# Here is the AI planned result

Course name: NETW 1027: Introduction to Networking and Security

Course outcomes:

1. Investigate elements of local area networks to support client connectivity.

2. Build a small office/home office (SOHO) local area network to support wired and wireless client connectivity.

3. Investigate elements of physical network infrastructure to support wired and wireless client connectivity.

4. Identify current security requirements to support IT operations by analyzing current threats and mitigation strategies.

Objective analysis:

Objective 1: Given an IPv4 address and mask, identify host and network using CIRD notation.

Pros: Helps learners understand how IP addressing works and how to identify hosts and networks.

Cons: Limited to IPv4 addressing, does not cover IPv6.

Objective 2: Identify common network topologies. e.g. LAN v WAN.

Pros: Provides foundational knowledge of different network topologies.

Cons: May be too basic for some learners who already have knowledge in this area.

Objective 3: Explain and give examples of common network services, such as DHCP, DNS, and Gateway.

Pros: Essential knowledge for understanding how networks function and connect to the internet.

Cons: Could benefit from more in-depth coverage of each service.

Objective 4: Identify common special-purpose IP addresses and ranges. e.g. loopback, APIPA, private IP ranges.

Pros: Ensures learners understand the different types of IP addresses and their uses.

Cons: May be too technical for beginners or those without prior networking knowledge.

Objective 5: Identify IPv6 addressing as it applies to a small local area network.

Pros: Introduces learners to IPv6 addressing, which is becoming more prevalent in networks.

Cons: May require additional resources or exercises to fully understand IPv6.

Objective 6: Identify standard network ports and associated services. (80: HTTP, 443: HTTPS, 22: SSH).

Pros: Important for understanding how different services communicate over networks.

Cons: May require further explanation or examples for learners to fully grasp the concepts.

Objective 7: Identify data packets and how they traverse a local area network using source and destination IP addressing.

Pros: Helps learners understand how data is transmitted over networks.

Cons: May be too technical for some learners, requiring additional explanations or examples.

Objective 8: Use common network utilities to test connectivity. e.g. ping, tracert, netsh nslookup.

Pros: Practical skills for troubleshooting network connectivity issues.

Cons: May require hands-on practice or access to network infrastructure for learners to fully benefit.

Objective 9: Create and interpret network diagrams. (e.g. paper, draw.io).

Pros: Essential skill for designing and documenting network architectures.

Cons: May require additional software or tools for learners to practice creating diagrams.

Objective 10: Implement a consumer-grade device to support wireless and/or wired client connectivity.

Pros: Hands-on experience with real-world networking equipment.

Cons: May require access to physical devices for learners to practice implementation.

Objective 11: Configure a SOHO local area network using Network Address Translation (NAT) and DHCP.

Pros: Practical skills for setting up and managing networks in small office/home office environments.

Cons: May require additional explanations or examples to fully understand NAT and DHCP.

Objective 12: Identify basic firewall settings on a consumer-grade device (port filtering, DMZ, port forwarding).

Pros: Introduces learners to basic firewall concepts and configurations.

Cons: May require further explanations or examples for learners to fully grasp the concepts.

Objective 13: Describe the components required for network and Internet communications.

Pros: Provides foundational knowledge of network infrastructure components.

Cons: May be too basic for learners with prior networking experience.

Objective 14: Explain the characteristics and benefits of the various network media (copper, fiber and wireless).

Pros: Helps learners understand the different types of network media and their advantages.

Cons: Could benefit from additional examples or real-world scenarios to illustrate the characteristics and benefits.

Objective 15: Trace wired and wireless network connectivity on a local area network from a client device to a network switch and/or consumer-grade device.

Pros: Practical skills for troubleshooting network connectivity issues.

Cons: May require hands-on practice or access to network infrastructure for learners to fully benefit.

Objective 16: Test network cabling using a certified network data tester with Time Domain Reflectometer (TDR).

Pros: Practical skills for testing and certifying network cables.

Cons: May require access to specialized equipment for learners to practice testing network cables.

Objective 17: Identify common WLAN elements to support connectivity. e.g. SSID, Encryption, Captive Portals.

Pros: Introduces learners to essential components of wireless networks.

Cons: May benefit from additional coverage of advanced WLAN features or security measures.

Objective 18: Explore global IT security threats.

Pros: Raises awareness of current security threats in the IT industry.

Cons: May require updates to ensure relevance to the latest security threats.

Objective 19: Identify common security vulnerabilities in SOHO wired and wireless networks.

Pros: Helps learners understand potential security risks in small office/home office networks.

Cons: May require more comprehensive coverage to address the ever-evolving nature of security vulnerabilities.

Objective 20: Identify elements of a secure browser-based connection to a web server or web application. e.g. SSL, Certificate types/Issuers request/response.

Pros: Introduces important concepts related to securing web connections.

Cons: May require additional explanation or examples for learners to fully grasp the concepts.

Objective 21: Explore encryption as a mitigation strategy against network attacks.

Pros: Highlights the importance of encryption in protecting network data.

Cons: May require additional coverage of different encryption algorithms and protocols.

Objective 22: Identify current practices for identity management on client devices. e.g. password complexity, MFA, passwordless authentication, hardware authentication, device-based authorization.

Pros: Provides an overview of different identity management practices and technologies.

Cons: May benefit from additional examples or case studies to illustrate the effectiveness of different practices.

Objective 23: Configure client firewall rules to mitigate vulnerabilities, using specific ports, protocols, and source/destination.

Pros: Practical skills for securing client devices through firewall configuration.

Cons: May require hands-on practice or simulations for learners to fully understand the concepts.

Objective 24: Identify strategies for establishing secure connections to remote hosts or networks - e.g. VPN, SSH.

Pros: Introduces different technologies for secure remote access to networks.

Cons: Could benefit from additional coverage of other secure connection methods (e.g., RDP, SSL/TLS).

Based on the objectives and analysis, an optimal instructional program for NETW 1027: Introduction to Networking and Security could include a combination of lectures, hands-on practical exercises, case studies, and assessments. The program should provide a balance between theoretical knowledge and practical skills. It should incorporate real-world examples and scenarios to help learners connect the concepts to practical applications. Access to network equipment and software tools, such as network simulators or virtual labs, would enhance the learning experience. Additionally, regular assessments and feedback would allow learners to gauge their progress and identify areas for improvement throughout the course.