ICTSAS530

Use network tools

Assessment 4 of 6

Portfolio

Assessor Guide

Version 1

Assessment Instructions

Task Overview
This Portfolio assessment is divided into three (3) parts. Read the simulated environment set-up and resource information in Part A and complete the associated tasks in Parts B and C. Portfolio tasks include completing hands-on practical tasks in a simulated workplace environment, documenting processes and capturing screenshot evidence of the tasks performed.

Please provide all required screenshot evidence and written responses in the spaces provided.

Important: Before commencing your work, you must update your *Student name* and *Student number* in the footer from **page 2** onwards.

Additional Resources and Supporting Documents
ICTSAS530_04_Portfolio_Scenario documents (compressed/zipped folder) - This folder contains the following scenario documents required for completing the tasks in this assessment.

- AUS Retail_Simulated network for server room access.pkt
- AUS Retail_Network device log collection procedure.pdf

Assessment Information

Submission

You are entitled to three (3) attempts to complete this assessment satisfactorily. Incomplete assessments will not be marked and will count as one of your three attempts.

All questions must be responded to correctly to be assessed as satisfactory for this assessment.

Answers must be typed into the space provided and submitted electronically via the Learning Platform. Hand-written assessments will not be accepted unless previously arranged with your assessor.

Reasonable adjustment

Students may request a reasonable adjustment for assessment tasks.

Reasonable adjustment usually involves varying:

- the processes for conducting the assessment (e.g. allowing additional time)
- the evidence gathering techniques (e.g. oral rather than written questioning, use of a scribe, modifications to equipment)

However, the evidence collected must allow the student to demonstrate all requirements of the unit.

Refer to the Student Handbook or contact your Trainer for further information.

Please consider the environment before printing this assessment.

Part A: Simulated environment set-up and resources

All tasks in this assessment refer to a simulated environment where conditions are typical of a work environment that is experienced in the information and communications technology (ICT) field of work. The scenario relates to a fictitious retail business organisation called '**AUS Retail**'.

Read the case study scenario carefully before completing the tasks in Part B.

A1. Company background

AUS Retail started as a single retail store based in Sydney, NSW. They now have retail store locations across several other states and territories in Australia, and the business continues to grow.

The company manages a large volume of sensitive data, including customer information, financial transactions, inventory details, and employee records. To ensure the security of this data and maintain the trust of its customers, AUS Retail needs to implement robust network security measures.

- **Your role**

You work at AUS Retail as a **Network Administrator.** You are responsible for selecting, operating and testing an array of networking tools to maintain the network security of the existing network.

A2. Equipment and resources

To carry out the assigned job tasks you must have access to:

- a computer with a reliable internet connection
- an active Cisco Networking Academy (NetAcad) account (Go to https://www.netacad.com/ to create a new netacad student account if you do not already have one.)
- network simulation software 'Cisco Packet Tracer'
- other industry software packages such as:
    - Web browsing software (e.g. Microsoft Edge, Firefox, Chrome, Safari).
    - Microsoft Office software (e.g. WORD, PowerPoint, Excel).
    - A PDF reader.

A3. Organisational policies, procedures and guidelines

You are provided with the following legislative requirements, organisational policies, procedures and document templates required for your job tasks.

- **AUS Retail_Network device log collection procedure.pdf** – provides guidelines on how to collect event logs from network devices.

