Packet Tracer Lab –Setting up WAN infrastructure

Background

In this packet tracer activity you will design and configure the network and all users in each LAN must communicate and also to the internet, to perform this PKT activity you must follow all procedures and steps need to finish setting up this network.

Objective

Part 1: Design and setup devices

Part 2: Configure the network devices

Part 3: Test the connectivity between devices

Addressing Table

Device	Interface	IP Address	Subnet Mask
ISP	Gi0/0	200.20.20.1	255.255.255.0
	Gi0/0/0	221.11.11.1	255.255.255.252
Central-Office	Gi0/0	172.16.1.1	255.255.255.0
	Gi0/1	172.16.2.1	255.255.255.0
	Se0/1/0	222.11.11.1	255.255.255.252
Edge-router	Se0/1/0	222.11 11.2	255.255.255.252
	Gi0/0/0	221.11.11.2	255.255.255.252
	Se0/1/1	223.11.11.1	255.255.255.252
ISP	Gi0/0	200.20.20.1	255.255.255.0
	Gi0/0/0	221.11.11.1	255.255.255.252
Branch-Office	Gi0/0.100	192.168.10.1	255.255.255.0
	Gi0/0.200	192.168.20.1	255.255.255.0
	Se0/1/1	223.11.11.2	255.255.255.252
WRT-LAN	Internet	172.16.2.254	255.255.255.0
Engineers-sw1	Vlan100	192.168.10.100	255.255.255.0
Finance-sw2	Vlan200	192.168.20.100	255.255.255.0
Google server	Fa0/0	200.20.20.222	255.255.255.0
FTP server	Fa0/0	172.16.1.100	255.255.255.0

Part 1: Design and setup devices

Design and setup all devices referring to given topology with every connection to its attached ports.

Part 2: Configure network devices

Step 1: Initial device configurations.

All network devices must be configured well configured with initial configurations including hostname, banner message and password to all access lines to prevent them from unauthorized access so for this case now you need begin with initial device configuration to all network devices.

1. Access the **Central office** router and configure the following.

a) Hostname to **Central-office**
b) Banner message to “ **This system is for the use of authorized users only**”
c) Secure the privilege Exec mode secret using **Centraloff11@**
d) Configure the clock set to active UTC time.
e) Configure the Syslog message.
f) Configure SSH remote access to this router remote passkey **Centraloff12@**
g) Assign ip address to all interfaces referring to the addressing table.
h) Configure DHCP for ip address auto assigment
i) Configure the Tacacs+ server configurations.
j) Configure FTP

2. Access the **Adm-Sw1** and configure the following configuration.

a) Hostname **Adm-Sw1**
b) Banner message to “ **This system is for the use of authorized users only**”
c) Secure the privilege Exec mode secret using **Admiswitch@11**
d) Secure all access lines using **Admiswitch@12**
e) Configure the clock set to active UTC time.
f) Configure the Syslog message.

g) Configure SSH remote access to this router remote passkey **Admiswitch@13**
h) Assign ip address to interface **vlan 1** using **172.16.1.200/24**
i) Configure a gateway address to switch
j) Configure Port security to all servers (FTP server: **Fa0/3 ,** AAA Tacacs server: **Fa0/23)**
k) Configure DHCP snooping for DHCP server.
l) enable Bpdu guard and root guard to all switches to secure STP attacks
m) Configure FTP

3. Access the **Sales-Sw2** and configure the following configuration.

a) Hostname **Sales-Sw2**
b) Banner message to " **This system is for the use of authorized users only**"
c) Secure the privilege Exec mode secret using **Salesswi@11**
d) Secure all access lines using **Salesswi@12**
e) Configure the clock set to active UTC time.
f) Configure the Syslog message.
g) Configure SSH remote access to this router remote passkey **Salesswi@13**
h) Assign Ip address to interface **vlan 1** using **172.16.2.200/24**
i) Configure a gateway address to switch
j) Configure Port security to WRT-LAN connected port **G0/2**
k) enable Bpdu guard and root guard to all switches to secure STP attacks
l) Configure FTP

