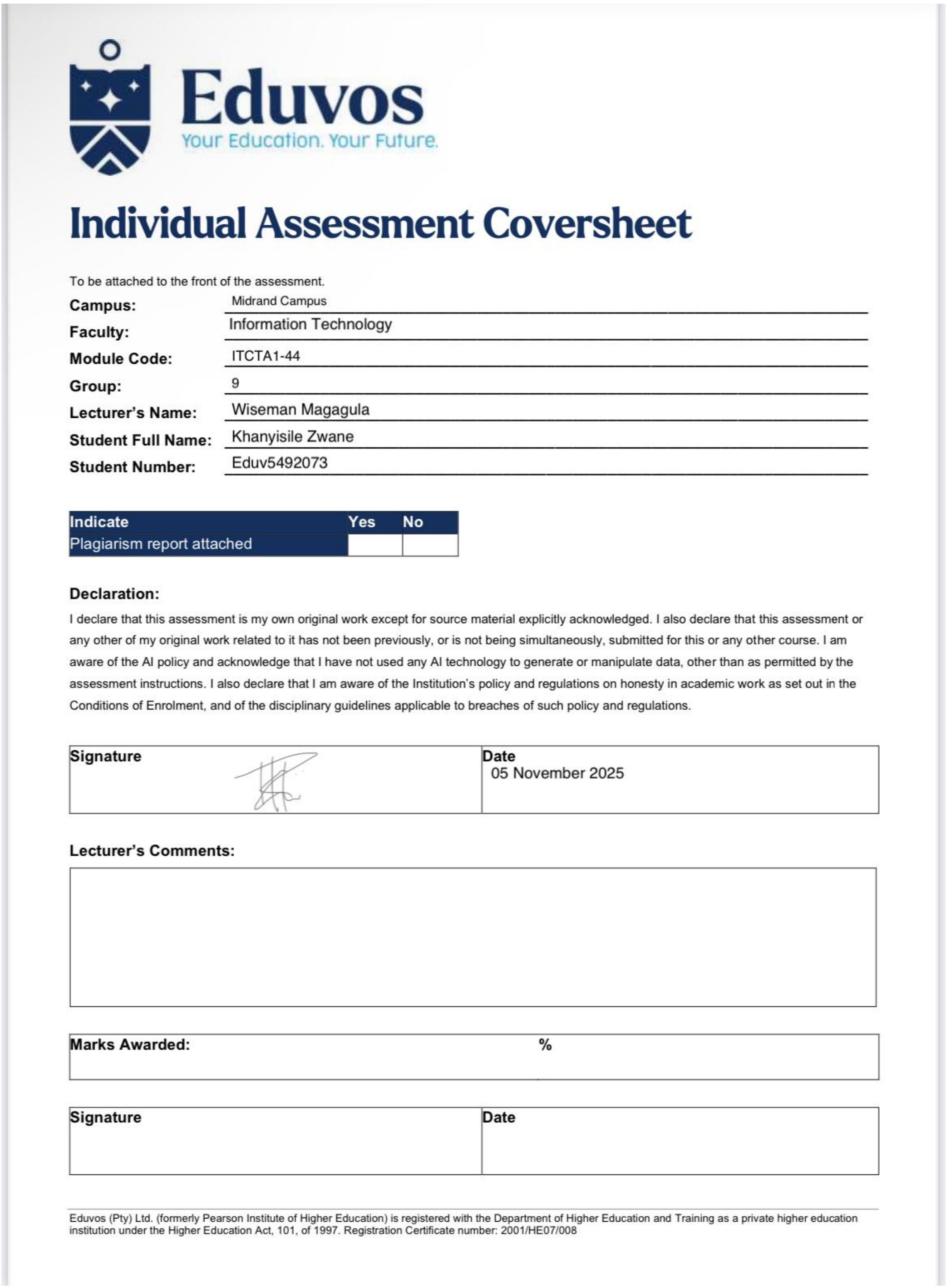


Eduvos
Your Education. Your Future.

Individual Assessment Coversheet

To be attached to the front of the assessment.

