***Simplified cheat sheet for all commands:***

**Note: all commands finished? Hit end, copy run start, enter to SAVE!!**

**OSPF:**

Router ospf <ID>

Network <ip> <wildcard mask> area <area ID>

Passive-interface <interface>

Auto-cost reference-bandwidth <value>

Ip ospf cost <value of cost to send traffic to interface>

**Addressing:**

Loopback address:

Int l0

Ip add <ip> <subnet mask>

IPv4:

Int <int>

Ip add <ip> <subnet mask>

No shutdown

IPv4 network (static) route:

Conf t

Ip route <destination network IP> <subnet mask> <next hop interface or IP>

IPv6:

Conf t

Ipv6 unicast-routing

Int <int>

Ipv6 add <ip>

IPv6 network (static) route:

Conf t

Ip route <destination network IP> <subnet mask> <next hop interface or IP>

**VLANs:**

Conf t

Vlan <#>

Name <name>

Int <int>

Switchport mode access

Switchport access vlan <vlan number>

**Trunks:**

Int <int>

Switchport mode trunk

Switchport trunk encapsulation dot1q (if needed)

Switchport trunk allowed vlan <vlan IDs>

Switchport trunk native vlan <vlan ID>

**Port Security:**

Int <int>

Switchport Port-security

Switchport Port-security maximum <# of allowed connections>

Switchport Port-security violation <protect/restrict/shutdown>

Switchport Port-security mac-address sticky (saves learned mac address)

Switchport port-security mac-address <mac> (to configure as a secure MAC)

**EtherChannel:**

Layer 2 EtherChannel:

Int range <int range>

Channel-group <ID> mode <active/passive/auto/desirable/on>

(a cisco proprietary PaGP EtherChannel will use auto or desirable)

(an open-standard protocol, LACP, will use active or passive)

(on is used to enable an EtherChannel, only)

sh etherchannel summary

Int po<id>

Switchport trunk encapsulation dot1q

Switchport mode trunk

Int range <same int range>

No shutdown

Layer 3 EtherChannel:

Conf t

Ip routing

Int range <int range>

Channel-group <id> mode <on>

Int po1

Ip add <ip> <subnet mask>

***CCNA Labs as per Exam Topics Outline:***

**Configure IPv4 addressing and subnetting -**

Ip routing

Int <int number>

Ip address <ip> <mask>

No shutdown

COPY RUN START

Do sh ip route

**Configure and verify IPv6 addressing and prefix -**

Ipv6 unicast-routing

Int <int number>

Ipv6 enable

Ipv6 address <address> eui-64 (optional)

Do wr

Do sh ipv6 int br

**Configure and verify VLANs (Normal range) spanning multiple switches:**

En

Conf t

Vlan <vlan number>

Name <vlan name>

Int <int on switch connected to vlan>

Switchport mode access

Switchport access vlan <vlan number>

Switchport mode trunk

Switchport trunk allowed vlan <allowed vlans>

Do sh vlan br

Do wr

**Configure and verify interswitch connectivity:**

Int <int id of interface to other switch>  
Switchport trunk encapsulation <dot1q/isl>

Switchport mode trunk

Switchport trunk allowed vlan <allowed vlans>

Do sh vlan br

Do wr

**Configure and verify L2 discovery protocols (CDP and LLDP):**

En

Sh cdp neigh

Sh controllers <int> \*find which is dce side of connection\*

Conf t

Int <int>

Clock rate <value>

Sh cdp interface

Cdp run

No cdp run \*will disable globally\* or if dont in int-config will do for interfaces\*

Sh cdp neigh detail

Sh version

Do wr

LLDP:

En

Conf t

No cdp run

Lldp run

Sh lldp

Sh lldp neighbors

Sh lldp neigh detail

Int <int>

No lldp ?

no lldp receive

No lldp transmit

Do wr

**Configure and verify L2 and L3 EtherChannel (LACP):**

En

Sh spanning-tree

Conf t

Int range <ints>

Channel-group ?

Channel-group <number, 1> mode ?

Channel-group <number> mode <mode> (active/passive for lacp)

Int po1

Switchport mode trunk

Do sh eth sum

L3 etherchannel:

Int range <range>

No switchport

Channel-group <number> mode ? on

Int po <number>

Ip add <ip> <subnet mask>

Do sh eth ch summ

**Configure and verify IPv4 and IPv6 static routing:**

En

Conf t

Int <int>

Ip add <ip> <subnet mask>

No shutdown

Loopback address:

Int loopback 0

Ip add <ip> <subnet>

Static routing:

Configure interfaces first…

En

Conf t

Int <int>

Ip add <ip> <mask> ?

Ip add <ip> <mask> <next hop ip>

Do sh ip route

s\* = static

Floating static route:

Ip add <ip> <mask> <AD - higher than protocol>

**Configure and verify single area OSPFv2:**

Sh run - see ip addresses on interfaces

Router ospf <version number (1)>

Network <ip address> <wildcard mask> area <area #>

Configure loopback address:

Int lo0

Ip address <ip> <subnet mask>

**Configure and verify inside source NAT using static and pools:**

En

Conf t

Int <int>

Ip nat inside (side facing switch)

int< int>

Ip nat outside (side facing internet)

Exit

Ip nat inside source static <inside ip of host ip, outside ip>

**Configure and verify NTP in client and server mode:**

ntp

En

Sh clock

Sh clock detail

Conf t

Clock timezone <zone> <time>

Clock set ?

Clock set <time - hh:mm:ss> <date - month day year>

Ntp ?

Ntp master 8 (default)

Ntp server <ip address of peer>

Ntp authentication-key <number> md5 <password>

Ntp trusted-key <corresponding number>

Copy run start

**Configure and verify DHCP client and relay:**

En

Conf t

Ip dhcp pool <name>

Network <ip address> <subnet mask>

Default-router <ip>

Dns-server <ip>

Exit

Ip dhcp excluded-address <ip range ip ip>

Int <int>

Ip address dhcp

No shut

Ip helper-address <ip>

**Configure network devices for remote access using SSH:**

On SSH server (ROUTER):

Hostname <hostname>

Ip domain-name <domain name>

Crypto key generate rsa

\*specify number of bits, usually 2048\*

Ip ssh version 2

Line vty 0 4

Transport input ssh

Login local

Username <username> password <password>

On SSH client (router or switch):

Hostname <hostname>

Login local

Username <username> password <password>

Ip domain-name <domain name>

Crypto key generate rsa

Ip ssh time-out <value>

Ip ssh authentication-retries <value>

Line vty 0 4

Transport input ssh

To prevent non telnet connections:

Line vty 0 4

Transport input ssh

**Configure and verify device access control using local passwords:**

Enable Password <password>

Enable secret <secret password>

Service password-encryption

Show running-config

**Configure and verify ACLs:**

Standard ACLs 1-99 1300-1999, configured as close to destination as possible

En

Conf t

Access-list ?

Access-list <number - 1-99> ?

Access-list <number> <permit/deny> <any/ individual ip> <wildcard>

Do sh acc

Int <int>

Ip access-group <number of ACL> <in/out - depending on traffic is coming into int or out of>

Extended ACL:

Access-list <number> ?

Access-list <number> permit ip host <host ip>

Access-list <number> deny ip any host <host ip>

**Configure and verify L2 security features (DHCP snooping, Dynamic ARP inspection, port security):**

Port security:

En

Sh mac address-table

Conf t

Int <int>

Switchport mode access

Switchport port-security \*wont work on trunk port, only access\*

To configure number of MAC-addresses allowed in interface:

Switchport port-security maximum 1

Port security violation:

Switchport port-security violation ?

