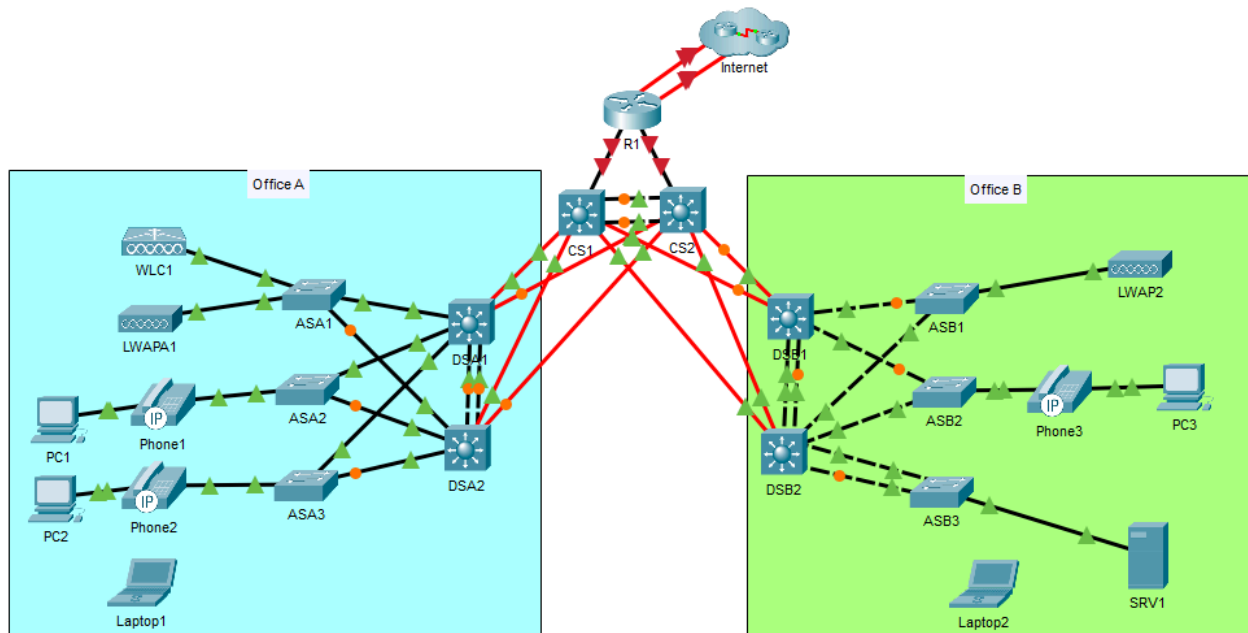# Packet Tracer Mega Lab

This lab will emulate a fictitious company (company xyz). This will be a three tier LAN consisting of 2 offices connected via a Core Layer. This lab will showcase many network protocols.

Network Topology

Part 1 - Initial Setup

1. Configure appropriate hostnames on each router and switch.
2. Configure enable secret **megalab** on each router and switch, use type 9 hashing if available, otherwise use type 5.
3. Configure user account **mega** with the secret **lab** on each router and switch using type 9 hashing if available otherwise use type 5.
4. Configure console line to require login with a local user.
5. Set a 30 minute inactive timer and enable synchronous logging.

