



Australian Government

Department of Education, Employment and Workplace Relations

ICASAS307A Install, configure and secure a small office home office network

Release: 1

ICASAS307A Install, configure and secure a small office home office network

Modification History

Release	Comments
Release 1	This Unit first released with <i>ICA11 Information and Communications Technology Training Package version 1.0</i>

Unit Descriptor

This unit describes the performance outcomes, skills and knowledge required to identify available network components relevant to client requirements and to install, configure and secure those components as part of a small office or home office (SOHO) network.

Application of the Unit

This unit applies to individuals required to network a small or home office. The unit covers the development of a suitable network design, the identification of relevant network components to meet the design brief and the installation, configuration and securing of the network to meet client requirements.

Licensing/Regulatory Information

No licensing, legislative, regulatory or certification requirements apply to this unit at the time of endorsement but users should confirm requirements with the relevant federal, state or territory authority.

Pre-Requisites

Not applicable.

Employability Skills Information

This unit contains employability skills.

Elements and Performance Criteria Pre-Content

Element	Performance Criteria
<i>Elements describe the essential outcomes of a unit of competency.</i>	<i>Performance criteria describe the performance needed to demonstrate achievement of the element. Where bold italicised text is used, further information is detailed in the required skills and knowledge section and the range statement. Assessment of performance is to be consistent with the evidence guide.</i>

Elements and Performance Criteria

1. Confirm client requirements and identify relevant network equipment	1.1 Identify and clarify the client requirement for the small office home office network 1.2 Identify the most suitable network design to meet the client requirement 1.3 Develop and document the network design 1.4 Identify the most suitable network technologies, devices and protocols and network cables and connectors to meet the network design 1.5 Review the available network technologies, devices and protocols and determine the most appropriate to meet the client requirements 1.6 Source vendors and service suppliers to obtain specifications, availability and cost of identified components 1.7 Ensure client sign-off for proposed network design and associated components
2. Install and configure hardware and software	2.1 Develop installation plans, with prioritised tasks and contingency arrangements, for installation of components with minimum disruption to client 2.2 Liaise with appropriate person to obtain approval for the plans, including security clearance and timing 2.3 Confirm and review supplier documentation that network cables and connectors have been installed according to industry standards, client requirements and building requirements 2.4 Install and configure computer and other hardware according to the network design and industry standards using knowledge of relevant installation and configuration tools 2.5 Install and configure network software according to network design and industry standards 2.6 Install and configure other software according to network design and industry standards
3. Configure and test network	3.1 Troubleshoot client-side connectivity using appropriate networking settings to review relevant network tools 3.2 Test the installed software and hardware, using available networking tools to ensure that components are functioning as expected 3.3 Test the network settings to ensure the network is functioning according to specification 3.4 Resolve problems identified through the testing process

4. Secure network	4.1 Identify possible <i>security concepts and technologies</i> relevant to securing the network 4.2 Apply specific protection using identified <i>security features</i> to protect against possible network attacks 4.3 Troubleshoot different types of <i>security intrusion symptoms and issues</i>
5. Document completed work, hand over to client and obtain client approval	5.1 Document final network design and associated hardware, software and security features 5.2 Document installation, bootup and configuration procedures as per client requirements 5.3 Complete handover and secure sign-off from client

Required Skills and Knowledge

This section describes the skills and knowledge required for this unit.

Required skills

- analytical skills to evaluate hardware, software and network specifications against client requirements
- communication skills to deal with clients and vendors
- literacy skills to:
 - review technical documentation
 - write detailed technical notes
- planning and organisational skills to:
 - set benchmarks and identify scope
 - develop plans, prioritise tasks and apply contingency strategy
- problem-solving skills to predict the range of network problems
- research skills to identify, analyse and evaluate technical information
- technical skills to:
 - identify and install components of hardware, software, cabling and wireless equipment
 - use network system software.

Required knowledge

- current industry-accepted hardware and software products
- current industry-accepted network hardware and software products
- data and voice transmission technologies and protocols
- hardware and software installation procedures
- local area network (LAN) capabilities and characteristics, including network type, such as ethernet, Appletalk IP addressing, switch or hub operation
- network connections, both wired and wireless
- networking technologies, incorporating substantial depth in areas relating to network operating systems and cabling standards
- operating system, such as Mac, Linux, Novell, Windows, to enable basic installation
- set-up and configuration procedures
- small business and home office networking requirements
- software packages supported by the organisation.

Evidence Guide

The evidence guide provides advice on assessment and must be read in conjunction with the performance criteria, required skills and knowledge, range statement and the Assessment Guidelines for the Training Package.

Overview of assessment	
Critical aspects for assessment and evidence required to demonstrate competency in this unit	Evidence of the ability to: • identify the most relevant network hardware and software equipment to meet client requirements • install, configure and test the network according to client requirements, and produce appropriate documentation • identify possible security threats and secure the network.
Context of and specific resources for assessment	Assessment must ensure access to: • current industry standard software, hardware, and networking technologies • server and workstation hardware and software • internet connection • live network • network components, hardware and software • networked computers • technical documentation and installation manuals • vendor hardware and software components • appropriate learning and assessment support when required • modified equipment for people with special needs.
Method of assessment	A range of assessment methods should be used to assess practical skills and knowledge. The following examples are appropriate for this unit: • verbal or written questioning to assess candidate's knowledge of: • current industry-accepted network hardware and software products • hardware and software installation procedures • direct observation of candidate: • configuring LAN equipment in a variety of scenarios • troubleshooting security issues • review of candidate's: • documented installation process • documented security settings.
Guidance information	Holistic assessment with other units relevant to the industry sector,

for assessment	workplace and job role is recommended, where appropriate. Assessment processes and techniques must be culturally appropriate, and suitable to the communication skill level, language, literacy and numeracy capacity of the candidate and the work being performed. Indigenous people and other people from a non-English speaking background may need additional support. In cases where practical assessment is used it should be combined with targeted questioning to assess required knowledge.
-----------------------	---

Range Statement

The range statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold italicised wording, if used in the performance criteria, is detailed below. Essential operating conditions that may be present with training and assessment (depending on the work situation, needs of the candidate, accessibility of the item, and local industry and regional contexts) may also be included.

