*CONFIGS AS PER PACKET TRACER LABS:*

*Lab 20: STP:*

**To see spanning tree details:**

en

Sh spanning-tree

Will tell you what type of stp is enabled, root id and bridge ID, which interface is root, interfaces and whether they are involved in STP, role and status

**To see spanning tree with particular VLAN:**

En

Sh spanning-tree VLAN #

**To see further details than what is above:**

En

Sh spanning-tree detail

**To see each VLAN and state of each interface:**

En

Sh spanning-tree summary

Will tell you blocking, listening, forwarding, learning, stp, active

*Lab 21: STP (PVST+)*

**To configure VLAN as primary root:**

Conf t

Spanning-tree vlan # root primary

**To configure a VLAN as root secondary:**

Conf t

Spanning-tree vlan # root secondary

**To change path cost of a VLAN interface:**

Conf t

Int \*int name\*

Span vlan # cost #

**To check this…**

Do sh spanning-tree vlan #

**To configure a port priority:**

Conf t

Int \*int name\*

Span vlan # port-priority #

**To configure PortFast and BPDU Guard:**

Conf t

Int \*int name\*

Spanning-tree portfast

Spanning-tree bpduguard enable

**To remove BPDU guard:**

On interface…

Conf t

Shutdown

No shutdown

*Lab 22: Rapid STP*

**To configure interface link type to point-to-point:**

Int \*int name\* or int \*int range\*

Spanning-tree link-type point-to-point

*Lab 23: Ether Channel*

**Configure interface for EtherChannel on Switch**

en

Conf t

Int range g\*# - #\*

Channel-group 1 mode \*active/passive\*

**Configure interface as a trunk on switch**

Int \*int #\*

Switchport mode trunk

**If receive message “interface whose trunk encapsulatio nis “auto” can not be configured to trunk mode**

Switchport trunk encapsulation dot1q

Switchport mode trunk

**To check switches running configuration**

Do sh run

**To check status of etherchannel**

Do sh etherchannel summary

If can see (SU) and in port channel, configured correctly.

**To check trunk interface**

Do sh interface trunk

**Configuration of etherchannel with desirable mode (PAGP version)**

En

Conf t

int -range \*#\*

Channel-group 1 mode desirable

**To configure the port channel interface on a switch**

Int \*#\*

Switchport mode trunk

**To make ports on a ether channel routed ports**

Int range \*#\*

No switchport

**To configure ports when using static ether channel**

Channel-group \*#\* mode on

**To configure an IP address on a port channel**

Int \*#\*

Ip add \*ip address\* \*subnet mask\*

**To configure static routes so PCs can reach SRV**

**Enable ip routing with**

En

Ip routing

Do sh ip route

**Configure a static route to a subnet**

Ip route \*ip and subnet mask\* \*next hop address\*

Do sh ip route

Then ping address, beware of arp

**Check default EtherLoad balance method on a switch**

Do sh etherchannel load-balance

**To configure laid balance method**

port -channel load-balance src-dst-ip

Do sh etherchannel load-balance

*Lab 24: Floating Static Routes*

**To check routing tables of a router**

En

Sh ip route

**Configure a floating static route on a router**

Conf t

Ip route \*dest network\* \*mask\* \*next hop\* ?

To make floating static route set AD higher than static route OSPF

Ip route \*dest network\*\*mask\*\*next hop\* \*ad value\*

Do sh ip route

Route will not appear yet

**To configure backup route on another router**

Conf t

Ip route \*ip\*\*mask\*\* next hop\*\*AD number\*

Do sh ip route

Route will not appear yet

**Shutdown interface of OSPF route**

Int \*int #\*

Shutdown

Do sh ip route

Then ping new route… to get ARP complete

**To check path traffic takes**

Tracert \*dest address\*

Like ping, but every third step in travel sends message back to interface

*Lab 25: EIGRP Configuration*

**To configure a loop back interface on a router**

En

Show ip int br (to see configured int)

Conf t

Interface ?

Loopback ?

