Network Management Activities

Network Management Y/618/5217 **AC 3.1:** Interrogate a network to identify the network asset and their configuration. **AC 3.2:** Carry out routine network management activities to meet requirements. **AC 3.3:** Keep accurate records of network management tasks. **AC 3.4:** Design a network security policy for a small organisation.			
Learner Name	Oluwaseun Folarin	**Tutor Name**	Shamim Khan

Scenario

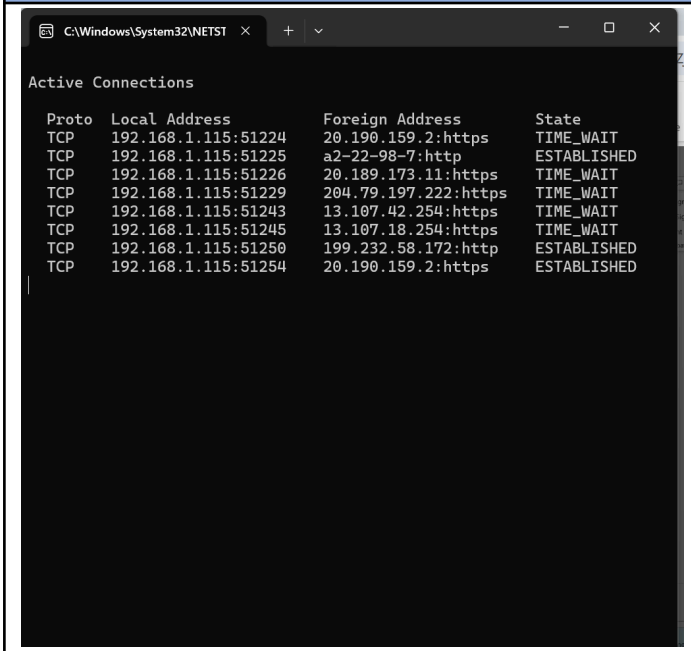
"Pentest Ground" *are a security services company based in New York and have employed you as their Network Administrator. They have requested that you undertake some network management activities on their existing network.*

You have been asked to undertake these network management activities on Pentest Ground's existing network:

- *Interrogate the network to identify the network assets (pc/server/router etc) and their configuration, such as user account location, choosing server and setting rights, drive mappings and/or virus scanning options (3.1).*
- *Undertake regular maintenance activities to meet requirements such as backup and restore files, user account creation and deletion, design and develop login scripts, virus scans and/or file cleanup (3.2).*
- *Keep an accurate record of network management tasks undertaken such as work logs, log resources used and/or system testing (3.3).*
- *Design a network security policy for Pentest Ground which could include a period review of user access and rights, penetration testing, security audits, review firewall and access control list policies (3.4).*

Ensure you use Cisco Packet Tracer and the file named "Pentest Ground Network Management 3.1, 3.2, 3.3, 3.4.pkt" to undertake the activities, ensuring you capture evidence as you go.

Task 1: Demonstrate open ports on the network using an appropriate command line network utility.



I searched for **Netstat** on my computer, a black command prompt page popped up which showed the active connections or ports that are currently open on my PC.