Int <int>

Switchport-port security mac-address sticky

Copy run start

**Dynamic arp inspection…**

En

Conf t

Ip arp inspection vlan <vlan number>

**DHCP snooping…**

En

Conf t

Ip dhcp snooping

**Configure and verify WLAN within GUI using WPA2 PSK:**

Jeremy’s IT LAB practice:

Vlan configuration:

**On switch interfaces hosts are connected to…**

En

Conf t

Int <int>

Switchport mode access

Switchport access vlan <vlan number>

End

Copy run start

**Configure interfaces as trunk interfaces… (interfaces between switches)**

En

Conf t

Int <int>

Switchport mode trunk

**Configuring trunk with q encapsulation…**

Int <int>

Switchport trunk encapsulation dot1q

Switchport mode trunk

End

Copy run start

**Naming VLANs…**

En

Sh vlan

Sh vlan br

Conf t

Vlan <vlan number>

Name <name>

**Configure cdp:**

Show cdp neighbors

**Change clock rate…**

En

Conf t

Int <int>

Clock rate <rate>

**To see cdp timers…**

Sh cdp interfaces

**enable/disable cdp…**

En

Conf t

Cdp run/no cdp run

**To enable on interface…**

Int <int>

Cdp enable/no cdp enable

**Ipv4 address…**

En

Conf t

Int <int>

Ip address <ip> <subnet mask>

No shutdown

**Configure loopback interface…**

Int L0

Ip address <ip> <subnet mask> (usually something like 1.1.1.1 255.255.255.255

**Port security…**

En

Conf t

Int <int>

Switchport mode access

Switchport port-security

Set max number of addresses…(default is 1)...

En

Conf t

Int <int>

Switchport mode access

Switchport port-security

Switchport port-security maximum <number>

**Change port-security violation mode…**

Protect: increase violation counter

Restrict: drops packet, increased violation counter, sends message

Shutdown: shutdown interface and increases counter

En

Conf t

Int <int>

Switchport mode access

Switchport port-security

Switchport port-security maximum <number>

Switchport port-security violation <violation mode>

Copy run start

**To enable sticky addressing…**

En

Conf t

Int <int>

Switchport port-security mac-address sticky

Sh port-security address

**Configure VTY lines…**

Sh run

En

Conf t

Line vty 0 15

Login local (if username and password configured)

Transport input <input type>

Copy run start

**Telnet to a device…**

Telnet <ip>

**Generate keys used to encrypt SSH packets…**

Crypto key generate rsa

<enter size>

En

Conf t

Line vty 0 15

Login local

Transport input <type> (ssh)

Exec-timeout <time unit>

**Connect to device via ssh…**

Ssh -l cisco <ip>

**To create a static route…**

En

Conf t

Ip route <destination ip> <subnet mask> <next hop address OR next hop interface>

Do sh ip route

**Standard ACL creation…**

En

Conf t

Access-list <number> <permit/deny> <ip address/any source> <wildcard mask>

**(if creating a deny access list, must apply follow command…)**

Access-list <number> permit any

**Create extended access list…**

En

Conf t

Access-list <number> permit/deny <type (ip host)> <ip> <network>

Access-list <number> deny/permit <type (ip host)> <ip>

**NTP configuration…**

En

Sh clock

Sh clock detail

Conf t

Clock timezone ?

Clock set ?

**Set router as ntp server…**

En

Conf t

Ntp master <number (default 8, lower better)>

**Configure ntp client for router…**

En

Conf t

Clock time ?

Ntp server <ip of server>

Exit

Copy run start

**Create authentication key for NTP**

En

Conf t

Clock time ?

Ntp authenticate

Ntp authentication-key <number> md5 <password>

Ntp trusted-key <number corresponding>

Ntp server <ip of server> key <corresponding number>

**Configure LLDP…**

En

Conf t

Int <int>

No cdp run (enabled by default)

Lldp run

Sh lldp

Sh lldp neighbors

**To disable lldp…**

En

Conf t

Int <int>

No lldp receive

No lldp transmit

**Configure DHCP server…**

En

Conf t

Ip dhcp pool <name>

Network <range of addresses ip> <subnet mask>

Default-router <ip address>

Dns-server <ip address>

Exit

Ip dhcp excluded-address <first ip of range> <last ip of range>

**Configure dhcp on interface as client…**

En

Conf t

Int <int>

Ip address dhcp

No shutdown

**Configure dhcp relay agent on interface (closest to host)...**

En

Conf t

Int <int>

Ip helper-address <dhcp server ip address>

Exit

**Etherchannel L2…**

En

Sh spanning-tree

Conf t

Int range <range>

Channel-group <number (usually 1)> mode ? <desirable,etc>

Int po1

Switchport mode trunk

(**encapsulation may need to be configured first)...**

En

Conf t

Int range <range>

Channel-group <number> mode <mode>

Int po2

Switchport trunk encapsulation dot1q

Switchport mode trunk

Int range <range>

No shutdown

Exit

Sh eth summary

**Etherchannel L3…**

En

Conf t

Ip routing

Int range <range>

No switchport

Channel-group <number> mode <on>

Int po <number correlating, (usually 1)>

Ip add <ip> <subnet mask>

**OSPF single area…**

En

Conf t

Router ospf <process ID, usually 1>

Network <ip address> <wildcard mask> <area # (usually 0)>

Do sh ip ospf neighbor

Do sh ip route

Copy run start

**Change reference bandwidth…**

Conf t

Auto-cost reference-bandwidth <value>

Do sh ip route

**On interface…**

Int <int>

Ip ospf cost <value>

Do sh ip route

Hostname R1

Ip domain-name cisco.com

Username cisco password ccna

Crypto key generate rsa

1024

Line vty 0 15

Login local

Transport input ssh

Exit

Hostname R1

Ip domain-name <domain name>

Username <un> password <pw>

Crypto key generate rsa

1024

Line vty 0 15

Login local

Transport input ssh

Ip ssh ver 2

Copy run start

**On host…**

Ssh -1 cisco <ip>

Ip dhcp excluded-address <ip> to <ip>

Ip dhcp pool <name>

Network <ip> <subnet mask>

Default-router <ip>

Dns-server <ip>

Exit

Ip dhcp excluded-address <ip> to <ip>

Ip dhcp pool <pool name>

Network <ip>

Default-router <ip>

Dns-server <ip>

exit

En

Conf t

Ip route ?

Ip route 0.0.0.0 0.0.0.0 ?

Ip route 0.0.0.0 00.0.0 <int>

Router ospf <number, 1>

Network <ip> <wildcard mask> area <number, 0>

Exit

Sh ip ospf neigh

**Jeremys it lab solutions:**

Basic serial connection configurations…

En

Sh cdp neighbors

On r1:

Int s0

Ip address 192.168.0.1 255.255.255.0

On r2:

En

Conf t

Int s0

Ip address 192.168.0.2 255.255.255.0

End

Ping 192.168.0.1

VLAN configuration…

On sw1..

Int f0/3

Switchport mode access

Switchport access vlan 2

Exit

Int f0/1

Switchport trunk encapsulation dot1q

Switchport mode trunk

On sw2…

Int f0/2

Switchport mode access

Switchport access vlan 2

Exit

Int f0/1

Switchport trunk encapsulation dot1q

Switchport mode trunk

Standard ACLs…

On r2…

En

Conf t

Access-list 1 permit 192.168.1.0 0.0.0.255

Do sh acc

Int f0/0

Ip access-group 1 out

End

Copy run start

On r1…

En

Conf t

Access-list 1 deny host 192.168.2.14

access-list 1 permit any

Exit

Int f0/0

Ip access-group 1 out

End

Copy run start

Example scenarios - Jeremy’s MEGA Lab:

“Configure hostnames on switches and routers, enable the secret   
**Jeremysitlab** on all network devices, using type 9 hashing if available, otherwise type 5.

Then, configure a user account with the username **“cisco”** and password **“ccna”**, again using type 9 hashing if available, otherwise type 5.

