



Australian Government

Department of Education, Employment and Workplace Relations

ICANWK611A Configure call processing network elements for secure VoIP networks

Release: 1

ICANWK611A Configure call processing network elements for secure VoIP networks

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 use tools, equipment, software and protocols to install or upgrade call processing network elements for secure and reliable internet protocol (IP)-based communications networks.

Application of the Unit

This unit applies to the use of voice management servers to support single site and centralised call processing models. Relevant job roles include advanced voice over internet protocol (VoIP) network support specialist, VoIP network engineer and VoIP systems installer.

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. Plan to implement enterprise IP communications	1.1 Produce design considerations for planning and implementing IP-based voice communications networks 1.2 Produce a solutions plan to meet business expectations 1.3 Select the required resources to effectively install or upgrade voice-management servers 1.4 Perform, test and evaluate the installation or upgrade of voice call-management software against the solutions plan
2. Plan, configure and test call-processing network elements for a single-site deployment	2.1 Produce a topology of the voice network and plan the location of the call-processing network elements to best support the business requirements 2.2 Install and test voice servers to support user requirements, third-party session initiation protocol (SIP) phones and lightweight directory access protocol (LDAP) integration 2.3 Install and configure local area network (LAN) switches to support IP phones 2.4 Configure and test voice gateways according to gateway requirements to allow for internal calls and external calls and provide voice features 2.5 Configure and test the integration of voice servers with other media systems 2.6 Test and evaluate final configuration against the design requirements
3. Manage security and privacy of IP voice network	3.1 Produce design and installation templates for bulk deployment across the enterprise 3.2 Research and implement the use of a network support model to manage the performance and security of the IP voice network 3.3 Design and conduct simple security deployment scenarios to test the integrity and security of the voice network

Required Skills and Knowledge

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

Required skills

- communication skills to liaise with internal and external personnel on technical, operational and business-related matters
- literacy skills to:
 - interpret technical documentation
 - write reports as required
- numeracy skills to:
 - take test measurements and interpret results
 - evaluate performance and interoperability of network
- planning and organisational skills to:
 - plan, prioritise and monitor own work
 - liaise with others to coordinate the process
- problem-solving and contingency-management skills to:
 - adapt configuration procedures to requirements of network
 - reconfigure depending on differing operational contingencies, risk situations and environments
 - troubleshoot and debug wireless local area network (WLAN) issues
- research skills to investigate appropriate hardware to meet requirements
- technical skills to:
 - assess and implement security requirements
 - select and configure networking devices
 - use networking and network management tools.

Required knowledge

- call-processing network element technology
- codecs and their protocols for use
- configuration, verification and troubleshoot procedures to undertake:
 - basic router operation and routing
 - switch with virtual local area network (VLANs) and inter-switching communications
- design considerations and deployment schemes
- interoperability of legacy private branch exchange (PBX) to IP voice communications
- internetwork operating system (IOS) and internet protocol (IP) networking and network support models
- LAN and wide area network (WAN) implementations
- network topologies, architectures and elements
- network, signalling and call management protocols
- networking standards and protocols
- security deployment scenarios
- voice applications and protocols

- VoIP technologies.

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: • produce design plan and requirements of call processing network elements • configure and test voice gateways and LAN switches • evaluate voice call manager server requirements and design voice call systems and applications • implement voice systems and applications on voice call manager • manage security of voice network.
Context of and specific resources for assessment	Assessment must ensure access to: • site where network installation may be conducted • hardware and software • organisational guidelines • computers • stand-alone and lightweight WLAN controllers and AP • hardware and software LAN/WLAN voice technologies • 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: • direct observation of the candidate installing, configuring and testing a new or updated network • evaluation of documentation prepared by the candidate outlining testing procedures, test results, recommendation to network changes and completion records • oral or written questioning of required knowledge.
Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, 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.

Design considerations may include:	• access • additional resources for new plan • call processing network element location • deployment plan: • centralised call processing model • distributed or decentralised call processing model • single or multiple LAN sites • dial plan • encryption • existing IP network capability • existing legacy PBX • failure to WAN and internet access • feasibility • grade of service (GoS) • growth • interoperability between systems and protocols • power back up • quality of service (QoS) • security.
Solution plans may include:	• design • execution • implementation testing • management • review and optimisation.
Resources may include:	• call-processing network equipment • protocols: • call control • H.323 • LDAP • media control • media gateway controller protocol (MGCP) • registration, admission and status (RAS) • signalling connection control part (SCCP)

	• SIP • software tools • support tools • technical support and backup.
Voice call-management software may include:	• Asterisk • Cisco voice call manager.
Call-processing network elements may include:	• call manager • call processing agent • IP phones • routers • SIP phones • switches • voice gateways • voice server.
User requirements may include:	• calling patterns • groups: • hunt • paging • profiles • roles • security access.
Gateway requirements may include:	• analog and digital trunking • call coverage • calling patterns • calling privileges • dial plans • digital signal processing (DSP) hardware • external calls to public switched telephone network (PSTN) • route patterns and filters.
Voice features may include:	• answer call • barge • call park • call pickup • call transfer • conference • intercom • music on hold • originate call • privacy.
Media systems may	• chat

include:	• email • instant messaging (IM) • presence.
Network support model may include:	• backup support and recovery • call manager monitoring • monitoring tools: • Call Manager • Microsoft Event Viewer • Microsoft Performance Monitor • Sniffer Trace • network management: • accounting • configuration • fault • performance • security • physical and network security • power backup • reporting mechanism • serviceability • troubleshooting.
Security deployment scenarios may include:	• exploiting the network: • denial of service (DoS) and OS exploitation and countermeasures • eavesdropping and interception attacks and countermeasures • infrastructure flooding attacks and countermeasures • simple network reconnaissance: • dynamic host configuration protocol (DHCP) response sniffing and spoofing and countermeasures • hacking devices and hacking countermeasures • port scanning and port scanning countermeasures • sniffing and sniffing countermeasures • virtual network computing (VNC) enumeration and VNC countermeasures.

Unit Sector(s)

Networking