Enterprise Network

Part 1 - Initial setup

1. Configure the appropriate hostname on each router/switch.
2. Configure the enable secret **jeremysitlab** on each router/switch. Use type 9 hashing if available; otherwise, use type 5.
3. Configure the user account **cisco** with secret **ccna** on each router/switch. Use type 9 hashing if available; otherwise, use type 5.
4. Configure the console line to require login with a local user account. Set a 30-minute inactivity timeout. Enable synchronous logging.

Part 2 – VLANs, Layer-2 EtherChannel

1. In Office A, configure a Layer-2 EtherChannel named **PortChannel1** between DSW-A1 and DSW-A2 using a Cisco-proprietary protocol. Both switches should actively try to form an EtherChannel.

2. In Office B, configure a Layer-2 EtherChannel named **PortChannel1** between DSW-B1 and DSW-B2 using an open standard protocol. Both switches should actively try to form an EtherChannel.

3. Configure all links between Access and Distribution switches, including the EtherChannels, as trunk links.

a. Explicitly disable DTP on all ports.

b. Set each trunk's native VLAN to VLAN 1000 (unused).

c. In Office A, allow VLANs 10, 20, 40, and 99 on all trunks.

d. In Office B, allow VLANs 10, 20, 30, and 99 on all trunks.

4. Configure one of each office's Distribution switches as a VTPv2 server. Use domain name **JeremysITLab**.

a. Verify that other switches join the domain.

b. Configure all Access switches as VTP clients.

5. In Office A, create and name the following VLANs on one of the Distribution switches. Ensure that VTP propagates the changes.

a. VLAN 10: PCs

b. VLAN 20: Phones

c. VLAN 40: Wi-Fi

d. VLAN 99: Management

6. In Office B, create and name the following VLANs on one of the Distribution switches. Ensure that VTP propagates the changes.

a. VLAN 10: PCs

b. VLAN 20: Phones

c. VLAN 30: Servers

d. VLAN 99: Management

7. Configure each Access switch's access port.

a. LWAPs will not use FlexConnect

b. PCs in VLAN 10, Phones in VLAN 20

c. SRV1 in VLAN 30

d. Manually configure access mode and explicitly disable DTP

8. Configure ASW-A1's connection to WLC1:

a. It must support the Wi-Fi and Management VLANs.

b. The Management VLAN should be untagged.

c. Disable DTP.

9. Administratively disable all unused ports on Access and Distribution switches.

Part 3 – IP Addresses, Layer-3 EtherChannel, HSRP

1. Configure the following IP addresses on R1's interfaces and enable them:

a. G0/0/0: DHCP client

b. G0/1/0: DHCP client

c. G0/0: 10.0.0.33/30

d. G0/1: 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 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

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

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

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

10. Manually configure SRV1's IP settings:

a. Default Gateway: 10.5.0.1

b. IPv4 Address: 10.5.0.4

c. Subnet Mask: 255.255.255.0

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

12. Configure HSRPv2 group 1 for Office A's Management subnet (VLAN 99). Make DSW-A1 the Active router by increasing its priority to 5 above the default, and enable preemption on DSW-A1.

a. Subnet: 10.0.0.0/28

b. VIP: 10.0.0.1

c. DSW-A1: 10.0.0.2

d. DSW-A2: 10.0.0.3

13. Configure HSRPv2 group 2 for Office A's PCs subnet (VLAN 10). Make DSW-A1 the Active router by increasing its priority to 5 above the default, and enable preemption on DSW-A1.

a. Subnet: 10.1.0.0/24

b. VIP: 10.1.0.1

c. DSW-A1: 10.1.0.2

d. DSW-A2: 10.1.0.3

14. Configure HSRPv2 group 3 for Office A's Phones subnet (VLAN 20). Make DSW-A2 the Active router by increasing its priority to 5 above the default, and enable preemption on DSW-A2.

a. Subnet: 10.2.0.0/24

b. VIP: 10.2.0.1

c. DSW-A1: 10.2.0.2

d. DSW-A2: 10.2.0.3

15. Configure HSRPv2 group 4 for Office A's Wi-Fi subnet (VLAN 40). Make DSW-A2 the Active router by increasing its priority to 5 above the default, and enable preemption on DSW-A2.

a. Subnet: 10.6.0.0/24

b. VIP: 10.6.0.1

c. DSW-A1: 10.6.0.2

d. DSW-A2: 10.6.0.3

16. Configure HSRPv2 group 1 for Office B's Management subnet (VLAN 99). Make DSW-B1 the Active router by increasing its priority to 5 above the default, and enable preemption on DSW-B1.