Lastly, configure the console line to require login with a local user account, set the inactivity timer to 30 minutes, and enable synchronous logging”

*Firstly, only layer 3 switches can handle type 9 hashing.*

*On routers and L2 switches (access switches):*

*En*

*Conf t*

*Hostname <hostname designated>*

*Enable secret jeremysitlab*

*Username cisco secret ccna*

*Line con 0*

*Login local*

*Exec-timeout 30*

*Logging synchronous*

*Exit*

*Exit*

*Copy run start*

*On L3 switches:*

*En*

*Conf t*

*Hostname <designated hostname>*

*Enable algorithm-type scrypt secret jeremysitlab*

*Username cisco algorithm-type scrypt secret ccna*

*Line con 0*

*Login local*

*Exec-timeout 30*

*Logging synchronous*

*End*

*En*

*Copy run start*

“Two offices. In office A, a L2 port channel 1 between DSWA1 and DSWA2 using a cisco prop. Protocol must be configured. Both switches should be actively trying to form an etherchannel.

In Office B, configure a L2 PortChannel1 between DSWB1 and DSWB2 using an open standard protocol. Both switches should be actively trying to form an EtherChannel.

*For office A:*

*On DSWA1:*

*En*

*Conf t*

*Do sh cdp neighbors (to see interfaces)*

*Int range g1/0/4-5*

*Channel-group 1 mode desirable/auto*

*On DSWA2:*

*En*

*Conf t*

*Int range g1/0/4-5*

*Channel-group 1 mode desirable/auto*

*Do sh etherchannel summary (to check)*

*For Office B*

*On DSWB1:*

*En*

*Conf t*

*Do sh cdp neighbors*

*Int range g1/0/4-5*

*Channel-group 1 mode active*

*On DSWB2:*

*En*

*Conf t*

*Int range g1/0/4-5*

*Channel-group 1 mode active*

*Do sh etherchannel summary*

Configure all links between Access and Distribution Switches, including the EtherChannels, as trunk links. Disable DTP on all ports, set each trunk’s native vlan to vlan 1000 (unused) and in office A, allow vlans 10, 20, 40 and 99 on all trunks. In office B allow vlans 10, 20, 30 and 99 on all trunks.”

*For Office A:*

*On DSWA1 and A2:*

*Do sh cdp neighbors*

*(confirm interfaces needing to be trunks)*

*Int range g1/0/1-3*

*Switchport mode trunk*

*Switchport nonegotiate*

*Switchport trunk native vlan 1000*

*Switchport trunk allowed vlan 10,20,40,99*

*Int po1*

*Switchport mode trunk*

*Switchport nonegotiate*

*Switchport trunk native vlan 1000*

*Switchport trunk allowed vlan 10,20,40,99*

*Exit*

*En*

*Copy run start*

*For Office B:*

*On DSWB1 and B2:*

*Do sh cdp neighbors*

*(confirm interfaces needing to be trunks)*

*Int range g1/0/1-3*

*Switchport mode trunk*

*Switchport nonegotiate*

*Switchport trunk native vlan 1000*

*Switchport trunk allowed vlan 10,20,30,99*

*Int po1*

*Switchport mode trunk*

*Switchport nonegotiate*

*Switchport trunk native vlan 1000*

*Switchport trunk allowed vlan 10,20,30,99*

*Exit*

*En*

*Copy run start*

Office A needs the following VLANs to be created on its distribution switches; vlan 10 - PCs, vlan 20 - Phones, vlan 40 - wifi, vlan 99 - management.  
  
Office B needs; vlan 10 - PCs, vlan 20 - phones, vlan 30 - servers, vlan 99 - management.

All changes must be propagated by VTP

*Office A, DSWA1:*

*En*

*Conf t*

*Do sh vtp status*

*Vtp domain <domain name, JeremysITLab>*

*Vtp version 2*

*On access switches (ASWA1, etc):*

*En*

*Conf t*

*Vtp mode client*

*Office B, DSWB1:*

*En*

*Conf t*

*Do sh vtp status*

*Vtp domain <name, JeremysITLab>*

*Vtp version 2*

*On access switches (ASWB1, etc):*

*En*

*Conf t*

*Vtp mode client*

*Do sh vtp status*

*Copy run start on all*

*Office A VLAN configs, ASWA1:*

*En*

*Conf t*

*Vlan 10*

*Name PCs*

*Vlan 20*

*Name phones*

*Vlan 40*

*Name wifi*

*Vlan 99*

*Name management*

*Exit*

*Do sh vlan br*

*Confirm vtp working by issuing do sh vtp neigh on access switches*

*Office B, DSWB1:*

*En*

*Conf t*

*Vlan 10*

*Name PCs*

*Vlan 20*

*Name phones*

*Vlan 30*

*Name servers*

*Vlan 99*

*Name management*

*Exit*

*Do sh vlan br*

*Confirm vtp working by issuing do sh vtp neigh on access switches*

Configure each Access switch’s access port, ensuring LWAPs are not using Flex Connect and putting PCs in VLAN 10, Phones in VLAN 20, and SRV1 in VLAN 30

Then, manually configure access mode and disable DTP

Configure ASW-A1s connection to WLC so that it supports wifi and management vlans, with the management vlan being untagged (native), and DTP disabled.”

*For office A, ASWA1:*

*En*

*Conf t*

*Int f0/1*

*Switchport mode access*

*Switchport nonegotiate (to disable dtp)*

*Switchport access vlan 99*

*Office B ASWB1:*

*En*

*Conf t*

*Int f0/1*

*Switchport mode access*

*Switchport nonegotiate (to disable dtp)*

*Switchport access vlan 99*

*ASWA2, A3, B2:*

*En*

*Conf t*

*Int f0/1*

*Switchport mode access*

*Switchport nonegotiate*

*Switchport access vlan 10*

*Switchport voice vlan 20*

*Exit*

*En*

*Copy run start*

*On ASWB3:*

*En*

*Conf t*

*Int f0/1*

*Switchport mode access*

*Switchport nonegotiate*

*Switchport access vlan 30*

*End*

*En*

*Copy run start*

*Back on ASWA1:*

*En*

*Conf t*

*Int f0/2*

*Switchport mode trunk*

*Switchport trunk allowed vlan 40,99*

*Switchport trunk native vlan 99*

*Switchport nonegotiate*

*Exit*

*On all D Switches:*

*Do sh int status*

*Int range g1/0/6-24,g1/1/3-4*

*Shutdown*

*Exit*

*Copy run start*

*On ASWA1:*

*En*

*Conf t*

*Int range f0/3-24 (as it is connected to WLC)*

*Shutdown*

*Exit*

*Copy run start*

*On all A Switches:*

*En*

*Conf t*

*Int range f0/2-24*

*Shutdown*

*Exit*

*Copy run start*

Configure the following IP addresses on R1s interfaces and enable them:

Dhcp client - g0/0/0

Dhcp client - g0/1/0

10.0.0.3/30 - g0/0

10.0.0.37/30 - g0/1

10.0.0.76/32 - loopback0

Then, enable IPv4 routing on all Core and Distribution switches.

