Assignment

Task 02

This is the second of the three (3) Tasks of the Assignment.

strictly** follow the ***"Assignment Guideline" *document* prior to working on this Assignment Task.

Objectives:

1. Configure a complex network to enable communication between multiple departments.
2. Understand the importance of VLANs while configuring VLANs where necessary.
3. Configure GRE (General Routing Encapsulation)/VPN between networks that are geographically apart from each other.
4. Network access control via ACLs (Access Control List).
5. Network device maintenance and access authorization.
6. Validate and troubleshoot the network connectivity.

Background:

You, as a network engineer, are now required to configure a complex network to enable communication between multiple departments (b314 - Computing Department. IT Services, Human Resources, Curtin Library, Cisco Lab). Also, you are required to configure a network in Curtin Energy Research division located in Technology Park.

Technology Park
Curtin University
- Perth campus
Curtin University
Basingha
Deven
Pinedale St
Creaton St
Jarrah Rd
Adie Ct
Kent St
Brand Dr
Lawson St

In Computing Department (Curtin University), unfortunately, a part of IT Services and Human Resources department is located, and they need to be on the respective VLANs as the IT Services Department and Human Resources Department. The Gateway Router of Curtin University and Curtin Energy Research Division is required to be configured with a public IP address. As a security measure, a set of ACLs (Access Control List) needs to be configured on Gateway Routers to restrict access to some parts of the network where necessary. Furthermore, Curtin Energy Research division which is geographically located away from the Curtin University has two branches for its HR and IT Services. Both branches must be connected to the Curtin HR and Curtin IT Services Departments respectively with a VPN (virtual private network)/GRE (General Routing Encapsulation) tunnel. These tunnels must be configured to carry on the relevant traffic for HR and IT Services. In addition to the tunnels designed for HR and IT services traffic, another tunnel must be configured to allow traffic to Curtin Library, and only to Curtin Library back and forth. **The devices with the required connections are already in place**. However, the network is yet to be configured, and all devices are offline.

You are only required to configure each device where necessary and set the network up and running according to the requirements stated below. Since this task is to deal with the configuration of devices, **adding/removing/moving devices or arranging devices in the physical view of the network is not required.** *(please work only with the logical view of the network).*

Required Skill:

Since you have been contracted before to work on a simple network with Assignment – Task 01 as a trainee network engineer, Assignment – Task 02 requires you be to an **experienced network engineer**, and it is **absolutely necessary** to complete the required **practical sheets** (with *try-me* challenging questions), following the **relevant reference materials** on Blackboard as stated in CNCO2000 unit outline.

Important Notes:

- You are given a laptop to connect and configure the devices where CLI is disabled (Refer to the laptop with the name **"You"**)
- Do not delete existing connections (wires). Refer to **C1.1** if a connection is removed by a mistake.
- Testing the connectivity of network segments or devices will help you to validate the configuration of the network devices once they are done. You may frequently test the connectivity while you progress step by step to double check your work appropriately.
- If you are using the simple PDU tool to test the connectivity, the first few attempts may fail due to ARP resolution (this is in line with the failures that one would see with the ping command. Ping command will send multiple ICMPs in which the first few may fail due to the same reason).
- Assignment – Task 02 must be completed using **Packet Tracer v7.3.1** (the latest version).
- **Strictly follow** the **"Assignment Guideline"** document prior to working on this Assignment Task.

This task consists of Six **(6) Components.** You will be guided through them to successfully configure the network according to the requirements stated above.

C1: Initial configuration of the devices

1. **IMPORTANT:** The connections are already made for you. **In case a connection is removed mistakenly by you, you will have to start it over with a fresh copy of the .pka file**

