Australian Government

Department of Education, Employment and Workplace Relations

ICTTEN5168A Design and implement an enterprise voice over internet protocol and a unified communications network

Release: 1

ICTTEN5168A Design and implement an enterprise voice over internet protocol and a unified communications network

Modification History

Not Applicable

Unit Descriptor

Unit descriptor	This unit describes the performance outcomes, skills and knowledge required to design and implement the infrastructure for enterprise voice over internet protocol (VoIP) and unified communications (UC) systems to meet business requirements using converging network technologies. 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	Telecommunications or IT technicians with significant technical expertise apply the skills and knowledge in this unit. They combine technical expertise with a range of analytical, research and planning skills to develop and tailor IP convergence solutions for particular business needs. This unit applies to individuals working to design and implement the infrastructure to enable enterprises to use VoIP and other packet-based services. It also applies to enterprises outlaying capital looking for return on investment by reducing operating costs and improved unified internet protocol (IP) based communication systems.

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. Plan and design VoIP infrastructure to meet business requirements	1.1. Ascertain ***end-user requirements*** in consultation with client 1.2. Select VoIP infrastructure in line with business and end-user requirements, within budget limitations 1.3. Select ***protocols for converged networks*** 1.4. Select ***hardware***, ***software***, ***network*** and security ***requirements*** according to agreed business and end-user specifications 1.5. Investigate ***factors*** affecting bandwidth and calculate bandwidth usage for various codecs, including considerations of overhead, connection quality and connection speeds
2. Install and configure VoIP infrastructure to meet business requirements	2.1. Implement telephone number mapping (ENUM), number portability, end point addressing, path selection, calling classes and overlapping number ranges 2.2. Install, configure and test ***gatekeepers*** 2.3. Install and test ***convergent terminal equipment*** and software 2.4. Install software and configure and test VoIP services 2.5. Configure security access levels to safeguard data, making use of appropriate tools
3. Configure a UC network	3.1. Obtain the topology and components of a UC network 3.2. Analyse the potential of IP multimedia subsystem (IMS) network architecture to enable the convergence of voice, video and data applications and various mobile network technologies over IP based layer 3.3. Incorporate the use of a communications server to provide ***real-time multimedia communications*** 3.4. Select common videoconferencing codecs according to standards and practices 3.5. Select ***voice and video conferencing hardware*** 3.6. Implement IP-private branch exchange (PBX) functionalities in the UC network
4. Test and evaluate the performance of convergent networks	4.1. Develop possible ***network congestion solutions*** for common network congestions to meet quality of service (QoS) specified 4.2. Provide solutions for problems in contacting emergency services 4.3. Analyse network traffic and resolve problems using packet sniffer, monitoring software and hardware

ELEMENT	PERFORMANCE CRITERIA
	solutions 4.4. Troubleshoot convergent communications over wireless networks 4.5. Analyse types and effects of ***attacks***, including ***man-in-the-middle attacks*** 4.6. Plan ways to counteract denial of service (DoS) and distributed DoS (DDoS) attacks 4.7. Predict the impact of virtual local area network (VLAN) hopping, media access control (MAC) address movements, additions and changes on network

ELEMENT	PERFORMANCE CRITERIA
5. Test and verify the security access levels	5.1. Analyse types of intrusion detection 5.2. Monitor and evaluate capability and reliability of security systems 5.3. Make system alterations to ensure protection against known and potential threats 5.4. Verify and test that user settings conform to security policies 5.5. Backup, upgrade and scan systems to minimise attacks
6. Complete documentation and sign off procedures	6.1. Complete required records and notify customer 6.2. Remove installation waste and debris from worksite and dispose of according to environmental requirements to maintain safe worksite conditions 6.3. Reinstate site according to customer and company requirements