4. Access the **Edge-router** router and configure the following.

a) Hostname to **Edge-router**
b) Banner message to " **This system is for the use of authorized users only**"
c) Secure the privilege Exec mode secret using **Edgerou@11**
d) Create account username using **Admin** password **Edgerou@12**
e) Secure console line using local account
f) Configure SSH remote access to this router remote passkey **Edgerou@13**
g) Configure the clock set to active UTC time.
h) Configure the Syslog message.
i) Assign ip address to all interfaces referring to the addressing table.
j) Configure FTP

5. Access the **ISP** router and configure the following.

a) Hostname to **ISP**
b) Banner message to “**This system is for the use of authorized users only**”
c) Secure the privilege Exec mode secret using **Isp@11**
d) Create account username using **Admin** password **Isp@12**
e) Secure console line using local account
f) Configure SSH remote access to this router remote passkey **Isp@13**
g) Configure the clock set to active UTC time.
h) Configure the Syslog message.
i) Assign ip address to all interfaces referring to the addressing table.

6. Access the **Branch-office** router and configure the following.

a) Hostname to **Branch-office**
b) Banner message to “**This system is for the use of authorized users only**”
c) Secure the privilege Exec mode secret using **Branch@11**
d) Create account username using **Admin** password **Branch@12**
e) Secure console line using local account
f) Configure SSH remote access to this router remote passkey **Branch@13**
g) Configure the clock set to active UTC time.
h) Configure the Syslog message.
i) Assign ip address to all interfaces referring to the addressing table.
j) Configure FTP

7. Access the **Engineers-Sw1** and configure the following configuration.

a) Hostname **Engineers-Sw1**
b) Banner message to “ **This system is for the use of authorized users only**”
c) Secure the privilege Exec mode secret using **Engin@11**
d) Secure all access lines using **Engin@12**
e) Configure the clock set to active UTC time.
f) Configure the Syslog message.
g) Configure SSH remote access to this router remote passkey **Engin@13**
h) Assign Ip address to interface **vlan 100** using **192.168.10.100/24**
i) Configure a gateway address to switch
j) Configure Port security to **Engineers-Ap** connected port **Fa0/24**
k) enable Bpdu guard and root guard to all switches to secure STP attacks
l) Disable all remaining ports to auto negation to secure Trunks attack
m) Configure FTP

8. Access the **Finance-Sw2** and configure the following configuration.

a) Hostname **Finance-Sw2**
b) Banner message to " **This system is for the use of authorized users only**"
c) Secure the privilege Exec mode secret using **Finance@11**
d) Secure all access lines using **Finance@12**
e) Configure the clock set to active UTC time.
f) Configure the Syslog message.
g) Configure SSH remote access to this router remote passkey **Finance@13**
h) Assign Ip address to interface **vlan 100** using **192.168.20.100/24**
i) Configure a gateway address to switch
j) Configure Port security to **Finance-Ap** connected port **Fa0/23**
k) enable Bpdu guard and root guard to all switches to secure STP attacks
l) Disable all remaining ports to auto negation to secure Trunks attack
m) Configure FTP

Step 2: Configure VLANs to all switches in Branch-office.

After now we are done with the initial device configurations to all device the next step now here is to configure Vlans on switches and assign the given connected interfaces to their corresponding vlans.

Addressing Table

Device	Interface	IP Address	VLAN
HOST-A	NIC	DHCP Assigned	100
HOST-B	NIC	DHCP Assigned	100
HOST-C	NIC	DHCP Assigned	100
HOST-D	NIC	DHCP Assigned	200
HOST-E	NIC	DHCP Assigned	200
HOST-F	NIC	DHCP Assigned	200
Engineers-Ap	NIC	DHCP Assigned	100
Finance-Ap	NIC	DHCP Assigned	200

1. Access **Engineers-Sw1** and create the given vlans
    A. Vlan 100 name **Engineers-Dpt**
    B. Vlan 99 name **Native**
    C. Assing the host computers to the given vlan to access using the addressing table

2. Access **Finance-Sw2** and create the given vlans
    D. Vlan 100 name **Finance-Dpt**
    E. Vlan 99 name **Native**
    F. Assing the host computers to the given vlan to access using the addressing table

Step 3: Configure Link aggregation/Ether-channel to all switches.