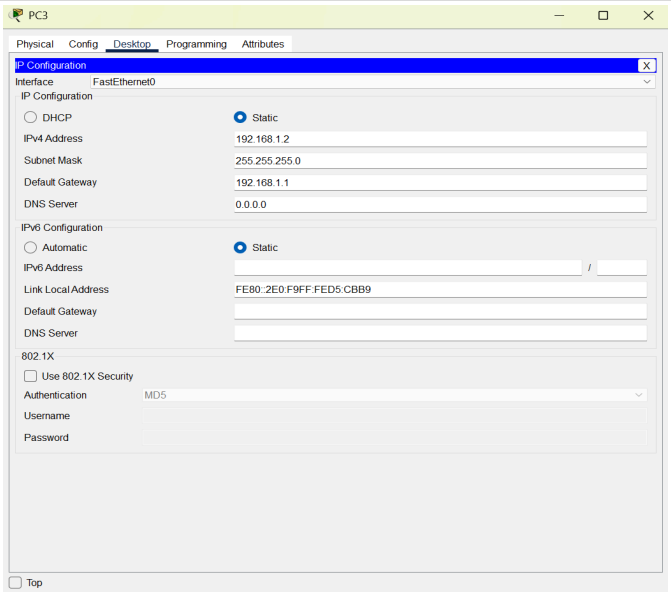
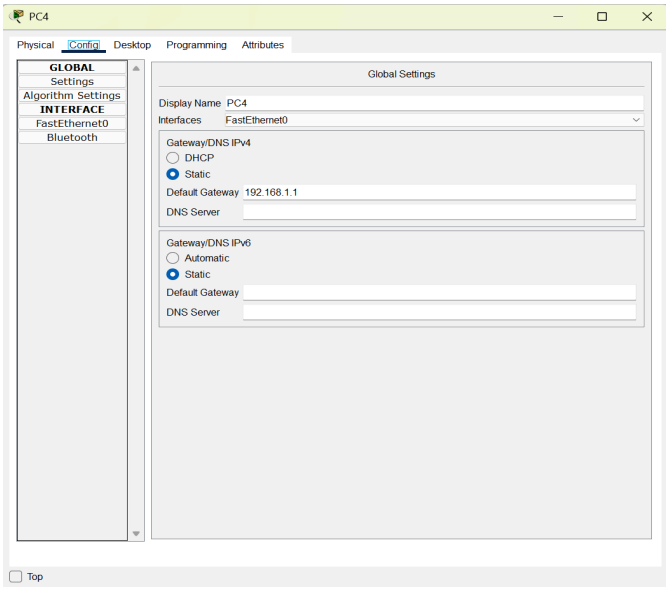
Under the **''Proto''** column, we have the TCP protocol that was used (Transmission Control Protocol).

Under **''Local Address''** is the IP Address assigned to my PC.

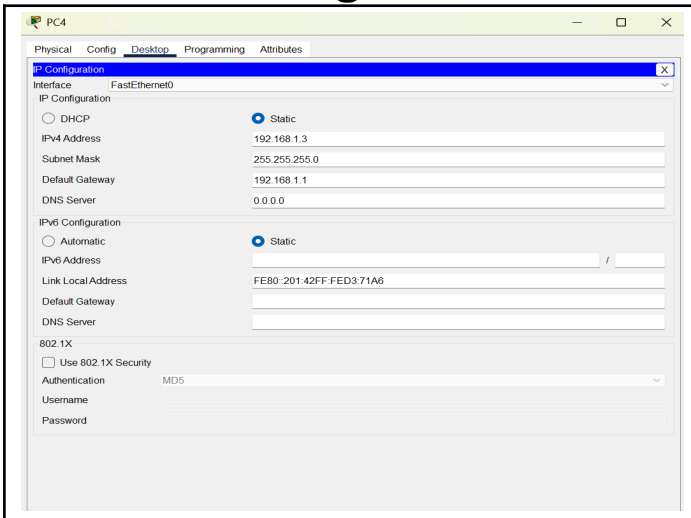
Under **''Foreign Address''**, a foreign number is linked to the port number through which it establishes the connection.

Under **''State''** is the current status of the active connections. It helps troubleshoot any problems relating to the network connection and detect unauthorized access to the computer

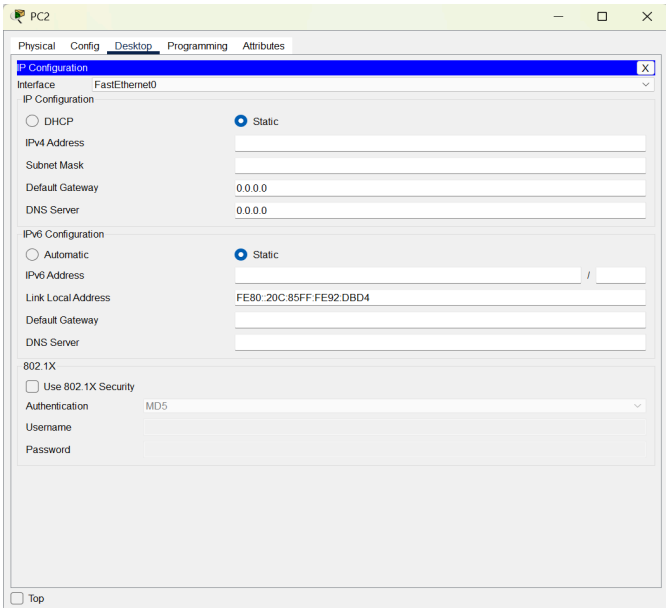
Example 1: The state of the first connection with the local address and port number (192.168.1.115:51224) shows 'Time_Wait' which means a holding period of about 2 minutes. It gives room for any packets that might have been delayed from previous connections and room for the previous packets sent to be

