



T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Network Cabling

Assignment 1 - Distinction

Guide standard exemplification materials

T Level Technical Qualification in Digital Support Services Occupational specialism assessment

Guide standard exemplification materials

Network Cabling

Assignment 1

Contents

Introduction	3
Assignment 1	4
Scenario	4
Task 1:	6
Task 2:	18
Examiner commentary	22
Overall grade descriptors	22
Document information	25
Change History Record	25

Introduction

The material within this document relates to the Network Cabling occupational specialism sample assessment. These exemplification materials are designed to give providers and students an indication of what would be expected for the lowest level of attainment required to achieve a pass or distinction grade.

The examiner commentary is provided to detail the judgements examiners will undertake when examining the student work. This is not intended to replace the information within the qualification specification and providers must refer to this for the content.

In assignment 1, the student must design a new network for a doctors' surgery and provide a network diagram.

After each live assessment series, authentic student evidence will be published with examiner commentary across the range of achievement.

Assignment 1

Scenario

You are required to provide the network data installation for a doctors' surgery based in a small, single-storey building.

The building will comprise a reception area and 3 surgery rooms.

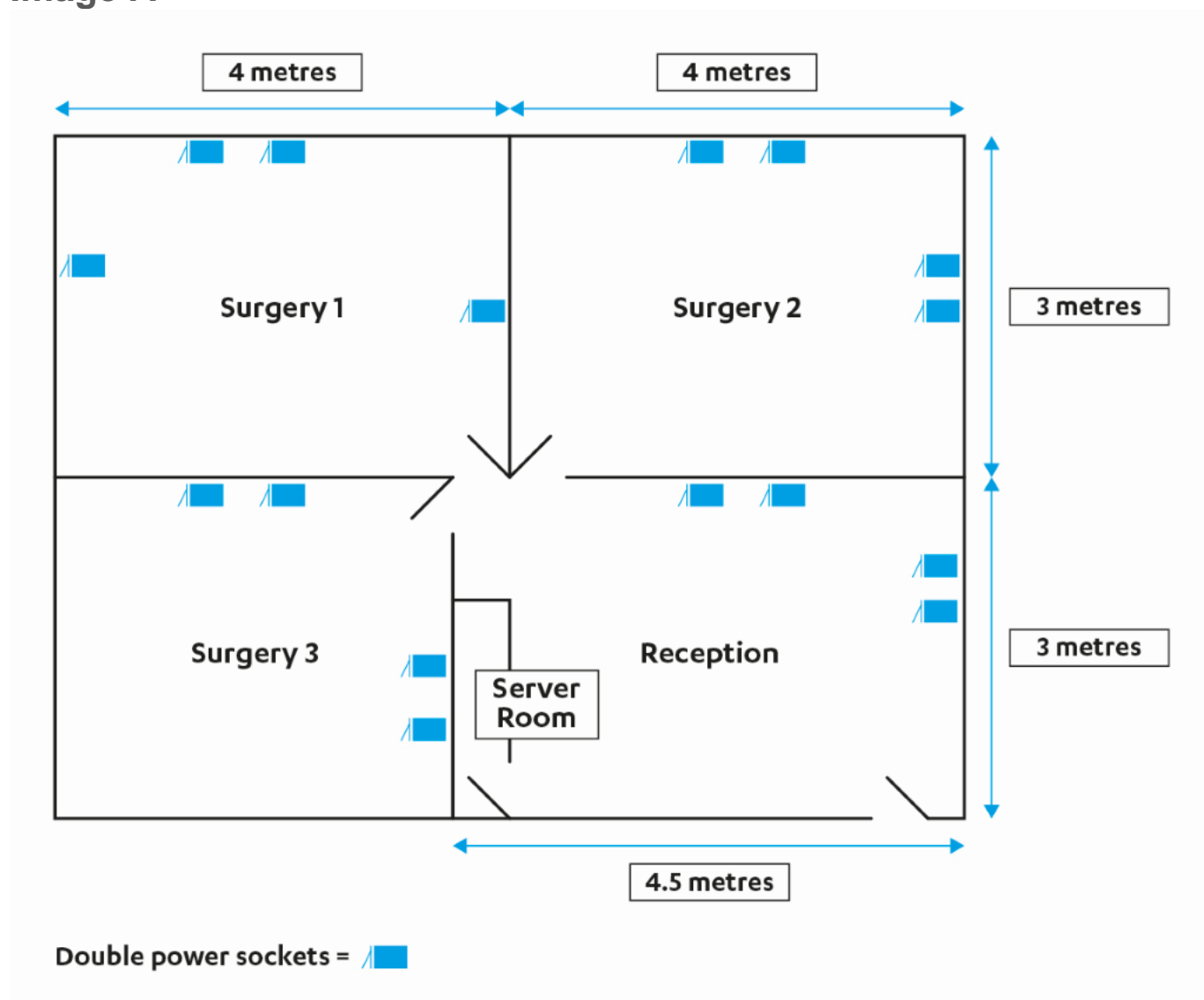
There is an ample supply of power sockets in each surgery room and the reception area.