Campus:	Midrand Campus
Faculty:	Information Technology
Module Code:	ITCTA1-44
Group:	9
Lecturer's Name:	Wiseman Magagula
Student Full Name:	Khanyisile Zwane
Student Number:	Eduv5492073

Indicate	Yes	No
Plagiarism report attached	□	□

Declaration:

I declare that this assessment is my own original work except for source material explicitly acknowledged. I also declare that this assessment or any other of my original work related to it has not been previously, or is not being simultaneously, submitted for this or any other course. I am aware of the AI policy and acknowledge that I have not used any AI technology to generate or manipulate data, other than as permitted by the assessment instructions. I also declare that I am aware of the Institution's policy and regulations on honesty in academic work as set out in the Conditions of Enrolment, and of the disciplinary guidelines applicable to breaches of such policy and regulations.

Signature	**Date** 05 November 2025

Lecturer's Comments:

Marks Awarded:	**%**

Signature	**Date**

Eduvos (Pty) Ltd. (formerly Pearson Institute of Higher Education) is registered with the Department of Higher Education and Training as a private higher education institution under the Higher Education Act, 101, of 1997. Registration Certificate number: 2001/HE07/008

QUESTION 1

1.1

A LAN (Local Area Network) connects computers and devices within a small area like an office or building. It uses Ethernet cables and provides high speeds, usually between 100 Mbps and 10 Gbps. All devices on a LAN share the same IP subnet and communicate directly without external providers.

A WAN (Wide Area Network) covers large distances such as cities or countries. It connects multiple LANs using leased lines or fibre links. WANs operate at slower speeds than LANs and are more expensive to maintain because they require telecommunications service providers.

A WLAN (Wireless Local Area Network) is a wireless version of a LAN, connecting devices through WiFi access points instead of cables. It provides mobility but is limited by signal range and interference from walls and obstacles.

A MAN (Metropolitan Area Network) links several LANs across a city or campus. It covers a larger area than a LAN but is smaller than a WAN. MANs use high-speed fibre connections and are managed by telecommunications providers or municipalities.

As a junior network engineer for a small business with about 25 employees working in one building, I believe a LAN with WLAN support is best. The LAN ensures stable wired connections for desktops and servers, while the WLAN provides mobility for laptops and smartphones. This combination is fast, reliable, and cost-effective. The company does not need a WAN because there are no branch offices in other cities that require connection. A MAN is also unnecessary because all operations happen in one building rather than across multiple locations in a city. A hybrid LAN with WLAN setup provides the right balance of performance and flexibility for this startup.

1.2 Networking Standards and Protocols

Networking standards are rules that define how devices communicate across networks, ensuring that devices from different manufacturers can work together effectively. Without standards, devices from different vendors couldn't communicate, so the standards improve compatibility, reliability, and simplify network maintenance. They define how data should be formatted, transmitted, received, and acknowledged between devices. Organizations like the Institute of Electrical and Electronics Engineers (IEEE) and the Internet Engineering Task Force (IETF) develop and maintain these standards.

TCP (Transmission Control Protocol) ensures reliable data transfer between applications. It establishes a connection through a three-way handshake before transmitting data. TCP checks for errors, maintains packet order, and resends lost data automatically if acknowledgment is not received. It is used in applications where reliability is critical, such as email, web browsing, and file transfers.

HTTP (Hypertext Transfer Protocol) allows communication between web browsers and servers. When I type a website address into my browser, it sends an HTTP request to the web server, which then processes the request and sends back the requested webpage. HTTP uses port 80 and transmits data in plain text. For secure communication, websites use HTTPS, which adds encryption using SSL or TLS protocols and operates on port 443 to protect sensitive information like passwords and credit card details during transmission.

1.3 Networking Devices

A router connects different networks and directs data packets to their destinations. It operates at Layer 3 of the OSI model and makes forwarding decisions based on IP addresses. Routers examine the destination IP addresses in packets and use routing tables to determine the best path. The router acts as a gateway between the local network and the internet. Routers also perform Network Address Translation (NAT) so multiple devices can share one public IP address, which conserves IP addresses and provides basic security.

A switch connects devices within the same network. It works at Layer 2 of the OSI model and uses MAC addresses to forward data. When a device sends data through the switch, the switch examines the destination MAC address in the frame and forwards it only to the correct port. This is more efficient than hubs, which broadcast data to all ports. Switches reduce unnecessary network traffic and improve overall efficiency.

A firewall protects the network by filtering incoming and outgoing traffic based on security rules. It can be hardware or software and sits between the internal network and external networks like the internet. The firewall examines all traffic and blocks anything that violates configured security policies. It can filter traffic based on IP addresses, port numbers, and protocols. Firewalls use packet inspection to analyze traffic and determine whether to allow or deny it, protecting networks from unauthorized access, cyberattacks, and malicious activity.

