Small Branch Office Network

Description:

This project scenario involves designing a small-scale network for a company that emphasizes wireless connectivity, VoIP services, and robust security features. The network will incorporate various protocols such as RSTP, VLANs, HSRP, EIGRP, DNS, DHCP, NAT/PAT, SSH, Wireless LAN Controller, RADIUS (AAA), Port Security, DHCP Snooping, Dynamic ARP Inspection, QoS, ACLs and VoIP. Cisco Packet Tracer has been used to design this network.

Network Topology:

The network will be divided into three layers: Core, Distribution, and Access. Each layer will have two switches to ensure redundancy and scalability.

The network consists of the following devices:

- 1 Cisco 2811 Router
- 3 Cisco 2911 Routers
- 6 Cisco 3650 Layer 3 Switches
- 4 Cisco 2960 Layer 2 Switches
- 2 Cisco 3702i Access Points
- 1 Cisco WLC-3504 Wireless LAN Controller
- 8 PCs
- 4 Laptops
- 2 Printers
- 2 Cisco 7960 IP Phones
- 1 Server

Connections:

- R1:
  F0/0 <> CSW1 G1/0/1
  F0/1 <> CSW2 G1/0/1
  G0/1/0 <> ISP1 G0/0/0
  G0/2/0 <> ISP2 G0/0/0
- ISPs:
  ISP1 G0/1/0 <> ISP2 G0/1/0
  ISP1 G0/2/0 <> Internet G0/1/0
  ISP2 G0/2/0 <> Internet G0/2/0

- CSW-1:
  G1/0/1 <> R1 F0/0
  G1/0/2 <> CSW-2 G1/0/2
  G1/0/3 <> CSW-2 G1/0/3
  G1/1/1 <> DSW-A1 G1/1/1
  G1/1/2 <> DSW-A2 G1/1/1
  G1/1/3 <> DSW-B1 G1/1/1
  G1/1/4 <> DSW-B2 G1/1/1
- DSW-A1:
  G1/0/3 <> DSW-A2 G1/0/3
  G1/0/4 <> DSW-A2 G1/0/4
  G1/1/1 <> CSW-1 G1/1/1
  G1/1/2 <> CSW-2 G1/1/1
  G1/0/5 <> Server-1
  G1/0/1 <> ASW-A1 G0/1
  G1/0/2 <> ASW-A2 G0/1
- DSW-B1:
  G1/0/3 <> DSW-B2 G1/0/3
  G1/0/4 <> DSW-B2 G1/0/4
  G1/1/1 <> CSW-1 G1/1/3
  G1/1/2 <> CSW-2 G1/1/3
  G1/0/1 <> ASW-B1 G0/1
  G1/0/2 <> ASW-B2 G0/1
- ASW-A1:
  F0/1 <> WLC
  F0/4 <> WLC
  F0/2 <> Phone-1
  F0/3 <> PC-A2
  G0/1 <> DSW-A1 G1/0/1
  G0/2 <> DSW-A2 G1/0/1
- ASW-B1:
  F0/1 <> Phone-2
  F0/2 <> PC-B2
  F0/3 <> AP-2
  G0/1 <> DSW-B1 G1/0/1
  G0/2 <> DSW-B2 G1/0/1

