



Australian Government

ICTTEN8195B Evaluate and apply network security

Release 1

ICTTEN8195B Evaluate and apply network security

Modification History

Release	Comments
Release 2	This version first released with <i>ICT10 Integrated Telecommunications Training Package Version 3.0</i>. References to other units updated. Outcomes deemed equivalent.
Release 1	This version first released with <i>ICT10 Integrated Telecommunications Training Package Version 1.0</i>.

Unit Descriptor

This unit describes the performance outcomes, skills and knowledge required to analyse the security features of an internet protocol (IP) based telecommunications network.

This applies to IT networking and telecommunications networking topologies.

Application of the Unit

Telecommunication engineers apply the skills and knowledge in this unit to analyse and report on the security of an ICT network, particularly Internet security.

They are responsible for the evaluation of security of ICT networks using converging switching and transmission technologies in local area networks (LAN) and wide area networks (WAN), broadband networks, internet protocol TV (IPTV) and virtual networks.

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. Analyse the operation of the Internet	1.1 Evaluate the interrelationship of IP to open systems interconnect (OSI) seven layer model and the impact on network topologies and network elements 1.2 Assess media access control (MAC) and IP addressing and their application in security 1.3 Report on transmission control protocol/internet protocol (TCP/IP) operations and the use of transport protocols for transmitting data over the network 1.4 Examine the various types of routing protocols and implication on security 1.5 Analyse forms of label switching as applied to data packets 1.6 Use software to simulate the least cost algorithms
2. Analyse internetwork protocols	2.1 Compare connection-oriented and connection-less networks in internetworking applications 2.2 Research the design parameters used in networks 2.3 Produce a report on IP multi-casting protocols and systems including IP frame fields of the data frames
3. Research and report internetwork operations	3.1 Analyse protocol considerations of voice over internet protocol (VoIP) 3.2 Research the protocols G723.1, G729 and G729A standards and evaluate their application in internetworking 3.3 Determine the format of JPEG and GIF files as applied to still pictures 3.4 Determine the format of MPEG-2 and H.32x series multimedia protocols for motion pictures 3.5 Evaluate the features of different of multi-service protocols and of different email system protocols in networking operations 3.6 Produce a report on the features the different web-based protocols used in internetworking operations
4. Analyse features and types of network security	4.1 Analyse procedures and processes used for security attacks and use of protection mechanisms 4.2 Research conventional encryption algorithms and determine possible locations of encryption devices 4.3 Produce a report on conventional encryption key distribution problems and how message authentication and verification is achieved

	4.4 Research one-way hashing and secure hashing functions 4.5 Produce a report on digital signature standard (DSS) principles including public key cryptography algorithms for network security
5. Research features of public key authentication and email network security protocols	5.1 Research public key authentication using Kerberos 5.2 Analyse how electronic mail security is achieved using pretty good privacy (PGP) 5.3 Research and report on IPSec protocol security 5.4 Produce a report on encapsulating security payload (ESP) including Internet key management processes
6. Research features of web, network management and system security	6.1 Analyse how web threats and attacks occur in an IP network and determine system intruders and threats 6.2 Research the operation of transaction protocols 6.3 Evaluate the processes used for selection and protection of system passwords 6.4 Evaluate system threats and methods used to counter act the threats 6.5 Produce a report on anti-virus protection strategies, including firewall design principles, types and configurations
7. Document evaluation report	7.1 Present a final report to include research and evaluation of network security management principles and the application to the network in the workplace with enhancement recommendations

Required Skills and Knowledge

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

Required skills

- analytical skills to evaluate a range of complex technical data
- communication skills to work effectively within a group and present information
- information technology skills to use:
 - software for desktop research
 - statistical data
 - word processing software
- literacy skills to prepare reports given a specific format and read and interpret technical standards
- planning and organisational skills to manage own work in specific time frames
- research skills to gather and record data from measurements
- technical skills to:
 - operate test equipment
 - use telecommunications management networks.
 -

Required knowledge

- administrative network management systems
- algorithms
- cryptography
- encapsulation
- encryption
- enterprise solutions
- firewalls
- network topologies
- operations network management systems
- organisational policy and procedures
- protocols
- routing theory
- system threats
- transaction protocols
- workplace and industry environment.

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 the operation of the Internet • implement Internet technology • select Internetwork protocols • research and report various internetwork operations • analyse features and types of network security methods and their weaknesses • analyse features of various cryptography systems • research and report the features of public key authentication and email network security protocols • research and report the features of web, network management and system security.
Context of and specific resources for assessment	Assessment must ensure: • a telecommunications operations site with a mentor or supervisor appropriately experienced in relevant telecommunications technology and infrastructure • networked computers and relevant software.
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: • oral or written questioning to assess required knowledge • direct observation of the candidate carrying out relevant security checks within a networked communication system • review of reports completed by the candidate for different security breached scenarios.
Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplaces and job role is recommended, for example: • ICTPMG8143B Manage a telecommunications project

	• ICTPMG8149B Evaluate and use telecommunications management networks. 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

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>Network elements</i> may include:	• bridges • gateways • routers • servers • switches.
<i>Transport protocols</i> may include:	• Ethernet • point-to-point protocol (PPP) • synchronous data link control (SDLC) • synchronous optical network (SONET).
<i>Routing protocols</i> may include:	• adaptive • enhanced interior gateway routing protocol (EIGRP) • fixed • flooding • interior gateway routing protocol (IGRP) • open shortest path first (OSPF) • random • routing information protocol (RIP).
<i>Label switching</i> may include:	• cell switching routers (CSR) • IP • tag.
<i>Least cost algorithms</i> may include:	• Bellman-Ford's • Dijkstra's.
<i>Design parameters</i> may include:	• datagram lifetime • error and flow control techniques • fragmentation • reassembly • routing.
<i>Frame fields</i> may include:	• datagram format • internet control message protocol (ICMP) • IPv6 header and addressing • protocol data unit (PDU).
<i>Multi-service protocols</i>	• border gateway protocol (BGP) • OSPF

may include:	• resource reservation protocol (RSVP) • real time control protocol (RTCP) • real time protocol (RTP).
Email system protocols may include:	• data transparency: • ASCII • binary • EBCDIC • radix64 coding • Unicode • multipurpose mail extensions (MIME) • simple mail transfer protocol (SMTP).
Web-based protocols may include:	• common gateway interface (CGI) • file transfer protocol (FTP) • hyper-text mark-up language protocol (HTML) • hyper-text transfer protocol (HTTP) • Java applets and application programmers interface (API).
Encryption algorithms may include:	• Blowfish • Data Encryption Standard (DES) • Feistel Cipher • International Data Encryption Algorithm (IDEA).
Hashing functions may include:	• hash message authentication checksum (HMAC) • Secure Hash (SHA-1).
Public key cryptography algorithms may include:	• Diffie-Hellman key exchange • Rivest Shamir Adleman (RSA).
IPSec may include:	• authentication header • internet protocol (IP) security • transport and tunnel modes of operation.
Key management processes may include:	• internet security association and key management protocol (ISAKMP) • Oakley key determination protocol (OKDP).
Transaction protocols may include:	• secure electronic transaction (SECT) • simple network management protocol (SNMP) • SNMPv1 (community facility and proxies) • SNMPv3 (message processing and the user security model) • secure socket layer (SSL).
System threats may include:	• logic bombs • trap doors • Trojans

	• viruses • worms.
--	--

Unit Sector(s)

Telecommunications - Telecommunications networks engineering