**ASSESSOR – PRACTICAL ASSESSMENT TASK**

|  |  |  |  |
| --- | --- | --- | --- |
| Task Number | 3 of 3. | Task Name | Practical observation |
| National unit/s code | VU23213 | National unit/s title | Utilise basic network concepts and protocols required in cyber security |
| National qualification code | 22603VIC | National qualification title | Certificate IV in Cyber Security |
| RMIT Program code | C4424 | RMIT Course code | INTE5058 |

**Instructions to Assessor**

|  |  |
| --- | --- |
| **Information on preparing, conducting and marking assessment** | |
| * Provide all students with a copy of the Student Version of this assessment task within the first week of starting this unit * The level of assistance from the assessor should be minimal – ideally, you are an observer only. If students are unsure of what is required of them, they can ask you. * Have a copy of the assessor version of this task on hand if asking questions during the observation (you’ll need this to refer to the questions and the model responses). * If not an RMIT event, use the documentation given by the student and the observations made in the Third-Party Report to inform you of the student’s skills, performance and knowledge. Also, ensure the Third-Party person is an industry professional. Complete the Marking Guide and give feedback (Section B) for each student. * Candidates must satisfactorily complete all assessment requirements. Write down if they have demonstrated the required observations on the student version of each candidates’ assessment task. Judge if it is satisfactory/not yet satisfactory against the model responses in the assessor version. * Add any comments for each candidate that you feel will add to their understanding of what they did well and need to improve on.   Once completed, distribute the completed Marking Guides and Feedback to students via Canvas and file for record-keeping, as required. | |
| **Information on recording and retaining assessments and dealing with assessment appeals can be found in the**  [**RMIT Assessment Processes document**](https://www.rmit.edu.au/content/dam/rmit/documents/about/policy/assessment/assessment-processes.pdf) | |
| **Approval by Program Manager** | Signature:  Name: |
| **Date this assessment was developed/modified** | 18/2/2023 |
| **Person/s who developed/modified assessment** | Donald Attard |