After now we are done with configuring vlan to all switches now the is to configure link aggregation to ports that connects Engineers and Finance switch.

Port Channel	Devices	Port Connections	Type
1	**Engineers-Sw1-Finance-Sw2**	G0/1 to G0/1	LACP
		G0/2 to G0/2	

1. Access **Engineers-Sw1** and configure the appropriate required configuration to apply Link aggregation
2. Access **Finance-Sw2** and configure the appropriate required configuration to apply Link aggregation.

Step 4: Configure Trunking on Switches.

After we are done now with applying the link aggregation to our switch, so now the step is to configure trunking to the Port-channel that connects the both switches we have created.

1. Access the **Engineers-Sw1**.

A. Access the **Port-channel 1** interface that we have created to our previous step we did.
B. Configure the **Port-channel 1** as a trunk port and assign to Native vlan 99 we have created.
C. Allow the port-channel 1 to carry all vlan traffics.
D. Exit the interface and disable all remaining port Auto-negation mode

2. Access the **Finance-Sw2**.

E. Access the **Port-channel 1** interface that we have created to our previous step we did.
F. Configure the **Port-channel 1** as a trunk port and assign to Native vlan 99 we have created.
G. Allow the port-channel 1 to carry all vlan traffics.
H. Exit the interface and disable all remaining port Auto-negation mode

Step 5: Configure Inter-Vlan

At this part now we are going to configure the Inter-vlan routing to allow different vlans to communicate.

1. Configure sub interfaces on Branch-office using the 802.1Q encapsulation.

a. Access the Branch-Office and create the sub interface G0/0.100 and G0/0.200.

- Set the encapsulation type to 802.1Q and assign VLAN 10 to the sub interface.
- Refer to the **Address Table** and assign the correct IP address to the sub interface.

Step 6: Configure all access points and Wireless router

You will apply your WLAN skills and knowledge by configuring a home wireless router and Access points. You will implement both WPA2-PSK security. Finally, you will connect hosts to each WLAN and verify connectivity.

WLAN	SSID	Authentication	Username	Password
WRT-Lan	SalesNet	WPA2-Personal	N/A	SalesOnly12
Engineers-Ap	EngineersNet	WPA-2 Personal	N/A	EngineOnly12
Finance-Ap	FinanceNet	WPA-2 Personal	N/A	FinanceOnly12

Note: It is not a good practice to reuse passwords as is done in this activity. Passwords have been reused to make it easier to work through the tasks

1. Change DHCP settings.

b. Open the WRT-Lan Router GUI and change the router IP and DHCP settings according to the information in the Addressing Table.

c. Permit a maximum of **20** addresses to be issued by the router.

d. Configure the DHCP server to start with IP address .**3** of the LAN network.

e. Configure the internet interface of the router to receive its IP address over DHCP.

f. Configure the static DNS server to the address in the Addressing Table.

2. Configure the Wireless LAN.

g. The network will use the 2.4GHz Wireless LAN interface. Configure the interface with the SSID shown in the Wireless LAN information table.

h. Use **channel 6**.

i. Be sure that all wireless hosts in the home will be able to see the SSID.

3. Configure security.

j. Configure wireless LAN security. Use WPA2 Personal and the passphrase shown in the Wireless LAN information table.

k. Secure the router by changing the default password to the value shown in the Wireless LAN information table.

4. Connect clients to the network.

l. Open the PC Wireless app on the desktop of the laptop and configure the client to connect to the network.

m. Open the Config tab on the Tablet PC and Smartphone and configure the wireless interfaces to connect to the wireless network.

n. Verify connectivity. The hosts should be able to ping each other and the web server. They should also be able to reach the web server URL.

5. Configure the Access points.

A. Access **Engineers-Ap** and configure the given appropriate Wlan settings (SSID and PSK).

B. Access **Finance-Ap** and configure the given appropriate Wlan settings (SSID and PSK).

Step 7: Configure Routing in routers

After all configuration we have done, now the next step is to configure routing to allow traffic to reach and access the internet.

Note: At this point we will learn how to configure RIP, EIGRP and OSPF

Part 3: Test the connectivity between devices

At this part now we are about to test the communication in all networks to check the connectivity and access to internet on all devices.