OCR
Oxford Cambridge and RSA

Cambridge **TECHNICALS LEVEL 3**

Cambridge TECHNICALS 2016

IT

MAPPING GUIDE
Unit 4 Computer networks

Version 1

ocr.org.uk/it

INTRODUCTION

Prodigy are delighted to work with OCR, a progressive Awarding Organisation, who share the ambition of providing high-quality qualifications, learning solutions that are industry-led and reliable and valid assessment. The Cambridge Technicals in IT qualifications provide 'future-ready' skills for a learner to further their ambitions, whether that is in terms of further academic study, enter an apprenticeship or as a springboard to gaining employment.

Prodigy Learning (Prodigy) is an award-winning EdTech business providing digital skills certifications and learning solutions for a range of technologies including Adobe, Autodesk and Microsoft. Established in 2000, Prodigy now have offices in Dublin, London and Sydney. Having worked closely with Microsoft since 2000, Prodigy is a Microsoft Authorised Education Gold Partner and a MS Global Training Partner supporting academic institutions utilise Microsoft Imagine Academy, Microsoft certifications and other Microsoft Education solutions.

Historically, the UK has thrived on a rich research and technology base and has been at the forefront of global technology innovation. Enthusing young learners about following exciting careers in science, technology, engineering and mathematics (STEM) subjects is fundamental to maintaining this success. However, currently the UK has a widely acknowledged skills gap in the pipeline of talent studying computing-related disciplines. Therefore, providing high quality, engaging and relevant qualifications that equip learners with current technical knowledge and skills is essential to encourage more young people into the computing discipline, and moreover to ensure they progress to jobs in the sector.

MAPPED TO MTA NETWORKING FUNDAMENTALS UNIT

1. Understanding Network Infrastructures

	1.1.3 firewalls	1.2.1 perimeter networks	1.2.2 addressing	1.2.3 reserved address ranges for local use (including local loopback ip)	1.2.4 VLANs	1.2.5 wired LAN	1.2.6 wireless LAN	1.3.1 leased lines	1.3.2 dial-up	1.3.3 ISDN, VPN, T1, T3, E1, E3, DSL,	1.3.4 cable and their characteristics (speed, availability)	1.5.1 star	1.5.2 mesh	1.5.3 ring
1.2.1 Network types - local area network (LAN)		X	X	X	X	X	X							
1.2.2 Network types - wireless local area network (WLAN)							X							
1.2.3 Network types - wide area network (WAN)								X	X	X	X			
1.4 Network topologies (layout) (e.g. bus, wireless, segments, backbones)												X	X	X
1.8.1 Network addressing - MAC Addressing			X	X										
1.8.2 Network addressing - APIPA			X	X										
1.8.3 Network addressing - Class addressing			X	X										

MAPPED TO MTA NETWORKING FUNDAMENTALS UNIT

	1.1.3 firewalls	1.2.1 perimeter networks	1.2.2 addressing	1.2.3 reserved address ranges for local use (including local loopback ip)	1.2.4 VLANs	1.2.5 wired LAN	1.2.6 wireless LAN	1.3.1 leased lines	1.3.2 dial-up	1.3.3 ISDN, VPN, T1, T3, E1, E3, DSL,	1.3.4 cable and their characteristics (speed, availability)	1.5.1 star	1.5.2 mesh	1.5.3 ring
1.8.4 Network addressing - Classless addressing			X	X										
1.8.5 Network addressing - Private addressing			X	X										
1.8.6 Network addressing - Loopback addressing			X	X										
1.10.2 Network Security - Security Systems (e.g. firewall, routers, WEP)	X													
2.5.7 Network Specification - security network security (e.g. firewall, MAC filtering)	X													
2.6.4 Network Plan - software (e.g. operating systems, firewall)	X													

MAPPED TO MTA NETWORKING FUNDAMENTALS UNIT

	1.1.3 firewalls	1.2.1 perimeter networks	1.2.2 addressing	1.2.3 reserved address ranges for local use (including local loopback ip)	1.2.4 VLANs	1.2.5 wired LAN	1.2.6 wireless LAN	1.3.1 leased lines	1.3.2 dial-up	1.3.3 ISDN, VPN, T1, T3, E1, E3, DSL,	1.3.4 cable and their characteristics (speed, availability)	1.5.1 star	1.5.2 mesh	1.5.3 ring
4.2.2 Maintenance issues - virus: treatment (e.g. virus protection, firewall, security update)	X													
4.2.11 Maintenance issues - security settings (e.g. router, firewall)	X													