A wireless access point (WAP) connects wireless devices to a wired network. It connects to a router or switch via an Ethernet cable and broadcasts WiFi signals that wireless devices can connect to. Access points allow laptops, smartphones, and tablets to join the network without physical cables. They transmit radio signals using WiFi standards within a limited range. Multiple access points can be installed to extend network coverage in large areas or buildings. The access point does not perform routing functions; it simply provides a wireless entry point to the existing network.

1.4 Network Security Threats

Malware is harmful software that can damage systems, steal information, or disrupt operations. Common types include viruses, worms, ransomware, and spyware. Viruses attach to files and spread when users open infected files. Ransomware encrypts files and demands payment for decryption. Networks can be protected by installing antivirus software on all devices to detect and remove malicious programs before they cause damage. Regular system updates close security vulnerabilities that malware exploits to gain access. Employee training helps users recognize suspicious emails, downloads, and websites that might contain malware. Email filtering helps block malicious attachments before they reach users.

A DDoS (Distributed Denial of Service) attack floods a server or network with massive traffic from multiple sources until it crashes. Attackers use botnets, which are networks of infected devices, to send overwhelming amounts of requests. This causes legitimate users to be unable to access services because the system is too busy processing fake traffic. Such attacks can be prevented by using web application firewalls that filter malicious traffic before it reaches servers. Rate limiting restricts the number of requests a server accepts within a time window to prevent overload. Content delivery networks distribute traffic across multiple servers to absorb large attacks. Organizations can also use specialized DDoS protection services from security providers that detect and block attack traffic in real-time.

Phishing tricks users into revealing personal information through fake emails or websites. Attackers disguise themselves as legitimate contacts like banks, vendors, or coworkers to gain trust. The messages contain links to fake websites that steal login credentials and personal data. This can be reduced through security awareness training that teaches employees to recognize phishing attempts by checking sender addresses and verifying unexpected requests. Organizations should use email filtering software to block suspicious messages before they reach users. Implementing multi-factor authentication adds extra protection so that even if attackers steal passwords, they cannot access accounts without the second authentication factor, such as a code from a mobile app.

1.5 Network Optimization Technologies

Load balancing distributes network traffic evenly across multiple servers or network links. When traffic arrives, the load balancer examines current server loads and directs new requests to the server with the most available capacity. This prevents any single server from becoming overloaded while others sit idle, improving response times, increasing overall performance, and ensuring reliability. If one server fails during operation, the load balancer automatically redirects traffic to functioning servers and maintains service availability without disruption.

Quality of Service (QoS) manages network traffic by giving priority to important applications based on their requirements. It ensures critical applications receive the bandwidth they need for optimal performance, even during network congestion. Network administrators configure QoS policies that assign priority levels to different types of traffic. QoS uses traffic shaping to regulate data flow and prevent bandwidth-hungry applications from consuming all available network resources.

References

Cisco (2024) Load Balancing. Available at:

https://video.cisco.com/detail/video/6363992667112?dtid=osscdc000283&linkclickid=srch (Accessed: 4 November 2025).

Fortinet (2024) What is a DDoS Attack? Available at: https://www.fortinet.com/resources/cyberglossary/ddos-attack (Accessed: 4 November 2025).

Kaspersky (2024) What is Malware? Available at: https://www.kaspersky.com/resource-center/threats/malware (Accessed: 4 November 2025).

Pengelly, J. (2022) The Official CompTIA Network+ Student Guide (Exam N10-008). 1st ed. CompTIA Learning.

QUESTION 2

2.1

Signal theory explains how information moves through networks using electrical or electromagnetic waves.

Analog signals use continuous variations to represent data. They can take any value within a range and change smoothly over time. Digital signals work differently; they use discrete values, usually 0s and 1s. Digital signals represent data with specific levels at set intervals rather than a continuous flow.

Modern computer networks rely on digital signals because they handle noise better and computers can process them more easily. Digital signals are less affected by interference, which makes them more reliable for data transmission. Analog signals are more prone to noise and distortion during transmission.

Bandwidth is the range of frequencies a signal can use, and it determines how much data can be transmitted in a given time. Bandwidth is measured in bits per second (bps), megabits per second (Mbps), or gigabits per second (Gbps). Higher bandwidth means more data can travel simultaneously through the connection.

Noise is unwanted disturbance that affects the signal quality. It comes from thermal sources, crosstalk from nearby cables, or electromagnetic interference from other devices. Noise causes transmission errors and reduces clarity. Digital signals handle noise better with error correction techniques that can detect and fix transmission problems.