To check numerical range

Loopback 0

**Now configure ip address**

Ip address \*ip\* \*mask\*

**To check above**

Do sh ip int br

Loopback int always up/up unless changed

**To configure EIGRP on a router**

Router eigrp \*autonomous system #\*

Network 0.0.0.0 255.255.255.255 (this will conf on all interfaces in Network)

Do sh ip protocols

No auto-summary (to turn auto network summarisation)

**To configure passive interfaces**

Passive-interface \*int #\*

**To go into eigrp config mode**

Router eigrp \*#\*

To get more info about eigrp routes, not just in routing table

**Do sh ip eigrp topology**

*Lab 26: Configuring OSPF (1)*

**To configure a loopback interface on router**

En

Conf t

Int l0

Ip address \*ip\*\*mask\*

Do sh ip int \*l0/br\*

**To apply OSPF to all interfaces globally**

Router ospf \*R #\*

Net 0.0.0.0 255.255.255.255 area 0

**To configure passive interfaces**

Passive-interface \*int #\*

Passive-interface l0

**To configure a router as ASBR that advertises default route in OSPF**

En

Ip route \*0.0.0.0 0.0.0.0\* \*next hop ip\*

Exit

Show ip protocols

**To view LSD (link state database)**

Show ospf database

**To view a router’s OSPF neighbours**

Show ip ospf neighbor

**To view ip ospf interface**

Show ip ospf interface

**To check routing tables of routers**

do sh ip route

*Lab 27: Configuring OSPF (2)*

**To enable OSPF directly on each interface of router**

En

Conf t

Interface range \*int range\* NOTE - if different interface speeds, split with comma

Ip ospf \*int#\* area \*area #\*

Do sh ip proto

**To configure passive interfaces as appropriate**

Router ospf \*int#\*

Passive-interface default

Passive-interface \*int#\*

**To remove a passive interface**

No passive-interface \*int #\*

**To configure reference bandwidth so FastEth interface has cost of 100 on router**

Auto-cost reference-bandwidth \*ref bandwidth\*

Auto-cost reference-bandwidth \*10000\* (as 10,000 / 100 = 1)

**To configure a router as an ASBR that advertises fault route in OSPF domain**

Default-information originate

Exit

Ip route 0.0.0.0 0.0.0.0 \*internet service providers router address\* 203.0.112.2

*Lab 28: Configuring OSPF (3)*

Command Line Interface:

Notes:

Device> = user EXEC mode

Device# = privileged EXEC mode

Device (config)# = global configuration mode

COMMANDS:

“ “

*DEVICE CONFIGURATION:*

**User exec mode:** For looking at details, not configuring

**Configure terminal:** enter global configuration mode

**Enable:** privileged exec mode, configuration of devices

**Enable password \*password\*:** to create secret in global config mode

**Show running-config:** Shows running configuration of device

**Write command:**Save a configuration

**Write memory command:**Save a configuration

**Copy running-config startup-config:** Save a configuration

**Service password-encryption:** encrypts the enable password 7

**Enable secret \*password\*:** enable secret 5

**Do sh run command:** followed “enable secret cisco” to enable secret 5

**No:** typed in front of a command to cancel it. E.g. “no service password-encryption”

**Run privileged-exec-level-command:** executes privileged-exec level command from GCM

**Show startup-config:** displays saved config file which will be loaded on device restart

**Ping 127.0.0.0 - 127.255.255.255:** test network stack on local device

**Show ip interface brief:** list interfaces and their details

**Interface \*interface name\*:** interface configuration mode

**Show ip int br:** display IP interface

**Show interfaces status:** displays details of interface(s)

**Conf t:**

**Int \*interface number\*:**

**Speed ?:** V

**Speed x:** V

**Duplex ?:** V

**Duplex full:** Set device speed AND duplex

**## \*desired device name\* ##:** set device name

**\*interface range\* (\*int number\*/ range x - x):** Set range of multiple interfaces to configure

**## not in use ##:** Set device description for multiple of interfaces

**Shutdown:** Shutdown multiple interfaces

*ROUTER CONFIGURATION:*

**Conf t:** v

**Interface \*int number\*:** V

**\*ip address\*:** V

**No shutdown:** V

**Interface \*int number\*:** configure a router with ip addresses

**Show ip int br:** confirm router configuration

**Show ip route:** show router’s routing table, diff protocol routers can use to learn routes

**Ip route \*sender ip address and subnet mask\* \*next-hop ip address\*:** V

**Do show ip route:** static route configuration

**Ip route \*ip address and subnet mask\* exit-interface:** V

**Ip route \*ip address and subnet mask\* exit-interface next-hop:** V

**Do show ip route:** static route configuration with exit-interface

*VLAN CONFIGURATION:*

**Show vlan brief:** configuration interface for a VLAN

**Interface range \*int number\* (range 0-x):** V

**Switchport mode access:** V

**Switchport mode access vlan x:** assign interfaces to VLAN

**Do show vlan brief:** go to config interface after assigning interfaces/confirm interface

**#vlan:** V

**#name:** general configuration settings to config for new interfaces

**Switchport trunk encapsulation dot1q:** V

**Switchport mode trunk:** configure trunk ports

**Switchport trunk allowed vlan:** allow vlan interface on trunk

**Do show interfaces trunk**: show trunk configurations

**Switchport trunk allowed vlan remove \*vlan number\*:** remove vlan from trunk

**Switchport trunk allowed vlan all:** allow all vlans on trunk

**Switchport trunk allowed vlan except \*vlan int numbers(eg 1-5, 10):** allow x vlans trunk

**Switchport trunk allowed vlan none:** remove all vlans from trunk

*ROUTER ON A STICK (ROAS) CONFIGURATIONS:*

**Interface \*int number\*:** show router interface

**No shutdown:** prevent shutdown of interface

**Interface \*int number\*/\*vlan number\* (e.g. g0/0.10):** specify vlan interface

**Encapsulation dot1q \*vlan number\* (e.g. 10):** specify interface to configure

**Ip address \*ip address and subnet mask\*:** configure vlan with ip address

**Show ip interface brief:** show interface of configured vlan ips

*NATIVE VLAN CONFIGURATIONS:*

ROUTER:

Method 1:

**Int \*int number/vlan number\* (e.g. int g0/0.10):** enable subif (sub interface) mode

**Encapsulation dot1q \*vlan number (e.g. 10)\* native:** make vlan native on router

Method 2:

**No interface \*int number/vlan number\*:** V

**Interface \*int number/vlan number\*:** V

**Ip address \*ip address and subnet mask\*:** configure native IP for vlan

*MULTILAYER (L3) SWITCH CONFIGURATIONS:*

ROUTER END:

**No interface \*int number/vlan number\* (e.g. g0/0.10):** remove subinterfaces

**Default interface \*int number/vlan number\*:** restore default int settings

**Show ip interface brief:** See interfaces, look at status

**Interface \*int number\*:** V

**Ip address \*ip address and subnet mask\*:** V

**Do show ip interface brief:** configure new interface and check it

SWITCH END:

**Default interface \*int number/vlan number\*:** restore default int settings

**Ip routing:** enable layer 3 routing on switch

**Interface \*int number\*:** V

**No switchport:** configure interface as ‘routed port’ (layer 3 port)

**Ip address \*ip address and subnet mask\*:** V

**Do show ip interface brief:** Configure IP address on interface and check it

**Ip route 0.0.0.0.0.0.0.0 \*next-hop ip address\*:** V

**Show ip route:** show final details of ip address configuration

SVI CONFIGURATIONS:

**Interface vlan\*vlan number\* (e.g. vlan10):** V

**Ip address \*ip address and subnet mask\*:** V

**No shutdown:** configure SVI

*DYNAMIC TRUNKING PROTOCOL CONFIGURATIONS:*

**Show interfaces g0/0 switchport:** see switchport configuration interface

**Switchport trunk encapsulation negotiate:** enable trunk encapsulation

**Show vtp status:** open status configurations for vtp

**Vtp domain \*name\*:** change domain name

**Vlan \*vlan number\*:** create vlan

**Name \*name\*:** assign vlan name

**Vtp mode client:** set device to vtp client mode for vlans

**Vtp mode transparent:** set device to vtp transparent mode for vlans

**Vtp version \*version number\*:** change vtp version number

*SPANNING TREE PROTOCOL*

**Spanning-tree portfast:** configure portfast

**Spanning-tree portfast default:** enable portfast on all access ports EXCEPT trunk ports

**Spanning-tree bpduguard enable:** enable bpdu guard

**Spanning-tree portfast bpduguard default:** enable bpdu guard on all portfast enabled interfaces

**Spanning-tree mode ?:** see spanning tree modes

**Spanning-tree mode pvst:** see spanning tree configurations

**Spanning-tree vlan 1 root primary:** set root bridge

**Do show spanning-tree:** see spanning tree configs

**Spanning-tree vlan 1 root secondary:** set secondary root bridge

**Spanning-tree mode pvst:** V

**Spanning-tree extend system-id:** V

**spanning -tree vlan 1 priority #(e.g. 28672):** set root bridge priority

**Spanning-tree vlan \*vlan #\* root primary:** V

**Spanning-tree vlan \*vlan #\* root secondary:** set vlans on a switch

Configuring STP ports:

**Spanning-tree vlan \*vlan #\*:** access vlan interface for STP

**Spanning-tree vlan \*vlan #\* cost \*cost number\*:** set root cost

**Spanning-tree vlan \*vlan #\* port-priority \*priority number\*:** set port-priority number

*RAPID SPANNING TREE PROTOCOL*

**Spanning-tree mode rapid-pvst:** enter rapid psvt mode

**Spanning-tree portfast:** configure edge link

**Spanning-tree link-type point-to-point:** configure connection as point-to-point RSTP link

**Spanning-tree link-type shared:** configure connection as shared RSTP link

*ETHER CHANNEL*

**ASW1# Show etherchannel load-balance:** show load balancing configuration

**ASW1(config)# Port-channel load-balance \*method\* (eg. src-dst-mac):** change load balancing method

**ASW1(config)# do show etherchannel load-balance:** show load balancing config

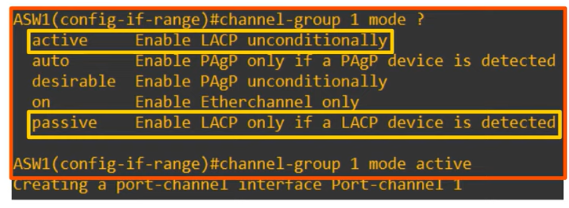
PAgP (Port Aggregation protocol) ether channel configuration:

**ASW1(config)# interface range \*range\* (ex. g0/0 - 3):** select interfaces

**ASW1(config-if-range)# channel-group 1 mode ?:** see options for etherchannel config modes

**ASW1(config-if-range)# channel-group 1 mode \*mode type\* (ex. desirable):** select mode type for channel

LACP (Link Aggregation Control protocol) ether channel configuration:



Static Etherchannel Configuration:

**ASW1(config-if-range)# channel-protocol ?**

**ASW1(config-if-range)# channel-group 1 mode active**

EtherChannel trunk Configuration:

**ASW1(config-if-range)# interface port-channel 1**

**ASW1(config-if-range)# switchport trunk encapsulation dot1q**

**ASW1(config-if-range)# switchport mode trunk**

**ASW1(config-if-range)# do show interfaces trunk**

**ASW1# show etherchannel summary:** see summary of EtherChannel

Change a port to down:

**ASW1(config)# interface \*interface #\***

**AW1(config-if)# shutdown**

Change a port mode:

**ASW1(config)# interface \*interface number\***

**ASW1(config-if)# switchport mode \*mode type\* (e.g. access)**

Configure a Layer 3 Ether Channel:

**Int range \*interface range\***

**No switchport**

**Channel-group 1 mode active**

Configure IP address on Layer 3 Port Channel:

**Int po1**

**Ip address \*ip address\* \*subnet mask\***

**Do sh etherch sum**

*DYNAMIC ROUTING*

*PRE-EXISTING COMMAND LIST*

**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 startup configuration)

**show ip protocol** (what routing protocol, which networks, passive interfaces, neighbors)

**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 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)

**Line editing 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 ping or trace)

**terminal length 0** [zero] (turn off paging – makes output without breaks)

**terminal length 24** (normal page breaks in output)

**wr** (shortcut for ‘copy running-config startup-config)

**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) [Note: Only do this on a switch]

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-config startup-config** (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)# **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)# **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 Mgt interface)

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

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)# **clock rate CLOCK** (on serial DCE interfaces, set the speed of the link)

R1(config-if)# **bandwidth VALUE** (used by the routing protocol for the speed of the link)

R1(config-if)# **no shutdown** (turn the interface on)

R1(config-if)# **shutdown** (turn the interface off)

**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)

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)

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** (set VLAN 99 to carry native traffic)

S1(config-if)# **switchport trunk allowed vlan 1,10,20,99** (optional, 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 172.16.10.1 255.255.255.255** (define 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)