*On R1:*

*En*

*Conf t*

*Int range g0/0/0,g0/1/0*

*Ip address dhcp*

*No shutdown*

*Exit*

*Int g0/0*

*Ip address 10.0.0.33 255.255.255.252*

*No shutdown*

*Int g0/1*

*Ip address 10.0.0.37 255.255.255.252*

*No shutdown*

*Int l0*

*Ip address 10.0.0.76 255.255.255.255*

*Do sh ip int br*

*End*

*Copy run start*

*On all switches:*

*En*

*Conf t*

*Ip routing*

3. Create a Layer-3 EtherChannel between CSW1 and CSW2 using a Cisco-proprietary protocol. Both switches should actively try to form an EtherChannel. Configure the following IP addresses:

a. CSW1 PortChannel1: 10.0.0.41/30

b. CSW2 PortChannel1: 10.0.0.42/30

*On CSW1:*

*En*

*Conf t*

*Do sh cdp neighb (check which connections to csw2)*

*Int range g1/0/2-3*

*No switchport (to make routed ports)*

*Channel-group 1 mode desirable*

*Int po1*

*Ip address 10.0.0.41 255.255.255.252*

*On csw2:*

*En*

*Conf t*

*Int range g1/0/2-3*

*No switchport*

*Channel-group 1 mode desirable*

*Int po1*

*Ip address 10.0.0.42 255.255.255.252*

*Do sh eth channel summary (RU means layer 3, in use)*

4. Configure the following IP addresses on CSW1. Disable all unused interfaces.

a. G1/0/1: 10.0.0.34/30

b. G1/1/1: 10.0.0.45/30

c. G1/1/2: 10.0.0.49/30

d. G1/1/3: 10.0.0.53/30

e. G1/1/4: 10.0.0.57/30

f. Loopback0: 10.0.0.77/32

*On csw1:*

*En*

*Conf t*

*Int g1/0/1*

*No switchport (to make routed port)*

*Ip address 10.0.0.34 255.255.255.252*

*Int g1/1/1*

*No switchport*

*Ip address 10.0.0.45 255.255.255.252*

*Int g/1/1/2*

*No switchport*

*Ip address 10.0.0.49 255.255.255.252*

*Int g1/1/3*

*No switchport*

*Ip address 10.0.0.53 255.255.255.252*

*Int g1/1/4*

*No switchport*

*Ip address 10.0.0.57 255.255.255.252*

*Int l0*

*Ip address 10.0.0.77 255.255.255.255*

*Int range g1/0/4-24*

*shutdown*

*End*

*Copy run start*

5. Configure the following IP addresses on CSW2. Disable all unused interfaces.

a. G1/0/1: 10.0.0.38/30

b. G1/1/1: 10.0.0.61/30

c. G1/1/2: 10.0.0.65/30

d. G1/1/3: 10.0.0.69/30

e. G1/1/4: 10.0.0.73/30

f. Loopback0: 10.0.0.78/32

*On csw1:*

*En*

*Conf t*

*Int g1/0/1*

*No switchport (to make routed port)*

*Ip address 10.0.0.38 255.255.255.252*

*Int g1/1/1*

*No switchport*

*Ip address 10.0.0.61 255.255.255.252*

*Int g/1/1/2*

*No switchport*

*Ip address 10.0.0.65 255.255.255.252*

*Int g1/1/3*

*No switchport*

*Ip address 10.0.0.69 255.255.255.252*

*Int g1/1/4*

*No switchport*

*Ip address 10.0.0.73 255.255.255.252*

*Int l0*

*Ip address 10.0.0.77 255.255.255.255*

*Int range g1/0/4-24*

*shutdown*

*End*

*Copy run start*

6. Configure the following IP addresses on DSW-A1:

a. G1/1/1: 10.0.0.46/30

b. G1/1/2: 10.0.0.62/30

c. Loopback0: 10.0.0.79/32

7. Configure the following IP addresses on DSW-A2:

a. G1/1/1: 10.0.0.50/30

b. G1/1/2: 10.0.0.66/30

c. Loopback0: 10.0.0.80/32

8. Configure the following IP addresses on DSW-B1:

a. G1/1/1: 10.0.0.54/30

b. G1/1/2: 10.0.0.70/30

c. Loopback0: 10.0.0.81/32

9. Configure the following IP addresses on DSW-B2:

a. G1/1/1: 10.0.0.58/30

b. G1/1/2: 10.0.0.74/30

c. Loopback0: 10.0.0.82/32

*On dswa1:*

*En*

*Conf t*

*Int g1/1/1*

*No switchport*

*Ip address 10.0.0.46 255.255.255.252*

*Interface g1/1/2*

*No switchport*

*Ip address 10.0.0.62 255.255.255.252*

*Interface l0*

*Ip address 10.0.0.79 255.255.255.255*

*End*

*Copy run start*

*On dswa2:*

*En*

*Conf t*

*Int g1/1/1*

*No switchport*

*Ip address 10.0.0.50 255.255.255.252*

*Interface g1/1/2*

*No switchport*

*Ip address 10.0.0.66 255.255.255.252*

*Interface l0*

*Ip address 10.0.0.80 255.255.255.255*

*End*

*Copy run start*

*On dswb1:*

*En*

*Conf t*

*Int g1/1/1*

*No switchport*

*Ip address 10.0.0.54 255.255.255.252*

*Interface g1/1/2*

*No switchport*

*Ip address 10.0.0.70 255.255.255.252*

*Interface l0*

*Ip address 10.0.0.81 255.255.255.255*

*End*

*Copy run start*

*On dswb2:*

*En*

*Conf t*

*Int g1/1/1*

*No switchport*

*Ip address 10.0.0.58 255.255.255.252*

*Interface g1/1/2*

*No switchport*

*Ip address 10.0.0.72 255.255.255.252*

*Interface l0*

*Ip address 10.0.0.82 255.255.255.255*

*End*

*Copy run start*

11. Configure the following management IP addresses on the Access switches (interface VLAN 99), and configure the appropriate subnet’s first usable address as the default gateway.

a. ASW-A1: 10.0.0.4/28

b. ASW-A2: 10.0.0.5/28

c. ASW-A3: 10.0.0.6/28

d. ASW-B1: 10.0.0.20/28

e. ASW-B2: 10.0.0.21/28

f. ASW-B3: 10.0.0.22/28

*On aswa1:*

*En*

*Conf t*

*Ip default-gateway 10.0.0.1*

*Int vlan 99*

*Ip address 10.0.0.4 255.255.255.240*

*Exit*

*End*

*Copy run start*

*On ASWA2:*

*En*

*Conf t*

*Ip default-gateway 10.0.0.1*

*Int vlan 99*

*Ip address 10.0.0.5 255.255.255.240*

*Exit*

*End*

*Copy run start*

*On ASWA3:*

*En*

*Conf t*

*Ip default-gateway 10.0.0.1*

*Int vlan 99*

*Ip address 10.0.0.5 255.255.255.240*

*Exit*

*End*

*Copy run start*

*On ASWB1:*

*En*

*Conf t*

*Ip default-gateway 10.0.0.17*

*Int vlan 99*

*Ip add 10.0.0.20 255.255.255.240*

*End*

*Copy run start*

*On ASWB2:*

*En*

*Conf t*

*Ip default-gateway 10.0.0.17*

*Int vlan 99*

*Ip add 10.0.0.21 255.255.255.240*

*End*

*Copy run start*

*On ASWB3:*

*En*

*Conf t*

*Ip default-gateway 10.0.0.17*

*Int vlan 99*

*Ip add 10.0.0.22 255.255.255.240*

*End*

*Copy run start*

Static and dynamic routing\*:

1. Configure OSPF on R1 (LAN-facing interfaces) and all Core and Distribution switches (all Layer-3 interfaces).

a. Use process ID 1 and Area 0.

b. Manually configure each device’s RID to match the loopback interface IP.

c. On switches, use the network command to match the exact IP address of each interface.

d. On R1, enable OSPF in interface config mode.

e. Make sure OSPF is enabled on all loopback interfaces, too. Loopback interfaces should be passive.

f. Each Distribution switch’s SVIs (except the Management VLAN SVI) should be passive, too.

g. Configure all physical connections between OSPF neighbors to use a network type that doesn’t elect a DR/BDR. NOTE: This doesn’t work on the Layer-3 PortChannel interfaces between CSW1/CSW2. Leave them as the default network type.