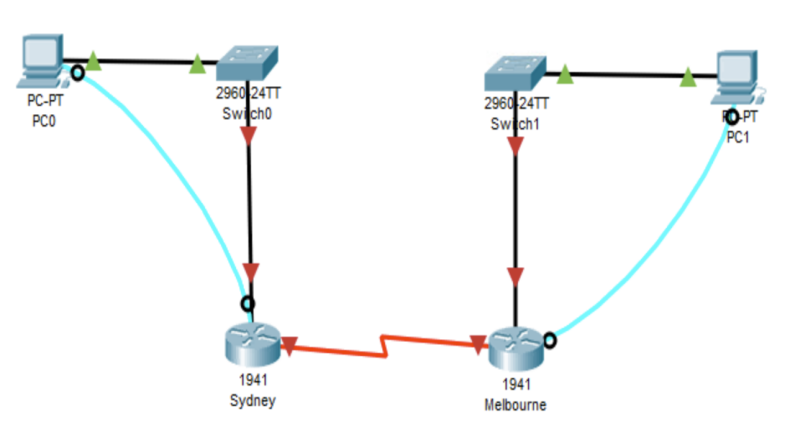
Section A – **Assessment Information**

|  |  |
| --- | --- |
| **Assessment duration and/or due date** | Four to five weeks. |
| **Task instructions** | |
| **Summary and Purpose of Assessment**  The purpose of this assessment task is for you to set-up, configure and test key networking devices. You will also need to demonstrate using Python scripting, troubleshooting, setting up IPv6, using MAC addresses, verifying Skype connectivity and analysing RTP packets.  **Assessment Instructions**  You will be required to complete a range of Lab exercises which are to be undertaken in the computer lab at RMIT. Each lab exercise involves a series of tasks, which are outlined in a step-by-step approach to assist you in completing these tasks. The lab exercises include:   * Lab A: Plan and configure a basic network set-up * Lab B: Networking IoT Devices * Lab C: Troubleshooting * Lab D: Setting up IPv6 * Lab E: Demonstrating layer 2 using port security * Lab F: Verify QUIC packets using Wireshark. * Lab G: Ransomware Attack. * Lab H: ARP Poisoning. * Lab I: Denial of Service Attack.   Some of the lab exercises require further consolidation of knowledge. Where this is apparent, your assessor will ask you to confirm your understanding via verbal questions.  **What**  Students need to complete the specific assessment tasks in each Practical lab. Please refer to the Practical lab section below for a detailed scope of work.  **Where**  Each practical lab will be undertaken and completed by the student in a work-related simulated environment.  This practical assessment will be carried out during class time under supervision in ‘Network Lab Communications Room’ - Computer Laboratory at RMIT building 56/57.  **How**  Students will be assessed against the criteria as listed in each lab and the Marking Guide. To achieve a satisfactory result in each lab, students need to address all criteria satisfactorily. Students need to achieve satisfactory (S) results in all practical labs (A to F) to gain satisfactory (S) in this assessment task. | |
| **Conditions for assessment** | |
| * Student must be observed undertaking this assessment task by a qualified assessor. * The assessor can negotiate a suitable time and location for the assessment at least one week prior to the assessment taking place. * Student must complete the task within the maximum allowed duration as directed by the assessor. * Student can make arrangements with the assessor at least one week prior to the assessment due date if they require special allowance or allowable adjustment to this task. * Students found in breach of assessment conditions can be charged with academic misconduct, have their results cancelled, be excluded from the program and receive other penalties. Penalties can also apply if a student’s test material is copied by others. * Plagiarism is the presentation of the work, idea or creation of another person as though it is one’s own. It is a form of cheating and is a very serious academic offence that may lead to expulsion from the University. Plagiarised material can be drawn from, and presented in, written, graphic and visual form, including electronic data, and oral presentations. Plagiarism occurs when the origin of the material used is not appropriately cited. * RMIT special consideration is to enable you to maintain your academic progress despite adverse circumstances. The process for special consideration can be found at<http://www1.rmit.edu.au/students/specialconsideration> * Students with a disability or long-term medical or mental health condition can apply for adjustments to their study and assessment conditions (Reasonable Adjustments and Equitable Assessment Arrangements) by registering with the Equitable Learning Services (ELS) at<https://www.rmit.edu.au/students/support-and-facilities/student-support/equitable-learning-services> * Please ensure students full and correct name is written on the student version of this assessment task (do not use nicknames or abbreviations). * Student will be assessed as satisfactory or not yet satisfactory. * Student can appeal the assessment decision according to the [RMIT Assessment Processes](https://www.rmit.edu.au/content/dam/rmit/documents/about/policy/assessment/assessment-processes.pdf)   **Additional Instructions for Students:**   1. Attempt ALL the questions/tasks in each Practical lab 2. Performance requirement for each Practical lab:    1. **Satisfactory (S) performance**- met the minimum requirement of all the actions listed for the practical tasks.    2. **Not Yet Satisfactory (NYS) performance** - did not meet the minimum requirement of all the actions listed for the tasks. 3. Students need to achieve satisfactory (S) results in all three (3) Practical labs to gain satisfactory (S) in assessment 2.   Students need to achieve satisfactory (S) results in all three (3) assessments to be deemed Competent (CA). | |
| **Equipment/resources students must supply (if applicable):** | **Equipment/resources to be provided by RMIT or the workplace (if applicable):** |
| * Stationary | * Safe working environment * Computer lab * ‘Network Lab Communications Room’ where router /network installation may be conducted * Hard copies of the student version of this assessment task OR access to soft copies * network design documentation * cable tester – measurement equipment * hardware (routers, switches) and software (putty /Terra Term, packet Tracer, windows server 2019) * network components – Ethernet cables, console cable, serial cables * networked (LAN) computers * a wide area network (WAN) service point of presence * a live network * equipment specification * RMIT internet access * RMIT classrooms   + RMIT Computer Labs and Learning Resources/Software |

**PRACTICAL LAB**

**Lab A: Plan and configure a basic network set-up**

You will need to refer to the following addressing scheme to plan and design a basic network topology.



Refer to the table below to connect the devices and also assign IP addresses to the devices.

|  |  |  |  |
| --- | --- | --- | --- |
| **Device Type** | **Device Name (on Topology)** | **Ports** | **Address Information** |
| **PC** | PC0  (Server) | Ethernet | IP: 192.168.10.2  SNM: 255.255.255.0  DG: 192.168.10.1 |
| PC1 | Ethernet | IP: 192.168.20.2  SNM: 255.255.255.0  DG: 192.168.20.1 |
| **Switch** | Switch0 | F0/1 from PC0  G0/1 to Sydney’s G0/0/0 | N/A |
| Switch1 | F0/1 from PC1  G0/1 to Melbourne’s G0/0/1 |
| **Router** | Sydney | G0/0/0  S0/0/0 | IP: 192.168.10.1  SNM 255.255.255.0  IP: 192.168.3.1  SNM 255.255.255.0 |
| Melbourne | G0/0/1  S0/0/1 | IP: 192.168.20.1  SNM 255.255.255.0  IP: 192.168.3.2  SNM 255.255.255.0 |

**Note:** the router port name and number may vary (it may be G0/0 Or G0/0/0). It depends on the series /version of the router in your ‘Network Lab Communications Room’.

DG=Default Gateway

SNM=Subnet Mask

The tasks below are assigned in a way that is carried out during the process of developing plans. It guides you to prioritise tasks and have alternate plans for the installation of components with minimum disruption to the client.

**Task 1: Select appropriate network elements and connect devices**

* You will need to select appropriate devices (routers, switches), communication cables, peripherals and WAN connectors
* Connect the devices. Make sure you follow the procedures, manufacturer requirements, guidelines and protocols while you assemble devices and peripherals.