2. Configure the device interfaces according to the following table.

Institute	Device Name	Interface	IP Address
Curtin University	PC1.b314.A	Fa0	192.168.10.2/24
	PC2.b314.A	Fa0	192.168.10.3/24
	PC1.b314.B	Fa0	192.168.20.2/24
	PC2.b314.B	Fa0	192.168.20.3/24
	PC1.b314.HR	Fa0	192.168.100.2/24
	PC2.b314.HR	Fa0	192.168.100.3/24
	PC1.b314.IT	Fa0	192.168.101.2/24
	PC2.b314.IT	Fa0	192.168.101.3/24
	PC1.b101.HR	Fa0	192.168.100.4/24
	PC2.b101.HR	Fa0	192.168.100.5/24
	PC1.b401.IT	Fa0	192.168.101.4/24
	PC2.b401.IT	Fa0	192.168.101.5/24
	PC1.b401.CISCO	Fa0	192.168.102.2/24
	PC2.b401.CISCO	Fa0	192.168.102.3/24
	PC1.b105.LIB	Fa0	192.168.103.2/24
	PC2.b105.LIB	Fa0	192.168.103.3/24
Curtin Energy Research Division	PC1.b601.HR	Fa0	10.0.2.2/24
	PC2.b601.HR	Fa0	10.0.2.3/24
	PC1.b602.IT	Fa0	10.0.1.2/24
	PC2.b602.IT	Fa0	10.0.1.3/24
	PC1.CUR_ENGY	Fa0	10.0.0.2/24
	PC2.CUR_ENGY	Fa0	10.0.0.3/24
Curtin University	CUR_UNI.GW	Gig0/1	-
	CUR_UNI.GW	Gig0/2	192.168.103.1/24
	CUR_UNI.GW	Gig0/0	209.165.100.30/28
Curtin Energy Research Division	CUR_ENGY.GW	Gig0/0	10.0.0.1/24
	CUR_ENGY.GW	Gig0/1	10.0.1.1/24
	CUR_ENGY.GW	Gig0/2	10.0.2.1/24
	CUR_ENGY.GW	Serial0/0/0	209.165.200.30/28

Internet Service Provider	ISP	Gig0/0	209.165.100.29/28
	ISP	Serial0/0/0	209.165.200.29/28

Hint: CLI of some devices are disabled. You will have to figure out a way login to those devices to configure them through `Laptop-PT (You)`

3. Shutdown all the ports that are not used in CUR_UNI.S1 Switch.

   (Hint: all ports are by default turned on in a switch unlike a router)

4. Configure the Default Gateway IP address on following PCs which are not on VLANs.

   (Hint: figure out the correct Default Gateway IP address by referring to the table above)

   (Important: Use the first address of the respective network as the default gateway)

PC Name
PC1.b105.LIB
PC2.b105.LIB
PC1.b601.HR
PC2.b601.HR
PC1.b602.IT
PC2.b602.IT
PC1.CUR_ENGY
PC2.CUR_ENGY

5. Add a static default route to CUR_UNI.GW and CUR_ENGY.GW Routers to forward traffic to ISP Router using the **forwarding interface_id method**

   (Hint: set the route 0.0.0.0 to <forwarding_interface_id>)

6. Change the hostnames of all the Routers to "**R**" and Switches to "**S**"

   (Hint: hostname is not the display name of the device. It is the name which is shown at the CLI prompt of the device)

C2: Configure VLANs

1. Configure the following VLANs in the devices where necessary:
   a. Make sure to "devices in vlan" belong to the respective vlans once configured

Device In the VLAN	VLAN ID	VLAN Name
PC1.b314.A, PC2.b314.A	10	CUR.b314.A
PC1.b314.B, PC2.b314.B	20	CUR.b314.B
PC1.b314.HR, PC2.b314.HR, PC1.b101.HR, PC2.b101.HR	100	CUR.HR
PC1.b314.IT, PC2.b314.IT PC1.b401.IT, PC2.b401.IT	101	CUR.CITS
PC1.b401.CISCO, PC2.b401.CISCO	102	CUR.CISCO

(Important: names are case-sensitive. Please use the vlan names as stated)

2. Configure trunk ports on the links only if trunking is **absolutely** needed. (if a link does not need to carry multiple VLAN data, it **must be** configured as an access link, **but not** as a trunk link).

   If you decide to configure a port as a trunk port, make sure to configure the trunk port with the **absolute necessary traffic** (for e.g. if a link is supposed to carry **only** the data belong to two VLANs (e.g. VLAN A, VLAN B) out of 5 VLANs, then **only allow** VLAN A, VLAN B traffic to be carried on the link but not others). Note that VLAN1 (default VLAN) traffic **must** be allowed on the trunk port in addition to the traffic of those VLANs which you will configure.