The needs of the various users are:

- there are 6 doctors working in the practice and all will require access to the network at any time of the day
- doctors will need to be able to access digital medical records which will be stored separately from all other data
- doctors will need to be able to access the digital appointments system
- the 3 reception staff only require access to the booking system and must not have access to digital medical records
- the data server room will be located in the reception area
- all doctors and reception staff need access to a network printer

An outline plan of the surgery (image A) is provided on the next page.

Image A



Task 1: designing the new network

Time limit

8 hours

You can use the time how you want but all parts of the task must be completed within the time limit.

(40 marks)

You are required to produce a network design specification, including a diagram of the physical layout, for the proposed installation of the new network, and supporting rationale.

Your proposal should:

- show the physical layout for the network and proposals for containment/trunking, cable management and separation from power
- clearly state how many users will be able to access the network at any given time
- specify the types of data, for example, VoIP, email and web traffic, which will be transmitted across the network and where the data is stored
- name the required hardware which will allow network access and the specifications of this hardware
- specify how data will be transferred throughout the entirety of the network, either wired or wirelessly, and justify your selection for each choice
- describe the security measures which will be put in place to best ensure the integrity and 24-hour availability of the network and justify your reasons for selecting these measures
- explain the type of cable you have chosen, justifying why it is fit for the required purpose
- provide an estimate for the amount of cable required for the installation, based on the dimensions shown in the outline plan of the surgery
- add 10% to the length of cable you have calculated will be required, in anticipation of encountering obstacles to your cable run
- show how you have arrived at your estimation

You will have access to the following equipment:

- word processing software
- an appropriate diagramming tool

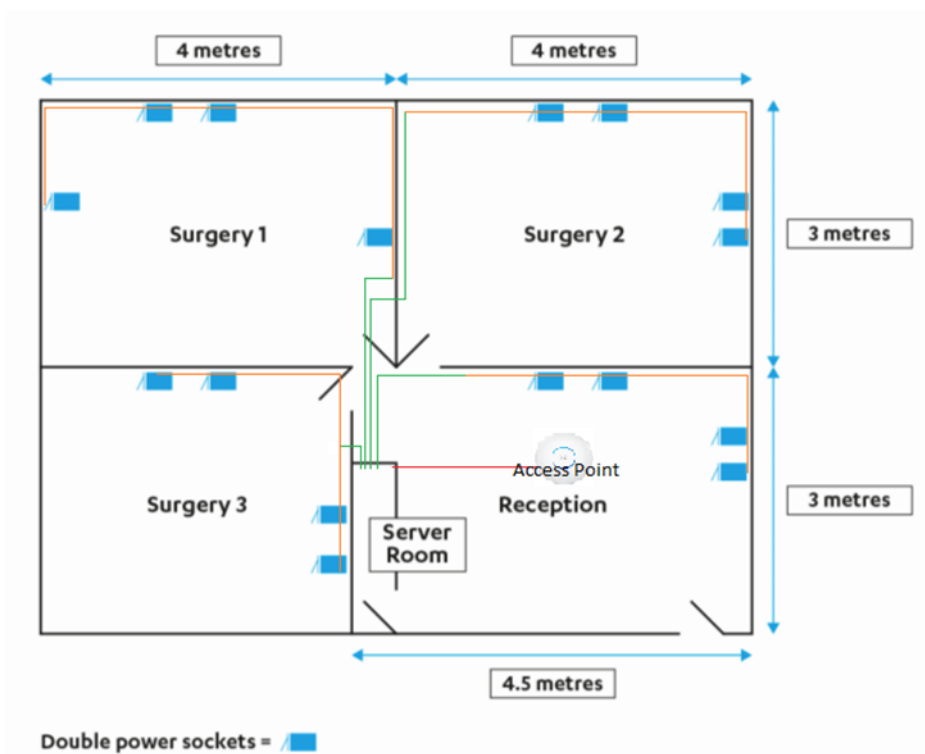
Evidence required for submission to NCFE

- a diagram of the physical network design with headings that clearly show your proposal for each of the points above, in .pdf format
- written justification for the design decisions you have made, where the task requires this

Student evidence

Proposed network diagram

Based on the requirements of the doctors' surgery, I propose the following network design:



In the above diagram:

A single cable (represented in red) will be located in the ceiling and run to the access point ceiling mounted in reception. Total = 2.5m including run to patch panel from ceiling.

Green represents 8 cables in a run. This totals approximately 64 metres of run within the ceiling, including runs from ceiling to patch panel and an additional 1.5m per cable to reach from ceiling to mid height trunking. 4 cable runs, with 8 cables per run, totals 48 metres of cable to get each cable from the ceiling to the mid height trunking. The ceiling run and ceiling to trunking run, represented by green, total to approximately 112m of cable.

Orange represents cable runs around the room where 2 cables are removed from the run and terminated in double network sockets next to each double power socket. In surgery 1, surgery 2 and reception, these orange lines start at 8 cables whereas in surgery 3, the cables split direction and each orange line starts at 4 cables.