Example - Part 1 DSA1

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname DSA1
```

```
DSA1(config)#enable algorithm-type scrypt secret megalab
DSA1(config)#username mega algorithm-type scrypt secret lab
DSA1(config)#line console 0
DSA1(config-line)#login local
DSA1(config-line)#exec-timeout 30
DSA1(config-line)#logging sync
DSA1(config-line)#do write
Building configuration...
Compressed configuration from 7383 bytes to 3601 bytes[OK]
[OK]
DSA1(config-line)#exit
DSA1(config)#
```

Part 2 - VLANs, Layer 2 EtherChannel

VLAN - A virtual LAN (VLAN) is a logical overlay network that groups together a subset of devices that share a physical LAN, isolating the traffic for each group.

EtherChannel - EtherChannel is a technology wherein we bundle physical interfaces together to create a single logical link. It is also known as Link Aggregation.

1. Office A and B, configure a Layer 2 EtherChannel named PortChannel1 between the distribution switches using open standard protocol 802.3ad (LAG). Both switches should actively try to form an EtherChannel.
2. Configure all links between Access and Distribution switches and trunk links including the EtherChannels.
3. Disable DTP on all ports.
4. Set each trunk's native VLAN to 1000. 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.
5. Configure DSA1 and DSB1 as VTPv2 servers using domain name **megalab,** verify the other switches have joined the domain and configure all access switches as VTP clients.
6. On DSA1 configure the following VLANs and ensure VTP propagates the changes.
   VLAN 10 - PCs
   VLAN 20 - Phones
   VLAN 40 - Wi-Fi
   VLAN 99 - Management
7. On DSB1 configure the following VLANs and ensure VTP propagates the changes.
   VLAN 10 - PCs
   VLAN 20 - Phones

VLAN 30 - Servers

VLAN 99 - Management

8. Configure Access switch's access ports with correct VLANs according to network topology. Disable DTP. LWAPS will not use FlexConnect.
9. Configure Access switch ASA1 to WLC1, it must support Wi-Fi and Management VLANs, Management VLAN should be untagged. Disable DTP.
10. Administratively disable all unused ports on all switches.

Example - Part 2 DSA1

```
DSA1(config)#Interface range gig1/0/4-5
DSA1(config-if-range)#channel-group 1 mode active
DSA1(config-if-range)#
Creating a port-channel interface Port-channel 1
DSA1(config-if-range)#exit
DSA1(config)#interface range gig1/0/1-3
DSA1(config-if-range)#switchport mode trunk
DSA1(config-if-range)#switchport nonegotiate
DSA1(config-if-range)#switchport trunk native vlan 1000
DSA1(config-if-range)#switchport trunk allowed vlan 10,20,40,99
DSA1(config-if-range)#int po1
DSA1(config-if-range)#switchport mode trunk
DSA1(config-if-range)#switchport nonegotiate
DSA1(config-if-range)#switchport trunk native vlan 1000
DSA1(config-if-range)#switchport trunk allowed vlan 10,20,40,99
DSA1(config-if-range)#exit
DSA1(config)#vtp domain megalab
Changing VTP domain name from NULL to megalab
DSA1(config)#vtp version 2
DSA1(config)#vlan 10
DSA1(config-vlan)#name PCs
DSA1(config-vlan)#vlan 20
DSA1(config-vlan)#name Phones
DSA1(config-vlan)#vlan 40
DSA1(config-vlan)#name Wi-Fi
DSA1(config-vlan)#vlan 99
DSA1(config-vlan)#name management
DSA1(config-if-range)#exit
DSA1(config)#int range gig1/0/6-24
DSA1(config-if-range)#shut
```