   Do not use dynamic trucking protocol (DTP) while performing the task stated above.
   (Hint: When configuring a trunk link, make sure to configure both ends of the link (ports) in a similar way in order to make both ends compatible with each other)

3. At this point, check the connectivity of the devices within a VLAN. The devices within the VLAN must be able to communicate within the same VLAN but not across VLANs. We are yet to configure inter VLAN communication.

Source	Destination	Connectivity	Comment
Any PC on b314.A VLAN	Any PC on b314.A VLAN	Successful	Successful
Any PC on	Any PC on	Successful	Successful

b314.B VLAN	b314.B VLAN		
Any PC on CUR.HR VLAN	Any PC on CUR.HR VLAN	Successful	Successful
Any PC on CUR.CITS VLAN	Any PC on CUR.CITS VLAN	Successful	Successful
Any PC on CUR.CISCO VLAN	Any PC on CUR.CISCO VLAN	Successful	Successful
Any PC on CUR.HR VLAN	Any PC on CUR.IT VLAN	**Fail** In fact, any inter (across) vlan communication will fail.	Once inter VLAN communication is configured, this test will be successful
Any PC in Curtin Library	Any PC on CUR.IT VLAN	**Fail.** In fact, any PC in an outside network will fail to communicate with a PC on a VLAN.	Once inter VLAN communication is configured, this test will be successful

4. Configure **CUR_UNI.GW** router for inter VLAN communication by defining a set of sub interfaces on Gig0/1 as shown below:

Sub Interface on Gig0/1	IP Address
10	192.168.10.1/24
20	192.168.20.1/24
100	192.168.100.1/24
101	192.168.101.1/24
102	192.168.102.1/24

5. Configure the Default Gateway IP address on following PCs which are supposed be on a VLAN.

(Hint: figure out the correct Default Gateway IP address by referring to the table above)

PC Name
PC1.b314.A
PC2.b314.A
PC1.b314.B
PC2.b314.B
PC1.b314.HR
PC2.b314.HR

strictly follow the "*Assignment Guideline" document* prior to working on this Assignment Task

PC1.b314.IT
PC2.b314.IT
PC1.b101.HR
PC2.b101.HR
PC1.b401.IT
PC2.b401.IT
PC1.b401.CISCO
PC2.b401.CISCO

6. Test the connectivity of the devices across VLANs (inter VLAN). It must be successful.

Source	Destination	Connectivity
Any PC on a VLAN	Any PC on the same or different VLAN in Curtin University	Successful
Any PC on a VLAN	Any PC outside the VLAN in Curtin University	Successful

strictly follow the "*Assignment Guideline" document* prior to working on this Assignment Task

C3: Configuring IPv4 Tunnels

1. Following **GRE**/VPN **Tunnels over IPv4** are required to be configured.

Tunnel	Tunnel IP on CUR_UNI.GW Router	Tunnel IP on CUR_ENGY.GW Router	Comment
1	192.168.200.1/24	192.168.200.2/24	Tunnel for HR traffic
2	192.168.201.1/24	192.168.201.2/24	Tunnel for IT Services traffic
3	192.168.202.1/24	192.168.202.2/24	Tunnel for Library traffic

*Note that these tunnels carry unencrypted traffic but can be configured to carry encrypted traffic with IPSec. You are **not required** to encrypt traffic in this task.*

2. Complete the rest of the mandatory configuration to setup the tunnels up and running.

   (Hint: source, destination, mode, etc.)

3. Add appropriate static routes to CUR_UNI.GW and CUR_ENGY.GW Routers (wherever necessary) according to the following table.

Tunnel	Define static routes for:
1	Curtin University – HR Network (192.168.100.0/24) Curtin Energy Research Division – HR Network (10.0.2.0/24)
2	Curtin University – IT Services Network (192.168.101.0/24) Curtin Energy Research Division – IT Services Network (10.0.1.0/24)
3	Curtin University – Library Network (192.168.103.0/24) Curtin Energy Research Division – CUR_ENGY Services Network (10.0.0.0/24) Curtin Energy Research Division – IT Services Network (10.0.1.0/24) Curtin Energy Research Division – HR Services Network (10.0.2.0/24)

You **must** use the best **summarized route** when configuring static routes for tunnel 3 for the networks (10.0.0.0/24, 10.0.1.0/24, 10.0.2.0/24)

*(Hint: Do not add any static routes to ISP Router. **DO NOT** configure any dynamic routing protocols on any of the Routers)*

4. At this point,

   a. HR Department of Curtin University should be able to communicate with the HR branch of Curtin Energy Research Division via tunnel 1.

   b. IT Department of Curtin University should be able to communicate with the IT branch of Curtin Energy Research Division via tunnel 2.

   c. Curtin Library must be accessible to all the PCs in Curtin Energy Research Division via tunnel 03.