Reception: 26m

Surgery 1: 34m

Surgery 2: 28m

Surgery 3: 20m

The total cable represented by orange, when taking into account the deduction of total cables represented by orange going down by 2 at each double power socket, is approximately 108m.

220 metres of network lead required.

Summary of hardware required:

- 1 x access point
- 1 x 48 port switch
- 1 x router/firewall
- 2 x 24 port patch panel
- 1 x network printer
- 16 x double gang network sockets and surface mount wall boxes
- 1 x single gang network socket and surface mount wall box

33 total network ports required.

Hardware and materials required

The cable chosen was CCS Cat6 FTP LSOH solid core cable. This cable is category 6, giving capability of 1Gbps speeds for up to 100 metres and 10Gbps for the first 55 metres. As no cable run is longer than 55 metres, this means the full 10Gbps is available and future proofs the doctors' surgery. The cable comes in 305m reels for £118.68, including the VAT, so is very affordable.



The cable is also S/FTP; this specification provides us with shielded cabling and foiled twisted pairs. Although more expensive, the advantage here is to avoid any possible electromagnetic fields (EMFs) as the most efficient routes for the network cabling may have long parallel runs next to power cables.

The cable is also low smoke zero halogen (LSOH). Although not a requirement specifically, this does have the added benefit of being less of an issue in the case of a fire within the doctors' surgery, leading to a safer network install.

After planning out the cable runs, there will be a requirement for 220 metres of network cable. To cover for unexpected obstacles, an additional 10% will be added, totalling 242 metres of cable. There will be 63 metres of spare cable from the reel, ensuring that any faulty cable runs can be easily replaced and there is enough cable left for any future additional runs.

Assuming the surgery has a suspended ceiling, like many commercial buildings, trunking is only required for runs down the wall to the wall sockets as most of the cable run will be hidden in the ceiling. The chosen trunking size is 25mm x 16mm with pre-applied sticky back tape for easy installation. This trunking size was chosen as it can easily fit several network leads for areas where double gang network face plates may be used. The trunking can be purchased in 2m lengths which can be shortened where necessary, to cover the surgery and to allow for unforeseen obstacles. 6 metres are required so 10 metres should be purchased to account for mistakes or obstacles.

To utilise the trunking and to avoid requiring any work done to the walls to bury cables and flush mount boxes, the RJ45 face plates will be mounted to surface mount wall boxes. This drastically reduces the amount of time required for the installation of cables and gives future access to the cabling if it was to be changed. A double gang network face plate will be required for every double power socket to ensure any rearrangements of the surgery in the future will not be hindered by the placement of network sockets. For this to be achieved, there will need to be 16 double gang network face plates and double gang surface mount back boxes. There will also be a need for 1 single gang network face plate to be mounted on a single gang surface mount wall box for the access point at ceiling height.

For the printer, I chose the HP OfficeJet Pro 9022 due to its wired and wireless capabilities and small form factor due to the lack of available room for a large multi-function device (MFD). This allows for the printer to be located where deemed most suitable by the staff without restrictions being imposed by the network only availability of power sockets. The OfficeJet Pro 9022 can be purchased for £200 to £220 depending on the supplier, however, the main disadvantage of a printer like this is the cost of the ink. A larger more commercial printer would be far cheaper on ink, however the low initial purchase cost of this and general low level of use makes this still a more cost effective purchase than a larger commercial printer which often require long leases rather than being purchased out right.



The patch panels chosen are the Kenable patch panels in the 24-port variety. 2 of these patch panels will be required for the capacity of ports being placed in the surgery. These patch panels were chosen as they do not require direct termination but instead have the cable end terminated in a RJ45 head to be plugged into the back of the patch panel. This allows for easy management and reusability of the rear of the patch panel. These patch panels are also Cat6 compliant.



As for the networking hardware, I chose to use Ubiquiti UniFi products for the entire network as they produce enterprise grade equipment which does not require a continuous costly license to operate within the network. All products chosen are capable of 10/100/1000 networking.

The router chosen is the UniFi Unified Security Gateway. This router is capable of gigabit networking and has several features which can be utilised by the surgery; this includes a built-in firewall, intrusion prevention and VPN capabilities for remote working. The Unified Security Gateway also offers QoS for enterprise VoIP, ensuring low latency and uninterrupted calls during heavy internet usage times.

If the Unified Security Gateway is to be rack mounted and not wall mounted, the rack mount bracket will need to be purchased separately.

A modem, if required, is generally supplied by the internet service provider. The UniFi Security Gateway does not have a built in modem so if the surgery has a fibre connection, the supplied modem will need to be used in conjunction with the Unified Security Gateway.

