



Australian Government

Department of Education, Employment and Workplace Relations

ICANWK605A Design and configure secure integrated wireless systems

Release: 1

ICANWK605A Design and configure secure integrated wireless systems

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 appropriate tools, equipment, software and protocols to produce a verified radio frequency (RF) design plan for a wireless local area network (WLAN) and to design, configure and troubleshoot secure integrated wireless systems.

Application of the Unit

This unit applies to those who plan and conduct a wireless network site survey to verify RF coverage design for installation and to the installation, operation and troubleshooting of small to medium enterprise wireless networks.

Relevant job roles include wireless network installer, wireless network support specialist and wireless network engineer.

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 and conduct a site survey for setting up a wireless network	1.1 Assess client requirements to plan for selecting appropriate WLAN technology and network elements 1.2 Evaluate existing network infrastructure and produce a wireless network topology to determine upgrade or new installation requirements 1.3 Prepare basic RF deployment considerations related to site survey design of data or voice over WLAN applications 1.4 Produce a survey model including deployment characteristics to meet client requirements 1.5 Produce a spectral analysis predictive layer 1 site survey verified by a physical site survey 1.6 Analyse the survey results produced with an RF network design for a secure wireless network 1.7 Conduct an RF field trial for final evaluation of network topology and network element placements
2. Prepare design specifications and plan for secure enterprise WLANs	2.1 Prepare for work according to relevant legislation, OHS, codes, regulations and standards 2.2 Produce design specifications and layout for wireless network using spread spectrum technology for enhanced network security 2.3 Review design plans to ensure sound WLAN RF principles and compliance with wireless regulatory bodies, standards and certifications
3. Configure and test a controller-based WLAN	3.1 Produce a controller based wireless architecture from a possible range of industry-based wireless network architectures 3.2 Configure and test a WLAN controller and access points using controller-based AP discovery and association to enable roaming facilities 3.3 Configure the basics of a stand-alone access point 3.4 Configure and test client operating system WLAN configuration and install vendor specific software and utilities where applicable
4. Configure and test WLAN security	4.1 Review the general framework of wireless security and security components for securing the WLAN 4.2 Configure and test identification assignments to network elements 4.3 Configure and test authentication methods using different sources of authentication

	4.4 Configure and test encryption methods to comply with network security policies
5. Conduct WLAN maintenance and troubleshooting	5.1 Evaluate WLAN troubleshooting methods for controllers, access points, and client methodologies 5.2 Use networking tools to maintain and troubleshoot network 5.3 Transfer device configurations and operating system (OS) using maintenance tools and commands

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:
 - coordinate the process in liaison with others
 - plan, prioritise and monitor own work
- problem-solving and contingency-management skills to:
 - troubleshoot and debug WAN issues
 - adapt configuration procedures to requirements of network
 - reconfigure depending on differing operational contingencies, risk situations and environments
- research skills to investigate appropriate hardware to meet requirements
- technical skills to:
 - select and configure networking devices
 - assess and implement security requirements
 - use networking tools and site survey tools.

Required knowledge

- authentication and encryption methods
- configuration, verification and troubleshooting procedures to undertake:
 - router-operation and routing
 - VLAN switching and inter-switching communications
- configuration of WLAN securities
- current wireless regulations, standards and certifications
- internetwork operating system (IOS) and IP networking models
- RF and WLAN technology and network design
- RF propagation and implementation issues
- spread spectrum technologies
- wireless network topologies and elements
- wireless networking protocols
- WLAN devices and their specification and use
- WLAN radio frequencies characteristics and their measuring techniques.

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: • plan and conduct a WLAN site survey • produce design specifications and layout of wireless network • configure and test a controller-based WLAN • test wireless security configurations.
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 WLAN site survey tools • 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 • verbal 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.