	acknowledged. No packet will be received or sent during the 'time_wait' period. **Example 2:** The second connection on the list with the local address and port number (192.168.1.115:51225) shows ''ESTABLISHED'' which indicates connection linked to a port. It is open and ready to receive transmission.
Task 2: Complete the following network management activities on the network.	
Check IP configuration is set up correctly for each device:	
	**Annotation:** IP configuration is set up correctly for PC-3
	PC-0 changed to PC-4

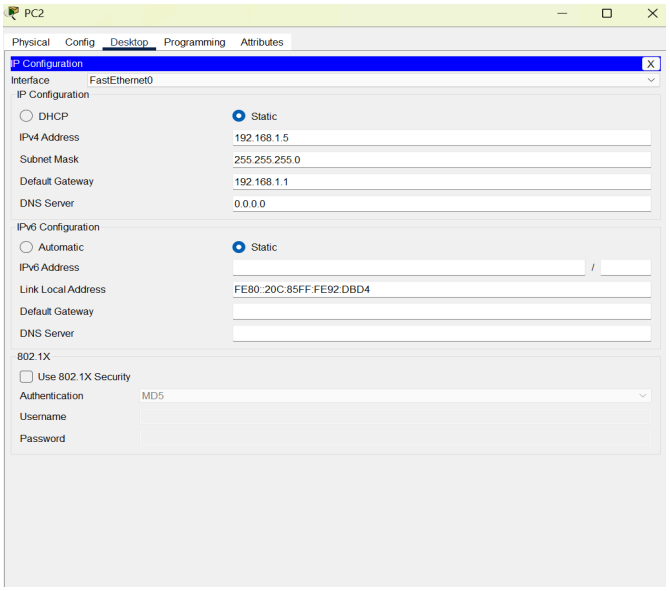
Network Management Activities



IP configuration is set up correctly for PC-4



PC-2 currently has no IP address, Subnet Mask, and a Default Gateway as shown on the screenshot.

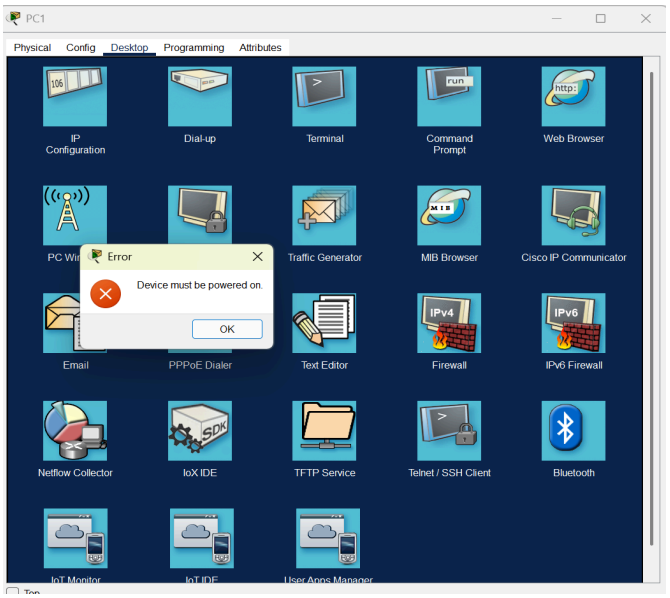


Configured IP properly for PC-2 by updating the IPv4 address and default gateway while Subnet mask generated automatically.