Below is the specification from the Unified Security Gateway datasheet ([UniFi Security Gateway datasheet \(ubnt.com\)](https://www.ubnt.com/unifi-security-gateway-datasheet)):

UniFi USG	
Dimensions	135 x 135 x 28.3 mm (5.32 x 5.32 x 1.11")
Weight	366 g (12.9 oz)
Max. Power Consumption	7W
Power Supply	12VDC, 1A Power Adapter (Included)
Power Input	9 to 24VDC, Supported Voltage Range
LEDs	Status
System	Power
Serial Console Port	Speed/Link/Activity
Data Ports	
Networking Interfaces	
Serial Console Port	(1) RJ45 Serial Port
Data Ports	(3) 10/100/1000 Ethernet Ports*
Layer 3 Forwarding Performance	
Packet Size: 64 Bytes	1,000,000 pps
Packet Size: 512 Bytes or Larger	3 Gbps (Line Rate)
Processor	Dual-Core 500 MHz, MIPS64 with Hardware Acceleration for Packet Processing
System Memory	512 MB DDR2 RAM
On-Board Flash Storage	2 GB
Certifications	CE, FCC, IC
Wall-Mountable	Yes
Operating Temperature	-10 to 45° C (14 to 113° F)
Operating Humidity	10 to 90% Noncondensing

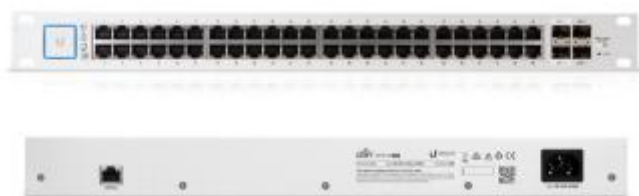
* VOIP port is available for port remapping in UniFi v5.



The switch chosen is a Unifi US-48-500W. This switch has many more ports than required; however, this will allow for any future expansions to the surgery in size, staff or equipment. The switch also has Power over Ethernet (POE) capabilities, allowing it to power the VoIP phones and access points.

Model: US-48-500W

- (48) Gigabit RJ45 Ports
- (2) SFP+ Ports
- (2) SFP Ports
- (1) Serial Console Port
- Non-Blocking Throughput: 70 Gbps
- Switching Capacity: 140 Gbps
- Forwarding Rate: 104.16 Mpps
- Maximum Power Consumption: 500W
- Supports PoE+ IEEE 802.3at/af and 24V Passive PoE
- Rack-Mountable



Below is the specification from the UniFi switch datasheet ([UniFi Security Gateway datasheet \(ubnt.com\)](https://www.ubnt.com/docs/default-source/unifi-us-48-500w-datasheet.pdf))

The access points chosen are the UniFi AP-AC-PRO as these offer the level of security required as well as high performance wireless capabilities. They offer wireless AC at 2.4 GHz and 5.0 GHz with the ability to manage the device within the UniFi management portal. At the time of creating this specification, the UniFi 6 range (utilising WiFi 6) is currently pre-order only and may be a consideration for future upgrading. For now, however, the AP-AC-PRO will far exceed the needs of the surgery.

Below is the specification from the UniFi AP datasheet ([UniFi AC AP datasheet \(ubnt.com\)](https://www.ubnt.com/docs/default-source/unifi-ap-datasheet.pdf)):

UAP-AC-PRO	
Dimensions	196.7 x 196.7 x 35 mm (7.74 x 7.74 x 1.38")
Weight	350 g (12.4 oz)
With Mounting Kits	450 g (15.9 oz)
Networking Interface	(2) 10/100/1000 Ethernet Ports
Port	(1) USB 2.0 Port
Buttons	Reset
Power Method	Passive Power over Ethernet (48V), 802.3af/802.3at Supported (Supported Voltage Range: 44 to 57VDC)
Power Supply	UniFi Switch (PoE)
Power Save	Supported
Maximum Power Consumption	9W
Maximum TX Power	
2.4 GHz	22 dBm
5 GHz	22 dBm
Antennas	(3) Dual-Band Antennas, 2.4 GHz: 3 dBi, 5 GHz: 3 dBi
Wi-Fi Standards	802.11 a/b/g/n/r/k/v/ac
Wireless Security	WEP, WPA-PSK, WPA-Enterprise (WPA/WPA2, TKIP/AES)
BSSID	Up to 8 per Radio
Mounting	Wall/Ceiling (Kits Included)
Operating Temperature	-10 to 70° C (14 to 158° F)
Operating Humidity	5 to 95% Noncondensing
Certifications	CE, FCC, IC

Advanced Traffic Management	
VLAN	802.1Q
Advanced QoS	Per-User Rate Limiting
Guest Traffic Isolation	Supported
WMM	Voice, Video, Best Effort, and Background
Concurrent Clients	250+

Supported Data Rates (Mbps)	
Standard	Data Rates
802.11ac	6.5 Mbps to 1300 Mbps (MCS0 - MCS9 NSS1/2/3, VHT 20/40/80)
802.11n	6.5 Mbps to 450 Mbps (MCS0 - MCS23, HT 20/40)
802.11a	6, 9, 12, 18, 24, 36, 48, 54 Mbps
802.11g	6, 9, 12, 18, 24, 36, 48, 54 Mbps
802.11b	1, 2, 5.5, 11 Mbps



An additional piece of hardware required is the UniFi Cloud Key. This is required to manage the UniFi products, allowing for their configuration, management and monitoring on-site and remotely via the UniFi cloud portal. An additional rack mount can be purchased for this device.