*Behind your PC, you should see a panel with a series of Ethernet ports like this:*

***2b. Ethernet Cabling***

***Note:*** *your class room may have slightly different setting.*

1. **Cabling**

Take your Ethernet cable and plug it into Port ‘B’.

1. **Console Cabling – connect peripherals**

Take your console cable and plug it into Port ‘C’ (or port ‘A’ – verify with your teacher).

1. **Connecting your cables to the cisco equipment**

Now that we have placed our cables into the ports behind our computers, we are ready to connect them to our networking devices. Think of the ports behind your computer as extension leads that run up into the roof and connect to a corresponding port in the ‘Network Lab Communications Room’ room (where the routers and switches are).For example: If you plug your Ethernet cable into port 3B, there will be a patch panel in the ‘Network Lab Communications Room’ room where that cable will terminate. From this patch panel, you can continue the “extension lead” of cabling to the required port.

1. **Connect two LANs using Serial Cables – through WAN connectors of your routers**

A Serial cable is a male to male connector with 2 ends:

* One end is DCE (the side we put the clock rate on)
* The other end it the DTE Data Terminating Equipment
* This cable connects a Router to another Router using a serial card.

***Note:*** *When plugging in or taking out the cable, take care. These cables need to be slotted in horizontally.*

*DO NOT FORCE OR JIGGLE THE CABLE TO GET IT IN OR OUT.*

*This can damage the cable, and the Serial card.*

**Physical Topology Overview**



PC3

PC2

2B

2A

2C

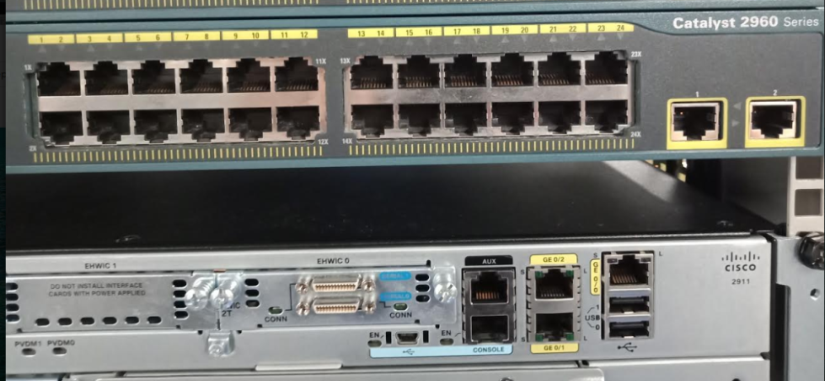
2D

3B

3A

3C

3D

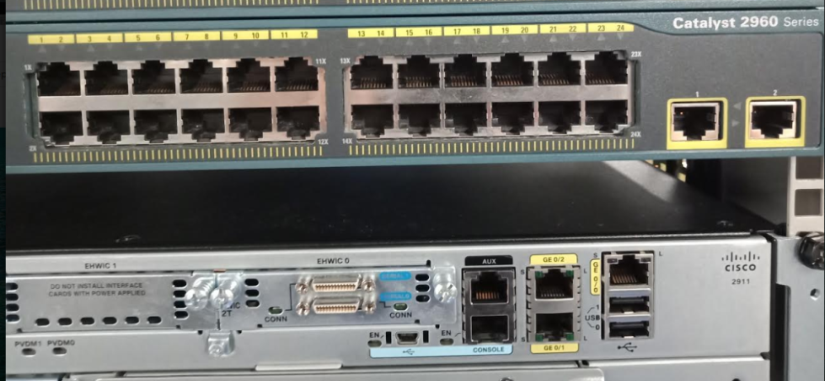
****

3B

2B

3C

2C





S0/0/0

G0/0/0

S0/0/1

G0/0/1

Melbourne Connection Guide

Sydney Connection Guide

Ethernet Cables are shown in Green

Console Cables are shown in Light Blue

Serial Cables are shown in Dark Blue

1. **Cabling data Ethernet cable**

We require 4 Ethernet cables in total. (2 for the Sydney half, 2 for the Melbourne Half)

* We take our first Ethernet cable and plug one end into our ‘B’ port and the other end into our assigned switch’s f0/1 port.
* We take an additional Ethernet cable and plug one end into our assigned switch’s g0/1 port, and the other end into our assigned routers f0/0 port

1. **Cabling console port**

We require 1 Ethernet cable (Ethernet cables can be used to extend a console cable’s connection)

* We take our third Ethernet cable and plug one end into our (or ‘A’) and the other end into our assigned router’s console port.
* Check your connections carefully!

1. **Cabling Serial Ports**

* Take a serial cable. Plug the DCE connection into the Sydney router’s s0/0/0 port.
* Plug the DTE connection into the Melbourne router’s s0/0/1 port.

If you are unable to determine which side is which, plug them into the ports as stated, it doesn’t matter which side. When you are in your router, go into privileged mode.

