

PERFORM COMPUTER NETWORKING

TVET CDACC UNIT CODE: SEC/OS/CS/CR/03/5/MA

UNIT DESCRIPTION

This unit covers the competencies required to perform computer networking activities. It involves identifying network types, configuring network devices, connecting network devices, monitoring network performance, documenting network report, training network users and maintaining of the network.

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT	PERFORMANCE CRITERIA
These describe the key outcomes which make up workplace function.	These are assessable statements which specify the required level of performance for each of the elements. <i>(Bold and italicised terms are elaborated in the Range)</i>
1. Identify network type	1.1. Site survey is conducted to determine the user needs and establish network topology 1.2. Network design is developed according to the site survey 1.3. Network components (cables, devices, media & software) are identified based on the site survey 1.4. Network type (LAN, MAN, WAN, WLAN, PAN) is identified as per the client's requirements and organizational needs.
2. Features and Functions of Computer networks	2.1 Functions of networks are explained in line with organization needs 2.2 Network devices (Switches, routers, access points and firewalls) are identified and their roles in supporting network functions 2.3 Common protocols are recognised and their importance in enabling communication is outlined. 2.4 Advantages and limitations of networks (cost, efficiency, reliability, security risks) are analysed

	with relevant examples. 2.5 Real live applications of network in business, education and personal communication are illustrated through case studies or scenario
3. Network Protocols and Standards	3.1 Importance of network standards (IEEE, ISO, IETF, ITU, ANSI) is explained in ensuring compatibility and interoperability. 3.2 Differences between proprietary and open standards are outlined with relevant examples. 3.3 Protocol layers in OSI and TCP/IP models are explained in relation to data communication. 3.4 Appropriate protocols are matched to given networking scenarios or client requirements. 3.5 Compliance of networking standards is recognised as essential for reliability, scalability and security
4. Configure Network devices	4.1 Network devices are identified and prepared for configuration according to vendor specifications. 4.2 IP addressing schemes are applied correctly to network devices. 4.3 Routing protocols and switching configurations are implemented according to network requirements. 4.4 Security settings (passwords, access control lists, encryption, firewall rules) are configured to protect devices and data. 4.5 Device configurations are tested to ensure connectivity, performance and compliance with device specifications. 4.6 Configuration files are documented and backed up according to organization policies.
5. Maintain Network	5.1 Network performance is monitored regularly using appropriate tools and utilities . 5.2 Network faults are identified through systematic troubleshooting techniques

	5.3 Corrective actions (hardware replacement, configuration adjustments, maintenance logs) is updated to reflect changes and maintenance activities. 5.4 Preventive maintenance tasks (updates, patches, backups and hardware checks) are carried out according to organization policies. 5.5 User support is provided to resolve connectivity, access and performance issues promptly. 5.6 Security measures are reviewed to maintain network protection.
6. Document network report	6.1 Network design, configuration and maintenance activity are documented clearly and accurately. 6.2 Standard documentation and organizational templates are followed. 6.3 Network diagrams (Topology maps, device configurations, addressing schemes) are prepared and updated as required. 6.4 Test results and performance data are recorded to verify network functionality. 6.5 Network documentation is reviewed and updated regularly to reflect changes infrastructure and usage. 6.6 Documentation is stored, shared and maintained to organization procedures and security policies.

RANGE

This section provides work environment and conditions to which the performance criteria apply. It allows for different work environment and situations that will affect performance.

Variable	Range
----------	-------

Network topology may include but not limited to:	• Star • Ring • Mesh • Hybrid • Point to point
Network components may include but not limited to:	• Routers • Switches • Hub • RJ 45 connectors • Ports • Computers • Printers
Network types may include but not limited to:	• WAN • LAN • PAN • WLAN
Network protocols may include but not limited to:	• OSI • TCP/IP
Network Standards	• IEEE 802.3 • IEEE 802.11 • IEEE 802.15. • IEEE 802.16:
IP addressing scheme	• IPv4 • IPv6
designing a Local Area Network	• Logical topology • Physical topology
Types of Network Maintenance	• Preventive • Corrective • Adaptive
Monitoring tools may include but not limited to:	• Wireshark • PRTG • NetFlow

	• SNMP • Syslog
--	--

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

- Network Architecture
- Network programming languages
- Network Components and devices
- Network types
- Network security Measures
- Network Monitoring procedures
- Network testing techniques
- Network configuration techniques
- Network protocols
- Network security techniques and procedures
- Network testing procedures

FOUNDATION SKILLS

The individual needs to demonstrate the following foundation skills:

- Communications (verbal and written);
- Proficient in digital literacy
- Problem solving
- Decision Making
- Leadership
- Self-training

EVIDENCE GUIDE

This provides advice on assessment and must be read in conjunction with the performance criteria, required knowledge and understanding and range.

1. Critical Aspects of Competency	Assessment requires evidence that the candidate: 1.1 Network design is developed according to the site survey 1.2 Network components are identified according to the site survey
-----------------------------------	---

	1.3 Network type is identified as per the client's requirements 1.4 Identified of the transmission media is done according to network types 1.5 Network topologies are established based on the computer network needs. 1.6 Network connection is performed according to Network standards 1.7 IP addressing scheme configuration is performed 1.8 Basic Troubleshooting is done according to network issue 1.9 Types of Network Maintenance are identified 1.10 Network monitoring tools are identified as per the type of tests to be carried out 1.11 Network scalability survey is done 1.12 Key Components of a Network Report are established.
2. Resource Implications for competent certification	The following resources should be provided: 2.1 Access to relevant workplace where assessment can take place 2.2 Appropriately simulated environment where assessment can take place 2.3 Materials relevant to the proposed activity or tasks
3. Methods of Assessment	Competency may be assessed through: 3.1 Observation 3.2 Oral questioning 3.3 Practical demonstration
4. Context of Assessment	Competency may be assessed individually in the actual workplace and simulated setting of the actual work place
5. Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.