<i>Client requirements</i> may relate to networking a:	• small business • small club • small home office • small network.
<i>Small office home office network</i> may refer to:	• a single or small number of rooms • linking a small number of personal computers (PCs) or laptops and associated peripherals • having or not having a server • sharing peripherals, files and other information • using single type or combination of wired or wireless connections: • category 5 (or similar) cabling • ethernet network hub • ethernet network switch • wi-fi wireless network.
<i>Network design</i> may include:	• Bluetooth • broadband: • cable • digital subscriber line (DSL) • fibre • satellite • cellular • dial-up • wireless: • all 802.11 types • dynamic host configuration protocol (DHCP) settings • MAC filtering • service set identifier (SSID) • wi-fi protected access (WPA) • wired equivalent privacy (WEP).
<i>Networking technologies, devices and protocols</i> may	• bandwidth and latency • basics class identification • basics of configuring IP addressing and transmission control

include:	- protocol or internet protocol (TCP/IP) properties (DHCP, DNS) - basics of workgroups and domains - common ports: - file transfer protocol (FTP) - hypertext transfer protocol (HTTP) - hypertext transfer protocol secure (HTTPS) - post office protocol (POP) - simple mail transfer protocol (SMTP) - Telnet - full-duplex and half-duplex - hub, switch and router - identify virtual private networks (VPN) - internet protocol version 6 (IPv6) versus internet protocol version 4 (IPv4): - address conventions - address length differences - local area network (LAN) or wide area network (WAN) - protocols, such as: - TCP/IP - network basic input/output system (NETBIOS) - status indicators.
Network cables and connectors may include:	- cables: - plenum or polyvinyl chloride (PVC) - shielded twisted-pair (STP) - fibre - coaxial cable - unshielded twisted-pair (UTP), such as CAT3, CAT5, 5e, and CAT6 - connectors: - RJ11 - RJ45.
Appropriate person may include:	- authorised business representative - client - supervisor.
Industry standards may include:	- Australian Standards (AS) - Institute of Electrical and Electronics Engineers (IEEE) - International Electrotechnical Commission (IEC) - International Organization for Standardization (ISO) - International Telecommunications Union (ITU)

	• Internet Engineering Task Force (IETF) • organisational standards • project standards.
Computer may include:	• iPad (or similar) • laptop • notebook • personal digital assistant (PDA) • Mac or PC • server • thin client • workstation.
Installation and configuration tools may include:	• basics of hardware and software firewall configuration: • port assignment or setting up rules (exceptions) • port forwarding or port triggering • connection types: • basic VoIP (consumer applications) • Bluetooth (1.0 versus 2.0) • broadband: • cable • DSL • ISDN • satellite • cellular • dial-up • LAN (10, 100, 1000BaseT, Speeds) • routers or access points: • change default username and password • change SSID from default • disable DHCP • disable SSID broadcast • firewall • MAC filtering • update firmware • use static IP • wireless: • all 802.11 • DHCP settings • MAC filtering • service set identifier (SSID) • wired equivalent privacy (WEP)

	• wi-fi protected access (WPA) • physical installation: • cable length • wireless router placement.
Network settings may include:	• characteristics of TCP/IP: • automatic IP addressing • loopback addresses • firewall settings: • open and closed ports • program filters • FTP settings: • exceptions • IP addresses • ports • programs • mail protocol settings: • internet message access protocol (IMAP) • POP • SMTP • proxy settings: • exceptions • IP addresses • ports • programs • TCP/IP settings: • DHCP (dynamic versus static) • DNS • gateway • NAT (private and public) • subnet mask.
Networking tools may include:	• secure connection protocols: • HTTPS • secure shell (SSH) • tools to use and interpret results: • ipconfig • Net use • Netstat • Nslookup • Ping

	• Telnet • Tracert.
Security concepts and technologies may include:	• authentication technologies: • biometrics • password • smart cards • user name • basics of data sensitivity and data security: • classifications • compliance • social engineering • data wiping or hard drive destruction or hard drive recycling • encryption technologies • software firewall: • exceptions • port security.
Security features may include:	• biometrics: • fingerprint scanner • bios security: • drive lock • intrusion detection • passwords • TPM • locking workstation: • hardware • operating system • malicious software protection: • adware • grayware • spam • spyware • trojans • viruses • worms • password management or password complexity • wireless encryption: • client configuration, such as service set identifier (SSID) • WEPx and WPAx.
Common security	• operating systems:

<i>intrusion symptoms and issues</i> may relate to:	• encryption (Bitlocker, EFS) • local users and groups: administrator, power users, guest, users • new technology file system (NTFS) versus share permissions: • allow versus deny • difference between moving and copying folders and files • file attributes • shared files and folders: • administrative shares versus local shares • inheritance • permission propagation • system files and folders • user authentication • Vista or Windows 7 User Account Control (UAC) • system: • network basic input/output system (BIOS) security: • drive lock • passwords • intrusion detection • TPM • virus and malware tools: • educate end user • identify malware symptoms • quarantine infected systems • remediate infected systems • repair boot blocks • research malware types, symptoms and solutions (virus encyclopaedia) • scan and removal techniques: • boot environment • safe mode • schedule scans • update antivirus software: • automatic versus manual • signature and engine updates • use antivirus software.
---	---

Unit Sector(s)

Systems administration and support