On Sydney, type the command: show controllers s0/0/0

On Melbourne type the command: show controllers s0/0/1

This should tell you whether your port is connected to a DCE or DTE connection.

If in doubt, please speak to your teacher.

When your cabling is complete, get it approved by your teacher and discuss to arrange secure site access to verify cabling compliance is correct.

Now we are ready to connect to our Router!

**Task 2 Locate and Run PuTTY or Teraterm**

Now, with your console connection physically set up, it’s time to set up the Terminal Emulation program. PuTTY is the software application used in your course. It’s a very versatile tool for remote access to another computer.

We need it to deliver a console window to input command line syntax to routers and switches in our Network Labs.

*Follow these steps:*

1. **Identify COM port used by your PC (where the Console / USB connects)**

* Open Windows Device Manager
* Click on Ports (COM & LPT)

Note the COM port the PC is using - USB-to-Serial Comm Port (COM?) – Substitute this number for your PC’s COM port number.

1. **Set up PuTTY**

([Download](https://www.putty.org/) if not on PC )

* select **serial** option

\*use default settings

1. **Edit Serial COM value to COM4:**

Now click on **Open**

* **Click** on **Black window**
* **Press ‘Enter’** on keyboard
* **router>** will appear

**Task 3: Resetting and initializing the router**

Commands will be in red

It’s a good idea to reset the router before you begin to configure anything on it, just in case someone else has left a config on there. To do this type the following commands:

Go From user mode to privileged mode:

Router>enable

If there is a password it should be ‘class’.

It’s a good idea to reset the router before you begin to configure anything on it, just in case someone else has left a config on there. To do this type the following commands:

Router#erase startup-config

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] (Hit the ‘Enter’ Key Here)

[OK]

Erase of nvram: complete

%SYS-7-NV\_BLOCK\_INIT: Initialized the geometry of nvram

Router#reload

Proceed with reload? [confirm] (Hit the ‘Enter’ Key Here)

**Task 4: Accessing the Router**

Go From user mode to privileged mode:

Router>enable

Enter configuration mode:

Router# configure terminal

**Task 5: Put a hostname on a router**

For Sydney:

Router(config)#hostname Sydney

For Melbourne:

Router(config)#hostname Melbourne

**Task 6: Place an IP address on the Router – Configure router interfaces**

For Sydney:

Sydney(config)#interface g0/0/0 (or adjust according to your router port)

Sydney(config-if)#ip address 192.168.10.1 255.255.255.0

Sydney(config-if)#no shutdown

Sydney(config-if)#exit

Sydney(config)#interface s0/0/0 (or adjust according to your router port)

Sydney(config-if)#ip address 192.168.3.1 255.255.255.0

Sydney(config-if)#clock rate 64000

Sydney(config-if)#no shutdown

Sydney(config-if)#exit

For Melbourne:

Melbourne(config)#interface g0/0/1 (or adjust according to your router port)

Melbourne(config-if)#ip address 192.168.20.1 255.255.255.0

Melbourne(config-if)#no shutdown

Melbourne(config-if)#exit

Melbourne(config)#interface s0/0/1 (or adjust according to your router port)

Melbourne(config-if)#ip address 192.168.3.2 255.255.255.0

Melbourne(config-if)#no shutdown

Melbourne(config-if)#exit

**Task 7: Set up Passwords – secure router access for network management and security**

To add the enable password (applies to both routers. The name Router has been used as a placeholder)

Router(config)#enable secret class

Telnet password:

Router(config)#line vty 0 4

Router(config-line)#password cisco

Router(config-line)#transport input all

Router(config-line)#logging synchronous

Router(config-line)#login

No privilege level 15

Console password:

Router(config)#line con 0

Router(config-line)#password cisco

Router(config-line)#logging synchronous

Router(config-line)#login

No privilege level 15

DO NOT CLOSE PuTTY. We will need it for Steps 8 and 9.

**Task 8: Setup IP on PC – configure PCs**

1. Hit Start and access the Control Panel
2. Click on Network and Internet
3. Click on Networking and Sharing Centre
4. Click on Change Adaptor Settings
5. Double click on your computers Ethernet adaptor
6. Double click on Internet Protocol Version 4 (TCP/UPv4)
7. Select Use the Following IP address

Type the following information into the fields:

Sydney PC (PC0)

IP: 192.168.10.2

SNM: 255.255.255.0

DG: 192.168.10.1

Melbourne PC (PC1)

IP: 192.168.20.2

SNM: 255.255.255.0

DG: 192.168.20.1

Click OK

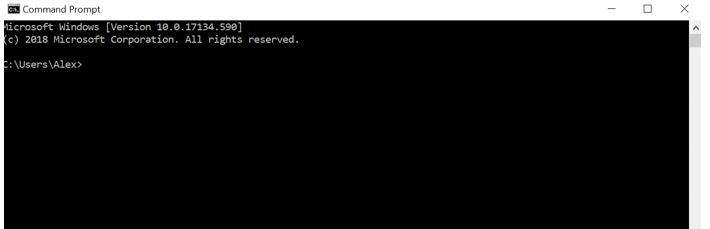
Click OK

Your IP address has now been applied.