*On r1:*

*En*

*Conf t*

*Router ospf 1*

*Do sh ip ospf (to see RID)*

*Router-id 10.0.0.76*

*Passive-interface l0*

*Int l0*

*Ip ospf 1 area 0*

*Int range g0/0-1*

*Ip ospf 1 area 0*

*Ip ospf network point-to-point*

*On CSW1:*

*En*

*Conf t*

*Router ospf 1*

*Router-id 10.0.0.77 (address of loopback int)*

*Passive-interface l0*

*do sh ip int br | exclude un (to see up interfaces for networks for OSPF)*

*Network 10.0.0.41 0.0.0.0 area 0*

*Network 10.0.0.34 0.0.0.0 area 0*

*Network 10.0.0.45 0.0.0.0 area 0*

*Network 10.0.0.49 0.0.0.0 area 0*

*Network 10.0.0.53 0.0.0.0 area 0*

*Network 10.0.0.57 0.0.0.0 area 0*

*Network 10.0.0.77 0.0.0.0 area 0*

*Int range g101,g1/1/1-4*

*Ip ospf network point-to-point*

*End*

*Copy run start*

*On CSW2:*

*En*

*Conf t*

*Router ospf 1*

*Router-id 10.0.0.77 (address of loopback int)*

*Passive-interface l0*

*do sh ip int br | exclude un (to see up interfaces for networks for OSPF)*

*Network 10.0.0.42 0.0.0.0 area 0*

*Network 10.0.0.38 0.0.0.0 area 0*

*Network 10.0.0.61 0.0.0.0 area 0*

*Network 10.0.0.65 0.0.0.0 area 0*

*Network 10.0.0.69 0.0.0.0 area 0*

*Network 10.0.0.73 0.0.0.0 area 0*

*Network 10.0.0.78 0.0.0.0 area 0*

*Int range g101,g1/1/1-4*

*Ip ospf network point-to-point*

*End*

*Copy run start*

*DSW-A1:*

*En*

*Conf t*

*Router ospf 1*

*Router-id 10.0.0.79*

*Passive-interface l0*

*Passive-interface vlan 10*

*Passive-interface vlan 20*

*Passive-interface vlan 40*

*Network 10.0.0.46 0.0.0.0 area 0*

*Network 10.0.0.62 0.0.0.0 area 0*

*Network 10.0.0.79 0.0.0.0 area 0*

*Network 10.1.0.2 0.0.0.0 area 0*

*Network 10.2.0.2 0.0.0.0 area 0*

*Network 10.0.0.2 0.0.0.0 area 0*

*Network 10.6.0.2 0.0.0.0 area 0*

*Int range g1/1/1-2*

*Ip ospf network point-to-point*

*End*

*Copy run start*

*Do sh ip ospf neighbor*

*DSW-A2:*

*En*

*Conf t*

*Router ospf 1*

*Router-id 10.0.0.79*

*Passive-interface l0*

*Passive-interface vlan 10*

*Passive-interface vlan 20*

*Passive-interface vlan 40*

*Network 10.0.0.50 0.0.0.0 area 0*

*Network 10.0.0.66 0.0.0.0 area 0*

*Network 10.0.0.80 0.0.0.0 area 0*

*Network 10.1.0.3 0.0.0.0 area 0*

*Network 10.2.0.3 0.0.0.0 area 0*

*Network 10.0.0.3 0.0.0.0 area 0*

*Network 10.6.0.3 0.0.0.0 area 0*

*Int range g1/1/1-2*

*Ip ospf network point-to-point*

*End*

*Copy run start*

*Do sh ip ospf neighbor*

*DSWB1:*

*En*

*Conf t*

*Router ospf 1*

*Router-id 10.0.0.79*

*Passive-interface l0*

*Passive-interface vlan 10*

*Passive-interface vlan 20*

*Passive-interface vlan 30*

*Network 10.0.0.54 0.0.0.0 area 0*

*Network 10.0.0.70 0.0.0.0 area 0*

*Network 10.0.0.81 0.0.0.0 area 0*

*Network 10.3.0.2 0.0.0.0 area 0*

*Network 10.4.0.2 0.0.0.0 area 0*

*Network 10.5.0.2 0.0.0.0 area 0*

*Network 10.0.0.18 0.0.0.0 area 0*

*Int range g1/1/1-2*

*Ip ospf network point-to-point*

*End*

*Copy run start*

*Do sh ip ospf neighbor*

*DSWB2:*

*En*

*Conf t*

*Router ospf 1*

*Router-id 10.0.0.79*

*Passive-interface l0*

*Passive-interface vlan 10*

*Passive-interface vlan 20*

*Passive-interface vlan 30*

*Network 10.0.0.58 0.0.0.0 area 0*

*Network 10.0.0.74 0.0.0.0 area 0*

*Network 10.0.0.82 0.0.0.0 area 0*

*Network 10.3.0.3 0.0.0.0 area 0*

*Network 10.4.0.3 0.0.0.0 area 0*

*Network 10.5.0.3 0.0.0.0 area 0*

*Network 10.0.0.19 0.0.0.0 area 0*

*Int range g1/1/1-2*

*Ip ospf network point-to-point*

*End*

*Copy run start*

*Do sh ip ospf neighbor*

2. Configure one static default route for each of R1’s Internet connections. They should be recursive routes.

a. Make the route via G0/1/0 a floating static route by configuring an AD value 1 greater than the default.

b. R1 should function as an OSPF ASBR, advertising its default route to other routers in the OSPF domain.

*On r1:*

*Do sh ip int br (to see addresses for next hop IPs)*

*Ip route 0.0.0.0 0.0.0.0 203.0.113.1*

*Ip route 0.0.0.0 0.0.0.0 203.0.113.5 2*

*Do sh ip route*

*Router ospf 1*

*Default-information originate*

*End*

*Copy run start*

1. Configure the following DHCP pools on R1 to make it serve as the DHCP server for hosts in Offices A and B. Exclude the first ten usable host addresses of each pool; they must not be leased to DHCP clients.

a. Pool: A-Mgmt

i. Subnet: 10.0.0.0/28

ii. Default gateway: 10.0.0.1

iii. Domain name: jeremysitlab.com

iv. DNS server: 10.5.0.4 (SRV1)

v. WLC: 10.0.0.7

b. Pool: A-PC

i. Subnet: 10.1.0.0/24

ii. Default gateway: 10.1.0.1

iii. Domain name: jeremysitlab.com

iv. DNS server: 10.5.0.4 (SRV1)

c. Pool: A-Phone

i. Subnet: 10.2.0.0/24

ii. Default gateway: 10.2.0.1

iii. Domain name: jeremysitlab.com

iv. DNS server: 10.5.0.4 (SRV1)

d. Pool: B-Mgmt

i. Subnet: 10.0.0.16/28

ii. Default gateway: 10.0.0.17

iii. Domain name: jeremysitlab.com

iv. DNS server: 10.5.0.4 (SRV1)

v. WLC: 10.0.0.7

e. Pool: B-PC

i. Subnet: 10.3.0.0/24

ii. Default gateway: 10.3.0.1

iii. Domain name: jeremysitlab.com

iv. DNS server: 10.5.0.4 (SRV1)

f. Pool: B-Phone

i. Subnet: 10.4.0.0/24

ii. Default gateway: 10.4.0.1

iii. Domain name: jeremysitlab.com

iv. DNS server: 10.5.0.4 (SRV1)

g. Pool: Wi-Fi

i. Subnet: 10.6.0.0/24

ii. Default gateway: 10.6.0.1

iii. Domain name: jeremysitlab.com

iv. DNS server: 10.5.0.4 (SRV1)

