Australian Government

Department of Education, Employment and Workplace Relations

ICANWK531A Configure an internet gateway

Release: 1

ICANWK531A Configure an internet gateway

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 connect network hardware devices, mainly personal computers (PCs), to an internet gateway.

Application of the Unit

This unit applies to middle managers, such as network engineers, technical specialists or security analysts, who are responsible for implementing and managing the connection of network hardware devices to an internet gateway.

They provide technical advice, guidance and leadership in the resolution of specified problems.

The role involves managing the installation, configuration and testing of gateway products and related hardware and software, as well as determining security threats. Related tasks include network planning, implementation and budgeting.

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. Confirm client requirements and network equipment	1.1 Confirm and validate ***client*** requirements 1.2 Determine scope of internet services with reference to client requirements 1.3 Identify and install both ***hardware*** and ***software*** components 1.4 Verify equipment specifications and availability of components
2. Review security issues	2.1 Assess security features of internet gateways with reference to ***architecture*** and ***security plan*** 2.2 Review security measures with the ***internet service provider*** (ISP) with reference to ***firewalls*** and other measures as required 2.3 Brief ***users*** on the security plan with reference to internet use and hazard possibilities
3. Install and configure gateway products and equipment	3.1 Identify and select installation and configuration options 3.2 Install and configure gateway products and equipment as required by technical guidelines 3.3 Plan and execute tests with reference to client requirements and ***network*** impact 3.4 Analyse error reports and make changes as required
4. Configure and test node	4.1 Assign node to specific gateway as required by network architecture and client requirements 4.2 Determine ***connection type*** and configure with reference to network architecture and client requirements 4.3 Ensure node software and hardware are configured as required according to vendor specifications and client requirements

Required Skills and Knowledge

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

Required skills

- analytical skills to confirm business and network requirements
- communication skills to:
  - communicate with clients
  - convey and clarify complex information
- literacy skills to interpret technical documentation, equipment manuals and specifications
- problem-solving skills to solve operational problems as they arise
- safety awareness skills to work systematically with required attention to detail without injury to self or others, or damage to goods or equipment
- technical skills to:
  - analyse error reports and correct as required
  - install and configure computer hardware and software
  - use proprietary software.

Required knowledge

- current browser software, such as MS Explorer, Netscape Navigator, Mozilla, Konqueror and Opera
- domain name server (DNS) resolution
- features and functions of:
  - network architecture:
    - bridges as required
    - desktop operating systems
    - hubs
  - network gateways
  - network operating systems:
    - routers
    - switches
- gateway software:
  - Cisco IpeXchange
  - Lotus Notes
  - Postoffices.

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: • connect network hardware devices to an internet gateway • configure and test gateway products • configure and test node according to vendor specifications and client requirements.
Context of and specific resources for assessment	Assessment must ensure access to: • network and internet where gateway products may be installed and configured • use of hardware and software currently used in industry • client requirements documentation • vendor specifications • 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:
	• verbal or written questioning to assess candidate's knowledge of hardware and software to be installed
	• direct observation of candidate:
	  • installing and configuring gateway products as required by technical guidelines
	  • configuring and testing node as required by vendor specifications and client requirements.

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.

Client may include:	• employees • external organisations • individuals • internal departments.
Hardware may include:	• digital subscriber line (DSL) modems • modems or other connectivity devices • networks • PCs • remote sites • servers • workstations.

Software may include:	• application software:
	  • database
	  • internet browser
	  • spreadsheet
	  • word-processing
	• commercial
	• customised software
	• in-house
	• programming software:
	  • assembler
	  • compiler
	  • development tools
	• system software:
	  • computer security software
	  • device drivers
	  • operating system.

Architecture may include:	• configuration:
	  • large memory model
	  • requests per second
	  • small memory model
	• database software:

	• DB2 • Informix • Ingres • Microsoft SQL (MS SQL) server • Mini SQL (mSQL) • MySQL • Oracle • Sybase • operating system: • Linux • Mac • multi-user ability • Novell NetWare • Windows.
Security plan may include:	• alerts relating to the security objectives of the organisation • audits • privacy • standards: • archival • backup • network • theft • viruses.
Internet service provider may include:	• broadband access: • asymmetric digital subscriber line (ADSL) • cable • fibre • satellite • wireless • dial-up access • ISP hierarchical structure: • Tier 1 ISP • Tier 2 ISP • Tier 3 ISP.
Firewalls may include:	• hardware appliances • individual PC solutions, with varying functionality: • network address translation (NAT) or internet protocol (IP) masquerading • routing to specific machines • proxy servers.

Users may include:	• contractors • departments within the organisation • persons within a department • support staff • third parties.
Network may include:	• data • internet • large and small local area networks (LANs) • private lines • use of the public switched telephone network (PSTN) for dial-up modems only • voice • virtual private network (VPN) • wide area network (WAN).
Connection type may include:	• ADSL • cable • dedicated or proxy connections • dial-up • integrated services digital network (ISDN) terminal adapter • optical network termination (ONT).

Unit Sector(s)

Networking