**Task 9: Test your connection**

To test your connection hit Start and type ‘cmd’

You should see this window appear:



This window will allow us to verify PCs IP address, perform a ping and telnet test.

To verify PCs IP address, type ipconfig /all

It should display your assigned address correctly.

To ping the router simply type:

To ping Sydney:

ping 192.168.10.1

To ping Melbourne:

ping 192.168.20.1

Ideally you should have 4 replies. If this does not happen, then you need to check your connections. This could be either a broken cable, or an incorrectly configured IP address.

Next, we are going to test our telnet connection. To do this simply type:

Sydney:

telnet 192.168.10.1

Melbourne:

telnet 192.168.20.1

We can now access our router using the Ethernet connection we have set up.

**Task 10: Routing protocol setup on routers – interoperability with remote networks**

Now we need to go back to PuTTY and add in our Network Addresses.

Set up RIP routing protocol on routers:

There are 3 different networks on this topology.

Sydney has the networks

192.168.10.0

192.168.3.0

Melbourne has the networks

192.168.20.0

192.168.3.0

On Sydney, type the following commands (fill up below with necessary commands first):

Sydney(config)#router rip

Sydney(config-router)#version 2

Sydney(config-router)#network 192.168.10.0

Sydney(config-router)#network 192.168.3.0

Sydney(config-router)#exit

On Melbourne, type the following commands:

Melbourne(config)#router rip

Melbourne(config-router)#version 2

Melbourne (config-router)#network 192.168.20.0

Melbourne (config-router)#network 192.168.3.0

Melbourne(config-router)#exit

**Task 11: Test connectivity between PC’s**

Now we are ready to test the connectivity between the 2 PC’s.

On Sydney’s PC (PC0), go back into CMD and type the following:

ping 192.168.20.2

On Melbourne’s PC (PC0), go back into CMD and type the following:

ping 192.168.10.2

If you get at least 3 responses back, then your network is running properly. If not:

* try the ping command again and see if starts to send information through.
* Check your IP or Route settings, troubleshoot if necessary.

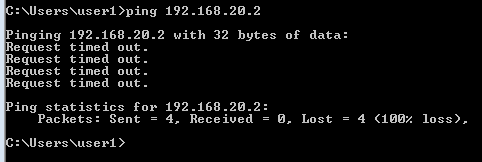
**Task 12: Install Windows 7 Software in Virtualbox.**

Download Windows 7 from website [https://tech-latest.com/download-windows-7-iso/.](https://tech-latest.com/download-windows-7-iso/) Download the Windows 7 Professional Edition 64 bit version.

Install Windows 7 in Virtualbox and rename the first one PC0 and the second one PC1. These machines will replace PC0 and PC1. Set the Network Adapter to “Bridged”.

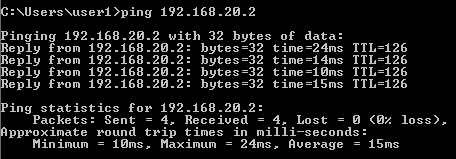
**Task 13:**

Have each virtual machine ping each other, your response should be:

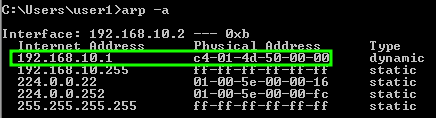


Modify the firewall to allow ICMP on both computers. To follow the steps, please refer to the filename **Allow ICMP.odt** located in Week 14.

* Verify that your computers can then ping each other:



* Verify that ARP is working. Check to see if PC0 has learnt Sydney’s router’s MAC Address.



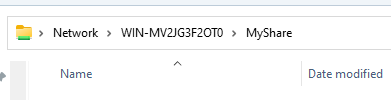
* Using the SMB protocol, share a folder on PC0 called MyShare and verify PC1 can access it. Assign Change Sharing Permissions to MyShare to everyone.

PC0

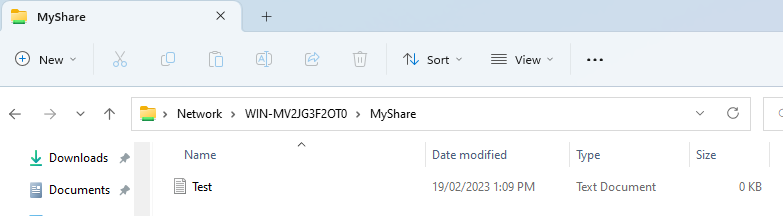
* + Right click on **MyShare**.
  + Go to **Properties**.
  + Click on the **Sharing** tab.
  + Click on **Advanced Sharing**.
  + Tick the checkbox “**Share this folder**”.
  + Click the **Permissions** button.
  + Under the Allow column, tick **Read** and **Change** permissions.
  + Click **OK** twice.
  + Click **Close**.