<i>Client requirements</i> may include:	• accessibility • dropout rates • future scalability • grade of service (GoS) • infrastructure costs • interoperability to existing network • network growth • network RF coverage • network security • network traffic • operating budget • quality of service (QoS) • serviceability • service level agreement (SLA).
<i>WLAN technology</i> may include:	• channels reuse and overlap • carrier sense multiple access/collision avoidance (CSMA/CA) • dynamic satellite survey (DSS) • multiple-input multiple-output (MIMO) • orthogonal frequency division multiplexing (OFDM) • rate-shifting • worldwide interoperability for microwave access (WiMAX) • wireless network topologies • wireless personal devices: • Bluetooth • cordless phones • personal digital assistant (PDA) • smartphone • wireless technology developed as an open global standard (ZigBee).
<i>Network elements</i> may include:	• adaptors • access point (AP) • client • communications cables and connectors

	• controller • host • hubs • routers • servers • switches.
Network infrastructure may include:	• additional antenna • lightning protection • mounting considerations • outdoor grounding • physical security • power over ethernet (PoE) • power including renewable sources • rack capacity • switch port capacity.
Wireless network topology may include:	• basic mesh • bridging • basic service set (BSS) • extended service set (ESS) • independent basic service set (IBSS) • point-to-multipoint using BSS • point-to-point using IBSS.
RF deployment considerations may include:	• AP location • basic RF site survey design related to channel re-use • building material • cell overlap • common RF interference sources such as devices • signal strength.
Survey model may include:	• data • point-to-multipoint bridging • video point-to-point bridging • voice.
Deployment characteristics may include:	• dense deployment • high mobility versus nomadic • internal meshing.
Physical site survey may include:	• actual AP • RF power • simulated data rate to conduct the site survey • test radio equipment.
RF network design may	• AP count • controller and licence requirements

include:	• location and type of network elements • location of additional APs for monitoring and sniffing • propagation patterns and attenuation • WLAN radio frequencies and characteristics.
Spread spectrum technology may include:	• channels reuse and overlap • carrier sense multiple access or collision avoidance (CSMA/CA) • direct sequence spectrum (DSS) • multiple-input multiple-output (MIMO) • modulation • orthogonal frequency division multiplexing (OFDM) • rate-shifting • techniques: • direct sequence (DS) • frequency hopping (FH) • hybrids, combination of FH and DS • time hopping (TH).
WLAN RF principles may include:	• antenna types • effective isotropic radiated power (EIRP) • reflection • refraction • RF gain/loss.
Wireless regulatory bodies, standards and certifications may include:	• 802.11a/b/g/n • European Telecommunications Standards Institute (ETSI) • Federal Communications Commission (FCC) • Wi-Fi Alliance.
Wireless network architectures may include:	• lightweight access point (LWAP) • split media access control (MAC) • stand-alone AP versus controller-based AP.
WLAN controller and access points may include:	• channel • command line interface (CLI) • graphical user interface (GUI) • interfaces • network time protocol (NTP) • power • wireless LANs (WLANs).
Controller-based AP discovery and association may include:	• dynamic host configuration protocol (DHCP) • domain name system (DNS) • master-controller • n+1 redundancy

	• over the air provisioning (OTAP) • primary-secondary-tertiary.
Roaming may include:	• Cisco centralised key management or proactive key caching (CCKM/PKC) • inter-controller • intra-controller • layer 2 • layer 3.
Client operating system WLAN configuration may include:	• Linux • Mac • Windows.
Security components may include:	• authentication • encryption • intrusion prevention system (IPS) • management frame protection (MFP).
Identification assignments may include:	• 802.1q trunking • interface • service set identifier (SSID) • virtual local area network (VLAN) • wireless LAN identifier (WLANID).
Authentication methods may include:	• 802.1X • extensible authentication protocol-flexible authentication via secure tunnelling (EAP-FAST) • frame types: • associated or unassociated • control • data • management • guest • lightweight extensible authentication protocol • open (LEAP) • protected extensible authentication protocol (PEAP) • pre-shared key (PSK) • shared • wi-fi protected access (WPA) with extensible authentication protocol-transport layer security (WPA or WPA2 with EAP-TLS).
Sources of authentication may include:	• local or external (EAP) • pre-shared key (PSK) • remote authentication dial-in user service (RADIUS).

<i>Encryption methods</i> may include:	• advanced encryption standard (AES) • WPA or WPA2 with temporal key integrity protocol (TKIP).
<i>Networking tools</i> may include:	• client troubleshooting • vendor debug • vendor logging.

Unit Sector(s)

Networking