*On r1:*

*En*

*Conf t*

*Ip dhcp excluded-address 10.0.0.1 10.0.0.10*

*Ip dhcp excluded-address 10.1.0.1 10.1.0.10*

*Ip dhcp excluded-address 10.2.0.1 10.2.0.10*

*Ip dhcp excluded-address 10.0.0.17 10.0.0.26*

*Ip dhcp excluded-address 10.3.0.1 10.3.0.10*

*Ip dhcp excluded-address 10.4.0.1 10.4.0.10*

*Ip dhcp excluded-address 10.6.0.1 10.6.0.10*

*Ip dhcp pool A-Mgmt*

*Network 10.0.0.0 255.255.255.240*

*Default-router 10.0.0.1*

*Domain-name jeremysitlab.com*

*Dns-server 10.5.0.4*

*Option 43 ip 10.0.0.7 (WLC address)*

*Ip dhcp pool A-PC*

*Network 10.1.0.0 255.255.255.0*

*Default-router 10.1.0.1*

*Dns-server 10.5.0.4*

*Domain-name jeremysitlab.com*

*Ip dhcp pool A-Phone*

*Network 10.2.0.0 255.255.255.0*

*Default-router 10.2.0.1*

*Dns-server 10.5.0.4*

*Domain-name jeremysitlab.com*

*Ip dhcp pool B-Mgmt*

*Network 10.0.0.16 255.255.255.240*

*Default-router 10.0.0.17*

*Dns-server 10.5.0.4*

*Domain-name jeremysitlab.com*

*Option 43 ip 10.0.0.7*

*Ip dhcp pool B-PC*

*Network 10.3.0.0 255.255.255.0*

*Default-router 10.3.0.1*

*Dns-server 10.5.0.4*

*Domain-name jeremysitlab.com*

*Ip dhcp pool B-Phone*

*Network 10.4.0.0 255.255.255.0*

*Default-router 10.4.0.1*

*Dns-server 10.5.0.4*

*Domain-name jeremysitlab.com*

*Ip dhcp pool Wi-Fi*

*Network 10.6.0.0 255.255.255.0*

*Default-router 10.6.0.1*

*Dns-server 10.5.0.4*

*Domain-name jeremysitlab.com*

*exit*

*Do sh ip dhcp binding*

2. Configure the Distribution switches to relay wired DHCP clients’ broadcast messages to R1’s Loopback0 IP address.

*On interfaces that receive the DHCP messages… SVIs on each switch*

*DSWA1, DSWA2:*

*En*

*Conf t*

*Interface vlan 10*

*Ip helper-address 10.0.0.76*

*Int vlan 20*

*Ip helper-address 10.0.0.76*

*Int vlan 40*

*Ip helper-address 10.0.0.76*

*Int vlan 99*

*Ip helper-address 10.0.0.76*

*End copy run start*

*DSWB1, DSWB2:*

*En*

*Conf t*

*Interface vlan 10*

*Ip helper-address 10.0.0.76*

*Int vlan 20*

*Ip helper-address 10.0.0.76*

*Int vlan 30*

*Ip helper-address 10.0.0.76*

*Int vlan 99*

*Ip helper-address 10.0.0.76*

*End*

*Copy run start*

4. Configure all routers and switches to use domain name jeremysitlab.com and use SRV1 as their DNS server.

*On all switches:*

*Ip domain name jeremysitlab.com*

*Ip name-server 10.5.0.4*

5. Configure NTP on R1:

a. Make R1 a stratum 5 NTP server.

b. R1 should learn the time from NTP server 216.239.35.0.

c. NOTE: NTP takes a LONG time to sync, especially in Packet Tracer. After making the configurations, you can move on – don’t wait for the devices to sync.

6. All Core, Distribution, and Access switches should use R1’s loopback interface as their NTP server.

a. Clients should authenticate R1 using key number 1 and the password ccna.

*On r1:*

*Ntp master 5*

*Ntp server 216.239.35.0*

*Ntp authentication-key 1 md5 ccna*

*Ntp trusted-key 1*

*On every switch:*

*En*

*Conf t*

*Ntp authentication-key 1 md5 ccna*

*Ntp-trusted key 1*

*Ntp server 10.0.0.76 key 1*

*End*

*Copy run start*

10. Configure SSH for secure remote access on all routers and switches.

a. Use the largest modulus size for the RSA keys.

b. Allow SSHv2 connections only.

c. Create standard ACL 1, only allowing packets sourced from Office A’s PCs subnet. Apply the ACL to all VTY lines to restrict SSH access.

d. Allow only SSH connections to the VTY lines.

e. Require users to log in with a local user account when connecting via SSH.

f. Configure synchronous logging on the VTY lines.

*On r1:*

*En*

*Conf t*

*Crypto key generate rsa*

*\*input modular size\* larger = more secure - 4096*

*Do sh ip ssh (to check ssh ver)*

*Ip ssh version 2*

*Do sh ip ssh (to check version)*

*Access-list 1 permit 10.1.0.0 0.0.0.255 (implicit deny will block all other traffic)*

*Line vty 0 15*

*Access-class 1 (ACL number) in*

*Transport input ssh*

*Login local*

*Logging-synchronous*

*End*

*Copy run start*

*On all switches:*

*En*

*Conf t*

*Crypto key generate rsa*

*4096*

*Ip ssh version 2*

*Access-list 1 permit 10.1.0.0 0.0.0.255*

*Line vty 0 15*

*Access-class 1 in*

*Transport input ssh*

*Login local*

*Logging synchronous*

*End*

*Copy run start*

*On pc1:*

*Ssh -l cisco 10.0.0.76*

*Password: ccna*

11. Configure static NAT on R1 to enable hosts on the Internet to access SRV1 via the IP address 203.0.113.113.

*On r1: (config static nat for srv1)*

*En*

*Conf t*

*Ip nat inside source static 10.5.0.4 203.0.113.113*

*Int range g0/0/0, g0/1/0*

*Ip nat outside*

*Int range g0/0-1*

*Ip nat inside*

*Exit*

12. Configure pool-based dynamic PAT on R1 to enable hosts in the Office A PCs, Office A Phones, Office B PCs, Office B Phones, and Wi-Fi subnets to access the Internet.

a. Use standard ACL 2 to define the appropriate inside local address ranges in the following order:

i. Office A PCs: 10.1.0.0/24

ii. Office A Phones: 10.2.0.0/24

iii. Office B PCs: 10.3.0.0/24

iv. Office B Phones: 10.4.0.0/24

v. Wi-Fi: 10.6.0.0/24

b. Define a range of inside global addresses called POOL1, specifying the range 203.0.113.200 to 203.0.113.207 with a /29 netmask.

c. Map ACL 2 to POOL1 and enable PAT. Confirm that hosts can access the Internet by pinging jeremysitlab.com.

*On r1:*

*Access-list 2 permit 10.1.0.0 0.0.0.255*

*Access-list 2 permit 10.2.0.0 0.0.0.255*

*Access-list 2 permit 10.3.0.0 0.0.0.255*

*Access-list 2 permit 10.4.0.0 0.0.0.255*

*Access-list 2 permit 10.6.0.0 0.0.0.255*

*Ip nat pool POOL1 203.0.113.200 203.0.113.207 netmask 255.255.255.248*

*Ip nat inside source list 2 pool POOL1 overload (to make it PAT over NAT)*

13. Disable CDP on all devices and enable LLDP instead.

a. Disable LLDP Tx on each Access switch’s access port (F0/1).

*On r1, core, dist switches:*

*En*

*Conf t*

*No cdp run*

*Lldp run*

*End*

*Copy run start*

*On access switches:*

*En*

*Conf t*

*No cdp run*

*Lldp run*

*Interface f0/1*

*No lldp transmit*

*End*

*Copy run start*

1. Configure extended ACL OfficeA\_to\_OfficeB where appropriate:

a. Allow ICMP messages from the Office A PCs subnet to the Office B PCs subnet.

b. Block all other traffic from the Office A PCs subnet to the Office B PCs subnet.

c. Allow all other traffic.

d. Apply the ACL according to general best practice for extended ACLs.