   Furthermore,

   d. IT Department of Curtin University should be able to communicate with all PCs in Curtin University and Curtin Energy Research Division.

   e. Curtin Library must be accessible to all the PCs (Curtin University and Curtin Energy Research Division).

5. Test the connectivity as shown below:

Source	Destination	Connectivity	Comments
Any PC in HR Department of Curtin University	Any PC in HR branch of Curtin Energy Research Division	Successful	
Any PC in IT Department of Curtin University	Any PC in Curtin University or Curtin Energy Research Division	Successful	
Any PC in Curtin University Library	Any PC in Curtin University or Curtin Energy Research Division	Successful	
Any PC in IT branch of Curtin Energy Research Division	Any PC in b314.A, b314.B or CISCO Lab in Curtin University	Fail	No static routes available

C4: Configure Access Control Lists to restrict access

1. Network access needs to be restricted according to the following conditions:
   a. HR Department of Curtin University **must only be accessed by** the IT Services and Library of Curtin University and HR branch of Curtin Energy Research Division.
   b. HR branch of Curtin Energy Division **must only be accessed by** the IT Services, Library of Curtin University, and IT branch of Curtin Energy Research Division, HR department of Curtin University.
2. In order to satisfy the conditions above, define a standard access list (ACL) with the name "**allow_CITS**" on CUR_UNI.GW and CUR_ENGY.GW Routers.
3. Apply the ACLs on relevant interfaces according to the following table.

ACL Name	ACL Type	Device	Interface
allow_CITS	Standard	CUR_UNI.GW	Gig0/1.100
allow_CITS	Standard	CUR_ENGY.GW	Gig0/2

When an ACL is placed on an interface, choose whether the ACL is applied on inbound or outbound traffic appropriately (Hint: Refer to P05 reference materials for more details on ACLs)

You **must not** have any **deny rules**, **but permit rules**

4. Test the connectivity according to the following table.

Source	Destination	Connectivity	Comment
Any PC in HR Department of Curtin University	Any PC in HR branch of Curtin Energy Research Division	Successful	
Any PC in IT Department of Curtin University	Any PC in Curtin University or Curtin Energy Research Division	Successful	
Any PC in IT branch of Curtin Energy Research Division	Any PC in Curtin Energy Research Division	Successful	
Any PC in IT branch of Curtin Energy Research Division	Any PC in b314.A, b314.B or CISCO Lab in Curtin University	Fail	No static routes available
Any PC in Library of Curtin University	Any PC in Curtin University or Curtin Energy Research Division	Successful	
Any PC in HR Department of Curtin University	Any PC in IT branch of Curtin Energy Research Division	Fail	Access Restricted by the ACL
Any PC in HR Department of Curtin University	Any PC **outside** IT Services, Library of Curtin University and HR branch of Curtin Energy Research Division	Fail	Access Restricted by the ACL
Any PC in HR branch of Curtin Energy Research	Any PC **outside** HR, IT Services, Library of Curtin University, and	Fail	Access Restricted by

Division	IT branch of Curtin Energy Research Division		the ACL

C5: Network Device Security & Management

1. Following security measures must be in place to prevent unauthorized access to the Routers:

Device Name	Access	Password
CUR_UNI.GW	Console Access	cur.gw.pass!
CUR_UNI.GW	All virtual terminals' access	cur.gw.telnet!
CUR_UNI.GW	Privileged mode access	cur.gw.priv!
CUR_ENGY.GW	Console Access	cur.engy.gw.pass!
CUR_ENGY.GW	All virtual terminals' access	cur.engy.gw.telnet!
CUR_ENGY.GW	Privileged mode access	cur.engy.gw.priv!