```
DSA1(config-if-range)#int range gig1/1/3-4
DSA1(config-if-range)#shut
DSA1(config-if-range)#do wr
```

Part 3 - IP addresses, Layer 3 EtherChannel, HSRP

IP Addresses - unique identifying number assigned to every device connected to the internet.

EtherChannel - EtherChannel is a technology wherein we bundle physical interfaces together to create a single logical link. It is also known as Link Aggregation.

HSRP - Cisco proprietary redundancy protocol that allows failover of the next-hop IP device. It operates with an Active-Standby Model where only one device is supporting end-user traffic at any time, and the other device is on standby waiting to take over should the active device fails.

1. Configure the following IP addresses on R1 interfaces and enable them:
   a. F4/0 203.0.113.2/30
   b. F5/0 203.0.113.6/30
   c. F0/0 10.0.0.33/30
   d. F1/0 10.0.0.37/30
   e. Loopback0 10.0.0.76/32
2. Enable IPv4 routing on all core and distribution switches.
3. Create a Layer 3 EtherChannel between the CS1 and CS2 core layer switches assigning the following IP to the port channel. Use Cisco prosperity protocol.
   - CS1 PortChannel1 10.0.0.41/30
   - CS2 PortChannel1 10.0.0.42/30
4. Configure the following IP addresses on CS1, Disable all unused interfaces.
   - g1/0/3 10.0.0.34/30
   - g1/1/1 10.0.0.45/30
   - g1/1/2 10.0.0.49/30
   - g1/1/3 10.0.0.53/30
   - g1/1/4 10.0.0.57/30
   - Loopback0 10.0.0.77/32
5. Configure the following IP addresses on CS2, Disable all unused interfaces.
   - g1/0/3 10.0.0.38/30
   - g1/1/1 10.0.0.61/30
   - g1/1/2 10.0.0.65/30
   - g1/1/3 10.0.0.69/30
   - g1/1/4 10.0.0.73/30
   - Loopback0 10.0.0.78/32
6. Configure the following IP addresses on Distribution Switches:

DSA1
- g1/1/1 10.0.0.46/30
- g1/1/2 10.0.0.62/30
- Loopback0 10.0.0.79/32

DSA2
- g1/1/1 10.0.0.50/30
- g1/1/2 10.0.0.66/30
- Loopback0 10.0.0.80/32

DSB1
- g1/1/1 10.0.0.54/30
- g1/1/2 10.0.0.70/30
- Loopback0 10.0.0.81/32

DSB2
- g1/1/1 10.0.0.58/30
- g1/1/2 10.0.0.74/30
- Loopback0 10.0.0.82/32

7. Manually configure SRV1's IP address
- Default Gateway 10.5.0.1
- IPv4 Address 10.5.0.4
- Subnet Mask 255.255.255.0

8. Configure management IP addresses on the Access switches VLAN 99 and use the first usable address as the default gateway.
- ASA1 10.0.0.4/28
- ASA2 10.0.0.5/28
- ASA2 10.0.0.6/28
- ASB1 10.0.0.20/28
- ASB2 10.0.0.21/28
- ASB3 10.0.0.22/28

9. Configure HSRPv2 groups on a per VLAN basis for redundancy, on all distribution switches. Enable preemption and increase priority on one of the layer 3 switches to make them the Active router.

OFFICE A - (4 VLANs)
- VLAN 99 management (g1), DSA1 is the active router. Subnet 10.0.0.0/28, VIP 10.0.0.1, DSA1 10.0.0.2, DSA2 10.0.0.3
- VLAN 10 PC's (g2), DSA1 is the active router. Subnet 10.1.0.0/24, VIP 10.1.0.1, DSA1 10.1.0.2, DSA2 10.1.0.3
- VLAN 20 Phone's (g3) DSA2 is the active router. Subnet 10.2.0.0/24, VIP 10.2.0.1, DSA1 10.2.0.2, DSA2 10.2.0.3
- VLAN 40 WiFi (g4) DSA2 is the active router. Subnet 10.6.0.0/24, VIP 10.6.0.1, DSA1 10.6.0.2, DSA2 10.6.0.3

OFFICE B - (4 VLANs)

- VLAN 99 Management (g1), DSB1 is the active router. Subnet 10.0.0.16/28, VIP 10.0.0.17, DSB1 10.0.0.18 DSB2 10.0.0.19
- VLAN 10 PC's (g2) DSB1 is the active router. Subnet 10.3.0.0/24, VIP 10.3.0.1, DSB1 10.3.0.2, DSB2 10.3.0.3
- VLAN 20 Phones (g3) DSB2 is the active router. Subnet 10.4.0.0/24, VIP 10.4.0.1, DSB1 10.4.0.2, DSB2 10.4.0.3
- VLAN 30 Sever (g4) DSB2 is the active router. Subnet 10.5.0.0/24, VIP 10.5.0.1, DSB1 10.5.0.2, DSB2 10.5.0.3

Example - Part 3 R1

```
R1(config)#int f4/0
R1(config-if)#ip address 203.0.113.2 255.255.255.252
R1(config-if)#no shut
%LINK-5-CHANGED: Interface FastEthernet4/0, changed state to down
R1(config-if)#int f5/0
R1(config-if)#ip address 203.0.113.6 255.255.255.252
R1(config-if)#no shut
%LINK-5-CHANGED: Interface FastEthernet5/0, changed state to down
R1(config-if)#int f0/0
R1(config-if)#ip address 10.0.0.33 255.255.255.252
R1(config-if)#no shut
R1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
R1(config-if)#int f1/0
R1(config-if)#ip address 10.0.0.37 255.255.255.252
R1(config-if)#no shut
R1(config-if)#int loopback0
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed
state to up
R1(config-if)#ip address 10.0.0.76 255.255.255.255
```

Example - Part 3 CS1