*Extended acls - applied closest to source*

*Standard acls - closest to destination*

*On dswA1:*

*En*

*Conf t*

*Ip access-list extended OfficeA\_to\_OfficeB*

*Permit icmp 10.1.0.0 0.0.0.255 10.3.0.0 0.0.0.255*

*Deny ip 10.1.0.0 0.0.0.255 10.3.0.0 0.0.0.255*

*Permit ip any any*

*Int vlan 10*

*Ip access-group OfficeA\_to\_OfficeB in*

*End*

*Copy run start*

*DSW-A2:*

*En*

*Conf t*

*Ip access-list extended OfficeA\_to\_OfficeB*

*Permit icmp 10.1.0.0 0.0.0.255 10.3.0.0 0.0.0.255*

*Deny ip 10.1.0.0 0.0.0.255 10.3.00 0.0.0.255*

*Permit ip any any*

*Int vlan 10*

*Ip access-group OfficeA\_to\_OfficeB in*

*End*

*Copy run start*

2. Configure Port Security on each Access switch's F0/1 port:

a. Allow the minimum necessary number of MAC addresses on each port.

i. SRV1 does not use virtualization, so it uses a single MAC address.

b. Configure a violation mode that blocks invalid traffic without affecting valid traffic. The switches should send notifications when invalid traffic is detected.

c. Switches should automatically save the secure MAC addresses they learn to the running-config.

*On ASWA1, B1, B3:*

*En*

*Conf t*

*Int f0/1*

*Switchport port-security*

*Switchport port-security violation restrict*

*Switchport port-security mac-address sticky*

*Exit*

*On ASWA2, A3, B2:*

*En*

*Conf t*

*Int f0/1*

*Switchport port-security*

*Switchport port-security maximum 2*

*Switchport port-security violation restrict*

*Switchport port-security mac-address sticky*

*Exit*

3. Configure DHCP Snooping on all Access switches.

a. Enable it for all active VLANs in each LAN.

b. Trust the appropriate ports.

c. Disable insertion of DHCP Option 82.

d. Set a DHCP rate limit of 15 pps on active untrusted ports.

e. Set a higher limit (100 pps) on ASW-A1’s connection to WLC1.

*ASWA1:*

*En*

*Conf t*

*Ip dhcp snooping*

*Ip dhcp snooping vlan 10,20,40,99*

*Ip dhcp snooping information option*

*Int range g0/1-2*

*Ip dhcp snooping trust*

*Int f0/1*

*Ip dhcp snooping limit rate 15*

*Int f0/2*

*Ip dhcp snooping limit rate 100*

*End*

*Copy run start*

*On ASWA2, A3:*

*En*

*Conf t*

*Ip dhcp snooping*

*Ip dhcp snooping vlan 10,20,40,99*

*Ip dhcp snooping information option*

*Int range g0/1-2*

*Ip dhcp snooping trust*

*Int f0/1*

*Ip dhcp snooping limit rate 15*

*End*

*Copy run start*

*On ASWB1, B2, B3:*

*En*

*Conf t*

*Ip dhcp snooping*

*Ip dhcp snooping vlan 10,20,30,99*

*Ip dhcp snooping information option*

*Int range g0/1-2*

*Ip dhcp snooping trust*

*Int f0/1*

*Ip dhcp snooping limit rate 15*

*End*

*Copy run start*

4. Configure DAI on all Access switches.

a. Enable it for all active VLANs in each LAN.

b. Trust the appropriate ports.

c. Enable all optional validation checks.

*ASWA1, A2, A3:*

*(enabled per vlan, not globally)*

*En*

*Conf t*

*Ip arp inspection vlan 10,20,40,99*

*Ip arp inspection validate dst-mac src-mac ip*

*Int range g0/1-2*

*Ip arp inspection trust*

*End*

*Copy run start*

*ASWB1, B2, B3:*

*En*

*Conf t*

*Ip arp inspection vlan 10,20,30,99*

*Ip arp inspection validate dst-mac src-mac ip*

*Int range g0/1-2*

*Ip arp inspection trust*

*End*

*Copy run start*

1. To prepare for a migration to IPv6, enable IPv6 routing and configure IPv6 addresses on R1, CSW1, and CSW2:

a. R1 G0/0/0: 2001:db8:a::2/64

b. R1 G0/1/0: 2001:db8:b::2/64

c. R1 G0/0 and CSW1 G1/0/1: Use prefix 2001:db8:a1::/64 and EUI-64 to generate an interface ID for each interface.

d. R1 G0/1 and CSW2 G1/0/1: Use prefix 2001:db8:a2::/64 and EUI-64 to generate an interface ID for each interface.

e. CSW1 Po1 and CSW2 Po1: Enable IPv6 without using the ‘ipv6 address’ command.

*On r1:*

*En*

*Conf t*

*Ipv6 unicast-routing*

*Int g0/0*

*Ipv6 address 2001:db8:a::2/64*

*Int g0/1/0*

*Ipv6 address 2001:db8:b::2/64*

*Int g0/0*

*Ipv6 address 2001:db8:a1::/64 eui-64*

*Int g0/1*

*Ipv6 address 2001:db8:a2::/64 eui-64*

*Do sh ipv6 int br*

*End*

*Copy run start*

*On CSW1:*

*En*

*Conf t*

*Ipv6 unicast-routing*

*Int g1/0/1*

*Ipv6 address 2001:db8:a1::/64 eui-64*

*Int po1*

*Ipv6 enable*

*Do sh ipv6 int br*

*End*

*Copy run start*

*On CSW2:*

*En*

*Conf t*

*Ipv6 unicast-routing*

*Int g1/0/1*

*Ipv6 address 2001:db8:a2::/64 eui-64*

*Int po1*

*Ipv6 enable*

*Do sh ipv6 int br*

*End*

*Copy run start*

2. Configure two default static routes on R1:

a. A recursive route via next hop 2001:db8:a::1.

b. A fully-specified route via next hop 2001:db8:b::1. Make it a floating route by configuring the AD 1 higher than default.

*On r1:*

*En*

*Conf t*

*Ipv6 unicast-routing*

*Ipv6 route ::/0 2001:db8:a::1*

*Ipv6 route ::/0 g0/1/0 2001:db8:b::1 2*

*End*

*Copy run start*

*Practice 1:*

*Vlan configuration, assign hosts to a VLAN and create a trunk connection between switches:*

*On switch:*

*Int <int>*

*Switchport mode access*

*Switchport access vlan <vlan #>*

*exit*

*Int <int>*

*Switchport mode trunk*

*End*

*Copy run start*

*VLAN trunk encapsulation, assign hosts to VLAN, create a trunk on interfaces that are “auto” encapsulation*

*On switch:*

*Int <int>*

*Switchport mode access*

*Switchport access vlan <vlan #>*

*exit*

*Int <int>*

*Switchport trunk encapsulation dot1q*

*Switchport mode trunk*

*End*

*Copy run start*

*Naming VLANs, set hostnames, create and name vlans, assign hosts, trunk link, save config*

*On switch:*

*En*

*Conf t*

*Hostname <hostname>*

*Vlan <vlan #>*

*Name <name>*

*Int <int>*

*Switchport mode access*

*Switchport access vlan <vlan #>*

*Int <int>*

*Switchport mode trunk*

*End*

*Copy run start*

*Loopback interface configuration, ip address configuration:*

*On router:*

*En*

*Conf t*

*Int <int>*

*Ip address <ip> <subnet mask>*

*No shutdown*

*Exit*

*Int l0*

*Ip address <ip> <subnet mask>*

*End*

*Copy run start*

*Port Security, maximum addresses, violation mode, sticky mac address (dynamically attach mac address to port when it changes), trusted MAC:*

*On switch:*

*En*

*Conf t*

*Int <int>*

*Switchport mode access*

*Switchport port-security*

*Switchport port-security maximum <number>*

*Switchport port-security violation mode <mode>*

*Switchport port-security mac-address sticky*

*Switchport port-security mac-address <mac>*

*End*

*Copy run start*

*Static routing, configure interfaces with IPs, configure static routes to different networks:*

*On router:*

*En*

*Conf t*

*Int <int>*

*Ip address <ip> <subnet mask>*

*No shutdown*

*Conf t*

*Ip route <route of network> <subnet mask> <either next hop IP or INT traffic coming from (without int)>*

