T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Network Cabling

Assignment 1 - Distinction

Guide standard exemplification materials

v2.1: Specimen assessment materials
12 December 2024
603/6901/2

Internal reference: DSS-GSEM-09

T Level Technical Qualification in Digital Support Services
Occupational specialism assessment

Guide standard exemplification materials

Network Cabling

Assignment 1

Contents

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.

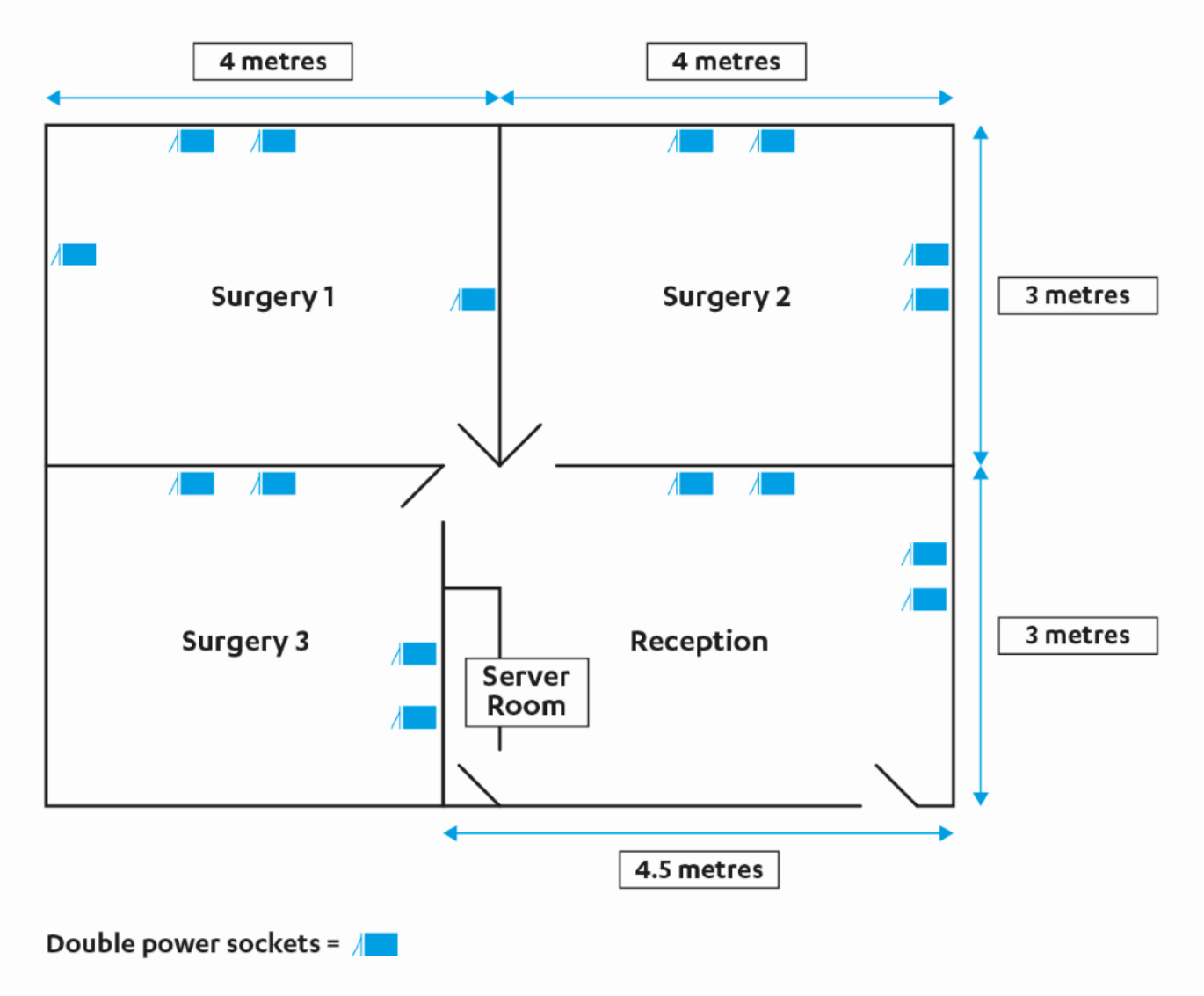
There is an ample supply of power sockets in each surgery room and the reception area.

