel:



```
R-1
!
interface Tunnel10
 ip address 10.10.10.1 255.255.255.252
 tunnel source Serial0/0/0
 tunnel destination 80.80.80.2
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 ip nat inside
!
interface Serial0/0/0
 ip address 50.50.50.1 255.255.255.0
 ip nat outside
!
router rip
 version 2
 passive-interface Serial0/0/0
 network 10.0.0.0
 network 192.168.10.0
 no auto-summary
!
ip nat inside source list 1 interface Serial0/0/0 overload
!
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
!
access-list 1 permit 192.168.10.0 0.0.0.255
access-list 1 deny any

R-1#sh ip route   *some output omitted*
Gateway of last resort is 0.0.0.0 to network 0.0.0.0

C      10.10.10.0 is directly connected, Tunnel10
C      50.50.50.0 is directly connected, Serial0/0/0
C   192.168.10.0/24 is directly connected, Fa0/0
R   192.168.20.0/24 [120/1] via 10.10.10.2, Tunnel10
S*   0.0.0.0/0 is directly connected, S0/0/0
```

```
R-5
!
interface Tunnel55
 ip address 10.10.10.2 255.255.255.252
 tunnel source Serial0/0/1
 tunnel destination 50.50.50.1
!
interface FastEthernet0/0
 ip address 192.168.20.1 255.255.255.0
 ip nat inside
!
interface Serial0/0/1
 ip address 80.80.80.2 255.255.255.0
 ip nat outside
!
router rip
 version 2
 passive-interface Serial0/0/1
 network 10.0.0.0
 network 192.168.20.0
 no auto-summary
!
ip nat inside source list NAT interface Serial0/0/1 overload
!
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
!
ip access-list standard NAT
 permit 192.168.20.0 0.0.0.255
 deny any

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

C      10.10.10.0 is directly connected, Tunnel55
C      80.80.80.0 is directly connected, Serial0/0/1
R   192.168.10.0/24 [120/1] via 10.10.10.1, Tunnel55
C   192.168.20.0/24 is directly connected, Fa0/0
S*   0.0.0.0/0 is directly connected, Serial0/0/1
```