```
CS1(config)#ip routing
```

Example - Part 3 CS1

```
CS1(config)#int range g1/0/1-2
CS1(config-if-range)#no switchport
CS1(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1,
changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1,
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/2,
changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/2,
changed state to up
CS1(config-if-range)#channel-group 1 mode desirable
CS1(config-if-range)#
Creating a port-channel interface Port-channel 1
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1,
changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1,
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/2,
changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/2,
changed state to up
CS1(config-if-range)#int po1
CS1(config-if)#ip address 10.0.0.41 255.255.255.252
```

Example - Part 3 ASA1

```
ASA1(config)#ip default-gateway 10.0.0.1
ASA1(config)#int vlan 99
ASA1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to
up
ASA1(config-if)#ip address 10.0.0.4 255.255.255.240
ASA1(config-if)#exit
ASA1(config)#do wr
```

Example - Part 3 DSA1

```
 DSA1(config)#int vlan 99
DSA1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to
up
DSA1(config-if)#ip address 10.0.0.2 255.255.255.240
DSA1(config-if)#standby ver 2
DSA1(config-if)#standby 1 ip 10.0.0.1
DSA1(config-if)#
%HSRP-6-STATECHANGE: Vlan99 Grp 1 state Init -> Init
DSA1(config-if)#standby 1 priority
%HSRP-6-STATECHANGE: Vlan99 Grp 1 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan99 Grp 1 state Standby -> Active
1
DSA1(config-if)#standby 1 priority 105
DSA1(config-if)#standby 1 preempt
```

Part 4 - RPVST+ (Rapid Per VLAN Spanning Tree Protocol)

1. Configure Rapid PVST+ on all Access and Distribution switches. All root bridges
   per VLAN should align with the HSRP active router (configure the lowest possible
   STP priority).
2. Configure the HSRP standby router for each VLAN with STP priority one
   increment above the lowest priority.
3. Enable PortFast and BPDU guard for all ports connected to end hosts including
   WLC1.

Example Part 4 - ASA1
```
ASA1(config)#spanning-tree mode rapid-pvst
ASA1(config)#int f0/1
ASA1(config-if)#spanning-tree portfast
ASA1(config-if)#spanning-tree bpduguard enable
ASA1(config-if)#int f1/1
ASA1(config-if)#spanning-tree portfast trunk
ASA1(config-if)#spanning-tree bpduguard enable
```

Example Part 4 - DSA1
```
DSA1(config)#spanning-tree vlan 10,99 priority 0
DSA1(config)#spanning-tree vlan 20,40 priority 4096
```

Part 5 - Static and Dynamic Routing -OSPF

1. Configure OSPF on Router 1 (LAN facing interfaces) and core and distribution switches on layer 3 interfaces.
   - Use process ID 1 and Area 0
   - Configure device RID (router ID) to match loopback IP address
   - Use the network command /32 mask to match exact IP address of each interface
   - Enable OSPF on router 1 in interface config mode
   - Enable OSPF on all loopback interfaces (passive)
   - Distribution switches SVI's should be passive apart from the Management VLAN (only send hello's out of the management SVI)
   - Configure point to point network type between OSPF neighbors (so no DR/BDR is elected)

2. Configure one static route recursive on R1 for each internet connection. Make the route on interface f5/0 a floating static route with AD value 1 greater than the default. R1 should function as an OSPF ASBR, advertising its default route to other routers in the domain.

Example Part 5 - R1

```
R1(config)#router ospf 1
R1(config-router)#router-id 10.0.0.76
R1(config-router)#passive-interface loopback0
R1(config)#int l0
R1(config-if)#ip ospf 1 area 0
R1(config-if)#int range f0/0,f1/0
R1(config-if-range)#ip ospf 1 area 0
R1(config-if-range)#ip ospf network point-to-point
```

Example Part 5 - CS1