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


4 metres
4 metres
Surgery 1
Surgery 2
3 metres
Surgery 3
Server Room
Reception
3 metres
4.5 metres
Double power sockets =

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

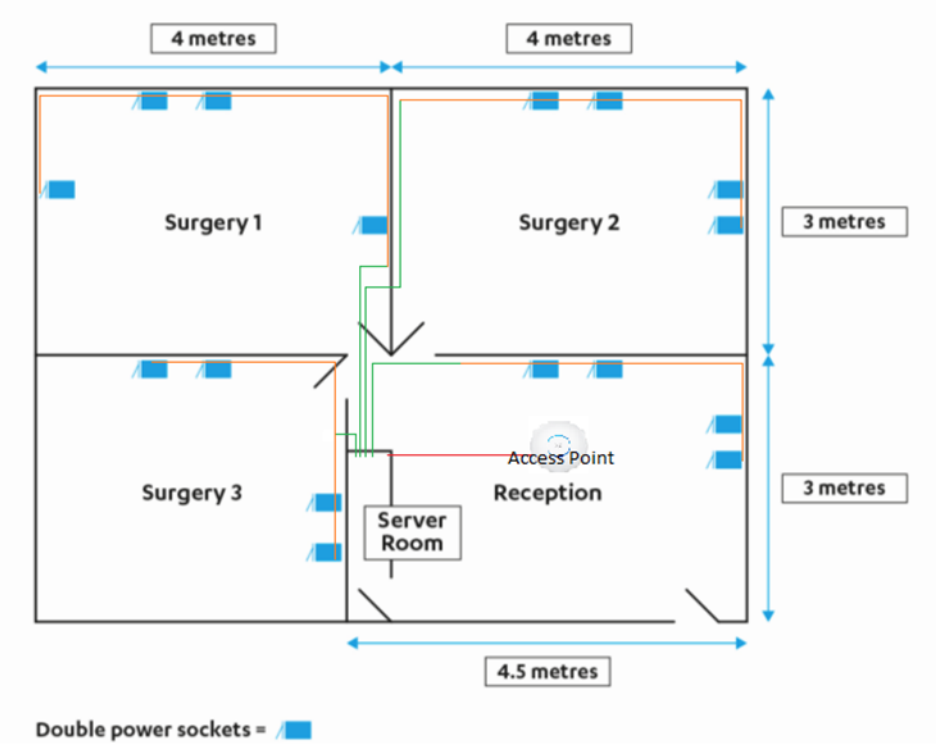
Evidence required for submission to NCFE

- 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 dedication 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 ideal cable chosen would be Cat6 FTP LSOH solid core cable. This cable should be category 6, giving capability of 1Gbps speeds for up to 100 metres and faster for smaller cable runs. As no cable run is longer than 55 metres, this means that faster speeds would be available and would future proofs the doctors' surgery.

Ideally the cable would be S/FTP as this would provide them 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.

Ideally the cable would also be 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. As a reel of cabling is typically 305m, if this was purchased there would 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 would choose an inkjet printer that supports both wired and wireless capabilities. It should also be 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. A disadvantage with this type of printer is going to be the cost of the ink. A larger more commercial printer would be far cheaper on ink; however the low initial purchase cost of an inkjet printer would still make this a more cost effective purchase. Larger commercial printers can often require long leases rather than being purchased outright.

The patch panels chosen would be 24-port. Two of these patch panels will be required for the capacity of ports being placed in the surgery. Ideally the patch panels chosen would 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 should also be Cat6 compliant.

As for the networking hardware, I would recommend choosing one main supplier, for example Ubiquiti UniFi, for the entire network as they produce enterprise grade equipment. All products chosen should be capable of 10/100/1000 networking.

The router chosen should be capable of gigabit networking and have features which can be utilised by the surgery, for example a built-in firewall, intrusion prevention and VPN capabilities for remote working.

If anything requires rack or wall mounting this will need to be purchased separately.

A modem, if required, is generally supplied by the internet service provider and will need to be used in conjunction with the hardware purchased.

I would recommend a switch with at least 48 ports as this will allow for any future expansions to the surgery in size, staff or equipment. The switch should ideally have Power over Ethernet (POE) capabilities, allowing it to power the VoIP phones and access points.