R1(config)# **ip classless** (classless routing behavior – default in IOS 11.3+)

R1(config)# **no ip classless** (classful routing behavior)

**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** (set this interface to LACP portchannel) -or--

S1(config-if)# **channel-protocol pagp** (set this interface to PAgP portchannel)

S1(config-if)#in **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)

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)# **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)# **standby version 2** (use the same version at each end)

R1(config-if)# **standby** [optional **group#**] **ip** [optional **IP-ADDRESS**] [optional **secondary**]

(The other end is configured the same)

R1(config-if)# **standby** [optional **group#**] **priority NUMBER** [optional **preempt**]

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

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

**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)

(The other end is configured the same)

R1(config-if)# **standby GROUP# priority NUMBER** [optional **preempt**]

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

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 - select 1024 bits)

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

R1(config)# **line vty 0 15** (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)

**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 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 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# **errdisable recovery cause psecure\_violation** (restore shutdown interfaces in 5 min)

S1# **show port-security interface fa0/12** (show security configuration for an interface)

**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)

**IP DHCP Snooping**

R1(config)# **ip dhcp snooping** (globally enable DHCP snooping)

R1(config-if)# **ip dhcp snooping trust** (interface with DHCP server)

Routing (Static, RIP, EIGRP, OSPF)

**Configuring 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 serial 0/1)

R1(config)# **ip route 47.151.2.0 255.255.255.0 192.168.12.2 fastethernet0/0** (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)

**Configuring RIP (IPv4)**

R1(config)# **no router rip** (remove all RIP configurations and routing table entries)

R1(config)# **router rip** (enter rip configuration commands)

R1(config-router)# **network 192.168.10.0** (define which directly connected network(s) to include in RIP update processes. No subnet mask – always classful)

R1(config-router)# **passive-interface fastethernet0/0** (prevent RIP updates from broadcasting out this interface)

R1(config-router)# **default-information originate** (configure RIP to include default-routes in updates to other routers. This is disabled by default. Only on router with default-route)

R1(config-router)# **redistribute static** (configure RIP to include classful static routes in updates to other routers. This is disabled by default. Only needed if there are static routes)

R1# **debug ip rip** (examine RIP updates in real-time)

**Additional Commands to configure RIP Version 2**

R1(config-router)# **version 2** (configure RIP for RIPv2)

R1(config-router)# **no auto-summary** (turn off automatic classful summarization- suggested)

**Configuring RIPng (for IPv6)**

R1(config)# **ipv6 route ::/0 S0/0/1** (default route goes out S0/0/1)

R1(config)# **ipv6 router rip NAME** (start the RIPng instance)

R1(config)# **interface fa0/1**

R1(config-if)# **ipv6 rip NAME enable** (include this interface and subnet in routing)

R1(config-if)# **ipv6 rip NAME default-information originate** (send default route

**Configuring IPv4 EIGRP**

R1(config)# **no router eigrp 100** (completely remove this instance of EIGRP in this router)

R1(config)# **router eigrp 100** (100=Process ID within this network – Cisco calls this Autonomous System)

R1(config)# **eigrp router-id 5.5.5.5** (use this ID when identifying EIGRP neighbors)

R1(config-router)# **no auto-summary** (the default is to summarize to classful boundaries)

R1(config-router)# **network 172.16.0.0** (no subnet or wildcard mask is needed if classful)

R1(config-router)# **network 172.16.25.0 0.0.0.255** (wildcard mask – this is inverse of /24)

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 0/0** (no routing updates out Fa0/0)

R1(config-router)# **redistribute static** (one statement redistributes static routes - including the default-route)

R1(config-if)# **maximum paths 2** (load balancing paths: default=4, no load balancing=1)

R1(config-router)# **metric weights 0 k1 k2 k3 k4 k5** (used to modify the metric multipliers)

R1(config-if)# **bandwidth 768** (indicate the serial line speed for the routing protocol – this example is 768-K)

R1(config-if)# **ip summary-address eigrp 100 172.16.24.0 255.255.252.0** (manually summarized network statement configured on outbound interface)

R1(config-if)# **ip bandwidth-percent eigrp 100 40** (ex. limit EIGRP AS=100 updates to a max of 40% of link bandwidth)

R1(config-if)# **ip hello-interval eigrp 100 30** (ex. set hello intervals on this interface to 30s for EIGRP AS=100)