*End*

*Copy run start*

*Standard ACLs, permit network traffic, deny host, apply ACL to interface, permit/deny:*

*Remember - apply closest to destination as possible, implicit deny rule*

*On router (interface closest to server):*

*En*

*Conf t*

*access-list 1 permit/deny <ip address> <wildcard mask>*

*Int <int to apply access list>*

*Ip access-group 1 <in/out>*

*End*

*Show access-list*

*Conf t*

*Access-list 1 permit/deny host <host ip>*

*Access-list 1 permit any (due to implicit deny rule)*

*Int <int to apply access list to>*

*Ip access-group 1 <in/out>*

*End*

*Copy run start*

*Extended ACLs, allow host to access Server, only hosts in particular network (192.168.2.0/24) can access Server 2:*

*On router (interface closest to source):*

*En*

*Conf t*

*Access-list 100 permit ip host <host ip source> host <host ip dest.>*

*Access-list 100 deny ip any host <host IP connected to same SW as dest.>*

*Access-list 100 permit ip <ip> <wildcard> host <destination ip>*

*Access-list 100 deny ip any host <dest ip>*

*Acces-list 100 permit ip any any*

*Int s2/0*

*Ip access-group 100 out*

*End*

*Copy run start*

*Configure router as NTP server with default stratum level, configure R2 to synch its time to server, configure R3 to synch time to R2:*

*On r1:*

*En*

*Sh clock detail*

*Clock ?*

*Conf t*

*Ntp master 8*

*End*

*Copy run start*

*On r2:*

*En*

*Conf t*

*Clock timezone <timezone>*

*Ntp server 192.168.12.1*

*Sh ntp associations*

*On r3:*

*En*

*Conf t*

*Ntp server 192.168.23.2*

*Exit*

***\*to add authentication to this\****

***On master router:***

***Ntp authenticate***

***Ntp authentication-key 1 md5 <key>***

***Ntp trusted-key 1***

***On clients:***

***Ntp authentication-key 1 md5 <key>***

***Ntp trusted-key 1***

*Configure DHCP, assign pool name, network range, default gateway, dns-server and excluded address range, make r1 dhcp server, r2 dhcp client and able to get ip address from dhcp*

*On r1:*

*En*

*Conf t*

*Ip dhcp pool <pool name> 10pool*

*Network <ip> <subnet mask> 10.0.0.0 255.255.255.0*

*Default-router <ip> 10.0.0.1*

*Dns-server <ip>10.0.0.1*

*Exit*

*Ip dhcp excluded-address <first ip> <second ip>10.0.0.1 10.0.0.10*

*Ip dhcp pool 20pool*

*Network 20.0.0.255.255.255.0*

*Default-router 20.0.0.1*

*Dns-server 20.0.0.1*

*Exit*

*Ip dhcp excluded-address 20.0.0.1 20.0.0.10*

*Ip dhcp pool 12pool*

*Network 192.168.12.0 255.255.255.0*

*End*

*Copy run start*

*On r2:*

*En*

*Conf t*

*Int g0/0*

*Ip address dhcp*

*No shutdown*

*Exit*

*Int g0/1*

*Ip helper-address <ip of dhcp server> 192.168.12.1*

*End*

*Copy run start*

*Static NAT:*

*On r1:*

*En*

*Conf t*

*Int <int> g0/0*

*Ip nat inside*

*Int <int> s0/3/0*

*Ip nat outside (facing internet)*

*Exit*

*Ip nat inside source static <host ip> <translated ip> 192.168.1.11 1.2.3.11*

*Ip nat inside source static 192.168.1.12 1.2.3.12*

*Ip nat inside source static 192.168.1.13 1.2.3.13 (host ip and translated ip provided)*

*End*

*Copy run start*

*Ipv6 addresses, SLAAC, routing:*

*En*

*Conf t*

*Ipv6 unicast-routing*

*Int <int>*

*Ipv6 address <ip>*

*No shutdown*

*En*

*Conf t*

*Int <int>*

*No shutdown*

*Ipv6 address autconfig*

*En*

*Conf t*

*Ipv6 route <next hop ip> <dest. ip>*

*End*

*Copy run start*

*Confirm root bridge, L2 etherchannel with cisco proprietary protocol, trunk configuration, L3 Etherchannel as static, L2 etherchannel with IEEE standards protocol, trunk configuration:*

*On switch 1 (and connecting switch):*

*En*

*Sh spanning-tree (to determine root bridge ID that matches device ID)*

*En*

*Conf t*

*Int range <range> f01-4*

*Channel-group <number> 1 mode <desirable/auto active/passive>*

*Int po1*

*Switchport trunk encapsulation dot1q (may need if cannot make port a trunk)*

*Switchport mode trunk*

*Do sh eth channel summary*

*End*

*Copy run start*

*On sw2 (and connecting switch):*

*En*

*Conf t*

*Ip routing*

*Interface range <range>*

*No switchport (to make interface L3)*

*Channel-group <number> 1, 2 mode on*

*Int po<number> 1, 2*

*Ip address <ip> 23.0.0.1 <subnet mask> 255.255.255.0*

*End*

*Copy run start*

*Configure loopback, configure OSPF on router, advertise all interfaces, suppress OSPF messages from L0:*

*On router:*

*En*

*Conf t*

*Int L0*

*Ip address <ip> <subnet mask>*

*Conf t*

*Router ospf <ID> 1*

*Network <ip> <wildcard mask> area <number> 0*

*Passive-interface l0*

*End*

*Copy run start*

*Standard ACLs, IPv6 ACLs, Extended named ACLs:*

*En*

*Conf t*

*Access-list <number> 1 deny host <host ip> 10.2.2.12*

*Access-list 1 permit any*

*Int <int> g0/0*

*Ip access-group 1 out (prevent traffic from exiting out of this int to 10.4.4.0 network)*

*End*

*Copy run start*

*On r1:*

*En*

*Conf t*

*Ipv6 access-list <name> g0/2\_IN*

*Deny ipv6 host <host ip> 2001:db8:3:3::11 <dest. ip> 2001:db8:22:22::/64*

*Permit ipv6 any any*

*Int <int> g0/2*

*Ipv6 traffic-filter g0/2\_IN*

*On r1:*

*En*

*Conf t*

*Ip access-list extended <name> G0/1\_IN*

*Deny ip host <ip add> 10.2.2.11 host <host ip> 10.1.1.11*

*Permit ip any any*

*Int <int> g0/1*

*Ip access-group G0/1\_IN in*

***ACLs:***

**Configure a standard ACL to only allow PC1 (172.16.1.1) and PC3 (172.16.2.1) to access the network 192.168.1.0/24:**

En

Conf t

Ip access-list standard <name> TO\_192.168.1.0/24

Permit 172.16.1.1

Permit 172.16.2.1

Deny any

Int <int closest to dest.>

Ip access-group <name of ACL> TO\_192.168.1.0/24 <in/out>

\*In this case, traffic is going out of the interface to dest.\*

**Configure a standard ACL to deny hosts in 172.16.2.0/24 network access to 192.168.2.0/24:**

En

Conf t

Ip access-list standard <name> TO\_192.168.2.0/24

Deny 172.16.2.0 0.0.0.255

Permit any

Int <int closest to dest>

Ip access-group <name> TO\_192.168.2.0/24 <in/out> out

**Configure names ACLs to deny 172.16.1.0/24 network access to 172.16.2.0/24 and to deny the 172.16.2.0/24 network access to 172.16.1.0/24:**

En

Conf t

Access-list 1 deny 172.16.1.0 0.0.0.255

Access-list 1 permit any

Access-list 2 deny 172.16.2.0 0.0.0.255

Access-list 2 permit any

Do hs access-lists

Int g0/1

Ip access-group 1 out

Int g0/0

Ip access-group 2 out