2. Understanding Network Hardware

	2.2.1 transmission speed considerations	2.2.2 directly connected routes	2.2.3 static routing	2.2.4 dynamic routing (routing protocols)	2.2.5 default routes	2.2.6 routing table and how it selects best routes	2.2.7 routing table memory	2.2.8 NAT	2.2.9 software routing in Windows Server
1.3.6 Network components – routers	X	X	X	X	X	X	X	X	X

MAPPED TO MTA NETWORKING FUNDAMENTALS UNIT

3. Understanding Protocols and Services

	3.1.1 OSI model	3.1.2 TCP model	3.1.3 examples of devices, protocols, and applications and which OSI/ TCP layer they belong to	3.1.4 TCP and UDP	3.1.5 well-known ports for most-used purposes (not necessarily Internet)	3.1.6 packets and frames	3.2.1 addressing, subnetting	3.2.2 NAT, static IP, gateway	3.2.3 APIPA	3.2.4 network classes, classful/ classless IP addressing	3.2.5 reserved address ranges for local use (including local loopback ip)
1.6.7 Networking models - OSI 7 layer model	X	X	X	X	X	X					
1.6.8 Networking models - TCP/IP model		X	X	X							
1.7 IP versions (e.g. IPv4, IPv6)		X					X	X	X	X	X
1.8.1 Network addressing - MAC Addressing							X				
1.8.2 Network addressing - APIPA									X		
1.8.3 Network addressing - Class addressing										X	
1.8.4 Network addressing - Classless addressing										X	
1.8.5 Network addressing - Private addressing										X	
1.8.6 Network addressing - Loopback addressing											X
1.8.7 Network addressing - TCP ports		X									
1.9.1 Network data units - Ethernet frames						X					

MAPPED TO MTA NETWORKING FUNDAMENTALS UNIT

	3.1.1 OSI model	3.1.2 TCP model	3.1.3 examples of devices, protocols, and applications and which OSI/ TCP layer they belong to	3.1.4 TCP and UDP	3.1.5 well-known ports for most-used purposes (not necessarily Internet)	3.1.6 packets and frames	3.2.1 addressing, subnetting	3.2.2 NAT, static IP, gateway	3.2.3 APIPA	3.2.4 network classes, classful/ classless IP addressing	3.2.5 reserved address ranges for local use (including local loopback ip)
1.9.2 Network data units - IP packets						X					
1.9.3 Network data units - TCP packets						X					

MAPPED TO MTA NETWORKING FUNDAMENTALS UNIT

	3.3.1 subnetting	3.3.2 IPconfig	3.3.3 why use IPv6	3.3.4 addressing	3.3.5 ipv4toipv6 tunnelling protocols to ensure backwards compatibility	3.3.6 dual ip stack	3.3.7 subnet mask	3.3.8 gateway	3.3.9 ports	3.3.10 packets	3.3.11 reserved address ranges for local use (including local loopback ip)
1.7 IP versions (e.g. IPv4, IPv6)	X	X	X	X	X	X	X	X	X	X	X
1.8.6 Network addressing - Loopback addressing											X
1.9.2 Network data units - IP packets										X	

MAPPED TO MTA NETWORKING FUNDAMENTALS UNIT

	3.5.1 DHCP	3.5.2 IPsec	3.5.3 remote access	3.6.1 tools such as ping; tracert; pathping	3.6.2 Telnet	3.6.3 IPconfig; netstat, reserved address ranges for local use (including local loopback ip)	3.6.4 protocols
1.5.3 Network protocols - TCP				X	X	X	X
1.6.8 Networking models - TCP/IP model				X	X	X	X
2.2.1 Network Services - DHCP	X						
2.2.4 Network Services - Other Services (e.g. printing, email, web, DNS)	X	X	X				
2.4.1 Testing Tools - Ping				X			
2.4.2 Testing Tools - ipconfig						X	
2.4.3 Testing Tools -pathping				X			
2.4.4 Testing Tools -tracert				X			

