New Ultimate CCNA Challenge

In this CCNA challenge you will be configuring a small company with two sites Seattle and Tacoma, these sites are connected to the internet and their local intranet domain via a frame relay WAN. There is also a remote home office that connects to the internet and the company intranet via a DSL connection to their local ISP.

## Objective:

* Configure two VTP domains.
* Configure multiple VLANs in each VTP domain.
* Configure VoIP in one of the VTP domains.
* Configure STP for Seattle VTP domain
* Configure NTP.
* Assign all IP addresses using DHCP.
* Configure frame relay to connect all the sites.
* Configure NAT to connect the company to the internet.
* Configure wireless access to each site.
* Configure a wireless DMZ zone to allow internet access.
* Configure ACLs to control access to resources.
* Configure DSL remote access for the home office.
* Configure Port Channel.
* Configure Port Security.
* Configure TACAS.

The ISP router and internet DNS server are already configured. There is also three web server’s freeciscolab.com, freeccnalab.com and freeccnplab.com configured as HTTP and Mail servers.

Local Area Network:

There are two VTP domains in the network. Seattle domain comprises SW1, SW2 and SW3, which have VLANS 10, 20, 30, 40, 50, AND 60. The Tacoma domain comprises S4 and S5 which have VLANS 10, 20, 30, 40, and 50. Each of the VTP domains has PC1 and 3 are assigned to VLAN 10 while PC2 and 3 belong to VLAN 20. VLAN 30 is the management VLAN and the native VLAN. The local servers are assigned to VLAN 40, and wireless access is assigned to VLA 50. VLAN 60 in the Seattle VTP domain is dedicated for the VoIP Phones. Note: that the IP Phone have built in switch which directs the voice and data VLANs.

## DHCP:

DHCP is configured on R1 and R2 to assign IP addresses for the PCs in VLAN 10 and 20 and the wireless in VLAN 50 of both sites as well as the VoIP in VLAN 60 of the Seattle site.

## Port Channel:

Configure a PAPG port channel between SW5 and SW6 as shown the network diagram.

## Port Security:

Configure ports FA0/1 and FA0/2 on switches SW5 and SW6 so the only host can be connected insuring that an additional switch can never be connected to the ports.

## Wireless Access:

All wireless connection in the Seattle, Tacoma and Home Office sites need to be secured to prevent unauthorized access.

## Wide Area Network:

A point-to-point hub and spoke Frame Relay network comprised of R1, R2, and R3 connects the Seattle and Tacoma site to the Data Center.

## Dynamic Routing:

In order for the hosts, servers to communicate over the WAN they will need a route to each other’s networks. Configure a dynamic routing protocol on the routers to insure connectivity.

## VoIP:

Telephone services need to be configured on the router to configure and assign phone numbers to the four IP phones. Additionally the switches need to be configured to properly trunk the voice and data VLANs.

## Internet Access:

In order for the host computers to access the internet/intranet a default rout will be required as well as the address will need to be translated.

## Access Control List:

Access Control List (ACL) needs to be created to filter certain traffic and restrict access to some services in the network. Configure ACLs to provide the follow results:

Only hosts in VLAN 10 of Seattle will have access the VTY lines of the Data Center.

Only hosts in VLAN 20 of Tacoma can access the ftp services of freelabs.com

The hosts in VLAN 10 of Seattle won’t be able to access the Internet.

DMZ wireless access can only access the internet.

## Remote Home Office:

Computers connected to the Home Office network need access to the web servers and the company intranet freelabs.com.

## TACAS Access:

Configure the server FS-1.seattle.freelabs.com as a TACAS server.

Configure the server so that it will provide authentication for access to R1, R2, and R3.

Configure the user on the TACAS server as Admin with the password “sanfran”.

Configure R1, R2, and R3 to use TACAS authentication.

## Verify the Final Configuration:

All hosts can ping each other.

All PCs and servers can ping each other and vice versa.

All PCs can access the web servers in the internet and internal intranet.

Only hosts in VLAN 10 of Seattle can access the vty lines of the Data Center.

Hosts in VLAN 10 of Seattle cannot access the Internet.

Only hosts in VLAN 20 of Tacoma can access the internal ftp server freelabs.com.

Internet web servers and internal web server can be accessed from the Home office.

DMZ wireless access can only access the internet.

Home Office can access the internet and the company intranet.

All IP Phones can call any other phone.

Verify R1, R2, and R3 are using TACAS authentication.

Verify that you can access R2 and R3 via TELNET from PC-1 and PC-5 and the TACAS authentication is required.