PC1

* Open up File Explorer.
* Type \\<Your computer name>\MyShare



* Create a text file inside MyShare.



**Task 14: Reset and pack up - Clean up and restore worksite, secure sign-off**

Congratulations! You have completed this lab. Now we need to reset everything back to the way we found it!

1. **First we need to reset our router**

Go back to Privileged mode on the router. Privileged mode will be denoted by a ‘#’ after the router name:

Sydney#

Sydney#erase startup-config

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] (Hit the ‘Enter’ Key Here)

[OK]

Erase of nvram: complete

%SYS-7-NV\_BLOCK\_INIT: Initialized the geometry of nvram

Sydney#reload

Proceed with reload? [confirm] (Hit the ‘Enter’ Key Here)

1. **Reset the PC**

Follow the steps from Task 6 to access the ‘Internet Protocol Version 4 (TCP/UPv4)’ settings

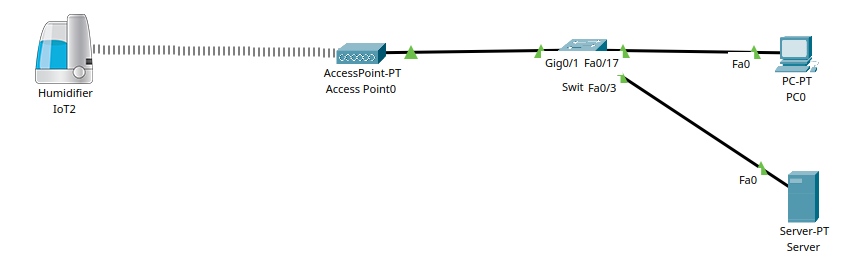
Now we simply need to reset the IP address settings to Automatically Obtain an IP address and DNS address:

Once you have completed this, you then need to plug your computers Ethernet cable back into the port that will be able to access the internet.

Access [www.google.com](http://www.google.com/) to verify that you have an internet connection.

**Lab B: Networking IoT Devices**

**Draw up the following network topology as shown below.**



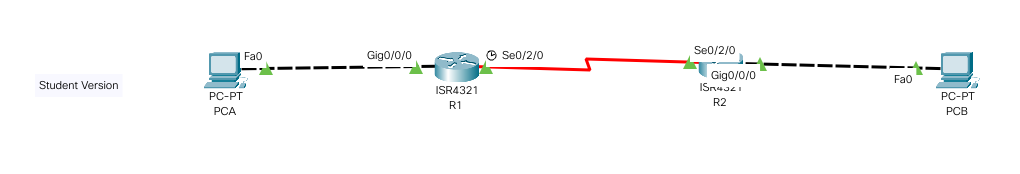
You are required to do the following:

* Set the SSID on the Access Point and Humidifier to *HOME2*.
* Server has to have an IP address of 20.20.20.1/24.
* Server will have a DHCP Server running, it will allocate IP addresses from 20.20.20.20 for 30 users.
* PC0 and the Humidifier will receive an IP address automatically.
* Set up IoT Monitoring on the Server using username *admin* and password *Rmit1234#*.
* Have the Humidifier register itself to the Server.
* Set up IoT Monitoring on PC0 for you to control the Humidifier.
* Set up WPA2-PSK on the Access Point and the Humidifier. Use Passphrase Key of *Rmit1234#*.
* Demonstrate it works by turning on the Humidifier from PC0.

**Lab C: Troubleshooting**

For this lab, each student will need to work individually

***Refer to the following diagram below. The teacher will send you the packet tracer file to assist you to troubleshoot.***

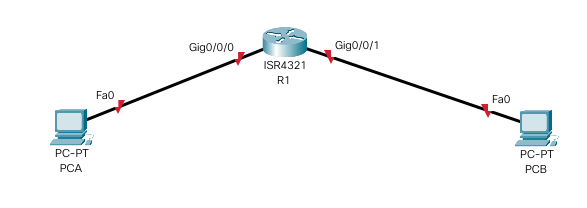


Troubleshoot this logical topology to get PCA to ping PCB.

**Lab D: Set-up an IPv6 network between two computers**

For this lab, each student will need to work individually.

**Task 1: Design the network topology as shown below**



* 1. **From the following table, enter the IPv6 address into the devices.**

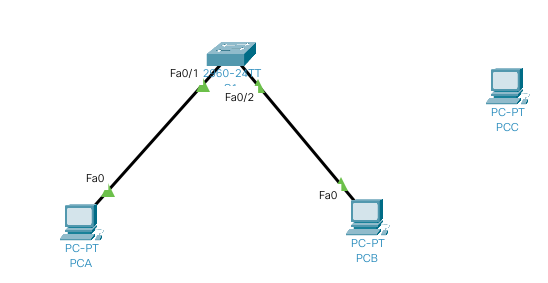
|  |  |  |  |
| --- | --- | --- | --- |
| **Device** | **Interface** | **IPv6 Address** | **Gateway** |
| R1 | G0/0/0 | 2001:def:cafe:1::1/64 | N/A |
| G0/0/1 | 4044:abc:fed0:1::1/64 | N/A |
| PCA | NIC | 2001:def:cafe:1::2/64 | 2001:def:cafe:1::1 |
| PCB | NIC | 4044:abc:fed0:1::2/64 | 4044:abc:fed0:1::1 |