2.2 Transmission Media

Copper cables transmit data using electrical signals through metal wires. They are inexpensive and easy to install in most environments. Common types include twisted-pair cables and coaxial cables. They are good for short distances but are subject to electromagnetic interference from nearby electrical devices. Copper suits small office networks where cost matters more than maximum performance.

Fiber optic cables use light for data transmission through glass or plastic fibers. They offer high bandwidth and very low signal loss over long distances. Fiber is also immune to electromagnetic interference, which makes it perfect for high-noise environments. The main drawbacks are that fiber is more expensive to purchase and install compared to copper. I use fiber for networks that connect buildings or data centers.

Wireless transmission media use radio waves to send data through the air. Being wireless provides flexibility and mobility because physical cables are not needed. However, wireless has limited bandwidth compared to wired connections because signals are affected by physical obstacles like walls and interference from other wireless devices. Wireless suits mobile users who need flexibility and convenience.

2.3 IPv4 and IPv6 Addressing

IPv4 addressing uses a 32-bit address written in four decimal numbers separated by dots, such as 192.168.1.1. Each number ranges from 0 to 255. This system has a limited address space, providing about 4 billion addresses. The address is split into network and host portions using subnet masks. A subnet mask tells the computer which part identifies the network and which part identifies individual devices. Private IP ranges exist for internal networks that do not need direct internet access.

Because available IPv4 addresses became limited, IPv6 was introduced. IPv6 uses a 128-bit address written in eight groups of four hexadecimal digits separated by colons, such as 2001:0db8:85a3:0000:0000:8a2e:0370:7334. Addresses can be shortened by removing leading zeros and replacing consecutive zero groups with double colons to form: 2001:db8:85a3::8a2e:370:7334. IPv6 provides a much larger address space to support many more devices than IPv4. This expansion ensures enough addresses for the growing number of internet-connected devices and improves security and efficiency with built-in support for authentication and encryption.

2.4 Domain Name System (DNS)

Networks are assigned names using the Domain Name System (DNS). DNS translates human-readable domain names to IP addresses for easier access. This converts names into the numerical IP addresses that computers actually use for communication. Each domain name must be unique and follow rules set by the Internet Corporation for Assigned Names and Numbers (ICANN). The DNS system works as a hierarchical database with root servers at the top, followed by top-level domain servers, and then authoritative name servers for specific domains.

2.5 The OSI Model

The OSI Model describes how data travels from one computer to another across a network. Data starts at the Application layer where user data is created, and it passes through layers: Presentation, Session, Transport, Network, Data Link, and Physical. Each layer adds headers or changes the data format to prepare for transmission.

Application Layer: Provides network services directly to users, which includes email, web browsing, and file transfer applications.

Presentation Layer: Formats and encrypts data for compatibility between different systems and handles data compression and translation.

Session Layer: Manages and maintains connections between devices. It establishes, controls, and terminates communication sessions.

Transport Layer: Ensures reliable delivery using protocols like TCP. It breaks data into segments and adds port numbers to identify specific applications.

Network Layer: Assigns logical IP addresses and routes packets to their destination. Routers work at this layer to determine the best path across networks.

Data Link Layer: Packages bits into frames and handles error detection. It uses MAC addresses to identify devices on the local network, and switches operate at this layer.

Physical Layer: Transmits raw bits through cables, fiber optics, or radio waves. Data is sent as electrical, light, or radio signals over the medium.

When I send data, the message starts at the Application Layer and moves down through each layer, with each adding its own header information in a process called encapsulation. When the receiving computer gets the data, it reverses the process up the layers, processing it in reverse order from Physical to Application. Each layer strips off its header and passes the data up until the Application reads the original message

References

GeeksforGeeks (n.d.) Analog vs Digital Signals. Available at: https://www.geeksforgeeks.org/difference-between-analog-and-digital-signal/ (Accessed: 5 November 2025).

Pengelly, J. (2022) The Official CompTIA Network+ Student Guide (Exam N10-008). 1st edn. CompTIA.