Industry guidelines: Guidelines for ICT Equipment | Cyber.gov.au

A4. Simulated network environment

Physical equipment layout inside AUS Retail's Corporate Office

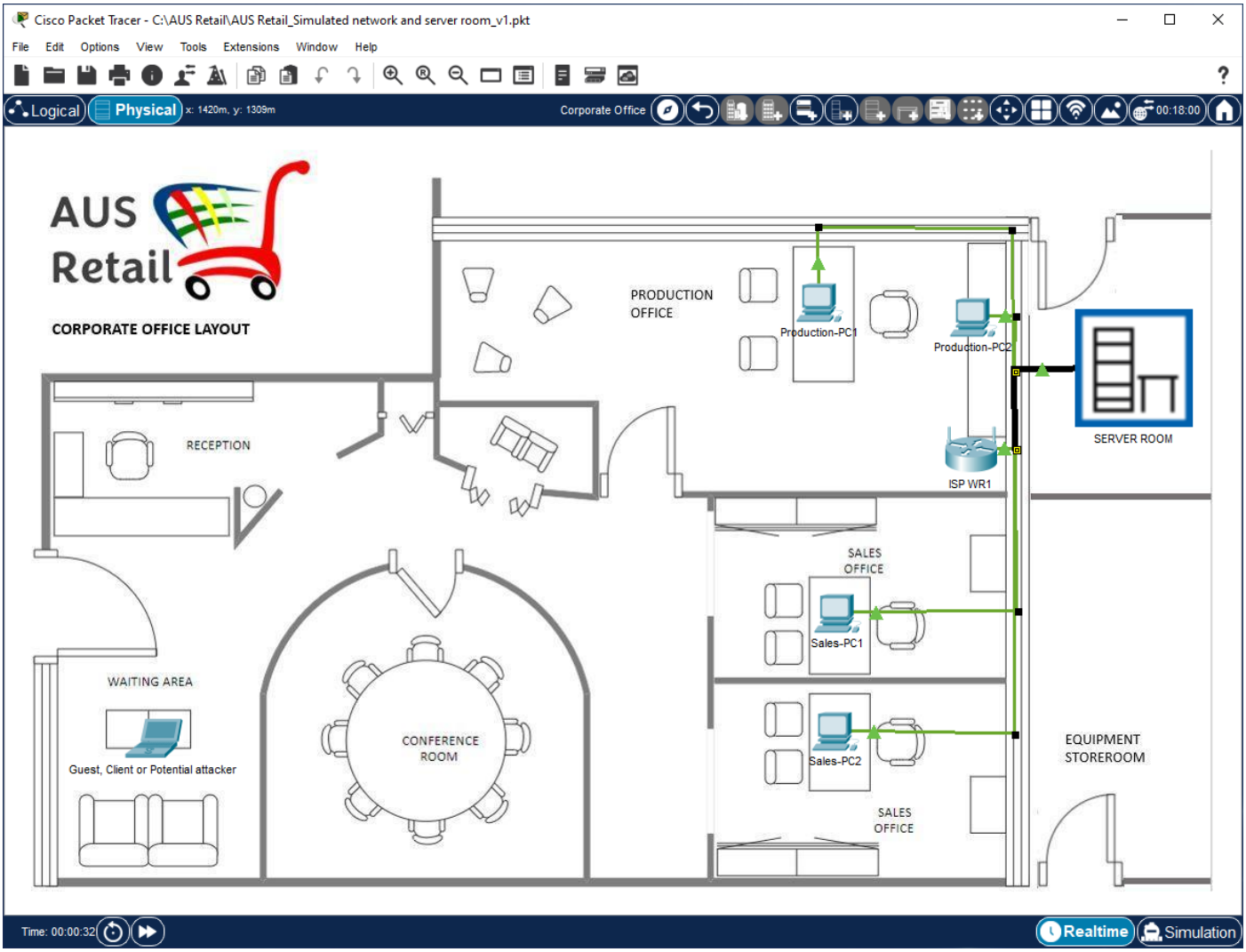


Figure 1 - AUS Retail Corporate Office equipment layout © Cisco Packet Tracer

Physical equipment layout inside the Server Room

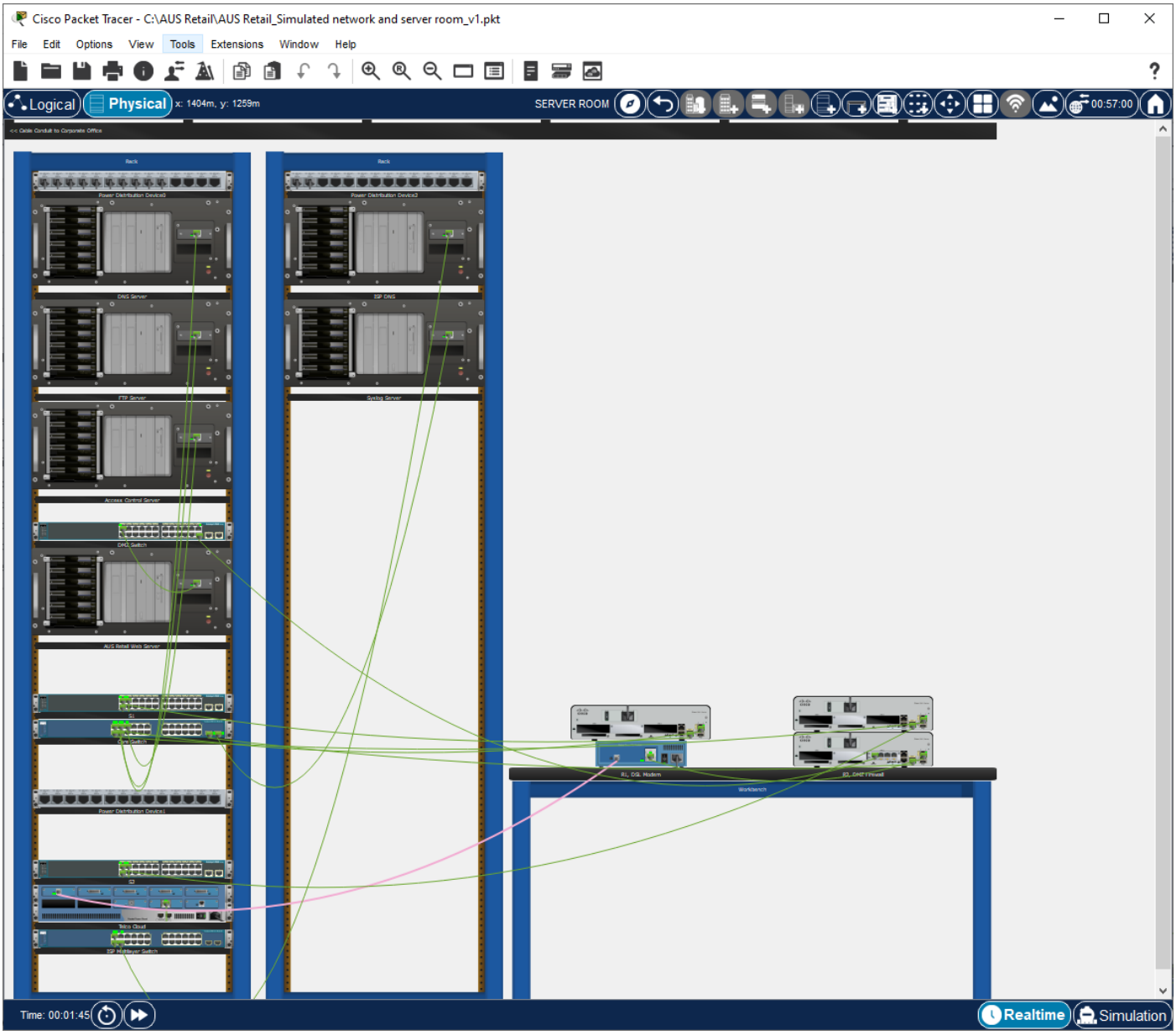


Figure 2 - AUS Retail Server Room equipment layout © Cisco Packet Tracer

Part B: Investigate organisational network equipment

To complete this part of the assessment, you are required to:

- access the simulated network environment using 'Cisco Packet Tracer' software and by opening the 'AUS Retail_Simulated network and server room.pkt' file provided
- follow organisational procedures and WHS guidelines in preparation for using hardware tools.

Scenario:

Prior to conducting any network security tests, you are required to investigate AUS Retail's network and identify the organisational computing hardware and components.

You will be conducting your inspections of equipment inside AUS Retail's 'Server Room' at the 'Corporate Office' site. Currently, the 'Server Room' contains devices and equipment that belong to the organisation as well as those installed by the ISP. You also notice that there are hazards present at the work site due to unmanaged

cabling. You were informed that there have been a few equipment and cabling upgrades within the wiring closet recently and it appears that WHS standards have not been followed by the contract installers.

According to the 'AUS Retail_SafeWork policy for network security testing.pdf', the following WHS standards and procedures should be followed within the 'Server Room'.

- All cables should be managed
- Rack-mountable network devices should be placed appropriately and safely on the racks
- Other network devices, that are not rack-mountable, should be placed on the 'Workbench'.

Tasks:

Task B1: Apply Organisational procedures and WHS standards

As preparation for conducting network security tests using hardware tools follow AUS Retail's equipment safe work policy and WHS standards within the 'Server Room'.