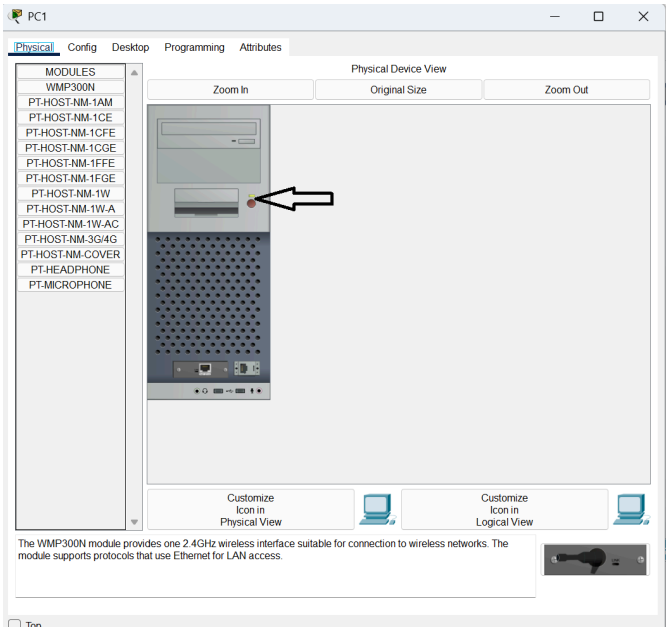
Network Management Activities

Ensure all device connections on the network are active, repair any which are not:

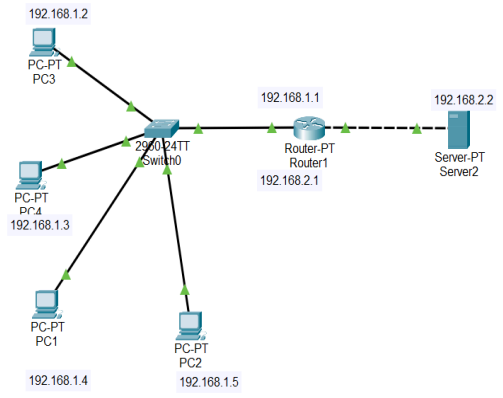
Screenshot(s):



When I clicked on PC-1, an error message popped up stating the device must be powered.

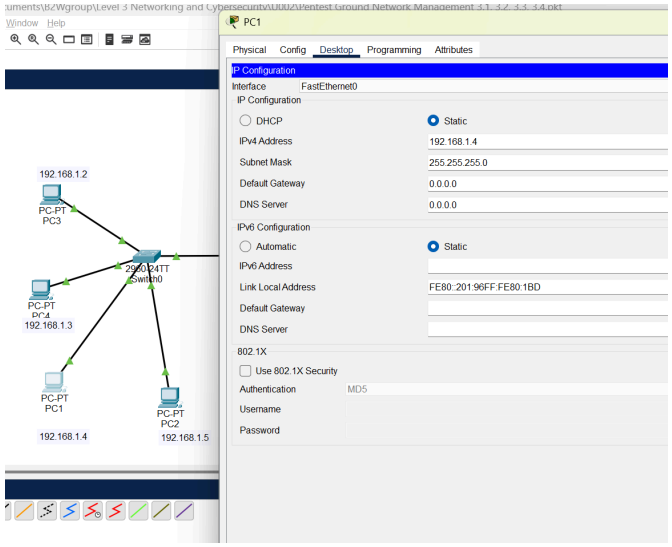


Then I went to ''Physical'' and switched it on by clicking on the red button. The arrow in the picture indicates how I switched it on.

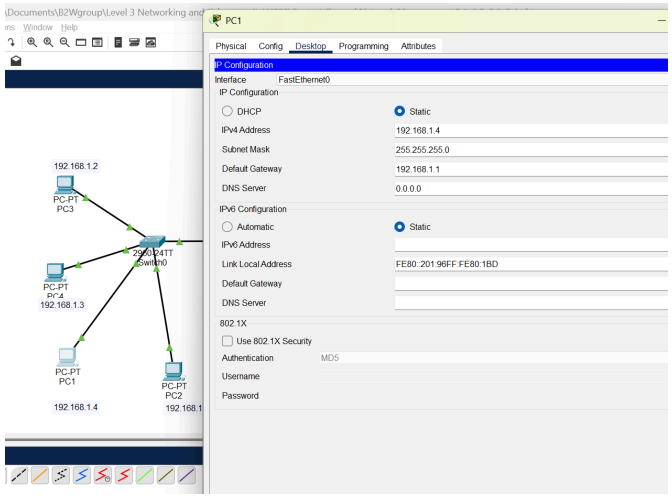


All device are now active on the network and all traffic are flowing to the switch

