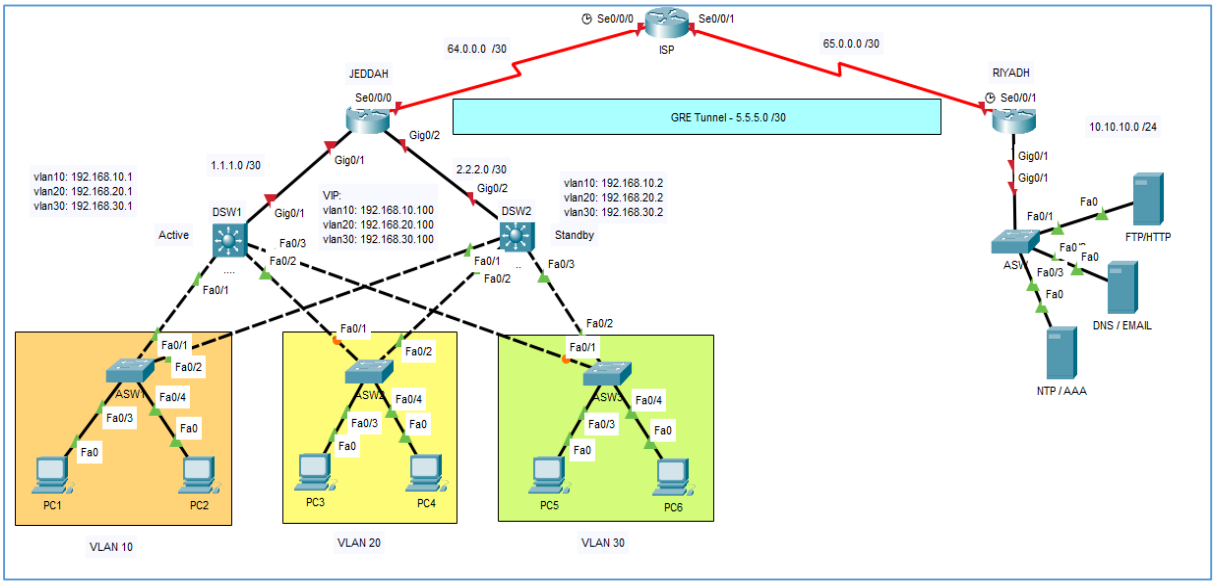
Taif College of Technology

Computer Network

Term Project – Cyber Security Lab – 144510



Requirements:

1) **Design the topology as shown using Packet Tracer simulation software.**
2) **Basic Configuration:**
    a. Configure the basic configuration for the network devices as shown in the topology.
        i. Hostname
        ii. IP Addresses.
        iii. Gateway if needed.
        iv. Vlans 10,20, and 30 in all switches.
        v. Configure trunk and access modes as needed in all switches.
        vi. Configure OSPF as a routing protocol.
        vii. Configure routed port and SVI in MLS switches.
3) **Redundancy:**
    a. Configure HSRP on MLS switches to achieve the High Availability.
        i. DSW1 is always in Active mode while DSW2 is in Standby.
        ii. All possible failures must be taken in your consideration and solved by HSRP (preempt and track).
4) **Routing Table:**
    a. Configure OSPF single area as a routing protocol with the following criteria:
        i. Process ID is 1.
        ii. Router id is: ISP (1.1.1.1), JEDDAH (2.2.2.2), RIYADH (3.3.3.3), DSW1 (4.4.4.4), DSW2 (5.5.5.5).
        iii. Disable the advertisements on ports that are not connecting to the routers.
5) **Services:**
    a. DHCP service:
        i. Enable DHCP service for vlan 10 and vlan 20 on JEDDAH router with excluding first 10 IP addresses.
        ii. Connect a new SERVER (name JSRV) to JEDDAH router (g0/0) and enable DHCP service for vlan 30.

b. Configure DNS server:

i. On DNS server, Click the **Services** tab and then click **DNS.** Turn on the DNS service using the radial button at the top.
ii. Create the A record ttc.gov.sa with IP address of HTTP server to be able to use FQDN.
iii. Create the A record ttc.gov.sa with IP address of Email server to be able to use email services.

c. Configure NTP server:

i. On NTP server, Click the **Services** tab and then click **NTP.** Turn on the NTP service using the radial button at the top.
ii. Secure the NTP server by enabling the NTP authentication feature using the radial button, Configure **Key 1** with a password of **cisco123**
iii. Adjust the date and time for each device in both branches using NTP.

d. Configure the Email Server:

i. Turn on both the SMTP and POP3 services using the radial buttons at the top.
ii. Create the domain name
iii. Create user account names of **PC-1**, **PC-2**, **PC-3** and **PC-4**, each with the password of **cisco123**.
iv.

e. Configure user Email clients:

i. Click the PC named **PC-1**, and click the Desktop
ii. Click Email and enter the following information:
    - Name: **PC-1**
    - Email Address: PC-1@ **ttc.gov.sa**
    - Incoming & Outgoing Email Server(s): **email**. **ttc.gov.sa**
    - Username: PC-1
    - Password: cisco123
iii. Repeat (a) and (b) on all PCs.

f. Configure FTP:

i. On FTP server, turn on the **FTP** service using the radial button at the top.
ii. Create user account names of bob, **mary**, and **mike**, each with the password of **cisco123**.
iii. Each user account should have full permissions (RWDNL).

g. Configure HTTP server:

i. Turn on both the HTTP and HTTPS services using the radial buttons at the top.

h. Configure AAA server:

i. On AAA server, Click the Services tab and then click AAA, turn on the AAA service using the radial button at the top.
ii. Configure the Client Name **RIYADH** with the Client IP **65.0.0.2** with a secret of **cisco123**. Click **Add** to save the client information.
iii. Configure the AAA user account of **admin** with a password of **cisco123**. Click **Add** to save the user information.

i. Configure NTP server:

i. On NTP server, Click the **Services** tab and then click **NTP,**

ii. Secure the NTP server by enabling the NTP authentication feature using the radial button, Configure **Key 1** with a password of **cisco123**.

6) Security:

a. PPP Authentication:

i. Configure PPP CHAP authentication on serial links between routers.

b. Layer 2 switches security:

i. On all access switches in JEDDAH branch, do the following:
   a. Configure port-security on all used ports.
   b. Set the maximum so that only one device can access each port.
   c. The MAC address of a device is dynamically learned.
   d. Set the violation so that the secured ports are not disabled when a violation occurs, but a notification of the security violation is generated and packets from the unknown source are dropped.
   e. Disable all the remaining unused ports.
   f. Add a **Rouge Laptop** with appropriate setting to test your security in this part; then record what you notice by using show commands.

ii. DHCP Snooping:
   a. Configure DHCP snooping on all L2 switches to protect DHCP service from any potential attack.

c. SSH:

i. Configure SSH on RIYADH router and ASW switch, so the legitimate user should be authenticated by AAA server.

ii. Configure SSH on all network devices in JEDDAH branch, so the legitimate user should be authenticated locally.

d. GRE:

i. Configure a GRE tunnel between JEDDAH and RIYADH.

e. NAT:

i. On both JEDDAH and RIYADH routers, configure NAT to translate private IPs into public IPs. (No more details here, do it as you see it is correct).