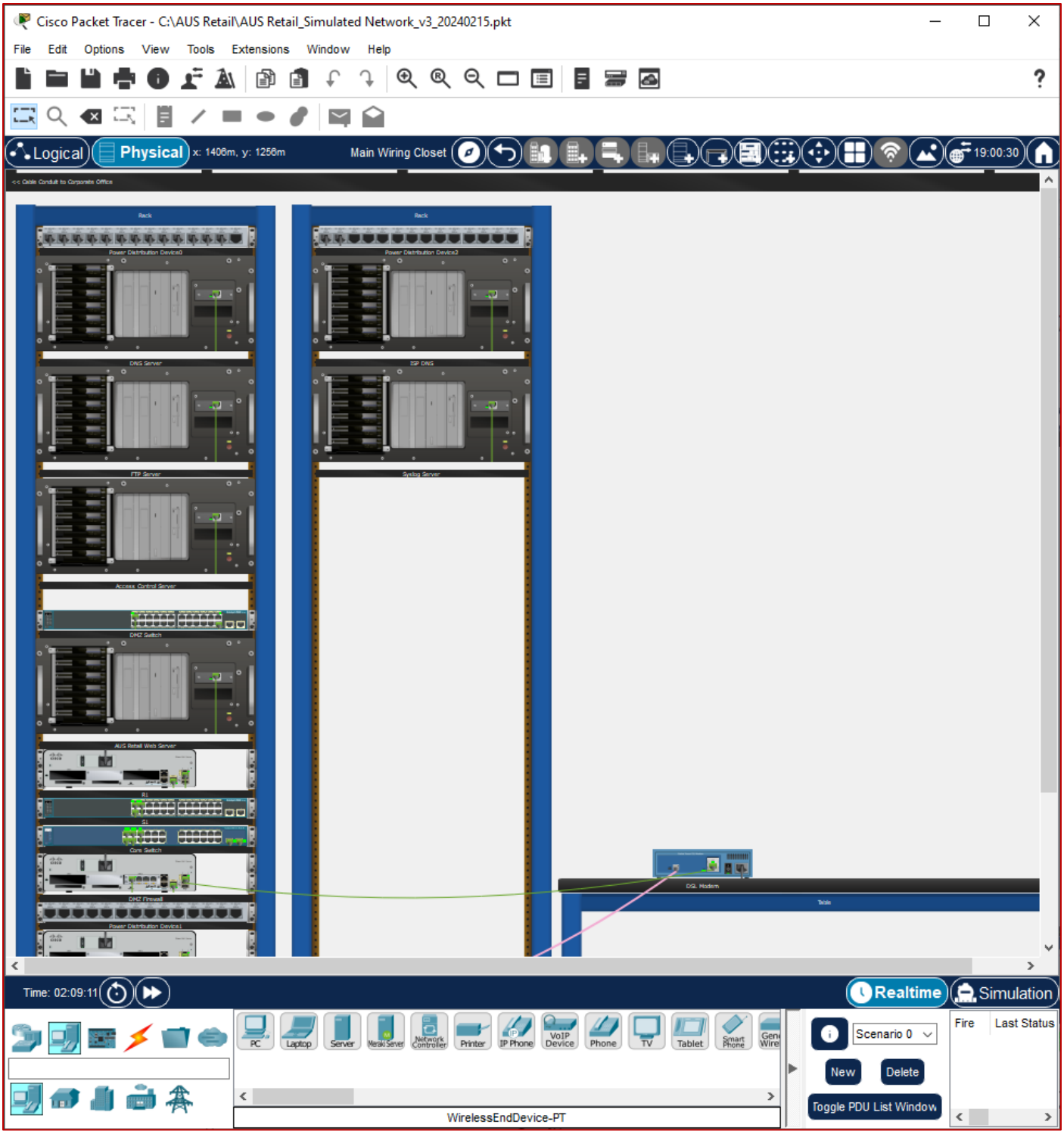
As evidence of completing this task,

- provide a screenshot of the 'Server Room' from the 'AUS Retail_Simulated network and server room.pkt' file.
  Note: You need to be in the 'Physical' view in 'Cisco Packet Tracer' file in order to access the 'Corporate office' and then the 'Server Room'.
- provide a brief explanation of the task performed and what other important considerations should be checked when testing network security using hardware tools. (Word count: 65-95 words)

Assessor instructions: Students must demonstrate:

- following WHS standards in the server room environment of the simulated network in Cisco Packet Tracer software by:
  - placing the rack mountable devices (e.g. routers) found on the workbench on server racks
  - managing the untidy cables so that tripping hazards are avoided
- their understanding of other important WHS considerations by providing a brief explanation of the task performed and their observations of the server room environment.

A sample screenshot of the server room environment after following WHS procedures given below.



Provide here a brief description of the task performed and its purpose.

Assessor instructions: Students are likely to use different wording in their responses. However, the acceptable responses must:

- be within the specified word limit
- reflect the characteristics described in the exemplar answer.

A sample answer is provided below.

Tasks performed:

- The three routers located on the Workbench were carefully mounted on the server rack following WHS procedures and guidelines for electrical safety.

- Cables were managed and tidied so to avoid any tripping hazards.

Other considerations: Adhering to Workplace Health and Safety (WHS) standards when testing network security using hardware tools is essential for maintaining a safe and healthy work environment. By following these standards, testers can mitigate risks, prevent accidents or injuries, and ensure the overall well-being of everyone involved in the testing process.

Assessor instructions: Assessors are to indicate the task result as Satisfactory (S) or Not Yet Satisfactory (NYS).

Assessor comments:

☐ S ☐ NYS

Task B2: Identify computing hardware and components

Identify and list the hardware equipment and components available in AUS Retail's 'Server Room' that belong to (or are controlled by) the organisation.

(Word count: 35-50 words)

Assessor instructions: Students must identify organisational computing hardware and components within the given simulated environment in Cisco Packet Tracer.

Note: The equipment within the 'Server Room' deliberately includes ISP-controlled devices. Students **should not** list these as part of their answer.

Students are likely to use different wording than the sample answer provided. However, the acceptable responses must:

- be within the specified word limit
- reflect the characteristics described in the exemplar answer.

A sample answer is provided below.

Hardware equipment

- Syslog Server
- DNS Server
- FTP Server
- Access control server
- AUS Retail Web Server
- Routers (R1, R2, DMZ Firewall)
- Switches (Core Switch, S1, S2, DMZ Switch)
- Power Distribution Devices x 3

Components:

- Ethernet cables (Copper Straight-through) - Multiple
- Server Racks X 2
- Workbench

Part C: Test network security using hardware tools

To complete this part of the assessment, you are required to:

- access the simulated network environment using 'Cisco Packet Tracer' software and by opening the 'AUS Retail_Simulated network and server room.pkt' file provided.
- use appropriate hardware tools to gather and log security event and alert data including a basic router, firewall and systems in the organisation's simulated network.
- follow organisational procedures when collecting logs and reported events

Scenario:

In order to test network security, AUS Retail's network needs to centrally capture and store data logs from network security devices.

For this purpose, AUS Retail's network is configured with a Syslog server and the critical network security devices are configured as Syslog clients. Therefore, the devices R1, R2, Core Switch, and DMZ Firewall in the network are configured to send their log entries (alerts, logs, reported events) to the syslog server.

The syslog server collects the log entries and allows them to be read using the 'NetFlow collector' which is a data recognition software tool.

Refer to the following AUS Retail's procedure when collecting data logs and reported events from the organisation's network security devices.