2. At this point, on **CUR_UNI.GW** and **CUR_ENGY.GW** Routers, if you inspect the "running-config" of the device, the password is stored on plain text. Avoid storing passwords on the devices in plain text by using **password encryption service** on those devices.
3. Once the password encryption service is in place, inspect the "running-config" of **CUR_UNI.GW** and **CUR_UNI.GW** Routers. The password should not be displayed in plain text!
4. Since Curtin IT Services department has access to all the network devices (Routers, Switches, PCs) in Curtin University and Curtin Energy Research Division, the Switches must be configured with a Switch Virtual Interface (SVI) with an IP address, so that IT Services could ping them.

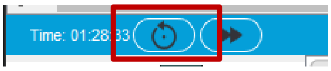
Swtich	SVI	IP
CUR_UNI.S1.314A	vlan 10	192.168.30.98/24
CUR_UNI.S1.314B	vlan 100	192.168.100.98/24
CUR_UNI.S1	vlan 101	192.168.101.99/24
CUR_UNI.S1.HR	vlan 100	192.168.100.98/24
CUR_UNI.S1.IT	vlan 101	192.168.101.98/24
CUR_UNI.S1.LIB	vlan 1 (default VLAN)	192.168.103.98/24
CUR_ENGY.S1	vlan 1 (default VLAN)	10.0.0.98/24
CUR_ENGY.S1.IT	vlan 1 (default VLAN)	10.0.1.98/24
CUR_ENGY.S1.HR	vlan 1 (default VLAN)	10.0.2.98/24

5. PCs in IT Department must be able to ping all the Switches and Routers (in Curtin University and Curtin Energy Research Division). To satisfy this requirement, set the default-gateways on the devices (Switches, Routers) where necessary.

   (Hint: figure out the correct default gateway IP address depending on the network in which the device resides in)
6. Once you complete step 4 and 5 above, you will notice that **ONE (or more) of the switches** cannot be ping-ed by the PCs outside the vlan it belongs to. Figure out the switch and fix the configuration error.

   When performing changes to the IP of a SVI, make sure to follow the same IP pattern which is used for other devices (Ref to IP patterns shown in the table above – Step 4)

7. Now, try to ping each of the communication devices (Router, Switch). You should be successful.
8. Finally, save the running configurations of all communication devices (Routers, Switches) to its NVRAM *(Hint: startup configuration).*
9. Power Cycle all the devices and see whether the saved configuration of Routers and Switches is automatically loaded to the running configuration.



C6: Validate Network Connectivity

Test the connectivity of the entire network according to the following table. **Save the test cases in your .pka file**

Source	Destination	Connectivity	Comment
Any PC in HR Department of Curtin University	Any PC in HR branch of Curtin Energy Research Division	Successful	
Any PC in IT Department of Curtin University	Any PC in Curtin University or Curtin Energy Research Division	Successful	
Any PC in IT branch of Curtin Energy Research Division	Any PC in Curtin Energy Research Division	Successful	
Any PC in IT branch of Curtin Energy Research Division	Any PC in b314.A, b314.B or CISCO Lab in Curtin University	Fail	No static routes available
Any PC in Library of Curtin University	Any PC in Curtin University or Curtin Energy Research Division	Successful	
Any PC in HR Department of Curtin University	Any PC in IT branch of Curtin Energy Research Division	Fail	Access Restricted by the ACL
Any PC in HR Department of Curtin University	Any PC **outside** IT Services, Library of Curtin University and HR branch of Curtin Energy Research Division	Fail	Access Restricted by the ACL
Any PC in HR branch of Curtin Energy Research Division	Any PC **outside** HR, IT Services, Library of Curtin University, and IT branch of Curtin Energy Research Division	Fail	Access Restricted by the ACL
Any PC in IT Department of Curtin University	CUR_UNI.GW, CUR_ENGY.GW	Successful	*Do Telnet*
Any PC in IT Department of Curtin University	All the Switches	Successful	*Do ping/ICMP*

Summary:

Congratulations, you have completed the Assignment – Task 02

C1: Initial configuration of the devices

C2: Configure VLANs

C3: Configuring IPv4 Tunnels

C4: Configure Access Control Lists to restrict access

C5: Network Device Security & Management

C6: Validate Network Connectivity