- CSW-2:
  G1/0/1 <> R1 F0/1
  G1/0/2 <> CSW-1 G1/0/2
  G1/0/3 <> CSW-1 G1/0/3
  G1/1/1 <> DSW-A1 G1/1/2
  G1/1/2 <> DSW-A2 G1/1/2
  G1/1/3 <> DSW-B1 G1/1/2
  G1/1/4 <> DSW-B2 G1/1/2
- DSW-A2:
  G1/0/3 <> DSW-A1 G1/0/3
  G1/0/4 <> DSW-A1 G1/0/4
  G1/1/1 <> CSW-1 G1/1/2
  G1/1/2 <> CSW-2 G1/1/2
  G1/0/1 <> ASW-A1 G0/2
  G1/0/2 <> ASW-A2 G0/2
- DSW-B2:
  G1/0/3 <> DSW-B1 G1/0/3
  G1/0/4 <> DSW-B2 G1/0/4
  G1/1/1 <> CSW-1 G1/1/4
  G1/1/2 <> CSW-2 G1/1/4
  G1/0/1 <> ASW-B1 G0/2
  G1/0/2 <> ASW-B2 G0/2
- ASW-A2:
  F0/1 <> AP-1
  F0/2 <> PC-A3
  F0/3 <> PC-A4
  F0/4 <> Printer-1
  G0/1 <> DSW-A2 G1/0/2
  G0/2 <> DSW-A2 G1/0/2
- ASW-B2:
  F0/1 <> PC-B3
  F0/2 <> PC-B4
  F0/3 <> Printer-2
  G0/1 <> DSW-B1 G1/0/2
  G0/2 <> DSW-B2 G1/0/2

IP Addressing Plan:

Networks:

VLAN 10 (Management)	10.1.0.0/24	10.1.1.0/24
VLAN 20 (PCs)	10.2.0.0/24	10.2.1.0/24
VLAN 30 (Phones)	10.3.0.0/24	10.3.1.0/24
VLAN 40 (Wireless)	10.4.0.0/24	10.4.1.0/24

NOTE: ".1" addresses are VIP for HSRP (DG for the subnet), ".2" and ".3" addresses are for SVIs.

Connections:

R1 <> CSW1	10.0.0.0/30
R1 <> CSW2	10.0.0.4/30
R1 <> ISP1	150.10.112.0/30
R1 <> ISP2	150.10.113.0/30

CSW1 <> DSW-A1	10.0.0.12/30
CSW1 <> DSW-A2	10.0.0.16/30
CSW1 <> DSW-B1	10.0.0.20/30
CSW1 <> DSW-B2	10.0.0.24/30
CSW1 <> CSW2	10.0.0.8/30

CSW2 <> DSW-A1	10.0.0.28/30
CSW2 <> DSW-A2	10.0.0.32/30
CSW2 <> DSW-B1	10.0.0.36/30
CSW2 <> DSW-B2	10.0.0.40/30

Loopbacks:

R1	10.0.0.100/32
CSW1	10.0.0.101/32
CSW2	10.0.0.102/32

DSW-A1	10.0.0.103/32
DSW-A2	10.0.0.104/32
DSW-B1	10.0.0.105/32
DSW-B2	10.0.0.106/32

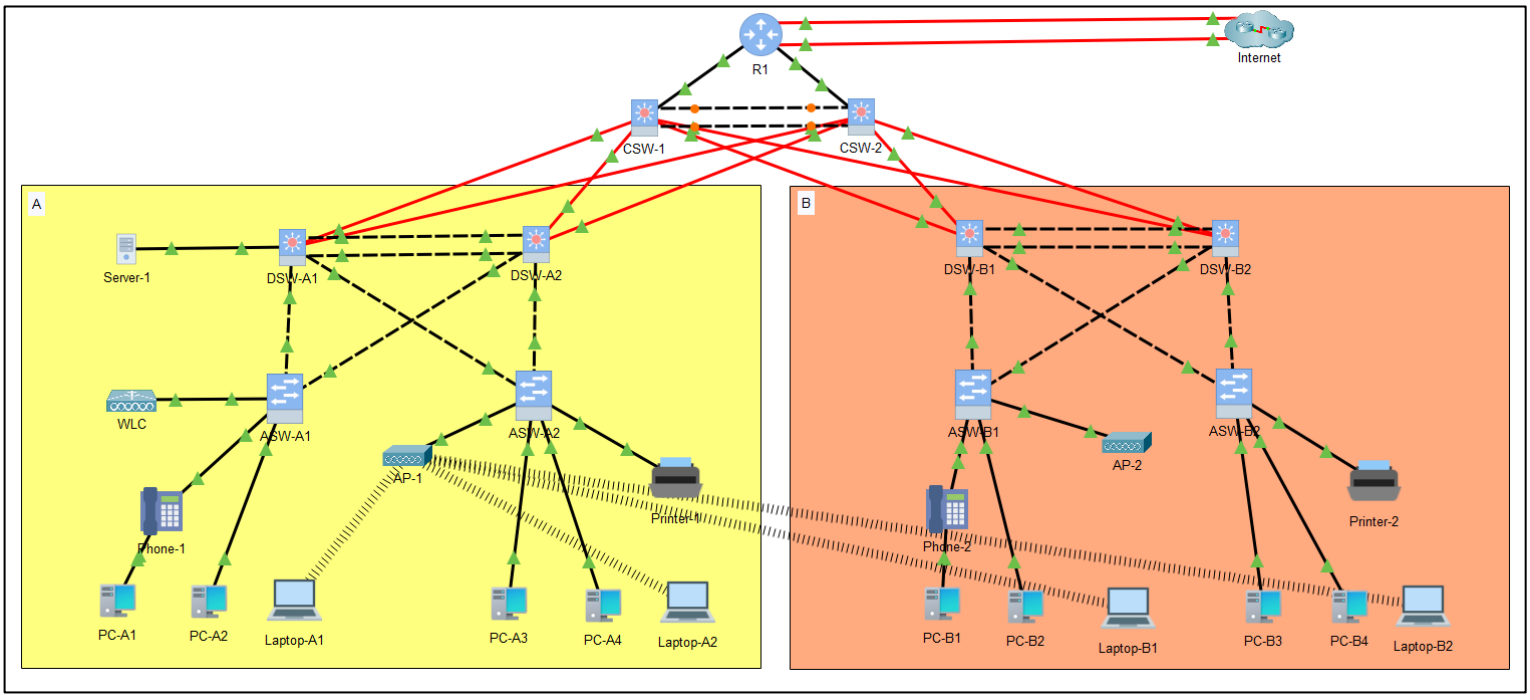
VLAN Interfaces:

ASW-A1	10.1.0.4/24
ASW-A2	10.1.0.5/24
ASW-B1	10.1.1.4/24
ASW-B2	10.1.1.5/24

Static IP Addresses:

WLC	10.1.0.6/24
AP1	10.1.0.7/24
AP2	10.1.1.7/24
SRV1	10.1.0.8/24

Topology Diagram:



Configuration:

Part 1:

1. Configure Hostnames for all devices.
2. Configure a Layer 2 EtherChannel b/w Distribution switches, which uses interfaces G1/0/3 and G1/0/4:
   - Disable DTP
   - Switchport mode is Trunk
   - Allowed VLANs: 10, 20, 30, 40
   - Native VLAN: 1000
   - Channel Protocol: LACP
   - Channel Mode: Active
3. Links b/w DSWs and ASWs are configured as trunks:
   - Disable DTP
   - Switchport mode is Trunk
   - Allowed VLANs: 10, 20, 30, 40
   - Native VLAN: 1000
4. DSW-A2 and DSW-B2 are configured as VTP servers and other Access and Distribution switches as VTP clients:
   - Domain Name: Office
   - VTP Version: 2
   - Configure VLAN names
5. Configure ASWs ports connecting to end devices:
   - Switchport mode is Access
   - Access VLAN is configured accordingly
   - Voice VLAN is 30
   - Disable DTP
6. Disable all the unused interfaces.

Part 2:

1. Configure all the IP addresses based on the connections and IP addressing plan above.
2. Configure Loopbacks and SVIs (for DSWs). Configure VLAN interfaces and default gateway for ASWs.
   NOTE: Enable ip routing on L3 switches.
3. Configure a Layer 3 EtherChannel b/w CSW1 <> CSW2:
   - Channel Protocol: PAgP

- Channel Mode: Desirable
- Configure IP addresses on Port Channel Interfaces.