The number of users capable of using the network, according to UniFi documentation, would be 45 to 50 due to the limitation of the UniFi Security Gateway. The other UniFi devices are capable of over 200 users. This bottleneck of 45 to 50 users is still beyond the requirements of the surgery which consists of 9 users in total on the network, if all staff are present. Each member of staff having their own wired network device and VoIP phone would result in a total of 18 devices. Even with the lower limit of 45 potential clients, there is still enough capability for the additional network devices, the printer, and the access points, as well as spare capacity for a guest wireless network.

Product summary table

Item	URL	Price (inc VAT)
Cabling	Cat6 FTP Shielded PVC Solid Cable Cat6 Cable (cablemonkey.co.uk)	£118.68
Printer	HP OfficeJet Pro 9025 Wireless All-in-One Color Printer - HP Store UK	£235
Patch panels	kenable 24 Port RJ45 CAT6 Gigabit Through Coupler Patch: Amazon.co.uk: Electronics	£28.03
Router/firewall	Ubiquiti UniFi USG Enterprise Security Gateway Broadband Router (broadbandbuyer.com)	£109.30
Switch	Ubiquiti US-48-500W UniFi 48-Port Layer 2 Managed Gigabit PoE+ Switch w/ 2 x 1GbE SFP Ports & 2 x 10GbE SFP+ Ports (500W) (broadbandbuyer.com)	£710.33
Access point	Ubiquiti UAP-AC-PRO UniFi WiFi 5 PoE Access Point, Indoor/Outdoor (1750Mbps AC) Inc Injector (broadbandbuyer.com)	£131.38
Cloud Key	Ubiquiti UCK-G2 UniFi Cloud Key Gen2 (broadbandbuyer.com)	£164.50
Total		£1497.22

A large benefit of the Ubiquiti equipment over other similar enterprise manufacturers, such as Cisco Meraki, is the quality of the hardware for the cost is very good and unlike their main competitors, they do not require a license to run and manage their products. This means the choice to use their equipment has a year on year saving. All Ubiquiti equipment also comes with support free of charge.

Data transmission

There are many different types of data which will be transmitted across the network both to other internal devices and externally.

VoIP data – UDP traffic – calls from end user VoIP devices to a phone system. This form of traffic will only be on the wired network as there are no wireless VoIP phones within the surgery. This data will be transmitted from each VoIP phone to the switch, then to the on-site phone system or cloud-based phone system.

HTTP/HTTPS data – TCP – all websites visited within the network using the HTTP/HTTPS protocol. This will also be the protocol used for most of the surgery's web-based applications. This data will be present on both the wired and wireless network depending on the devices being used.

SMTP – UDP and TCP – all mail sent uses port 25, so this will need to be left open on the firewall. The surgery machines are all wired so all email communication will be transmitted on the wired network from PCs to the cloud-based mail server.

DHCP requests will be made from all devices that do not have a static IP address. These requests will be handled by the DHCP server and will occur on both the wired and wireless network.

Security measures

There are many physical and digital security measures which can be taken to ensure security of the devices and the data.

Physical security

CCTV can be installed to monitor key areas for the safety of people within and outside of the building, as well as acting as a deterrent to potential thieves or vandals who may intend to damage or steal the surgery's equipment.

Keypad entry can be installed on the server room door to have controlled access to the networking equipment within the surgery. This can be limited to specific members of the team to avoid any unauthorised access. Access should be limited to this room as access to these devices could lead to a loss of data or connectivity if handled incorrectly or configuration maliciously altered.

Using kensington locks on equipment that is portable or easy to lift and attaching it to walls or through desks will reduce the chance of theft of important equipment, such as equipment required for connectivity or access to the network.

Different types of alarm systems should be considered, such as an alarm system to protect from break-ins which may result in theft of important networking equipment and other devices, as well as a fire suppression system. For the server room, there are fire suppression systems, such as an inert gas system, which reduces the oxygen in the room to extinguish a fire without causing harm to the equipment.

Disaster recovery plans should be put in place which detail the different possible risks to the infrastructure and the specific process to overcome these disasters once they occur, to reduce the time and cost of regaining connectivity and core systems.

Digital security measures

The router chosen has a built-in firewall which removes the need to implement a dedicated separate firewall. The router's built-in firewall can be used in conjunction with its automatic intrusion detection and prevention system to block specific devices, IP addresses, protocols and ports from communicating from within the network to external locations or vice versa. No devices will be located within the demilitarized zone (DMZ), so all devices will be protected by the firewall.

Each of the surgery's end devices, PCs and laptops should have enterprise level malware protection installed. Recommendations which could be considered are Sophos Endpoint Protection or ESET Security. These programs offer a level of security to protect devices from malware infections and ransomware attacks, which will protect the surgery's data from loss, damage or theft from malicious software.