```
CS1(config)#router ospf 1
CS1(config-router)#router-id 10.0.0.77
CS1(config-router)#passive-interface l0
CS1(config-router)#network 10.0.0.41 0.0.0.0 area 0
CS1(config-router)#network 10.0.0.34 0.0.0.0 area 0
CS1(config-router)#network 10.0.0.45 0.0.0.0 area 0
CS1(config-router)#network 10.0.0.49 0.0.0.0 area 0
CS1(config-router)#network 10.0.0.53 0.0.0.0 area 0
CS1(config-router)#network 10.0.0.57 0.0.0.0 area 0
CS1(config-router)#network 10.0.0.77 0.0.0.0 area 0
```

```
CS1(config-router)#int range g1/0/3,g1/1/1-4
CS1(config-if-range)#ip ospf network point-to-point
```

Example 5 - R1

```
R1(config)#ip route 0.0.0.0 0.0.0.0 203.0.113.1
R1(config)#ip route 0.0.0.0 0.0.0.0 203.0.113.5 2
R1(config)#router ospf 1
R1(config-router)#default-information originate
```

Part 6 - DHCP and DNS

1. Configure DHCP pools on R1 for Office A and B. Exclude the first 10 usable host addresses so they are not leased.
   - Pool a-management (LWAPA1): Subnet 10.0.0.0/28, Default Gateway 10.0.0.1, Domain name sp.com, DNS server 10.5.0.4 (Server1), WLC 10.0.0.7
   - Pool a-pc: Subnet 10.1.0.0/24, default gateway 10.1.0.1, dns server 10.5.0.4, Domain name sp.com.
   - Pool a-phone: Subnet 10.2.0.0/24, default gateway 10.2.0.1, dns server 10.5.0.4, domain name sp.com
   - Pool b-management: subnet 10.0.0.16/28, default router 10.0.0.17m dns server 10.5.0.4, domain name sp.com, option 43 ip 10.0.0.7
   - Pool b-pc: subnet 10.3.0.0/24, default router 10.3.0.1, dns server 10.5.0.4, domain name sp.com
   - Pool b-phone: subnet 10.4.0.0/24, default router 10.4.0.1, dns server 10.5.0.4, domain name sp.com
   - Pool wifi: subnet 10.6.0.0/24, default router 10.6.0.1, dns server 10.5.0.4, domain name sp.com
2. Configure the distribution switches to relay wired DHCP client broadcast messages to R1's Loopback0 IP address.
3. Configure DNS entries on Server1: google.com 172.253.62.100, youtube.com 152.250.31.93, sp.com = 66.235.200.145, www.sp.com = sp.com.
4. Configure Domain name sp.com and DNS server 10.5.0.4 on all routers and switches.

Example 6 - R1

```
R1(config)#ip dhcp excluded-address 10.0.0.1 10.0.0.10
R1(config)#ip dhcp excluded-address 10.1.0.1 10.1.0.10
R1(config)#ip dhcp excluded-address 10.2.0.1 10.2.0.10
R1(config)#ip dhcp excluded-address 10.0.0.17 10.1.0.26
R1(config)#ip dhcp excluded-address 10.3.0.1 10.3.0.10
```

