



Australian Government

Department of Education, Employment and Workplace Relations

ICANWK612A Plan and manage troubleshooting advanced integrated IP networks

Release: 1

ICANWK612A Plan and manage troubleshooting advanced integrated IP 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 plan, manage and implement troubleshooting and monitoring strategies to ensure reliability and performance on advanced integrated internet protocol (IP) networks.

Application of the Unit

This unit applies to maintaining and troubleshooting infrastructure supporting voice, video and data networks. Relevant job roles include advanced support engineer, network support specialist and information and communications technology (ICT) 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 the strategies for troubleshooting and monitoring the performance of advanced integrated IP networks	1.1 Develop a plan to monitor and manage the IP network to optimise its performance and reliability 1.2 Plan the isolation of network segments for troubleshooting procedures 1.3 Plan the testing sequences and scenarios of network infrastructure 1.4 Select appropriate network testing and monitoring tools and software application to suit the specific network troubleshooting and monitoring sequence
2. Manage and monitor troubleshooting strategies for complex enterprise networks	2.1 Manage and monitor strategies for network monitoring structure 2.2 Produce a routine internetwork operating system (IOS) device maintenance plan to include monitoring of routing protocols and router configurations 2.3 Isolate sub-optimal internetwork operations at the appropriate open systems interconnection (OSI) model layer 2.4 Produce a plan troubleshooting and monitoring security issues related to IOS services for mission critical applications 2.5 Produce a plan troubleshooting and monitoring internet protocol version 6 (IPv6) and version 4 (IPv4) interoperability
3. Implement test plans for advanced network solutions	3.1 Test switch-to-switch connectivity, access ports and loop prevention for the virtual local area network (VLAN) based solution 3.2 Test private VLANs 3.3 Test switch virtual interfaces (SVI) 3.4 Test switch support of advanced services 3.5 Troubleshoot switch configuration

Required Skills and Knowledge

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

Required skills

- communication skills to liaise with internal and/or 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:
 - adapt configuration procedures to requirements of network
 - reconfigure depending on differing operational contingencies, risk situations and environments
 - troubleshoot and debug WLAN issues
- research skills to investigate appropriate hardware to meet requirements
- technical skills to:
 - select and configure networking devices and assess and implement security requirements
 - use networking and network testing and management tools.

Required knowledge

- advanced network solutions
- configuration, verification and troubleshoot procedures to undertake:
 - router operation and routing
 - VLANs switching and inter-switching communications
- deployment schemes
- IOS and IP networking models
- IOS services
- IP network topologies, architectures and elements
- networking standards and protocols
- threat mitigation strategies
- VLAN 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: • plan and monitor IP networks for performance and reliability • evaluate, design and implement a troubleshooting structured plan • use network testing and monitoring tools • produce a maintenance plan for monitoring routing protocols and configurations • implement tests of advanced network solutions.
Context of and specific resources for assessment	Assessment must ensure access to: • site where complex network installation may be conducted • hardware and software • organisational guidelines • computers • LAN and WAN systems, including voice and video hardware and software • 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>IP network</i> may include:	• integrated network • internet • intranet • local area network (LAN) • router-based network • switch-based network • VPN • WAN • WLAN.
<i>Network testing and monitoring tools</i> may include:	• applications, services or systems monitor • bandwidth tester • connection speed • fingerprinting monitor • flow monitor • latency calculator • mapping tools • network: • connectivity • monitor • security monitor • simulator • packet capture and analyser • packet tracer • path characterisation • protocol analyser • sniffer or analyser • simple network management protocol (SNMP) tools • voice over internet protocol (VoIP) monitors.
<i>Strategies</i> may include:	• use of internetwork operating system (IOS) tools • use of vendor-recommended software and hardware: • Apple • Billion • Cisco

	• Juniper Networks.
Routing protocols may include:	• external border gateway protocol (EBGP) • enhanced interior gateway routing protocol (EIGRP) • open shortest path first (OSPF) • routing information protocol (RIP).
Router configurations may include:	• dynamic host configuration protocol (DHCP) • link control settings • network address translation (NAT) • usernames and passwords.
IOS services may include:	• auto-upgrade manager (AUM) • embedded event management (EEM) • flexible netflow • file transfer protocol (FTP) • hypertext transfer protocol (HTTP) • identity-based network services (IBNS) • IOS firewall • IP service level agreement (IPSLA) • network-based application recognition 2 (NBAR2) • network time protocol (NTP) • performance routing (PfR) • remote copy or rate control protocol (RCP) • service advertisement framework (SAF) • web services management agent (WSMA).
Advanced services may include:	• internet protocol TV (IPTV) • video • voice over internet protocol (VoIP) • wireless.
Switch configuration may include:	• spanning tree • switch virtual interface (SVI) • virtual LAN (VLAN).

Unit Sector(s)

Networking