Network Management Activities



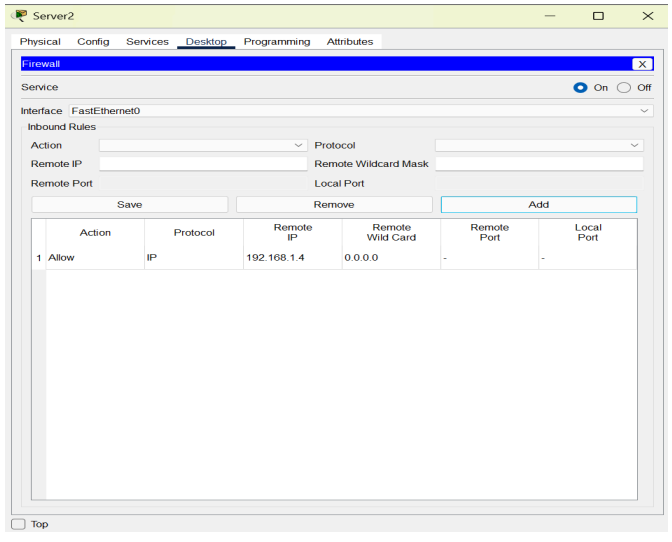
PC-1 default gateway was not available as shown in the screenshot



Default gateway now updated on PC-1

Check firewall is set up correctly on server 2 to allow PC 1 and PC 2 to access files as needed from the backup server:

Screenshot(s):

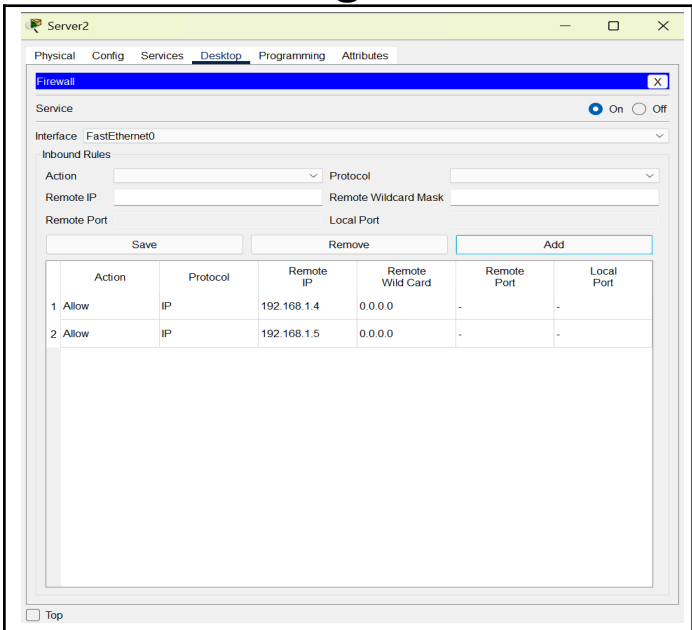


Annotation:

To confirm that firewall is set up properly for PC-1 and PC-1, I clicked on 'Server2', clicked on 'Desktop', clicked on 'IPv4', I removed both already set actions, switched on the 'Service Button, set up firewall to allow both PC-1 and PC-2 by selecting allow for action, IP for protocol, entered the correct respective details for 'remote IP' and 'Remote Wildcard Mask' as shown in the screenshot.