- 'AUS Retail_Network device log collection procedure.pdf'

Additionally, refer to information from the device manufacturers on how to interpret log messages from devices such as routers and firewalls:

- Cisco System Messages - Cisco System Messages Overview [Support] - Cisco (Long URL: https://www.cisco.com/c/en/us/td/docs/ios/system/messages/guide/consol_smg/sm_cnovr.html)

Tasks:

Do the following tasks to collect the required logs and event reports from the simulated network following organisational policies and procedures.

Task C1: Collect debug events from router 'R1'

Do the following in AUS Retail's simulated network environment following the relevant procedures where necessary.

a. Ensure that the 'NTP' service in the 'Access Control Server' is set to reflect the current date and time.

b. Turn on the Syslog service in the 'Syslog Server'.
Note: Have the Syslog service window open while doing the next sub-tasks (c and d).

c. Enable debugging to collect NTP information from the 'R1' router.
Observe the 'Syslog Server' window for log entries that will begin to appear. Ensure that the log message reflects the correct date and time. (Note: You may have to wait a few minutes until the NTP packets start to reflect the correct time.)

d. Enable debugging to collect EIGRP protocol information from the 'R1' router.

e. Observe the 'Syslog Server' window for log entries that will begin to appear. When you have captured the required types of debug messages, turn 'Off' the syslog service to stop capturing the messages. Note: Do not clear the log.

f. Provide a screenshot of the Syslog service window with captured log events (showing EIGRP and NTP) from the router 'R1', under 'Evidence of performing task C1'.

g. Outline the type of information that can be obtained from the logs collected. Include in your answer the interpretation of results through mathematical data (i.e. IP addresses, timestamps, device interface numbers etc.).

(Word Count: 60-100 words)

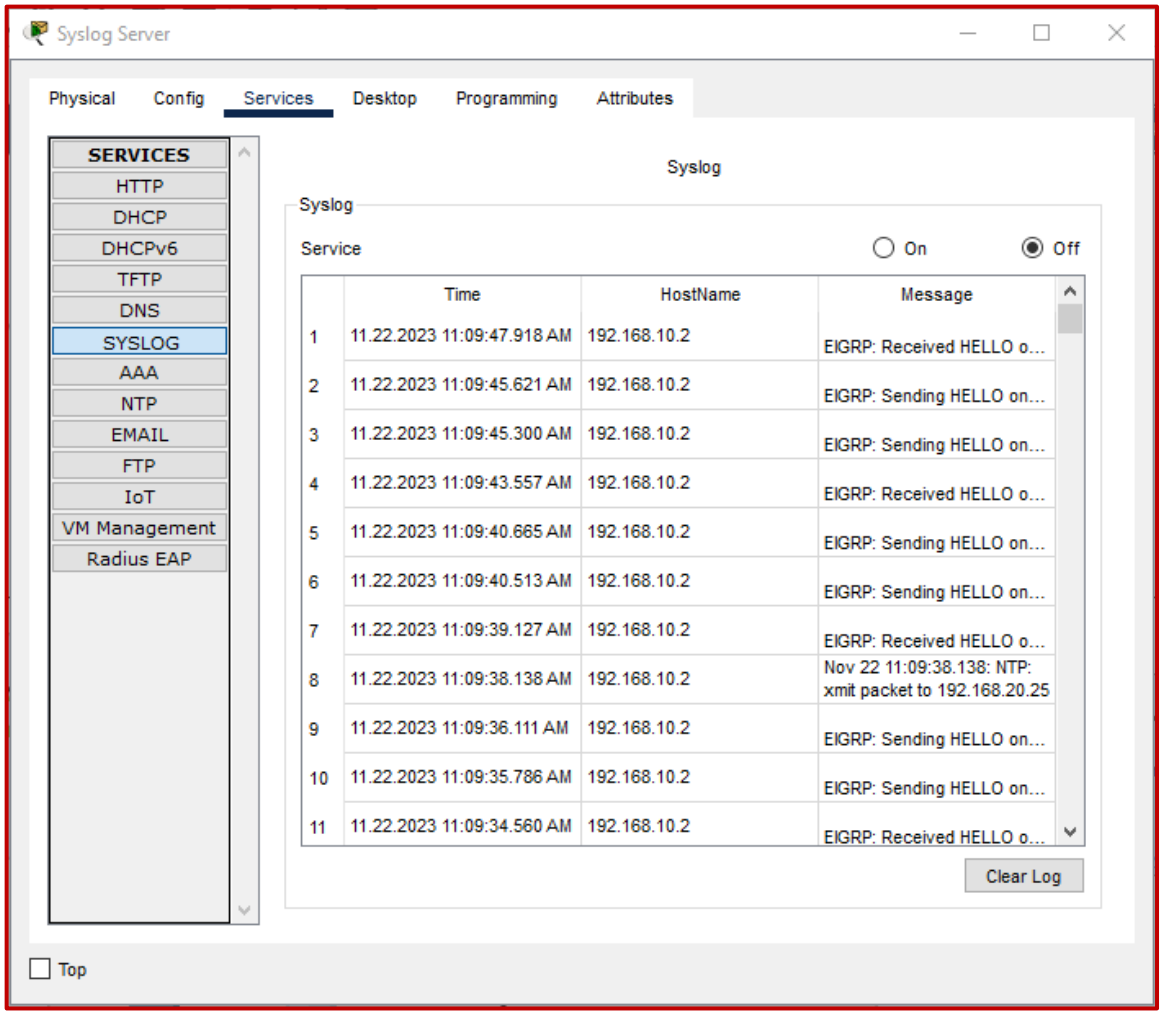
Evidence of performing task C1:

Assessor instructions: Students must:

- demonstrate the use of required tools within the simulated network and provide evidence of the data logs collected from the router in the form of a screenshot.
- outline their interpretation of the results through mathematical data. This may include the identification of numerical information such as timestamps, IP addresses, device interface numbers etc.

Provide here a screenshot of the captured data logs.

A sample screenshot is provided below.



Provide here an interpretation of the log data collected.

Assessor instructions: Students are likely to use different wording in their responses. However, the acceptable responses must:

- be within the specified word limit
- reflect the characteristics described in the exemplar answer.

A sample answer is provided below.

The data logs include:

- Time stamps of exact date (22nd November 2023) and time (around 11AM) of the logs collected,
- the hostname/ IP address (e.g. 192.168.10.2) from which the logs are generated from
- details of the eigrp packets sent/received (e.g. HELLO)
- details of the ntp information from ntp server at 192.168.20.25
- device interfaces from which packets were sent/received (e.g. GigabitEthernet0/0, GigabitEthernet0/1)

Assessors are to indicate the task result as Satisfactory (S) or Not Yet Satisfactory (NYS).

Assessor comments:

☐ S ☐ NYS

Task C2: Collect user access event logs from router 'R2'

Router 'R2' is configured with the TACACS+ protocol which allows remote authentication through a centralised server. In this task, you will attempt to log in to 'R2' with login credentials and then collect user access event logs by accessing the 'AAA Accounting service records'.

a. From the 'Access Control Server', access 'Desktop' > 'AAA Accounting'. Keep the 'AAA Accounting Records' window open and do the rest of the sub-tasks.
Note: Observe the 'AAA Accounting Records' window for any log entries upon completing each of the following sub-tasks.

b. Go to 'R2' router's 'CLI' tab and press 'Enter'.
Here, R2 will ask for the username and password to be entered before granting access to its command line interface. Use the following credentials to log in to the router:
    a. Username: cyberanalyst
    b. Password: security15KEY

c. Logout from the 'R2' router's CLI by typing 'logout'.

d. Attempt to log in to 'R2' router's CLI using the following false credentials:
    - Username: Attacker
    - Password: some incorrect password

Note: Keep entering the above false credentials at least three (3) times.

h. Provide a screenshot of the 'AAA Accounting Records' window showing the captured user access log events from the router 'R2', under 'Evidence of performing task C2'.

i. Outline the type of information that can be obtained from the logs collected. Include in your answer the interpretation of results through mathematical data (i.e. timestamps, IP addresses etc.). You may include portions of the debug messages in your answer. (Word Count: 60-100 words)

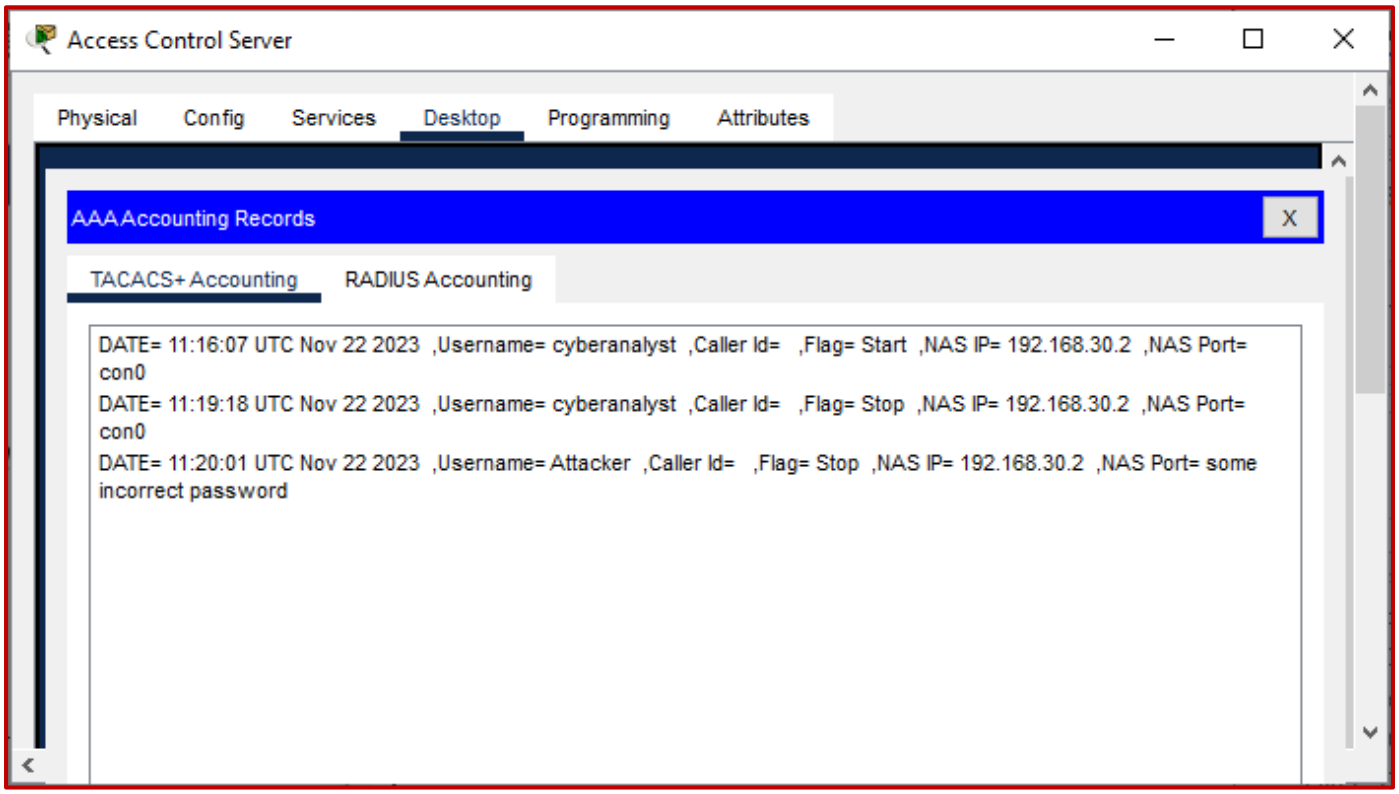
Evidence of performing task C2:

Assessor instructions: Students must:

- demonstrate the use of required tools within the simulated network and provide evidence of the data logs collected from the router in the form of a screenshot.
- outline their interpretation of the results through mathematical data. This may include the identification of numerical information such as timestamps, IP addresses, etc.

Provide here a screenshot of the captured data logs.

A sample screenshot is provided below.



Provide here an interpretation of the log data collected.

Assessor instructions: Students are likely to use different wording in their responses. However, the acceptable responses must:

- be within the specified word limit
- reflect the characteristics described in the exemplar answer.

A sample answer is provided below.

The data logs include:

- Time stamps of the date/time of when the event occurred.
- The username and password used

- The IP address of the host device (R2's IP address 192.168.30.2) from which the login attempt occurred.
- 'Start' flag indicates the time of login by the 'cyberanalyst' user and the 'Stop' flag indicates the time the user logged out. For example:
- Upon third time of the incorrect login attempt by the 'Attacker' was recorded with a 'Stop' flag with the incorrect password included in the log as plain text.

Assessors are to indicate the task result as Satisfactory (S) or Not Yet Satisfactory (NYS).

Assessor comments:

☐ S ☐ NYS

Task C3: Collect and visualise network flow logs

In this task, you will use the 'Netflow Collector' tool in the 'Syslog Server' to collect and visualise the network logs.

In the 'Syslog Server', go to the 'Desktop' tab, > 'Netflow Collector' service, and turn it 'On'. Keep this window opened and do the following:

a. From any PC on AUS Retail's internal network, ping the AUS Retail web server's IP address.
b. Observe the data visualisation in the 'Netflow Collector' window.
c. Select the wedge of the Pie chart that displays details of the traffic flow relevant to the web server ping request.
d. Provide evidence of the 'Netflow Collector' window with details of the captured network flow event under 'Evidence of performing task C3'.
e. Outline the type of information that can be obtained from the logs collected. Include in your answer the interpretation of results through mathematical data (i.e. timestamps, IP addresses, statistics of data traffic flows etc.)
(Word Count: 60-100 words)