As well as using the router's firewall, the built-in Windows Defender Firewall can also be configured to further protect devices, offering firewall protection per machine which can be customised where appropriate. The Windows Defender Firewall can be used to block specific applications or ports from communicating on the network. This can be made even more effective by whitelisting only the allowed applications and blocking all other applications. As there is no cost in using the Windows Defender Firewall, just a small amount of configuration time, it is a big increase to security for next to no cost.

For data integrity and to avoid data loss, secure off-site backups could be considered, taking file level backups throughout the day. These backups could be made to a cloud hosted backup service or to an off-site building related to the surgery.

To ensure the security of the wireless communication between devices and the access point, WPA2-PSK will be utilised to secure the connection and the wireless key will not be kept in sight of clients. The key will be suitably complex with a combination of uppercase and lowercase letters, numbers and symbols.

MAC address filtering can also be utilised to specifically limit what devices can connect to the network, reducing the chance of a device being connected to the network which is unknown to the Doctors Surgery. Although there are ways to circumvent MAC address filtering, it will stop more low-level attempts to get a device on the network. MAC address filtering is often not implemented as it can be time consuming to maintain however the small number of devices that will be used on the doctor's surgery means it would not be out of the question to implement if required.

WPA2/PSK has been implemented currently which has a strong level of encryption and is more than suitable for the current setup, this can be improved in the future with WPA3 once it is more widely adopted by larger vendors as currently UniFi access points do not support it and it is only in the beta branch of their firmware. This will further increase the protection of their wireless data transmissions.

Task 2: creating the network diagram

Time limit

5 hours

You can use the time how you want but all parts of the task must be completed within the time limit.

(20 marks)

Using Cisco Packet Tracer, you are required to produce a network diagram of the logical network layout for the doctors' surgery. Your network diagram should clearly show all devices and connection points which make up the network.

Your diagram screenshots and accompanying documentation should evidence:

- all resources/components identified to meet requirements in task 1
- identification of each component on the network, demonstrating how they are connected
- the IP addressing structure, evidenced by detailing the IP addressing and subnetting scheme, and how this will be applied to each networked component
- details of the security measures implemented
- how all components on the network work together

You will have access to the following equipment:

- word processing software
- Cisco Packet Tracer

Evidence required for submission to NCFE

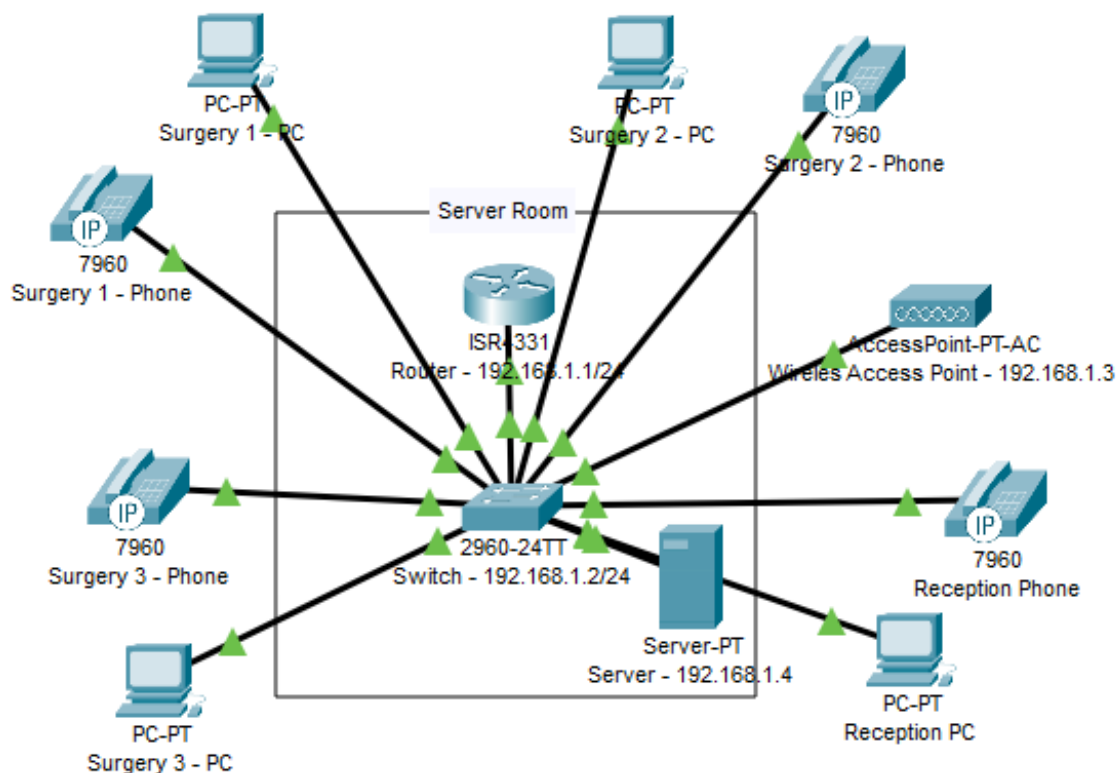
- screenshots of your logical network diagram which demonstrate how the network is configured
- a word-processed description of how all components on the network work together, in .pdf format

Student evidence

As there is only a small amount of networking equipment required and only a small number of users, an IP 192.168.1.0 with a subnet mask of 255.255.255.0 is more than suitable. It allows for the single network to have usable addresses. Some of these addresses will be statically assigned/reserved and a majority will be left in the DHCP pool to be used by clients on the network.