4. HSRP Configuration:

	VLAN 10 (Grp 1)	VLAN 20 (Grp 2)	VLAN 30 (Grp 3)	VLAN 40 (Grp 4)
DSW-A1	Active	Active	Standby	Standby
DSW-A2	Standby	Standby	Active	Active
DSW-B1	Active	Active	Standby	Standby
DSW-B2	Standby	Standby	Active	Active

- Configure HSRP on the SVIs of DSWs.
- For each subnet the ".1" address will be the Virtual IP.
- Preempt active gateway and increase its priority to 105.

Part 3:

1. RSTP:
   - Spanning tree mode: Rapid PVST+
   - DSW-A1 & DSW-B1: Primary for VLAN 10 & 20, Secondary for VLAN 30 & 40
   - DSW-A2 & DSW-B2: Primary for VLAN 30 & 40, Secondary for VLAN 10 & 20
   - Ensure that the RSTP topology matches that of HSRP.
2. Configure PortFast and BPDU Guard on ASWs interfaces.

Part 4:

1. EIGRP:
   - Configure EIGRP on R1, CSWIs and DSWs.
   - AS Number: 65000
   - Configure loopbacks as Router IDs.
   - Configure loopbacks and SVIs as Passive.
   - Disable auto-summarization.
2. Configure static routes on R1 to ISPs and redistribute them in EIGRP.

Part 5:

1. DHCP:
   - Server 1 is configured as the DHCP server for Management, PCs and Wireless subnets only.
   - First 10 addresses if all subnets are reserved, so the start IP for all pools is from ".11"

- DNS server for all subnets is Server 1 (10.1.0.8)
- Default router will be ".1" address of each subnet.
- Configure DSWs as relay agents.

2. VoIP:
   - R1 is configured as DHCP server for the Phones' subnets.
   - DHCP option 150 (TFTP server) is configured as 10.0.0.100 and domain name is "myoffice.com"

   NOTE: Only the Cisco 2811 router supports IP Telephony configuration in Packet Tracer, hence it has been used as the CUCME.

   - Configure telephony service on R1:
     - Max-ephones: 10
     - Max-dn:10
     - Source-address: 10.0.0.100
     - Port: 2000
     - Auto assign 1 to 10
   - Configure the 10 directory numbers.
   - Configure DSWs as relay agents.
3. Port-Security, DHCP Snooping, DAI:

   a) Port-Security:
      - Enable Port-Security on interfaces connecting to end devices.
      - Enable sticky MAC address learning.
      - Max MAC addresses allowed on the interfaces should be 2 for interfaces connected to IP Phones and default for other interfaces.
      - Interfaces connected to printers are configured with static MAC addresses of the printers.
      - Violation mode: Restrict

   b) DHCP Snooping:
      - Enable DHCP snooping on ASWs and DSWs
      - Enable for all VLANs.
      - Downlink ports are to remain untrusted, uplink ports are configured as trusted.
      - Disable option 82 on ASWs.
      - Configure rate limiting to 10 on untrusted interfaces.

      NOTE: Packet tracer doesn't support configuring PortChannel interfaces as trusted interfaces, which causes DSWs to not function properly as relay agents. A workaround is to configure the following commands:

      - *"ip dhcp snooping information option allow-untrusted"* is configured on DSWs.

- *"ip dhcp relay information trust all"* is configured on R1 to allow IP telephony to work properly.

c) Dynamic ARP Inspection:
   - Enable DHCP snooping on ASWs and DSWs
   - Enable for all VLANs.
   - Interfaces connected to end hosts are untrusted.
   - Interfaces connected to network devices are trusted.
   - Enable validation using src-mac, dst-mac, and ip.