MAPPED TO MTA SECURITY FUNDAMENTALS 98-367 UNIT

2. Understand operating system security

	2.1.1 Multifactor authenti-cation	2.1.2 physical and virtual smart cards	2.1.3 Remote Authen-tication Dial-In User Service (RADI-US)	2.1.4 biometrics	2.1.5 use Run As to perform admin-istrative tasks	2.2.1 File system permissions	2.2.2 share permissions	2.2.3 registry	2.2.4 Active Directory	2.2.5 enable or disable inheritance	2.2.6 behaviour when moving or copying files within the same disk or on another disk	2.2.7 multiple groups with different permissions	2.2.8 basic permissions and advanced permissions	2.2.9 take ownership	2.2.10 delega-tion	2.2.11 inheritance
2.5.5 Network Specification - security risk assessment	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
2.5.6 Network Specification - security Wi-Fi security	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
4.2.1 Maintenance issues - virus: sources (e.g. email, hacking, software install)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
4.2.2 Maintenance issues - virus: treatment (e.g. virus protection, firewall, security update)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

MAPPED TO MTA SECURITY FUNDAMENTALS 98-367 UNIT

	2.3.1 Password complexity	2.3.2 account lockout	2.3.3 password length	2.3.4 password history	2.3.5 time between password changes	2.3.6 enforce by using Group Policies	2.3.7 common attack methods	2.3.8 password reset procedures	2.3.9 protect domain user account passwords	2.4. Under-stand audit policies	2.4.1 Types of auditing	2.4.2 what can be audited	2.4.3 enable auditing	2.4.4 what to audit for specific purposes	2.4.5 where to save audit information	2.4.6 how to secure audit information
2.5.5 Network Specification - security risk assessment	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
2.5.6 Network Specification - security Wi-Fi security	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
4.2.1 Maintenance issues - virus: sources (e.g. email, hacking, software install)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
4.2.2 Maintenance issues - virus: treatment (e.g. virus protection, firewall, security update)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

MAPPED TO MTA SECURITY FUNDAMENTALS 98-367 UNIT

	2.5.1 Encrypting file system (EFS)	2.5.2 how EFS-encrypted folders impact moving/ copying files	2.5.3 BitLocker (To Go); TPM	2.5.4 software-based encryption	2.5.5 MAIL encryption and signing and other uses	2.5.6 virtual private network (VPN)	2.5.7 public key/ private key	2.5.8 encryption algorithms	2.5.9 certificate properties	2.5.10 certificate services	2.5.11 PKI/certificate services infrastructure	2.5.12 token devices	2.5.13 lock down devices to run only trusted applications
2.5.5 Network Specification - security risk assessment	X	X	X	X	X	X	X	X	X	X	X	X	X
2.5.6 Network Specification - security Wi-Fi security	X	X	X	X	X	X	X	X	X	X	X	X	X
4.2.1 Maintenance issues - virus: sources (e.g. email, hacking, software install)	X	X	X	X	X	X	X	X	X	X	X	X	X
4.2.2 Maintenance issues - virus: treatment (e.g. virus protection, firewall, security update)	X	X	X	X	X	X	X	X	X	X	X	X	X

MAPPED TO MTA SECURITY FUNDAMENTALS 98-367 UNIT

	2.6.1 Buffer overflow	2.6.2 viruses, polymorphic viruses	2.6.3 worms	2.6.4 Trojan horses	2.6.5 spyware	2.6.6 ransomware	2.6.7 adware	2.6.8 rootkits	2.6.9 backdoors	2.6.10 zero day attacks
2.5.5 Network Specification - security risk assessment	X	X	X	X	X	X	X	X	X	X
2.5.6 Network Specification - security Wi-Fi security	X	X	X	X	X	X	X	X	X	X
4.2.1 Maintenance issues - virus: sources (e.g. email, hacking, software install)	X	X	X	X	X	X	X	X	X	X
4.2.2 Maintenance issues - virus: treatment (e.g. virus protection, firewall, security update)	X	X	X	X	X	X	X	X	X	X

MAPPED TO MTA SECURITY FUNDAMENTALS 98-367 UNIT

3. Understand network security

	3.1.1 Types of hardware firewalls and their characteristics	3.1.2 when to use a hardware firewall instead of a software firewall	3.1.3 stateful vs. stateless firewall inspection	3.1.4 Security Compliance Manager	3.1.5 security baselines	3.2.1 Routing	3.2.2 honeypot	3.2.3 perimeter networks	3.2.4 network address translation (NAT)	3.2.5 VPN	3.2.6 Ipsec	3.2.7 server and domain isolation
2.5.7 Network Specification - security network security (e.g. firewall, MAC filtering)	X	X	X	X	X	X	X	X	X	X	X	X
4.2.1 Maintenance issues - virus: sources (e.g. email, hacking, software install)	X	X	X	X	X	X	X	X	X	X	X	X
4.2.2 Maintenance issues - virus: treatment (e.g. virus protection, firewall, security update	X	X	X	X	X	X	X	X	X	X	X	X
4.2.11 Maintenance issues - security settings (e.g. router, firewall)	X	X	X	X	X							