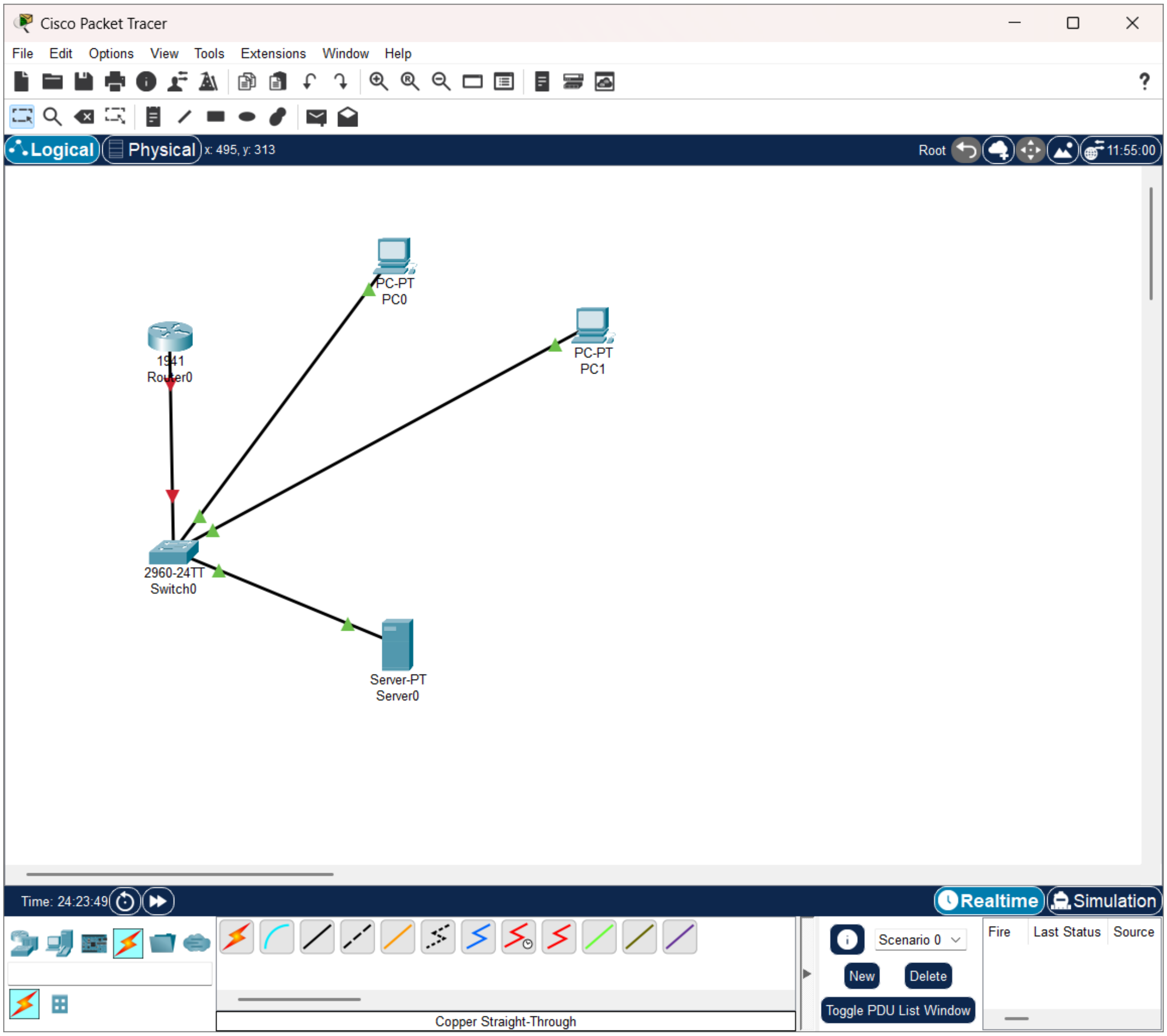
Wikipedia (n.d.) IPv4. Available at: https://en.wikipedia.org/wiki/IPv4 (Accessed: 5 November 2025).

Wikipedia (n.d.) IPv6. Available at: https://en.wikipedia.org/wiki/IPv6 (Accessed: 5 November 2025).

QUESTION 3

3.1

I am implementing a Network Topology for the company where in this workspace I used one switch to connect all my network endpoints which then connects directly to my router, which provides access to the external Internet.