R1(config-if)# **ip hold-time eigrp 100 90** (in this example, set the hold-time on this interface to 90s for EIGRP AS=100)

R1(config)# **key chain MYCHAIN** (name the key chain – done in global config)

R1(config-keychain)# **key 1** (must assign a number – same at both ends of link)

R1(config-keychain-key)# **key-string securetraffic** (‘securetraffic’ is the passphrase)

R1(config)# **interface serial 0/1** (interface to the other EIGRP router)

R1(config-subif)# **ip authentication mode eigrp 10 md5** (turn on authentication)

R1(config-subif)# **ip authentication key-chain eigrp 10 MYCHAIN** (use this key)

R1# **show ip eigrp neighbors** (see neighbor adjacencies)

R1# **show ip eigrp topology** (see the EIGRP topology table)

R1# **debug eigrp fsm** (see what DUAL does when a route is removed from the routing table)

**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)

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)# **area 7 range 172.16.8.0 255.255.248.0** (on ABR summarize addresses)

R1(config-router)# **summary address 172.16.8.0 255.255.248.0** (On ASBR – to summarize non-OSPF routes imported into OSPF)

R1(config-router)# **auto-cost reference-bandwidth ?** (optionally change ref bw - Mbits/s 1-4294967; must be same on all routers)

R1(config-router)# **area AREA-ID authentication message-digest** (globally activate MD-5 authentication within an OSPF area)

R1(config-router)# **ip ospf message-digest-key 1 md5 PASSWORD** (authentication key)

R1(config-if)# **ip ospf message-digest-key 1 md5 PASSWORD** (on this interface, configure the OSPF auth key – will not activate authentication)

R1(config-if)# **ip ospf authentication message-digest** (activate OSPF authentication)

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)

**Configure IPv6 OSPF(v3)**

R1(config)# **ipv6 unicast-routing** (turn on ipv6 routing)

R1(config)# **no ipv6 router ospf 55** (remove this instance of OSPF in this router)

R1(config)# **ipv6 router ospf 100** (create the OSPF process in this router)

R1(config-rtr)# **router-id 5.5.5.5** (must have router id)

R1(config-rtr)# **default-information originate** (redistribute default route to other routers)

R1(config-rtr)# **redistribute static** (redistribute classful static routes, including default)

R1(config-rtr)# **redistribute static subnets** (redistribute classless static routes)

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

R1(config-rtr)# **no passive-interface gi 1/0** (allow updates out this interface)

R1(config-rtr)# **passive-interface gi 1/1** (no routing updates out gi 1/1)

R1(config-rtr)# **no shutdown** (turn it on)

R1(config)# **interface gi 1/1** (networks are assigned through the interface)

R1(config-if)# **ipv6 enable** (allow IPv6 on this interface)

R1(config-if)# **ipv6 ospf 100 area 0** (associate this interface with IPv6 OSPF 55, area 0)

**Configure IPv6 EIGRP**

R1(config)# **ipv6 unicast-routing** (turn on ipv6 routing)

R1(config)# **no ipv6 router eigrp 100** (remove this instance of EIGRP in this router)

R1(config)# **ipv6 router eigrp 100** (create the EIGRP process)

R1(config-rtr)# **eigrp router-id 5.5.5.5** (must have a router id)

R1(config-rtr)# **redistribute static** (redistribute static and default routes to other routers)

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

R1(config-rtr)# **no passive-interface gi 1/0** (allow updates out this interface)

R1(config-rtr)# **passive-interface gi 1/1** (no routing updates out gi 1/1)

R1(config-rtr)# **no shutdown** (must turn on EIGRP in this router)

R1(config)# **interface gi 1/1** (networks are assigned through the interface)

R1(config-if)# **ipv6 enable** (allow IPv6 on this interface)

R1(config-if)# **ipv6 eigrp 100** (associate this interface with IPv6 EIGRP process 100)

R1(config-if)# **ipv6 summary-address eigrp 100 2001:123A:AAA0::/60** (EIGRP summary address)

R1(config-if)# **ipv6 bandwidth-percent eigrp 100 40** (in this example limit EIGRP AS=100 updates to a maximum of 40% of the link bandwidth)

R1(config)# **key chain MYCHAIN** (name the key chain – done in global config)

