Australian Government

Department of Education, Employment and Workplace Relations

ICTTEN2105A Install and test an internet protocol device in convergence networks

Release: 1

ICTTEN2105A Install and test an internet protocol device in convergence networks

Modification History

Not Applicable

Unit Descriptor

Unit descriptor	This unit describes the performance outcomes, skills and knowledge required to install and test internet protocol (IP) based telecommunications networking using convergent technologies. This entry-level unit introduces IP convergence of the emerging technologies used in telecommunications to deliver services of Next Generation Networks (NGN) by configuring and testing an IP device. NGN services include internet protocol TV (IPTV), IP security, digital home networks, IP based cable access TV (CATV), IP Core and Access Networks, home automation, interactive TV, radio frequency identification (RFID), biometric recognition systems, mesh networks, smart grids and cloud computing. 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.

Application of the Unit

Application of the unit	Technicians and cable installers who install and maintain IP based equipment for customer and service providers apply the skills and knowledge in this unit. They may be up-skilling from traditional legacy telecommunications technologies or cross-skilling from related industries to provide services in NGN using IP technologies.

Licensing/Regulatory Information

Refer to Unit Descriptor

Pre-Requisites

Prerequisite units		

Employability Skills Information

Employability skills	This unit contains employability skills.

Elements and Performance Criteria Pre-Content

Elements describe the essential outcomes of a unit of competency.	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.

Elements and Performance Criteria

ELEMENT	PERFORMANCE CRITERIA
1. Gather information to prepare the installation of an IP device	1.1. Obtain and clarify occupational health and safety (***OHS***) ***requirements*** and ***environmental requirements*** for a given work area with ***appropriate person*** 1.2. Identify safety hazards and notify appropriate personnel 1.3. Obtain identified operating instructions, manuals, hardware and software testing methodologies 1.4. Obtain documentation on a range of ***IP devices*** that can be networked according to the ***open system interconnection*** (***OSI***) ***reference model*** in networking 1.5. Obtain the range of required IP devices to be connected to the ***network*** and identify the ***IP based telecommunications application*** that will be provided
2. Prepare for the installation of an IP device	2.1. Select an IP device for installation that can be integrated into the existing network 2.2. Obtain appropriate ***hardware***, ***software***, ***network protocols***, ***peripheral devices*** and ***media types and connectors*** for configuration process 2.3. Draw the physical topology of the device connection to the network and seek approval from the appropriate person 2.4. Obtain ***configuration details*** to start setting up the device
3. Configure and test the IP device	3.1. Determine ***network addressing scheme*** for mapping network connectivity and verify by ***calculations*** 3.2. Assign a valid static IP address to the device 3.3. Use ***network commands*** to determine and verify the media access control (MAC) address, the IP address and network performance of the device 3.4. Determine ***security threats*** and initiate ***security solutions*** to prevent security breaches according to enterprise procedures
4. Complete and document network installation	4.1. Restore work site to safe condition according to established safety procedures 4.2. Record and store ***essential installation information*** according to enterprise procedures 4.3. Notify appropriate person about the completion of the task according to enterprise procedures

Required Skills and Knowledge

REQUIRED SKILLS AND KNOWLEDGE

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

Required skills

- communication skills to work effectively within a group
- literacy skills to interpret configuration instructions
- numeracy skills to gather and record data from measurements
- technical skills to:
  - configure and test an IP device
  - recognise security threats and offer solutions

Required knowledge

- basic testing and troubleshooting of an IP device
- computer networking
- configuration instructions
- IP addressing
- IP devices
- OHS requirements
- organisational policy and procedures
- personal safety issues
- protocols
- security configurations

Evidence Guide

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: • prepare for the installation of an IP device connected to a network • set up and configure IP device with simple addressing schemes • test and secure the device against security threats • produce essential installation information • follow OHS workplace procedures and practices.
Context of, and specific resources for assessment	Assessment must ensure: • a small network with IP devices • tools, equipment, materials and documentation required for installing and testing IP device • relevant workplace procedures, product and manufacturing specifications, codes, standards, manuals and reference materials.
Methods of assessment	A range of assessment methods should be used to assess practical skills and knowledge. The following examples are appropriate for this unit: • direct observation of the candidate installing and testing IP devices • review of drawings of and records for installation • oral or written questioning to assess knowledge of personal computer systems.
Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended, for example: • ICTTEN2207A Install and configure a home or small office network • ICTTEN2208A Install and configure a small to medium business network. Aboriginal people and other people from a non-English speaking background may have second language issues.