3.2

I am using the 192.168.1.0/24 network

Device	IP Address	Type	Purpose

Router (default gateway)	192.168.1.1	static	Gateway for the entire local network
Server	192.168.1.10	static	Hosts DNS and DHCP
DHCP pool start	192,168.1.100	DHCP dynamic	Range start for all employee PC clients

3.3

Built the network by placing the devices and cabling them like this

1 1941 Router

1 2960 Switch

1 Server

2 PC endpoints

Copper straight-through

Router GigabitEthernet0/0 to Switch GigabitEthernet0/1

Server FastEthernet0 to Switch FastEthernet0/1

PC0 FastEthernet0 to Switch FastEthernet0/2

PC1 FastEthernet0 to Switch FastEthernet0/3

3.4 a

Below are the Router CLI Commands

```
enable

configure terminal
```

```
interface GigabitEthernet0/0

ip address 192.168.1.1 255.255.255.0

no shutdown

exit 2 times

copy running-config startup-config
```

b

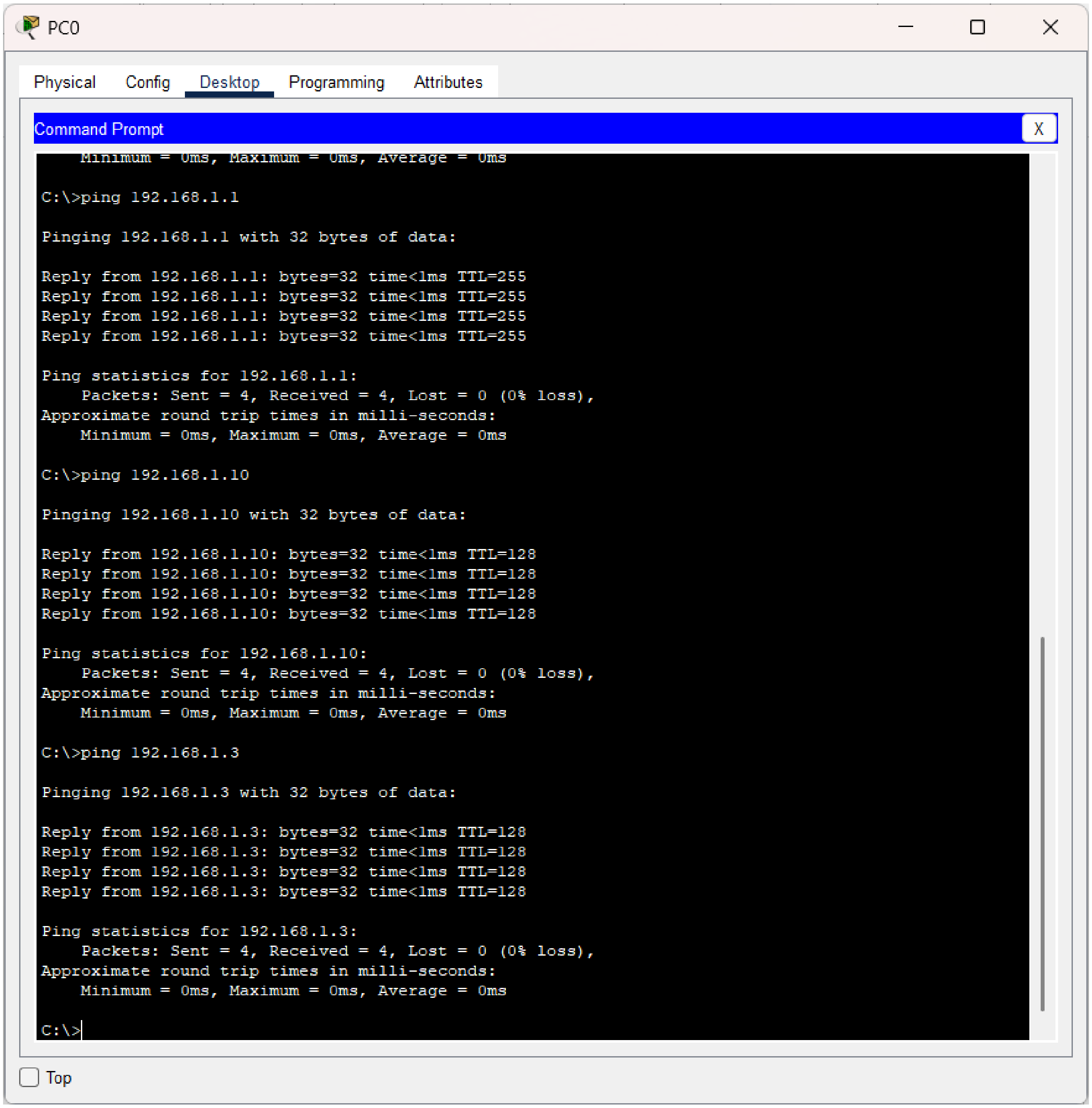
then for the server configuration

Static IP 192.168.1.10, Gateway 192.168.1.1 and DNS 192.168.1.10

DHCP service on Gateway 192.168.1.1, DNS 192.168.1.10 and Start IP 192.168.1.100

DNS service on server.company,local points to 192.168.1.10

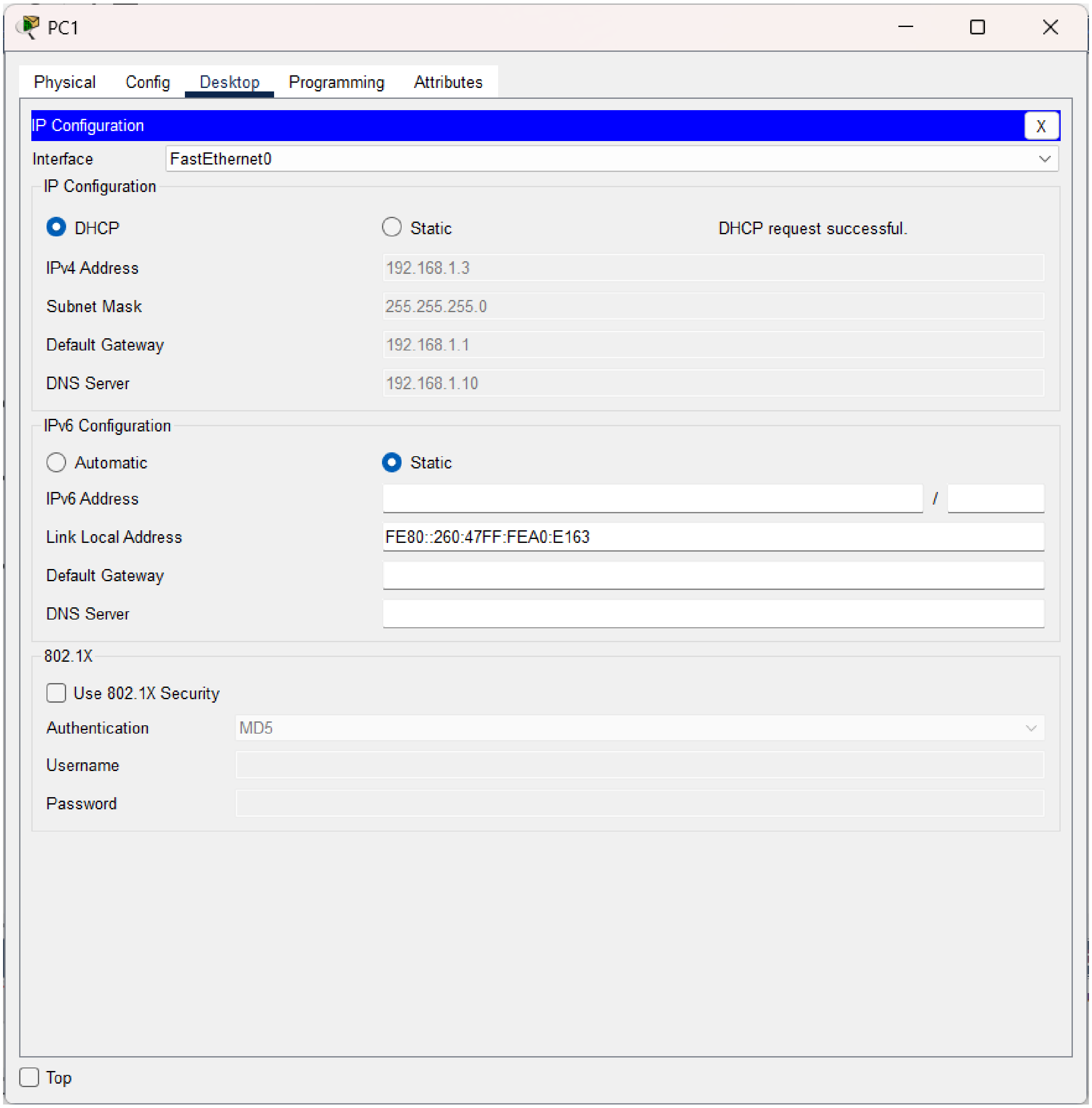
3.5



```
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

3.6

DHCP



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static DHCP request successful.

IPv4 Address	192.168.1.3
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	192.168.1.10