MAPPED TO MTA SECURITY FUNDAMENTALS 98-367 UNIT

	3.3.1 Protocol spoofing	3.3.2 Ipsec	3.3.3 tunnelling	3.3.4 DNSsec	3.3.5 network sniffing	3.3.6 denial-of-service (DoS) attacks	3.3.7 common attack methods
2.5.7 Network Specification - security network security (e.g. firewall, MAC filtering)	X	X	X	X	X	X	X
4.2.1 Maintenance issues - virus: sources (e.g. email, hacking, software install)	X	X	X	X	X	X	X
4.2.2 Maintenance issues - virus: treatment (e.g. virus protection, firewall, security update)	X	X	X	X	X	X	X

MAPPED TO MTA SECURITY FUNDAMENTALS 98-367 UNIT

4. Understand security software

	4.1.1 Antivirus	4.1.2 protect against unwanted software installations	4.1.3 User Account Control (UAC)	4.1.4 keep client operating system and software updated	4.1.5 encrypt offline folders	4.1.6 software restriction policies	4.1.7 principal of least privilege	4.2.1 Antispam, antivirus, spoofing, phishing, pharming; client vs. server protection	4.2.2 Sender Policy Framework (SPF) records	4.2.3 PTR records
2.5.6 Network Specification - security Wi-Fi security	X	X	X	X	X	X	X	X	X	X
2.5.7 Network Specification - security network security (e.g. firewall, MAC filtering)	X	X	X	X	X	X	X	X	X	X
4.2.1 Maintenance issues - virus: sources (e.g. email, hacking, software install)	X	X	X	X	X	X	X	X	X	X
4.2.2 Maintenance issues - virus: treatment (e.g. virus protection, firewall, security update)	X	X	X	X	X	X	X	X	X	X
4.2.9 Maintenance issues - security: security update	X	X	X	X	X	X	X			
4.2.10 Maintenance issues - security: security breach	X	X	X	X	X	X	X			
4.5.1 Software/Hardware updates - security updates				X						

MAPPED TO MTA SECURITY FUNDAMENTALS 98-367 UNIT

	4.3.1 Separation of services	4.3.2 hardening	4.3.3 keep servers updated	4.3.4 secure dynamic Domain Name System (DNS) updates	4.3.5 disable unsecure authentication protocols	4.3.6 Read-Only Domain Controllers (RODC)
2.5.6 Network Specification - security Wi-Fi security	X	X	X	X	X	X
2.5.7 Network Specification - security network security (e.g. firewall, MAC filtering)	X	X	X	X	X	X
4.2.1 Maintenance issues - virus: sources (e.g. email, hacking, software install)	X	X	X	X	X	X
4.2.2 Maintenance issues - virus: treatment (e.g. virus protection, firewall, security update)	X	X	X	X	X	X

The small print

We'd like to know your view on the resources we produce. By clicking on the 'Like' or 'Dislike' button you can help us to ensure that our resources work for you. When the email template pops up please add additional comments if you wish and then just click 'Send'. Thank you.

Whether you already offer OCR qualifications, are new to OCR, or are considering switching from your current provider/awarding organisation, you can request more information by completing the Expression of Interest form which can be found here: www.ocr.org.uk/expression-of-interest

Looking for a resource?

There is now a quick and easy search tool to help find **free** resources for your qualification:

www.ocr.org.uk/i-want-to/find-resources/

www.ocr.org.uk

OCR Customer Contact Centre

Vocational qualifications

Telephone 02476 851509
Facsimile 02476 851633
Email vocational.qualifications@ocr.org.uk

OCR is part of Cambridge Assessment, a department of the University of Cambridge. *For staff training purposes and as part of our quality assurance programme your call may be recorded or monitored.*

Cambridge Assessment

CERTIFIED ISO 9001 UKAS MANAGEMENT SYSTEMS 001