Required Skills and Knowledge

REQUIRED SKILLS AND KNOWLEDGE

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

Required skills

- analytical skills to evaluate network traffic protocols and bandwidth considerations
- communications skills to liaise with clients and determine business requirements
- planning and organisational skills to plan, design and implement VoIP infrastructure
- project planning skills in relation to setting benchmarks and identifying scope
- problem solving skills in a predictable range of network problems
- research skills for identifying, analysing and evaluating broad features of a particular business domain and best practice in networking technologies
- technical skills to :
  - compare session initiation protocol (SIP), H323 and media gateway control protocol (MGCP) or media gateway control (Megaco)
  - configure a VoIP and a UC network and assess the performance of convergent networks and test and verify security access levels
  - define latency, jitter and wander and implement methods for reducing or eliminating them using jitter buffer, QoS, traffic shaping and VLANs
  - describe the format of a SIP uniform resource identifier (URI)
  - evaluate and implement SIP trunking to connect enterprise internet protocol

REQUIRED SKILLS AND KNOWLEDGE
(IP)-based communications systems over long distances • identify common G.7xx codes and describe the impact of compression on voice quality • identify the components of SIP • identify the functions of signalling protocols for converged networks
Required knowledge
• broad knowledge of: • client business domain, business function and organisation • current and emerging industry accepted hardware and software products • current and emerging transmission technologies and protocols • networking technologies

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: • design and implement the infrastructure for enterprise VoIP and UC systems to meet business requirements using converged networks • apply knowledge of current networking, transmission technologies and protocols • evaluate network traffic protocols and bandwidth considerations • configure a UC network • assess the performance of convergent networks • test and verify security access levels.
Context of and specific resources for assessment	Assessment must ensure: • live network • networked computers • network design documentation • equipment specifications • network components.
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: • review of report prepared by the candidate outlining design process undertaken, including challenges faced and how these were addressed • direct observation of the candidate installing and configuring VoIP infrastructure and configuring a UC network • evaluation of system designed and implemented by the candidate in terms of performance and suitability of for business needs.
Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended, for example: • ICTTEN5201A Install, configure and test a server.

EVIDENCE GUIDE	
	Aboriginal people and other people from a non-English speaking background may have second language issues. 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.	

End-user requirements may include:	• how and what the organisation wants in regard to:
	  • preventative maintenance and diagnostic policy
	  • problem solution processes
	  • return on investment (RoI)
	  • roles and technical responsibilities in the IT department
	  • vendor and product service level support agreements

RANGE STATEMENT	
	• work environment.

RANGE STATEMENT	
Protocols for converged networks may include:	• H225 • H320 • H323 • H450 • Megaco • MGCP • SIP.
Hardware may include:	• cable or DSL modems • IP phones • modems • multi-layer switches • networks • other connectivity devices • personal computers • remote sites • routers • servers • switches • wireless devices • workstations.
Software may include:	• commercial software applications • communications software • in-house or customised software • networking device operating systems • organisation-specific software • packaged software.
Network may include:	• data and voice • internet • large and small LANs • national wide area networks (WANs) • private lines • use of public switched telephone network (PSTN) for dial-up modems only • virtual private networks (VPNs).
Requirements may include:	• reference to the business, system, application, network or people in the organisation • simple addition or upgrade to a major new installation.
Factors may include:	• codec choice • compression

RANGE STATEMENT	
	• latency • packet reordering • protocol incompatibility • QoS issues.

RANGE STATEMENT	
Gatekeepers may include:	• call manager • media gateway • media gateway controller (call agent) • signalling gateway (SG).

Convergent terminal equipment may include:	• analogue telephone adapter (ATA)
	• IP phones
	• single line adapter
	• soft phones:
	  • personal digital assistant (PDA)
	  • wireless fidelity (WiFi).

Real-time multimedia communications may include:	• directory look-up • email • file exchange • instant messaging (IM) • presence • video conferencing.
Voice and video conferencing hardware may include:	• multi-point control unit (MCU) • session border controller (SBC) • set-top box.
Network congestion solutions may include:	• changing configurations • monitoring network traffic and protocols • upgrades.
Attacks may include:	• brute force and dictionary attacks • illicit servers • man-in-the-middle attacks • unsolicited calls • viruses • voicemail compromises.
Man-in-the-middle attacks include:	• packet sniffing • registration hijacking • TP connection hijacking.

Unit Sector(s)

Unit sector	Telecommunications

Competency field

Competency field	Telecommunications networks engineering