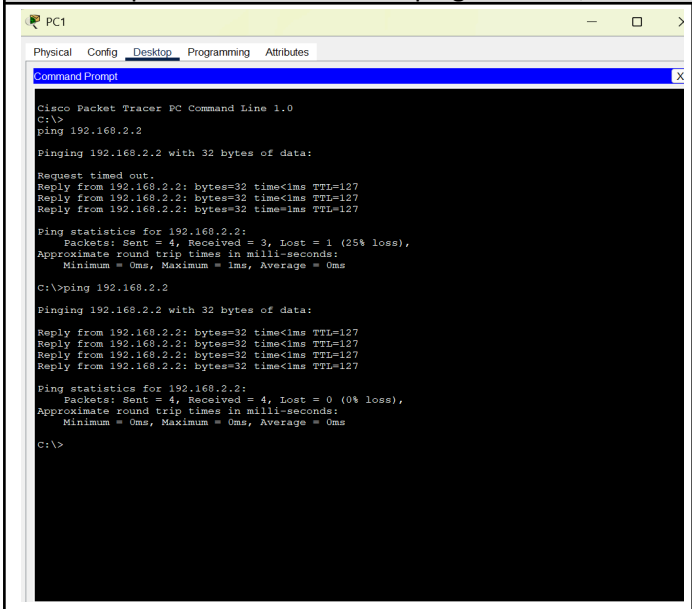
This shot shows access allowed for PC-1

Network Management Activities

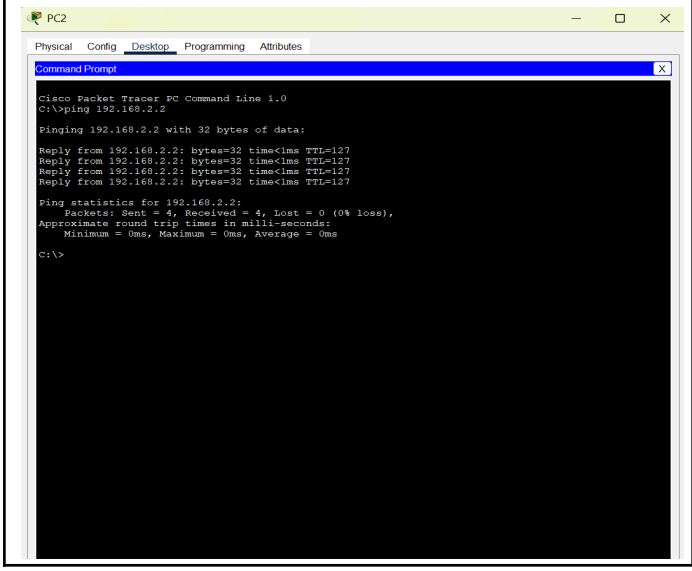


This shot shows access allowed for PC-2

Check response times when PC 1 pings server 2, consider the response and whether working as intended:



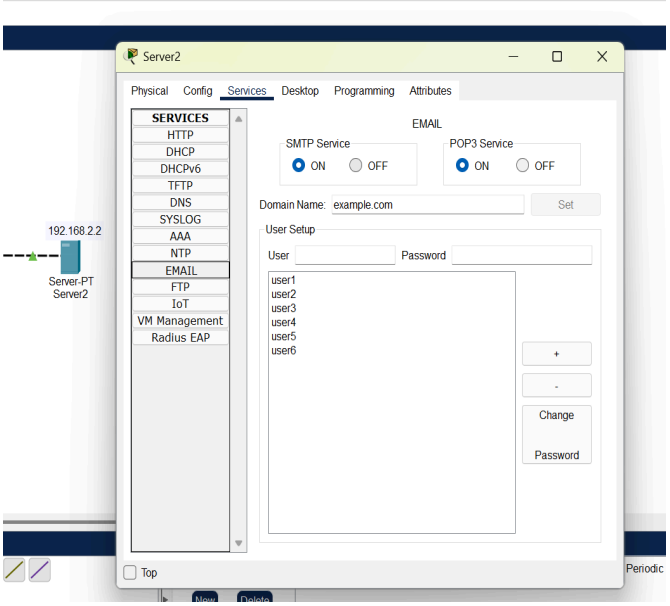
To check the response time PC-1 ping the server, I clicked on PC-1, followed by ‘desktop’, then ‘command prompt’. I typed in 192.168.2.2 to ping server from PC-1. At first attempt, out of 4 packets sent, 1 was lost and 3 was received by the server. I pinged again and this time all packets were successfully received.



To check the response time PC-2 ping the server, I clicked on PC-2, followed by ‘desktop’, then ‘command prompt’. I typed in 192.168.2.2 to ping server from PC-2. All packets were successfully received.

Network Management Activities

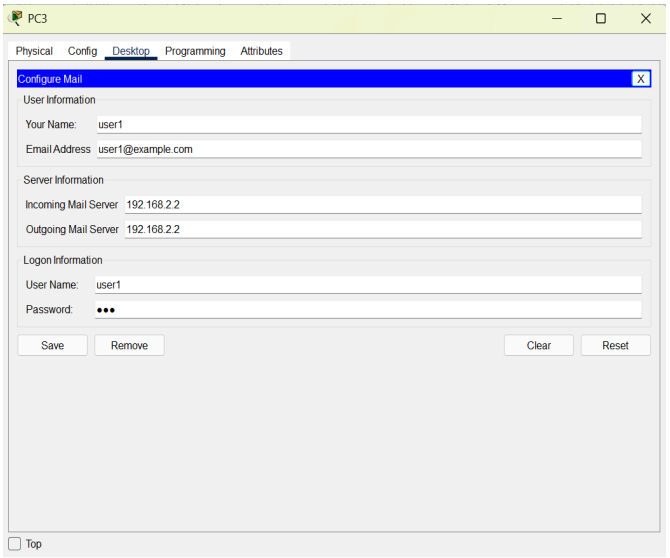
Check to see there are no outdated/unused users on the email server, disable any former employees email accounts present:



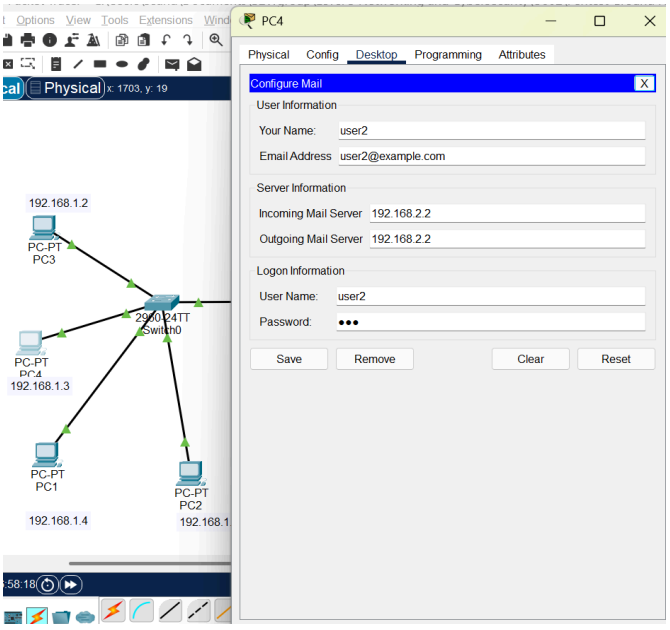
Annotation:

To verify no outdated users, disable former employees and set up a new user I clicked on Server2, followed by 'Service', then I clicked on 'EMAIL'.

This screenshot indicates that both services are switched on (SMTP and POP3) and all the users.

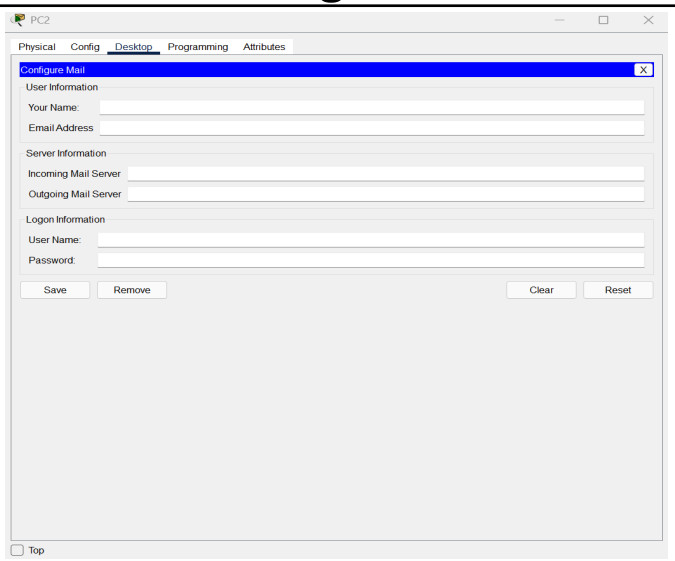


There is a user setup for PC-3 and the email has been configured.

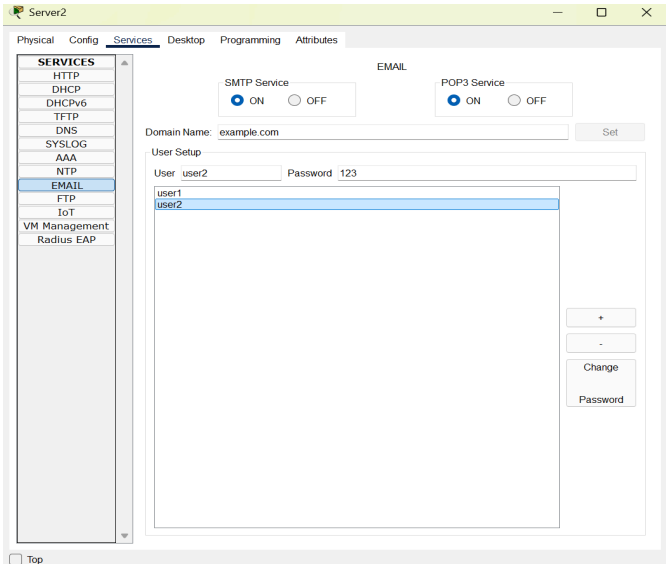


There is a user setup for PC-4 and the email has been configured.