IPv6 Configuration

○ Automatic ● Static

IPv6 Address	/
Link Local Address	FE80::260:47FF:FEA0:E163
Default Gateway	
DNS Server	

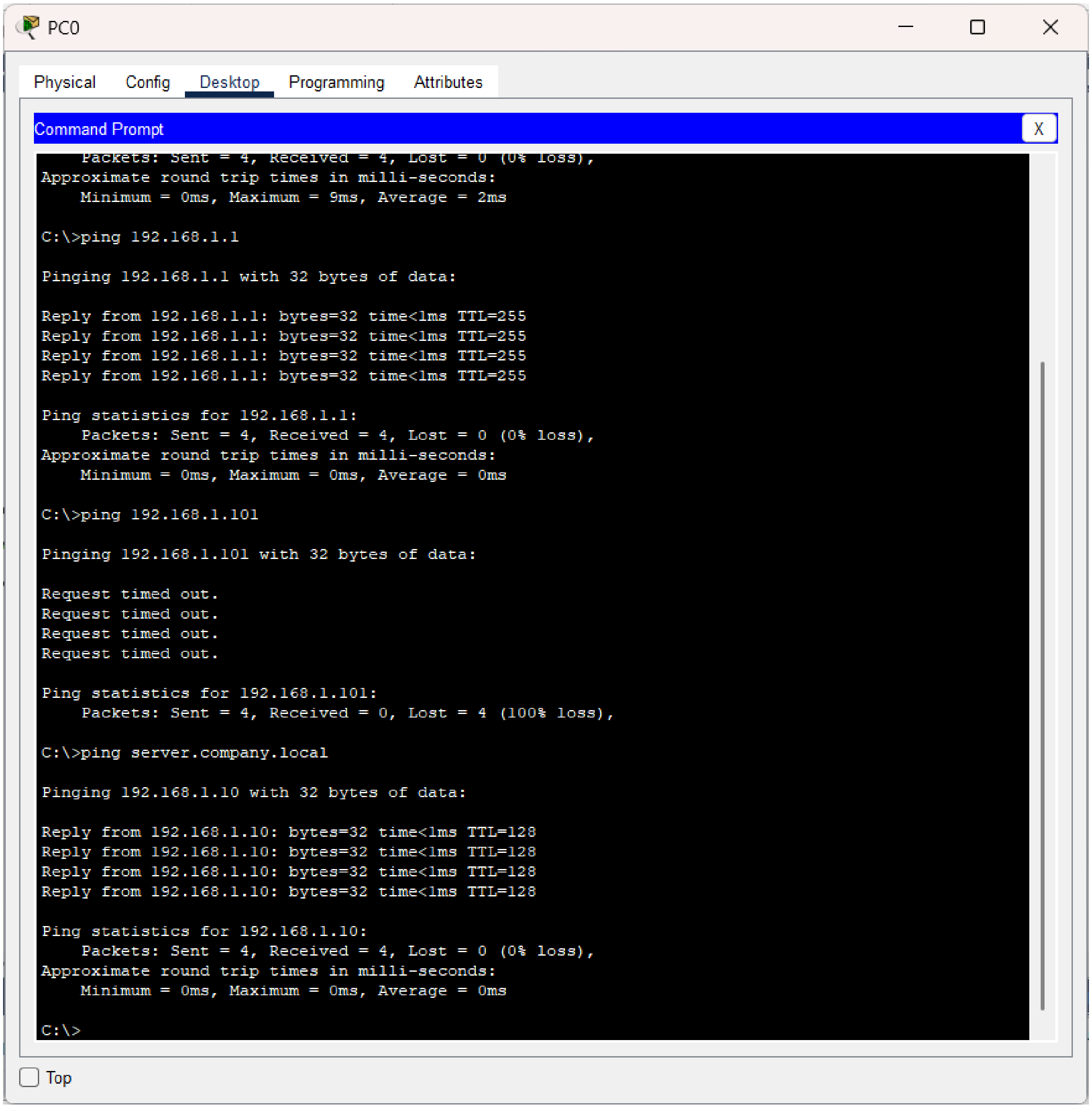
802.1X

□ Use 802.1X Security

Authentication	MD5
Username	
Password	

□ Top

DNS



```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 9ms, Average = 2ms

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.101

Pinging 192.168.1.101 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.101:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping server.company.local

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Refences

Pengelly, J. (2021) The Official CompTIA Network + Student Guide (Exam N10-008). 1st ed. CompTIA.