IP addresses	Usage
192.168.1.1	Router/gateway
192.168.1.2	Switch
192.168.1.3	Access point
192.168.1.4	Server
192.168.1.5–10	Reserved for any potential future network equipment
192.168.1.11–254	DHCP pool for client addresses

The network design demonstrates the connectivity of devices in the surgery:



The server is configured as a DHCP server to complete DHCP requests made by devices on the network. All devices communicate via the switch unless access to resources outside of the network are required, then the router is utilised.

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 192.168.1.1

DNS Server: 192.168.1.4

Start IP Address: 192 168 1 11

Subnet Mask: 255 255 255 0

Maximum Number of Users: 245

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168.1.1	192.168.1.4	192.168.1.11	255.255.255.0	245	0.0.0.0	0.0.0.0

The switch has a password set to enable user level. The password has been encrypted and for additional security has had Telnet connectivity disabled and secure shell (SSH) connectivity enabled. This is due to the poor security of Telnet as it is not encrypted.

```

service password-encryption
!
hostname Switch
!
enable password 7 08071F45031F553D3C253E56783B257578
!

```

The access point has been configured with WPA2-PSK security with a complex password. This is to ensure the secure communication with wireless devices and is far more secure than the other options for securing the wireless connection that are available on this access point. The key has also been made sufficiently complex to avoid it being easy brute-forced.

Port 1

Port Status: ☒ On

SSID: Default

2.4 GHz Channel: 36

5 GHz Channel: 36

Coverage Range (meters): 140.00

Authentication:

☐ Disabled ☐ WEP ☒ WPA-PSK ☐ WPA2-PSK

WEP Key:

PSK Pass Phrase: TfjkRF12%%3fka!@fasFF

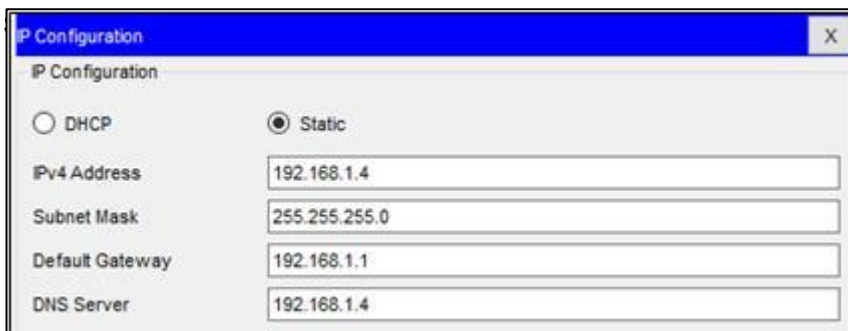
User ID:

Password:

Encryption Type: AES

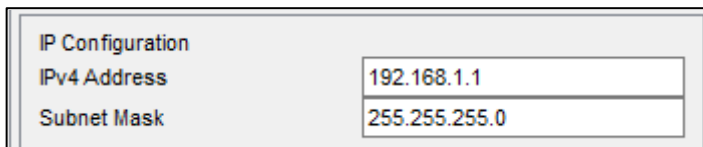
Whilst WPA2/PSK is not completely secure, it gives a good balance of security against disadvantages. Due to its limitations, if someone has got access to the key, they could share it with someone, or if a staff member leaves then they could continue to access the network. One option to consider would be to enable MAC address filtering at the switch, this would allow only specific devices to be usable on the network and prevent anyone accessing the network who should not have access.

The IP addresses, the PCs and the phones have been configured to utilise DHCP for their configuration. The router, switch, access point and server are all statically assigned.



The screenshot shows a window titled "IP Configuration" with a close button (X) in the top right corner. Inside the window, there is a section labeled "IP Configuration". Below this, there are two radio buttons: "DHCP" and "Static". The "Static" radio button is selected. Below the radio buttons, there are four text input fields with the following values: "IPv4 Address" is "192.168.1.4", "Subnet Mask" is "255.255.255.0", "Default Gateway" is "192.168.1.1", and "DNS Server" is "192.168.1.4".

Router static IP address configuration



The screenshot shows a window titled "IP Configuration". Inside the window, there are two text input fields: "IPv4 Address" with the value "192.168.1.1" and "Subnet Mask" with the value "255.255.255.0".

Switch static IP address configuration

```
interface Vlan1
ip address 192.168.1.2 255.255.255.0
shutdown
!
ip default-gateway 192.168.1.1
```

The router has been configured with a basic firewall to ensure traffic in and out is from approved sources and network traffic types. The configuration is very bare and will be updated while in use to ensure more restriction without impacting productivity. Once fully configured to the doctors' surgery requirements, only specific protocols will be allowed to inbound and outbound of the network and, where appropriate, some security can be applied on the firewall for inbound and outbound IP addresses as well.