a. Subnet: 10.0.0.16/28

b. VIP: 10.0.0.17

c. DSW-B1: 10.0.0.18

d. DSW-B2: 10.0.0.19

17. Configure HSRPv2 group 2 for Office B's PCs subnet (VLAN 10). Make DSW-B1 the Active router by increasing its priority to 5 above the default, and enable preemption on DSW-B1.

a. Subnet: 10.3.0.0/24

b. VIP: 10.3.0.1

c. DSW-B1: 10.3.0.2

d. DSW-B2: 10.3.0.3

18. Configure HSRPv2 group 3 for Office B's Phones subnet (VLAN 20). Make DSW-B2 the Active router by increasing its priority to 5 above the default, and enable preemption on DSW-B2.

a. Subnet: 10.4.0.0/24

b. VIP: 10.4.0.1

c. DSW-B1: 10.4.0.2

d. DSW-B2: 10.4.0.3

19. Configure HSRPv2 group 4 for Office B's Servers subnet (VLAN 30). Make DSW-B2 the Active router by increasing its priority to 5 above the default, and enable preemption on DSW-B2.

a. Subnet: 10.5.0.0/24

b. VIP: 10.5.0.1

c. DSW-B1: 10.5.0.2

d. DSW-B2: 10.5.0.3

Part 4 – Rapid Spanning Tree Protocol

1. Configure Rapid PVST+ on all Access and Distribution switches.

a. Ensure that the Root Bridge for each VLAN aligns with the HSRP Active router by configuring the lowest possible STP priority.

b. Configure the HSRP Standby Router for each VLAN with an STP priority one increment above the lowest priority.

2. Enable PortFast and BPDU Guard on all ports connected to end hosts (including WLC1). Perform the configurations in interface config mode.

Part 5 – 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.

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.

Part 6 – Network Services: DHCP, DNS, NTP, SNMP, Syslog, FTP, SSH, NAT

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)

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

3. Configure the following DNS entries on SRV1:

a. google.com = 172.253.62.100

b. youtube.com = 152.250.31.93

c. jeremysitlab.com = 66.235.200.145

d. www.jeremysitlab.com = jeremysitlab.com

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

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**.

7. Configure the SNMP community string **SNMPSTRING** on all routers and switches. The string should allow GET messages, but not SET messages.

8. Configure Syslog on all routers and switches:

a. Send Syslog messages to SRV1. Messages of all severity levels should be logged.

b. Enable logging to the buffer. Reserve 8192 bytes of memory for the buffer.

9. Use FTP on R1 to download a new IOS version from SRV1:

a. Configure R1's default FTP credentials: username **cisco**, password **cisco**.

b. Use FTP to copy the file **c2900-universalk9-mz.SPA.155-3.M4a.bin** from SRV1 to R1's flash drive.

c. Reboot R1 using the new IOS file, and then delete the old one from flash.

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.

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

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.

d. Verify that Internet link failover works by disabling R1's G0/0/0 interface and pinging again.

i. You will need to remove and re-configure the OSPF default-information originate command for this to work. In real Cisco routers, you can configure the default-information originate always command that supports failover like this, but the command isn't available in Packet Tracer.

ii. Re-enable G0/0/0 (and remove and re-configure default-information originate once again).

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

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

Part 7 – Security: ACLs and Layer-2 Security Features

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.

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.

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.

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.

Part 8 – IPv6

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.

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.

Part 9 – Wireless

1. Access the GUI of WLC1 (https://10.0.0.7) from one of the PCs.

a. Username: admin

b. Password: adminPW12

2. Configure a dynamic interface for the Wi-Fi WLAN (10.6.0.0/24)

a. Name: Wi-Fi

b. VLAN: 40

c. Port number: 1

d. IP address: .4 of its subnet

e. Gateway: .1 of its subnet

f. DHCP server: 10.0.0.76

3. Configure and enable the following WLAN:

a. Profile name: Wi-Fi

b. SSID: Wi-Fi

c. ID: 1

d. Status: Enabled

e. Security: WPA2 Policy with AES encryption, PSK of cisco123

4. Verify that both LWAPs have associated with WLC1.

a. Due to Packet Tracer's limitations, wireless clients won't be able to lease an IP address from the Wi-Fi DHCP pool.