Network Management Activities



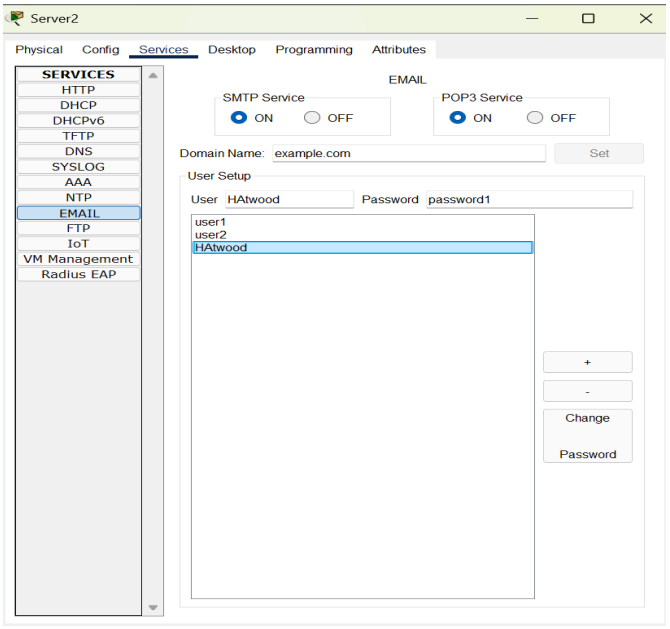
There is no user setup for PC-2



This screenshot shows the removal of unused users namely user3, user4, user5, and user6

Create a new user's email account on the server with details *Username: HAtwood* and *Password: Example1*:

Screenshot(s):



Annotation:

This screenshot shows a new user being set up namely *Username: HAtwood* and *Password: password1*

Network Management Activities

Task 3: Design a “network security policy” for Pentest Ground which should include:	
Policy Area	**Policy Details**
Periodic review of user access and rights	**User creation** To create a new user account, some details will be needed. The purpose of these is for personalization and to prevent unauthorized access. Details such as; Full name, Job role, Start date, Department, Fingerprint. **Acceptable Use of Policy** With the new user account access comes its responsibilities. Users must abide by these policies to ensure smooth business operations and prevent unauthorized access. Users must ensure to use the account access for intended data only and must not share the access with external bodies. Users must not attempt at any point, for any reason, try logging in with the access details on a public computer. Users must not share accessed data with external users and must use data for work related and/or intended purposes only after accessing. Users must use an account to communicate for work purposes only. **Periodic Review** Yearly audit access control to ensure no former employee's account is still active, if yes, delete them. Constant and immediate update of user account details when applicable.
Security audit	**These are to ensure maximum security during employment.** Retake fingerprints every 3 months and change fingers when retaking fingerprints every 3 months. Passwords must be 10 digits and must be a mix of digits, alphabets and special characters. It must also be updated every 60 days. Previous passwords must not be repeated, memorize it to not forget, and never write it down where it can be easily accessed. Set up 2 Factor Authentication and retina Authentication if and when applicable. **Steps to be taken at the end of an employee's employment contract** Employees who are no longer employed must return all company's equipment in their possession. Ensure after each termination or resignation, a letter/email is sent to IT for notification.
Review firewall	**Firewall policies to abide by.** The firewall will block all traffic and only allow the two devices granted access. In this case, PC-1 and PC-2. This is known as Default Deny Policy. It grants allowed users (PC-1 and PC-2) with enough access required to perform their specific tasks. All firewall rules should be documented. In this case, PC-1 and PC-2 being allowed access should be documented along with their respective IP addresses and remote wildcard. Also, Consistently review and update firewall rules to maintain their effectiveness and relevance.

Network Management Activities

	Set up firewalls with robust security settings, ensuring unnecessary services and features are disabled. Frequently back up firewall configurations and ensure only the right people have access to the firewall settings, no one else. Regular checks on firewall rules and settings to spot any weaknesses. Frequently test firewall rules and configurations to validate its functionality. Also, set up rigid logging and alert systems to enable you to quickly spot and deal with any security issues that may occur.