R1(config-keychain)# **key 1** (must assign a number – same at both ends of link)

R1(config-keychain-key)# **key-string securetraffic** (‘securetraffic’ is the passphrase)

R1(config)# **interface serial 0/1** (interface to the other EIGRP router)

R1(config-subif)# **ipv6 authentication mode eigrp 10 md5** (turn on authentication)

R1(config-subif)# **ipv6 authentication key-chain eigrp 10 MYCHAIN** (use this key)

PPP and Frame-Relay

**Configuring PPP with Authentication**

R1(config)# **username R-2 password PASSWORD** (configure for PAP / CHAP)

* If **PAP**, the username and password must match the sent-username and password from other router.
* If **CHAP**, the username must be the hostname of the other router and the passwords must be the same in each routers username configuration.

R1(config)# **interface serial 0/0/0** (select the interface for ppp configuration)

R1(config-if)# **encapsulation ppp** (set interface to PPP)

R1(config-if)# **compress [predictor / stac]** (optional-configure data compression)

R1(config-if)# **ppp quality [percentage]** (optional-set a threshold of throughput before the ppp link will reset)

R1(config-if)# **ppp authentication pap** (optional-configure for PAP authentication)

R1(config-if)# **ppp pap sent-username R-1 password PASSWORD** (if PAP is used, this must be configured)

R1(config-if)# **ppp authentication chap** (optional-configure for CHAP authentication)

R1(config-if)# **ppp multilink** (optional-combine multiple PPP links for more bandwidth)

R1(config-if)# **encapsulation hdlc** (reset the interface to the default value of HDLC)

**Frame-Relay Commands**

-There are two basic types of Frame-Relay configuration: Point-to-Point and Multi-Point.

-A Point-to-Point link involves a single IP subnet and one DLCI. It may be configured directly on the physical interface or may be done as a sub-interface.

**\*\*FR Point-to-Point no sub-interface; Sample Configuration 1:**

R1(config)# **interface serial 0/0/0**

R1(config-if)# **ip address 192.168.5.1 255.255.255.252** (typically /30)

R1(config-if)# **encapsulation frame-relay [ietf, cisco]** PVC=IEFT is optional, cisco=default)

R1(config-if)# **frame-relay lmi-type [ansi, q933a, cisco]** (optional, cisco=default)

R1(config-if)# **frame-relay map ip 192.168.5.1 752** (to allow local ping- 192.168.5.1 is the local interface IP, DLCI=752 is a valid DLCI for this interface)

R1(config-if)# **frame-relay map ip 192.168.5.2 752 broadcast** [**ietf, cisco]** (192.168.5.2 is next hop, DLCI=752, broadcast is optional, PVC=IEFT is optional – cisco is default)

**\*\*FR Point-to-Point with sub-interface; Sample Configuration 2:**

R1(config)# **interface serial 0/0/0**

R1(config-if)# **no ip address** (no IP address on the main interface)

R1(config-if)# **encapsulation frame-relay** **[ietf, cisco]** PVC=IEFT is optional, cisco=default)

R1(config-if)# **frame-relay lmi-type [ansi, q933a, cisco]** (optional, cisco=default)

R1(config-if)# **interface serial 0/0/0.752 point-to-point** (sub-int # is customarily DLCI #)

R1(config-subif)# **ip address 192.168.5.1 255.255.255.252** (typically /30)

R1(config-subif)# **frame-relay interface-dlci 752** (DLCI=752, next hop and broadcast are dynamically assigned)

-Multi-point configurations are when there is one IP subnet with multiple connections (DLCIs). It may be configured directly on the physical interface or may be done as a sub-interface.

**\*\*Multi-Point no sub-interface; Sample Configuration 3:**

R1(config)# **interface serial 0/0/0**

R1(config-if)# **ip address 192.168.5.1 255.255.255.248** (not /30)

R1(config-if)# **encapsulation frame-relay**

R1(config-if)# **frame-relay lmi-type [ansi, q933a, cisco]** (optional, cisco=default)

R1(config-if)# **frame-relay map ip 192.168.5.1 752** (to allow local ping- 192.168.5.1 is the local interface IP, DLCI=752 is a valid DLCI for this interface)

R1(config-if)# **frame-relay map ip 192.168.5.2 752 broadcast** [**ietf, cisco]** (192.168.5.2 is next hop, DLCI=752, broadcast is optional, PVC=IEFT is optional – cisco is default)