Examiner commentary

The student has earned a distinction due to having demonstrated a significantly higher level of knowledge and ability to apply this to the scenario.

They have specified precisely which hardware they have chosen and explained why they selected each piece. The hardware that they have selected is not only fit for choice, but it is also suitable for upgradability in the future.

The student has gone further and identified potential purchase locations and prices, demonstrating good research skills and being able to apply this to a real-world scenario.

One area for improvement would be to review and summarise the information from the research rather than simply stating it and being able to translate this information into non-technical speak for the client (for example, explaining the benefits and USPs to a client).

A range of effective security solutions are described and are relevant to the scenario, realistic to implement and have had some explanation.

The network diagram is clear and the configuration would be functional with the IP addresses clear. Static IP addresses have been assigned for vital pieces of network equipment. Evidence is shown of the key parts of the network setup. An appropriate level of security has been implemented or described. There are areas of the configuration which have been mentioned that have not been evidenced; evidencing these would further improve this submission. There are other less obvious security measures which could be taken to show higher-level thinking, such as downing the ports that are not in use and MAC address filtering on the wireless connection, or discussing why these security measures were not implemented.

Overall grade descriptors

The performance outcomes form the basis of the overall grading descriptors for pass and distinction grades.

These grading descriptors have been developed to reflect the appropriate level of demand for students of other level 3 qualifications and the threshold competence requirements of the role, and have been validated with employers within the sector to describe achievement appropriate to the role.

Occupational specialism overall grade descriptors:

Grade	Demonstration of attainment
Distinction	The evidence is logical and provides an excellent response to the demands of the brief
	Makes use of relevant knowledge and is well-informed by the practices of the sector
	Demonstrates an understanding of the different perspectives/approaches associated within the sector
	Makes excellent use of facts/theories/approaches/concepts
	Demonstrates comprehensive use of breadth and depth of knowledge and understanding

	Consistently selects appropriate skills/techniques/methods
	Identifies information from a range of suitable sources and makes use of appropriate Information/appraises relevancy of information
	Combines information to make accurate and appropriate decisions
	Makes sound judgements/takes appropriate action/seek clarification and guidance
	Successfully tackles both routine and non-routine problems that reflect real life situations in the sector
	Effectively demonstrates skills and knowledge of the relevant concepts and techniques reflected in the sector, applied across a variety of contexts
	Tackles unstructured problems that have not been seen before, using their knowledge to analyse and find suitable solutions to the problems
	Analyses data/information in context and applies appropriate analysis in confirming or refuting conclusions and carrying out further work to evaluate conclusions
	Justifies strategies for solving problems, giving <u>clear</u> explanations for their reasoning
Pass	The evidence is logical and a good response to the demands of the brief
	Makes use of relevant knowledge and is generally informed by the practices of the sector
	Demonstrates an understanding of some perspectives or approaches associated within the sector
	Makes good use of facts/theories/approaches/concepts
	Demonstrates breadth and depth of knowledge and understanding
	Generally selects appropriate skills/techniques/methods
	Identifies information from appropriate sources
	Makes use of appropriate information/appraises relevancy of information
	Combines information to make accurate decisions
	Makes generally sound judgements/takes appropriate action/seek clarification and guidance
	Successfully tackles routine problems and makes some progress on solving non-routine problems in real life situations
	Demonstrates most skills and knowledge of the relevant concepts and techniques reflected in the

	sector, applied across different contexts
	Makes some progress on unstructured problems that have not been seen before, using their knowledge to find solutions to problems
	Makes some justification for strategies for solving problems, giving explanations for their reasoning

* threshold competence refers to a level of competence that:

- signifies that a student is well placed to develop full occupational competence, with further support and development, once in employment
- is as close to full occupational competence as can be reasonably expected of a student studying the TQ in a classroom-based setting (for example, in the classroom, workshops, simulated working and (where appropriate) supervised working environments)
- signifies that a student has achieved the level for a pass in relation to the relevant occupational specialism component

U grades

If a student is not successful in reaching the minimum threshold for the core and/or occupational specialism component, they will be issued with a U grade.

Document information

The T Level Technical Qualification is a qualification approved and managed by the Institute for Apprenticeships and Technical Education.

Copyright in this document belongs to, and is used under licence from, the Institute for Apprenticeships and Technical Education, © 2020-2021.

'T-LEVELS' is a registered trade mark of the Department for Education.

'T Level' is a registered trade mark of the Institute for Apprenticeships and Technical Education.

'Institute for Apprenticeships & Technical Education' and logo are registered trade marks of the Institute for Apprenticeships and Technical Education.

Owner: Head of Assessment Design

Change History Record

Version	Description of change	Approval	Date of Issue
v1.0	Published final version.		May 2021
v1.1	NCFE rebrand		September 2021