

Variable	Range
	secondary storage (Solid state devices, Hard Drives, CDs & DVDs, Memory cards, Flash drives • Computer Ports e.g. HDMI, DVI, VGA, USB type C etc.
Computer software may include but are not limited to:	• System software e.g. Operating System (Windows, Macintosh, Linux, Android, iOS) • Application Software e.g. Word Processors, Spreadsheets, Presentations etc. • Utility Software e.g. Antivirus programs
External devices may include but are not limited to:	• Printers • Projectors • Smart Boards • Speakers • External storage drives • Digital/Smart TVs

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

- Hardware and software tools
- Troubleshooting techniques
- Safety standards and reporting procedures
- System audit procedures

FOUNDATION SKILLS

The individual needs to demonstrate the following foundation skills:

- Communications (verbal and written);
- Time management;
- Problem solving;
- Planning;
- Decision making;
- Report writing;

EVIDENCE GUIDE

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

6. Critical Aspects of Competency	Assessment requires evidence that the candidate: 6.1 Diagnosed and operated software and hardware in line with the standard operating procedure 6.2 Dismantled components in line with the manufacture's manuals 6.3 Tested components functionality as per the manufacturer's manuals 6.4 Tested repaired/replaced components functionality according to standard operating procedure 6.5 Monitoring reassembled components as per the industries best practice 6.6 Test environment was developed for hardware and software as per industry best practices 6.7 Prepared maintenance report in line with organizations approved format 6.8 Tested upgraded computer hardware and software were tested in line with the organization policy 6.9 Security threats were identified and classified as per the organization ICT policy 6.10 Security control measures were identified and categorized
7. 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
8. Methods of Assessment	Competency may be assessed through: 8.1 Observation 8.2 Oral questioning 8.3 Practical test in conducting test

	8.4 Demonstration of interpretation of test results
9. Context of Assessment	Competency may be assessed individually 9.1 In the actual workplace 9.2 Simulated environment of the work place
10. Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.

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 These describe the key outcomes which make up workplace function.	PERFORMANCE CRITERIA 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.