R1(config-if)# **frame-relay map ip 192.168.5.3 339 broadcast** [**ietf, cisco]** (192.168.5.3 is next hop, DLCI=339, broadcast is optional, PVC=IEFT is optional – cisco is default)

**\*\*Multi-Point with sub-interface; Sample Configuration 4:**

R1(config)# **interface serial 0/0/0**

R1(config-if)# **no ip address** (no IP address on the main interface)

R1(config-if)# **encapsulation frame-relay** (not configured on sub-interface)

R1(config-if)# **frame-relay lmi-type [ansi, q933a, cisco]** (optional, cisco=default)

R1(config-if)# **interface serial 0/0/0.752 multipoint** (sub-interface # is customarily DLCI #)

R1(config-subif)# **ip address 192.168.5.1 255.255.255.248** (not /30)

R1(config-subif)# **frame-relay map ip 192.168.5.1 752** (to allow local ping- 192.168.5.1 is the local interface IP, DLCI=752 is a valid DLCI for this interface)

R1(config-subif)# **frame-relay map ip 192.168.5.2 752 broadcast** [**ietf, cisco]** (192.168.5.2 is next hop, DLCI=752, broadcast is optional, PVC=IEFT is optional – cisco is default)

R1(config-subif)# **frame-relay map ip 192.168.5.3 339 broadcast** [**ietf, cisco]** (192.168.5.3 is next hop, DLCI=339, broadcast is optional, PVC=IEFT is optional – cisco is default)

R1# **show frame-relay map** (display mapping of IPs and DLCIs)

Static: Map entry was from a ‘frame-relay map’ statement.

Dynamic: Map entry was created through inverse-ARP.

R1# **show frame-relay lmi** (see status of local link to Frame-Relay cloud)

R1# **show frame-relay pvc** (see which links are actually up end-to-end)

Active: PVC is fully connected and functional.

Inactive: Connected to FR switch, but other side isn’t seen.

Delete: Not talking to the FR switch.

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)

**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… |  |  |  |  |  |  |

There can be additional optional commands (log, time-of-day, established, etc) on the end of most statements. The protocol field must match destination port/protocol - if 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)

**Dynamic Access List (Stateful-Firewall)**

R1(config)# **ip access-list extended OUTBOUND-TRAFFIC**

R1(config-ext-nacl)# **permit tcp any any reflect TCP-TRAFFIC**

R1(config-ext-nacl)# **permit udp any any reflect UDP-TRAFFIC**

R1(config-ext-nacl)# **permit icmp any any reflect ICMP-TRAFFIC**

R1(config-ext-nacl)# **deny ip any any**

R1(config)# **ip access-list extended EVALUATE-INBOUND**

R1(config-ext-nacl)# **evaluate TCP-TRAFFIC**

R1(config-ext-nacl)# **evaluate UDP-TRAFFIC**

R1(config-ext-nacl)# **evaluate ICMP-TRAFFIC**

R1(config)# **interface serial 0/0/0**

R1(config-if)# **ip access-group OUTBOUND-TRAFFIC out**

R1(config-if)# **ip access-group EVALUATE-INBOUND in**

**Time-Based ACL**

R-1(config)# **time-range MON-WED-FRI**

R-1(config-time-range)# **periodic Monday Wednesday Friday 8:00 to 17:00**

R-1(config)# **access-list 133 permit tcp 192.168.20.0 0.0.0.255 any eq telnet time-range** **MON-WED-FRI**

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)

DHCP and NAT

**Configuring DHCP for IPv4**

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** (entire network range)

R-1(dhcp-config)# **default-router 172.16.2.1** (address on router port)

R-1(dhcp-config)# **dns-server 140.198.8.14** (DNS server – can have up to 4)

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 DHCP for IPv6 Stateless Address Auto-Configuration (SLAAC)**

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

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

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

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

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

R1(config-if)# **ipv6 address 2001:A1B5:C13:10::1/64** (configure IPv6 address)

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

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

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

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

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

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

R1(config-if)# **ipv6 address 2001:D7B:CAFE:10::1/64** (configure IPv6 address)

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

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)

R-3(config-if)# **ip dhcp relay destination 2001:A123:7CA1::15** (IPv6 DHCP server address)

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)