1. **Assign an IP address to PCA.**
2. **Assign an IP address to PCB.**
3. **Verify that PCA can ping PCB by IPv6.**

**Lab E: Demonstrating layer 2 using port security**

For this lab, each student will need to work individually

Using the topology below, you are required to respond to the tasks listed below.



|  |
| --- |
| **Task 1: Cable the network as shown above.** |
| **Task 2: Assign the following IP addresses for computer and laptop.** |
| |  |  |  | | --- | --- | --- | | **Device** | **IP Address** | **Subnet Mask** | | PCA | 20.0.0.1 | 255.0.0.0 | | PCB | 20.0.0.2 | 255.0.0.0 | | PCC | 20.0.0.3 | 255.0.0.0 | | S1 (VLAN1) | 20.0.0.10 | 255.0.0.0 | |
| **Task 3: Perform the following on S1**  **Have PCA ping PCB.**  **Review what’s on the switch and see what MAC addresses the switch has learnt from the PC.** |
| **Task 4: Perform the following on S1**   * **Enable port security on the ports of the switch connected to the computers.** * **Have each port of the switch connected to the computers port secure one MAC address connected to the switch's ports.** * **Implement MAC Address sticky on port f0/1. This should allow the switch to learn the MAC address of PCA.** * **Associate PCB’s MAC Address to port f0/2** * **Have ports f0/1 and f0/2 go in shutdown state if a PC with the incorrect MAC address is plugged into those ports.** * **Verify that PCA can still ping PCB.** |
| **Task 5: Perform the following on S1**   * **Disconnect PCB from port fa0/2 on switch S1.** * **Assign PCC an IP address.** * **Plug PCC in its place to port fa0/2 on switch S1. Ping the switch.** |
| **Task 6: Reset the switch port to function by reconnecting PCB**   * **Disconnect PCC and plug back in PCB in its place making sure it connects to fa0/2 on the switch S1.** * **On S1, disable and enable the interface port fa0/2.** * **Verify that PCA can still ping PCB.** |

**Lab F: Verify connectivity with QUIC packets**

For this lab, each student will need to work individually. This is the final lab exercise to complete as part of this assessment.

* Go to [www.youtube.com](http://www.youtube.com/) in web browser.
* Open up Wireshark on your computer.
* In Wireshark, filter **quic** packets.
* Play a youtube clip.
* Have Wireshark capture the **quic** packets.

**Lab G - Ransomware attack**

For this lab, you need a Windows 11 Virtual Machine.

* + Create a **Demo** folder on C:.
  + Create a text file called **secrets.txt** with a message in it called “This is my message”.
  + Turn off Real Time Protection in Windows 11.
  + Download ransomware\_testfile\_unsigned.exe from Canvas in Week 8.
  + Run the ransomware file.

**Lab H: Demonstrating ARP Poisoning**

This lab requires two virtual machines, Windows 11 and Kali Linux.This lab can only be done in the home environment.

* Bridge the Network Adapter for both Virtual Machines.
* On both virtual machines, set the IP address to automatic.
* Ensure both virtual machines have Internet access.
* Note down the IP address of your WiFi router and your Windows machine.
* On Kali Linux, run Ettercap.
* Turn on Ettercap. (Click the tick).
* Click the Magnifying Glass in Ettercap.
* Click the Host Lists button to locate the IP address of your WiFi router and Windows Machine.
* Select the WiFi Router’s IP address and add it as Target 1.
* Select the Windows Virtual Machine’s IP address and add it as Target 2.
* Click the Globe button and select ARP Poisoning. Sniff for Remote Connections and click OK.
* Go to the Windows Machine and open a Web Browser. Type <http://testphp.vulnweb.com/login.php>. Enter user name *admin* and password *test* then click Login.
* Verify Kali Linux has intercepted the username and password.

**Lab I**

* Assign IP address of 192.168.1.1/24 to the router’s port.
* Set up Telnet access to the router.
* Bridge Kali Linux to the network.
* Assign IP address of 192.168.1.2/24 to Kali Linux attached to the router.
* Perform a denial of service attack on a router using the hping command.
* Attempt to Telnet to the router, it should fail.
* Check to see how busy the processor of the router is.