```
R1(config)#ip dhcp excluded-address 10.4.0.1 10.4.0.10
R1(config)#ip dhcp excluded-address 10.6.0.1 10.6.0.10
R1(config)#ip dhcp pool a-management
R1(dhcp-config)#network 10.0.0.0 255.255.255.240
R1(dhcp-config)#default-router 10.0.0.1
R1(dhcp-config)#domain-name sp.com
R1(dhcp-config)#dns-server 10.5.0.4
R1(dhcp-config)#option 43 ip 10.0.0.7
```

Example 6 - DSA1
```
DSA1(config)#int vlan 10
DSA1(config-if)#ip helper-address 10.0.0.76
DSA1(config-if)#int vlan 20
DSA1(config-if)#ip helper-address 10.0.0.76
DSA1(config-if)#int vlan 40
DSA1(config-if)#ip helper-address 10.0.0.76
DSA1(config-if)#int vlan 99
DSA1(config-if)#ip helper-address 10.0.0.76
```

Example 6 - R1
```
R1(config)#ip domain name sp.com
R1(config)#ip name-server 10.5.0.4
```

Part 7 - NTP, SNMP and Syslog

1. Configure R1 as a NTP server - stratum 5 NTP server - IP 216.239.35.0
2. All core, distribution and access switches should use R1's loopback interface as their NTP server. Authenticate with R1 using key **2** and password **time**.
3. Configure SNMP community string **snmpstr** on all routers and switches, should allow all get messages nothing else (read only string not read write)
4. Configure syslog messages to SRV1. All severity levels should be logged. Enable logging to buffer 8196 bytes of memory.

Example 7 - R1
```
R1(config)#ntp master 5
R1(config)#ntp server 216.239.35.0
R1(config)#ntp authentication-key 2 md5 time
R1(config)#ntp trusted-key 2
```

Example 7 - CSA1
```
CS1(config)#ntp authentication-key 2 md5 time
```

CS1(config)#ntp trusted-key 2
CS1(config)#ntp server 10.0.0.76 key 2

Example 7 - R1

R1(config)#snmp-server community snmpstr ro
%SNMP-5-WARMSTART: SNMP agent on host R1 is undergoing a warm start
R1(config)#logging 10.5.0.4
R1(config)#logging trap debugging
R1(config)#logging buffered 8192

Part 8 - FTP, SSH and NAT

1. Use FTP on R1 to download a new IOS version from SRV1, R1 FTP credentials username **mega** password **lab,** Copy the file to R1's flash and reboot using the new file and then delete the old file.
2. Configure SSH for all routers and switches.
   ● Use the largest modulus RSA key
   ● Allow SSHv2 only
   ● Create standard ACL 1 to allow packets from source Office A, PC's subnet, apply to all VTY lines and only allow SSH connection on VTY lines.
   ● Require Login from local user accounts when connecting via SSH.
   ● Configure synchronous logging on VTY lines.
3. Configure static NAT on R1 to enable hosts on the internet to access SRV1 via IP address 203.0.113.133
4. Configure pool based PAT on R1 to enable hosts in both offices to access the internet.
   ● Use standard ACL 2 to define appropriate inside local address ranges in the following order. Office A PC's 10.1.0.0/24, Office A Phones 10.2.0.0/24, Office B PC's 10.3.0.0/24, Office B Phones 10, WiFi 10.6.0.0/24
   ● Define a range of global addresses called POOL1, using range 203.0.113.200 to 203.0.113.207/29 netmask.
   ● Map ACL2 to POOL1 and enable PAT.

Example Part 8 - R1

R1(config)#ip ftp username mega
R1(config)#ip ftp password lab
R1(config)#do copy ftp flash
Address or name of remote host []? 10.5.0.4
Source filename []? pt1000-i-mz.122-28.bin

Destination filename [pt1000-i-mz.122-28.bin]?
%Warning:There is a file already existing with this name
Do you want to overwrite? [confirm]
R1(config)#boot system flash: pt1000-i-mz.122-28.bin
R1(config)#do reload
R1(config)#delete flash: pt1000-i-mz.122-28.bin

Example Part 8 - R1
R1(config)#crypto key generate rsa
The name for the keys will be: R1.sp.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]
R1(config)#ip ssh version 2
*Mar 1 0:5:26.579: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#access-list 1 permit 10.1.0.0 0.0.0.255
R1(config)#line vty 0 15
R1(config-line)#access-class 1 in
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#logging synchronous

Example Part 8 - R1
R1(config)#ip nat inside source static 10.5.0.4 203.0.113.113
R1(config)#int range f4/0,f5/0
R1(config-if-range)#ip nat outside
R1(config-if-range)#int range f0/0,f1/0
R1(config-if-range)#ip nat inside

Example Part 8 - R1
R1(config)#access-list 2 permit 10.1.0.0 0.0.0.255
R1(config)#access-list 2 permit 10.2.0.0 0.0.0.255
R1(config)#access-list 2 permit 10.3.0.0 0.0.0.255
R1(config)#access-list 2 permit 10.4.0.0 0.0.0.255
R1(config)#access-list 2 permit 10.6.0.0 0.0.0.255
R1(config)#ip nat pool POOL1 203.0.113.200 203.0.113.207 netmask
255.255.255.248
R1(config)#ip nat inside source list 2 pool POOL1 overload

Part 9 - Security

1. Extended ACLs: OfficeAtoOfficeB only allows ICMP traffic from Office A PC's subnet to Office B PC's subnet. Block all other traffic from the PC's subnet and allow all other traffic.
2. Port security on each access switch to allow a minimum number of MAC addresses.
3. Configure a violation mode that blocks invalid traffic and a notification should be sent when invalid traffic is detected. Switches should save the secure MAC address they learn to the running configuration. (sticky MAC)
4. IP DHCP snooping on all Access switches - all active VLANS in each LAN. Trust the appropriate ports and disable DHCP option 82, set dhcp rate limit 15pps on active untrusted ports, set a higher 100pps on ASA1 connection to WLC1.
5. Configure DAI on all access switches, enable for all active VLANs, trust appropriate ports and enable all optional validation checks.

Example 9 - DSA1