4. CDP:
   - By default CDP is enabled for all interfaces on Cisco devices.
   - Disable CDP on interfaces connected to end hosts.
   - Disable CDP on interfaces on R1 that are connected to the ISPs.
5. NAT(PAT):
   - Configure a standard ACL to permit the 10.0.0.0/8 network.
   - Configure PAT on R1.
6. DNS:
   - Configure A records and CNAME records for the following, on Server 1:
     - google.com – www.google.com - 171.26.10.62/32
     - youtube.com – www.youtube.com – 153.16.120.10/32
   - Configure the above IP addresses as loopbacks on the router named "Internet"
7. QoS:
   - Match traffic using NBAR - Configure class-maps on DSWs to match RTP and ICMP traffic, and configure descriptions for each.
   - Configure policy-map name "Office"
     - For class RTP configure priority bandwidth of 200 kbps and set DSCP value to EF.
     - For class ICMP configure minimum bandwidth of 50 kbps and set DSCP value to AF11.
   - Configure the policy-map for outbound traffic on interfaces connected to CSWs.
   - Configure QoS on R1 for ICMP traffic using the same parameters as above and enable the policy-map for outbound traffic on interfaces connected to CSWs.

NOTE: Packet tracer seems to have an issue with marking RTP packets. But a workaround method is used:

- Configure extended ACL "*access-list 100 permit udp any range 1024 65535 any*" on DSWs.
- The port range "1024-65535" is used because RTP uses random port numbers from the ephemeral port range.

- Remove the "*match protocol rtp*" command from the class-map for RTP, and add the command, *"match access-group 100"*. This means that the class-map will match packets using ACL 100 and not using NBAR.

8. WLC configuration:
   - Basic setup for WLC is done by connecting a PC directly to it. Configure the PCs IP address from the 192.168.1.0/28 range.
   - Parameters configured during basic setup:
     - Admin Username: admin
     - Admin Password: Myoffice#1
     - System Name: WLC
     - Management IP Address: 10.1.0.6/24
     - Default Gateway: 10.1.0.1
     - Management VLAN ID: 10
     - Network Name: CORP
     - Security: WPA2 enterprise
     - Authentication Server: 10.1.0.8
     - Authentication Server Shared Secret: Myoffice#2
   - Once basic setup is completed, WLC's web UI can be accessed through HTTPS connections from any of the PCs.
   - Configure interfaces for the 2 wireless subnets.
   - Configure WLANs:
     - Profile name and SSID should be the same for each WLAN.
     - Select the Interface to be matched.
     - L2 security – WPA2 AES – PSK: Myoffice#3
9. AAA:
   - Configure credentials for the network devices:
     - Username: admin
     - Password: myoffice3
     - Enable Secret: myoffice3
     - Configure type 5 (md5) secret for ASWs & R1 and type 9 (scrypt) secret for CSWs & DSWs.
   - Server 1 will be configured as the RADIUS server.
   - Configure Client name, IP and Key for all hosts, on Server 1. Key will be "Myoffice1" for all hosts.

     NOTE: Packet tracer doesn't support configuring the source interface for RADIUS packets, hence the packets are not sent from their loopbacks. Instead they are sent

from the physical interfaces itself. To solve this problem configure multiple entries on Server 1 for each of the interfaces of each host from which RADIUS packets can be sent.

- Configure the network devices:
  - Configure Username: admin & Password: myoffice2 for AAA authentication.
  - Enable AAA new-model.
  - Configure AAA authentication for login and enable using default group of "radius" and a fallback of "local"
  - Configure RADIUS server's IP address "10.1.0.8" and key "myoffice1"

10. SSH:
    - SSH is enabled on all network devices.
    - Domain Name: myoffice.com
    - Generate SSH keys – Key length should be the maximum possible value.
    - Enable SSH version 2
    - On vty lines 0 to 4:
      - Only SSH connections should be allowed.
      - Enable logging synchronous.
      - Login authentication method is default.
      - Configure standard ACL to permit connections only from the 10.2.0.0/24 network.
    - On vty lines 5 to 15, disable both telnet and SSH connections.

Finally, verify all the configurations using the corresponding show commands.