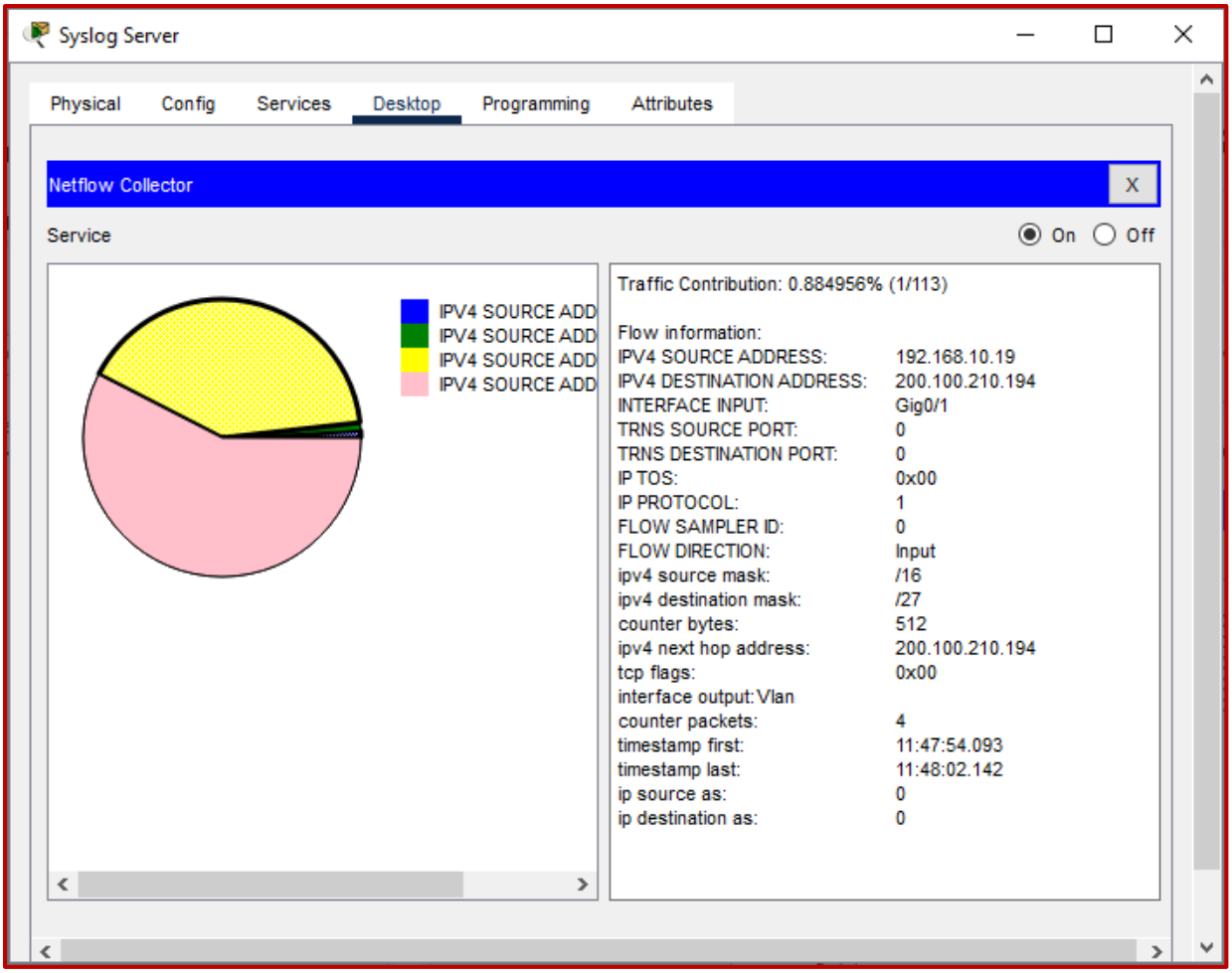
Evidence of performing task C3:

Assessor instructions: Students must:

- demonstrate the use of required tools within the simulated network and provide a screenshot as evidence of the data logs collected from the 'Netflow Collector'.
- outline their interpretation of the results through mathematical data. This may include the identification of numerical information such as timestamps, IP addresses, traffic contribution %, etc.
- the pie chart displayed will vary based on the traffic on the simulated network. As other packet flows such as eigrp, ntp and other traffic are being sent between devices, NetFlow will continue to capture these packets and export statistics to the NetFlow Collector. Therefore, the longer NetFlow is allowed to run on the network simulation, the more traffic statistics will be captured.

Provide here a screenshot of the captured data logs.

A sample screenshot is provided below.



Provide here an interpretation of the log data collected.

Assessor instructions: Students are likely to use different wording in their responses. However, the acceptable responses must:

- be within the specified word limit
- reflect the characteristics described in the exemplar answer.

A sample answer is provided below.

- The particular traffic category selected from the pie chart representation accounts for 0.8849% of the total traffic collected.

The details of the logged data include:

- Time stamps of the date/ time of when the event occurred.
- Source IP addresses (192.168.10.19) Sales-PC2 and destination IP address of the web server (200.100.210.194)
- Interface input number G0/1
- No. of counter packets (4) as the ping/echo message sends out 4 requests/replies.

Assessors are to indicate the task result as Satisfactory (S) or Not Yet Satisfactory (NYS).

Assessor comments:

☐ S ☐ NYS

Appendix 1: Assessment submission checklist

Submit a PDF version of this completed assessment document. Make sure you have also included each of the following files as evidence of your performance. Remember to create a compressed folder for each module before uploading them for submission

Part B: Investigate organisational network equipment		
B1	One (1) screenshot and outline of other important WHS considerations	☐
B2	List of organisational computing hardware and components	☐
Part C: Test network security using hardware tools		☐
C1	Screenshot of the captured data logs from router 'R1' Interpretation of the log data collected (brief description).	☐
C2	Screenshot of the captured data logs from router 'R2' Interpretation of the log data collected (brief description).	☐
C3	Screenshot of the captured data logs from network devices using the data recognition software 'Netflow Collector'. Interpretation of the log data collected (brief description). Submission of the completed Cisco Packet Tracer file: <student ID>_AUS Retail_Simulated Network for server room access.pkt	☐

Assessment feedback

Assessors are to indicate the assessment outcome as Satisfactory (S) or Not Yet Satisfactory (NYS).

Assessor comments:	☐ S	☐ NYS

Congratulations, you have reached the Assessment 4!