ICANWK613A Develop plans to manage structured troubleshooting process of enterprise networks

Release: 1

ICANWK613A Develop plans to manage structured troubleshooting process of enterprise networks

Modification History

Release	Comments
Release 1	This Unit first released with *ICA11 Information and Communications Technology Training Package version 1.0*

Unit Descriptor

This unit describes the performance outcomes, skills and knowledge required to manage the maintenance of a complex integrated enterprise network to ensure availability and performance standard.

Application of the Unit

This unit applies to an information and communications technology (ICT) network specialist, network engineer, network infrastructure engineer, senior network administrator, network and systems manager, ICT security specialist, security engineer, communications engineer, communications manager.

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
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

1. Plan the strategies for structured troubleshooting and monitoring of enterprise networks	1.1 Develop strategies to monitor and manage an *enterprise network* to ensure availability and performance standard
	1.2 Conduct equipment and skills audits as required
	1.3 Evaluate the business value of service level agreements (SLAs), formal maintenance plans and monitoring procedures against best practices for maintenance and fault procedures
	1.4 Assign functional responsibilities to *stakeholders* according to the maintenance plan
	1.5 Select and use appropriate *network fault management* tools and monitor and improve network performance
2. Manage and monitor structured troubleshooting strategies for complex enterprise networks	2.1 Implement structured network *maintenance management processes and procedures* in line with *enterprise design plans and policies* for ensuring high network reliability
	2.2 Undertake risk assessment evaluation and rank threats for minimal impact
	2.3 Develop and implement *disaster recovery strategies* for reliable contingencies and business continuity in a complex routing environment
	2.4 Measure and analyse performance against an agreed baseline
3. Conduct structured network troubleshooting strategies	3.1 Analyse and troubleshoot *layer 2 and 3 switch configuration* to ensure the availability and resilience of a switched environment
	3.2 Implement effective control of broadcast and multicast traffic in a switched environment
	3.3 Analyse and troubleshoot scalable network layer connectivity with routing data structures and routing functions
	3.4 Analyse and troubleshoot enterprise intra and internetwork *routing protocols*, architectures and processes
	3.5 Analyse and troubleshoot route redistribution operations in inter-autonomous system routing architectures and processes
	3.6 Test and manage internet protocol version 6 (IPv6) and version 4 (IPv4) addressing schema and verify internal and external IP address translation standards
	3.7 Analyse and troubleshoot communication filtering techniques, *automated address allocation* systems and IPv6 operational issues in the context of enterprise routing protocols
	3.8 Analyse and troubleshoot wireless network configuration issues

	3.9 Analyse and resolve network performance issues in an integrated voice or video network

Required Skills and Knowledge

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

Required skills

- analytical skills to identify functional, performance and management features associated with the operation of complex network infrastructure
- communication skills to:
  - communicate complex concepts and issues technically and in plain language
  - liaise with diverse clients
- literacy skills to:
  - develop and prepare operational documentation, such as policies and procedures, technical and management reports
  - interpret and prepare technical documentation
  - prepare project-management documentation
- problem-solving skills suitable for complex and dynamic environments with demanding service levels
- risk-management skills for complex and dynamic environments
- technical skills to investigate, analyse and resolve faults and performance problems in complex network infrastructure.

Required knowledge

- benefits of a formal or structured approach to network management
- disaster recovery strategies
- emerging viable business and social technologies
- enterprise network technologies, design plans and policies
- enterprise network topologies, architectures and elements
- external developments or factors that affect network design
- IPv4 and IPv6 addressing configurations
- maintenance and fault procedures
- maintenance and management tools and practices suitable for complex networks
- networking standards and protocols
- risk management strategies and practices suitable for a complex network environment
- routing and routed protocols
- routing and switching technologies for an enterprise environment
- security for enterprise networks
- security standards and technologies for network environments
- SLAs
- skills audit
- troubleshooting and threat-mitigation strategies.

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: • analyse, document and troubleshoot a given complex network using industry methodologies and resources • develop monitoring and management plans • use networking and network fault management tools • evaluate risk assessments and minimise threats on enterprise networks.
Context of and specific resources for assessment	Assessment must ensure access to: • location where the network configuration can be implemented • routers and switches with appropriate operating systems • computers • suitable testing and analyses 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 preparing, installing, configuring, testing, analysing and correcting network problems • documentation of the tools and methodologies adopted by the candidate to test, analyse, network functionality and performance (system audits) • documentation of the options and justification for the selected solutions developed to address network problems • evidence of the success of the corrective measures • delivery of the revised configuration documentation of the entire network • verbal and 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.

Innovation and Business Skills Australia

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.

Enterprise network may include:	- integrated network - internet - intranet - local area network(LAN) - router-based network - switch-based network - virtual LAN (VLAN) - virtual private network (VPN) - wide area network (WAN) - wireless LAN (WLAN).
Stakeholders may include:	- contractor - staff - vendor.
Network fault management tools may include:	- accounting and resource audits - configuration and version control - fault finding - generic and proprietary system management resources - monitoring and testing functions within device operating systems - open systems interconnection (OSI) and transmission control protocol or internet protocol (TCP/IP) models - performance - security - troubleshooting tools: - debug - netflow - network security monitor - operating system verification (show) commands - packet capture and analyser - packet sniffers - packet tracer - ping - protocol analysers

	• simplified network management protocol (SNMP) • Telnet.

Maintenance management processes and procedures may include:	• change control
	• communication
	• identification
	• methodologies:
	   • analyse
	   • execute preferred solution
	   • gather information
	   • identify solution options
	• planning
	• scheduling.

Enterprise design plans and policies may include:	• change logs • change-management request • configuration details • equipment inventory • equipment specifications • industry and regulatory standards • logical diagram • physical diagram • policy and procedures • reports • SLAs • templates.
Disaster recovery strategies may include:	• backup • rollback.
Layer 2 and 3 switch configuration may include:	• 802.1q (trunking) • 802.1w • access ports for the VLAN-based solution • dynamic trunking protocol (DTP) • dynamic and virtual trunking protocol operations • EtherChannel • first-hop redundancy protocol (FHRP) • general switch security • inter-switch link (ISL) for trunking • loop prevention for the VLAN based solution • multiple spanning tree protocol (MSTP) • multilayer switching • port-based access control list (PACL) • port security

          Innovation and Business Skills Australia

	• private VLANS • rapid spanning tree protocol (RSTP) • spanning tree protocol (STP) • switch virtual interface (SVI) • switch supervisor redundancy • switch-to-switch connectivity for the VLAN-based solution • VLAN access control list (VACL) • VLAN trunking protocol (VTP).
Routing protocols may include:	• border gateway protocol (BGP) • external border gateway protocol (EBGP) • enhanced interior gateway routing protocol (EIGRP) • first-hop redundancy protocols (FHRP): 　• gateway load balancing protocol (GLBP) 　• hot standby router protocol (HSRP) 　• virtual router redundancy protocol (VRRP) • open shortest path first (OSPF).
Automated address allocation may include:	• automatic private IP addressing (APIPA) • dynamic host configuration protocol (DHCP) • IPv6 stateless address auto-configuration.

Unit Sector(s)

Networking