Section B – **Marking Guide**

Observation checklist

|  |  |
| --- | --- |
| **TASK:**  Describe the task – context and conditions for assessment. | *The task should be work related and performed in a fully simulated or workplace environment. (Context of the assessment)*  *Describe the task to be undertaken and under what conditions e.g. List the materials and equipment the students will have access to complete the task and any contingencies that must be dealt with such as time constraints and workplace interruptions. (Conditions of assessment)*  *Identify any specific workplace/organisational/regulatory requirements to be met.* |

| **Actions to be Observed** | | **Satisfactory** | **Not Satisfactory** | **Assessor comments** |
| --- | --- | --- | --- | --- |
| **Lab A: Plan and configure a basic network set-up** | | | | |
| **T1** | Select appropriate network elements and connect devices:   * Cabling the devices safely and accurately * Cables connected to the right ports |  |  |  |
| **T2** | Locate and Run PuTTY or Teraterm   * Ensuring that putty/Teraterm is installed to make a connection to the router |  |  |  |
| **T3** | Resetting and initializing the router   * Erasing any configuration of the router and then reloading the router |  |  |  |
| **T4** | Accessing the Router   * Accessing privileged exec mode to configure the router |  |  |  |
| **T5** | Put a hostname on a router   * Assign a host name to the router |  |  |  |
| **T6** | Place an IP address on the Router – Configure router interfaces   * Assigning IP addresses to the interfaces of the routers and activate the ports |  |  |  |
| **T7** | Set up Passwords – secure router access for network management and security   * Assigning a console and vty passwords to the routers |  |  |  |
| **T8** | Setup IP on PC – configure PCs   * Assigning an IP address to the PCs |  |  |  |
| **T9** | Test connection   * Testing the connection of the PCs * Testing PING * Testing telnet |  |  |  |
| **T10** | Routing protocol setup on routers – interoperability with remote networks   * Assigning RIP routing protocol on the routers |  |  |  |
| **T11** | Test connectivity between PC’s   * Testing connectivity between PC’s using PING |  |  |  |
| **T12** | * Install Windows 7 in Virtualbox with one called PC0 and the other called PC1. |  |  |  |
| **T13** | * Configure the firewall on Windows 7 to enable ICMP so that the two virtual machines can ping each other successfully. * Have PC0 discover what is the MAC address of Sydney Router’s port it is attached to through a ARP request. |  |  |  |
|  | * Share a folder using the SMB protocol. |  |  |  |
| **T14** | Reset and pack up - Clean up and restore worksite, secure sign-off   * Erasing router configuration and reboot the router |  |  |  |
| **Lab B: Networking IoT Devices** | | | | |
| **T1** | You are required to do the following:   * Set the SSID on the Access Point and Humidifier to *HOME2*. * Server has to have an IP address of 20.20.20.1/24. * Server will have a DHCP Server running, it will allocate IP addresses from 20.20.20.20 for 30 users. * PC0 and the Humidifier will receive an IP address automatically. * Set up IoT Monitoring on the Server using username *admin* and password *Rmit1234#*. * Have the Humidifier register itself to the Server. * Set up IoT Monitoring on PC0 for you to control the Humidifier. * Set up WPA2-PSK on the Access Point and the Humidifier. Use Passphrase Key of *Rmit1234#*. * Demonstrate it works by turning on the Humidifier from PC0. |  |  |  |
| **Lab C: Troubleshooting** | | | | |
| **T1** | Troubleshooting   * Packet tracer file from assessor is referred to * Troubleshoot the devices and see what needs to be fixed in order for PCA to communicate to PCB |  |  |  |
| **Lab D: Setting up IPv6** | | | | |
| **T1** | Set-up an IPv6 network between two computers   1. Use virtual box to have a virtual machine called PCA, and have another virtual box on a machine called PCB 2. Assign IPv6 addresses to all the devices – router, PCA virtual machine and PCB virtual machine 3. Have PCA ping PCB |  |  |  |
| **Lab E: Demonstrating layer 2 using port security** | | | | |
| **T1** | Draw or physically connect the devices |  |  |  |
| **T2** | Assign IP addresses to each device |  |  |  |
| **T3** | Ensure PCA communicates to PCB by PING   * Check to see if the switches have learnt the MAC addresses of those PC’s |  |  |  |
| **T4** | Set up port security   * Ensure that the PC’s can still PING each other |  |  |  |
| **T5** | Disconnect PCB and connect PCC to the port   * Verify that the port can shut down automatically due to incorrect MAC address |  |  |  |
| **T6** | Disconnect PCC and connect PCB   * Reset the port and verify PCB can communicate on the network |  |  |  |
| **Lab F: Verify connectivity with QUIC packets** | | | | |
| **T1** | * Verify connectivity using QUIC packets using Wireshark. |  |  |  |
| **Lab G: Ransomware Testing** | | | | |
| **T1** | Run the ransomware file to encrypt the contents of secrets.txt in the Demo directory. |  |  |  |
| **Lab H: ARP Poisoning** | | | | |
|  | Have Kali Linux be an attacker machine to impersonate the MAC Address of the victim and the WiFi router. |  |  |  |
| **Lab I: Denial of Service Attack** | | | | |
|  | Have Kali Linux perform a Denial of Service attack |  |  |  |