EVIDENCE GUIDE	
	Access must be provided to appropriate learning and assessment support when required. Assessment processes and techniques must be culturally appropriate, and appropriate to the oral communication skill level, and language and literacy capacity of the candidate and the work being performed. In all cases where practical assessment is used it will be combined with targeted questioning to assess required knowledge. Questioning techniques should not require language, literacy and numeracy skills beyond those required in this unit of competency. Where applicable, physical resources should include equipment modified for people with special needs.

Range Statement

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.	
OHS requirements may include:	• awards provisions • hazardous substances and dangerous goods code • legislation • local safe operation procedures • material safety management systems • protective equipment.
Environmental requirements may include:	• dust • excessive energy and water use • excessive noise • fume • gas

RANGE STATEMENT	
	• liquid waste • smoke emissions • solid waste • vapour.

RANGE STATEMENT	
Appropriate person may include:	• customer • network manager • site manager • supervisor.

IP devices may include:	• asymmetric digital subscriber line (ADSL) router
	• biometric device:
	  • face recognition
	  • fingerprint scanner
	  • iris recognition scanner
	  • voice recognition
	• computer network:
	  • data switch
	  • gateway
	  • hub
	  • router
	  • server
	  • wireless access point (AP)
	• IP CCTV unit or camera
	• IP security alarm panel
	• IP wireless router
	• radio frequency identification (RFID) device
	• voice over internet protocol (VoIP) phone.

Open System Interconnection (***OSI***) ***reference model*** has 7 layers including:	• L1 - physical • L2 - data link • L3 - network • L4 - transport • L5 - session • L6 - presentation • L7 - application.
Network may include:	• carrier access network • carrier core network • client-server network • Ethernet • home network • internet • intranet • IPTV • local area networks (LAN)

RANGE STATEMENT	
	• mesh network • peer-to-peer network • RFID • smart grid network • virtual private network (VPN) • VoIP • wide area network (WAN) • wireless local area network (WLAN or WiFi).

RANGE STATEMENT	
IP based telecommunications application may include:	• IP security network • IP-PBX • IPTV • VoIP • Web 2 applications.
Hardware may include:	• displays • DSL modems • external drives • IP device • memory • mobile equipment • motherboard • network interface card (NIC) card • uninterrupted power supply (UPS) • workstations.
Software may include:	• configuration software • diagnostic software • modem driver • MS office suite • operating system (OS) • printer driver.
Network protocols may include:	• address resolution protocol (ARP) • dynamic host configuration protocol (DHCP) • file transfer protocol (FTP) • H.323 • hypertext transfer protocol HTTP • IP • simple network management protocol (SNMP) • transmission control protocol (TCP)/IP • telnet • wireless application protocol (WAP).
Peripheral devices may include:	• Bluetooth device • IP speakers • modem • printer • RFID reader • scanner • USB and Firewire devices • webcam.

RANGE STATEMENT	

Media types and connectors may include:	• type:
	  • cable:
	  • Category 5, 5e, 6 or 7
	  • coaxial
	  • crossover
	  • optical fibre
	  • roll over
	  • straight through
	  • wireless
	• connectors:
	  • BNC
	  • FC
	  • RJ45
	  • SC
	  • ST.

Configuration details may include:	• access levels • authorisation level • encapsulation • encryption • IP addressing and subnet mask • security level.
Network addressing scheme may include:	• dynamic addressing • IPv4 addressing • IPv6 addressing • static addressing • subnet addressing.
Calculations may include:	• binary addition • binary conversion • binary multiplication • binary number system • binary subtraction.
Network commands may include:	• ping • prompt • traceroute • tracert.
Security threats may include:	• denial of service (DoS) attack • hacking • phishing

RANGE STATEMENT	
	• spoofing • trojans • viruses • worms.
Security solutions may include:	• firewalls • hacking preventions • IPSec • password logons • public key infrastructure (PKI) • secure sockets layer (SSL) • wired equivalency protection (WEP) • WiFi protected access (WPA).
Essential installation information may include:	• installation software • IP addressing schemes • logical and physical diagrams • network administrator codes • passwords • security access codes.

Unit Sector(s)

Unit sector	Telecommunications

Co-requisite units

Co-requisite units		

Competency field

Competency field	Telecommunications networks engineering