```
DSA1(config)#ip access-list extended officeatoofficeb
DSA1(config-ext-nacl)#permit icmp 10.1.0.0 0.0.0.255 10.3.0.0 0.0.0.255
DSA1(config-ext-nacl)#deny ip 10.1.0.0 0.0.0.255 10.3.0.0 0.0.0.255
DSA1(config-ext-nacl)#permit ip any any
DSA1(config-ext-nacl)#int vlan 10
DSA1(config-if)#ip access-group officeatoofficeb in
```

Example 9 - ASA1

```
ASA1(config)#int f0/1
ASA1(config-if)#switchport port-security
ASA1(config-if)#switchport port-security violation restrict
ASA1(config-if)#switchport port-secuirty mac-address sticky
ASA1(config-if)#switchport port-security mac-address sticky
```

Example 9 - ASA1

```
ASA1(config)#ip dhcp snooping
ASA1(config)#ip dhcp snooping vlan 10,20,40,99
ASA1(config)#no ip dhcp snooping information option
ASA1(config)#int range f2/1,f3/1
ASA1(config-if-range)#ip dhcp snooping trust
ASA1(config-if-range)#int f0/1
ASA1(config-if)#ip dhcp snooping limit rate 15
ASA1(config-if)#int f1/1
```

ASA1(config-if)#ip dhcp snooping limit rate 100

Example 9 - ASA1
    ASA1(config)#ip arp inspection vlan 10,20,40,99
    ASA1(config)#ip arp inspection validate dst-mac src-mac ip
    ASA1(config)#int range f2/1,f3/1
    ASA1(config-if-range)#ip arp inspection trust

Part 10 - IPv6
1. Enable IPv6 Routing on R1 and the Core switches.
    - R1 f4/0 2001:db8:a::2/64
    - R1 f5/0 2001:db8:b::2/64
    - R1 f0/0 and CS1 G1/0/3 2001:db8:a1::/64 EUI 64 interface ID
    - R1 f1/0 and CS2 g1/0/3 2001:db8:a2::/64 EUI 64 interface ID
    - CS1 po1 and CS2 po1 enable IPv6 auto generate IP

Example 10 CS1
    CS1(config)#ipv6 unicast-routing
    CS1(config)#int g1/0/3
    CS1(config-if)#ipv6 add
    CS1(config-if)#ipv6 address 2001:db8:a1::/64 eui-64
    CS1(config-if)#int po1
    CS1(config-if)#ipv6 enable

Part 11 - WiFi
1. Access the GUI on WLC1 10.0.0.7 via PC1
2. Configure dynamic interface for WiFi WLAN 10.0.0.6/24
    - Name Wi-Fi
    - VLAN 40
    - Port number 1
    - IP .10.6.0.2
    - Gateway 10.6.0.1
    - DHCP server 10.0.0.76 (R1 Loopback)
3. Enable the following WLAN
    - Profile Name Wi-Fi
    - SSID WiFi
    - ID 1
    - Status Enabled
    - Security WPA2 police with AES encryption, PSK of megalab1