The wireless access points chosen should offer the best level of security required as well as high performance wireless capabilities. They should offer wireless AC at 2.4 GHz and 5.0 GHz with the ability to manage the device through an online management portal.

Depending upon the network equipment selected additional hardware may be required to support the management, configuration and on-site / remote monitoring of the network.

Other considerations would be the number of users accessing the network. Based on the scenario the surgery consists of nine users in total on the network if all the staff are present at the same time. Each member of staff having their own wired network device and VoIP phone would result in a total of 18 devices. Based on this low number of staff the equipment recommended would provide enough capability for additional network devices if required, the printer, the wireless access points, as well as spare capacity for a guest wireless network if required at a late date.

Product summary table

Item	Approx lower price range	Approx higher price range
Cabling	£100	£150
Trunking and plates	£250	£500
Printer	£150	£250
Patch panels	£25	£40
Router/firewall	£100	£150
Switch	£500	£1000
Access point	£100	£150
Additional monitoring hardware	£100	£300
Approximate total	£1325	£2540

A large benefit of the Ubiquiti equipment over other similar enterprise manufacturers, such as Cisco, 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.

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 should have 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 built in 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 should have enterprise level malware protection installed. 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 end user 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 approve listing only the allowed applications and block listing 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.

Although we-mention WPA2/PSK being 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 will further increase the protection of their wireless data transmissions

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.

.

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

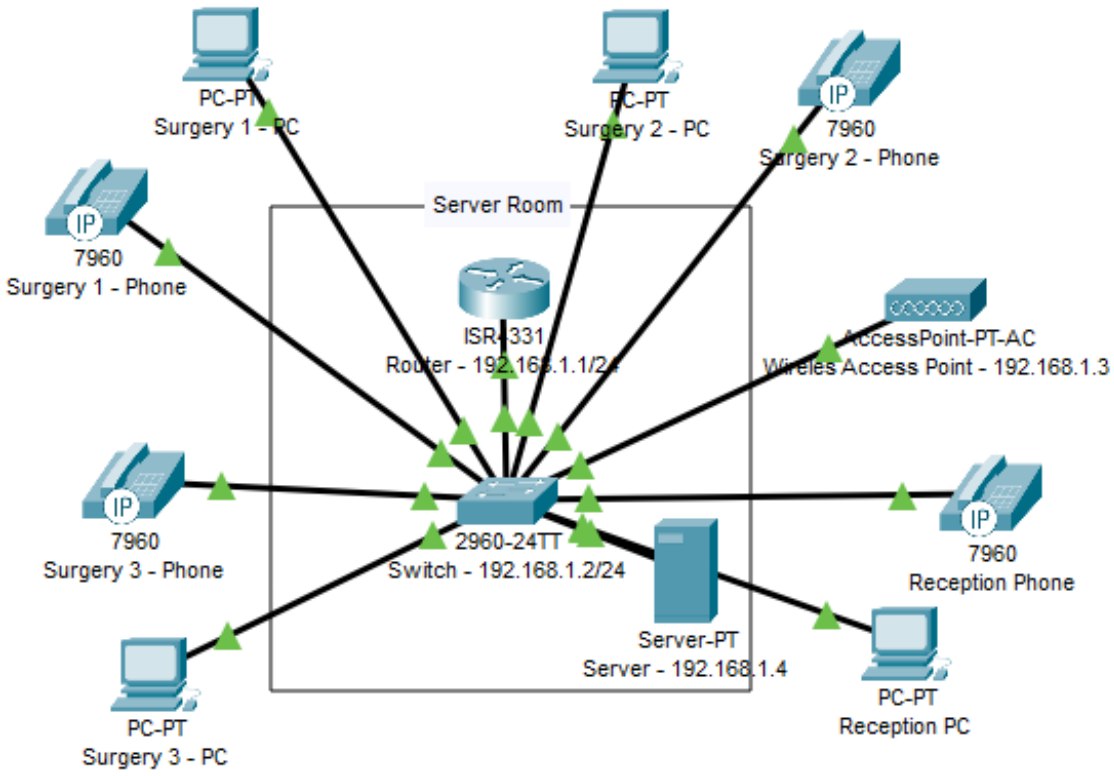
- screenshots of your logical network diagram which demonstrate how the network is configured
- a word-processed description of how all components on the network work together, in .pdf format

Student evidence

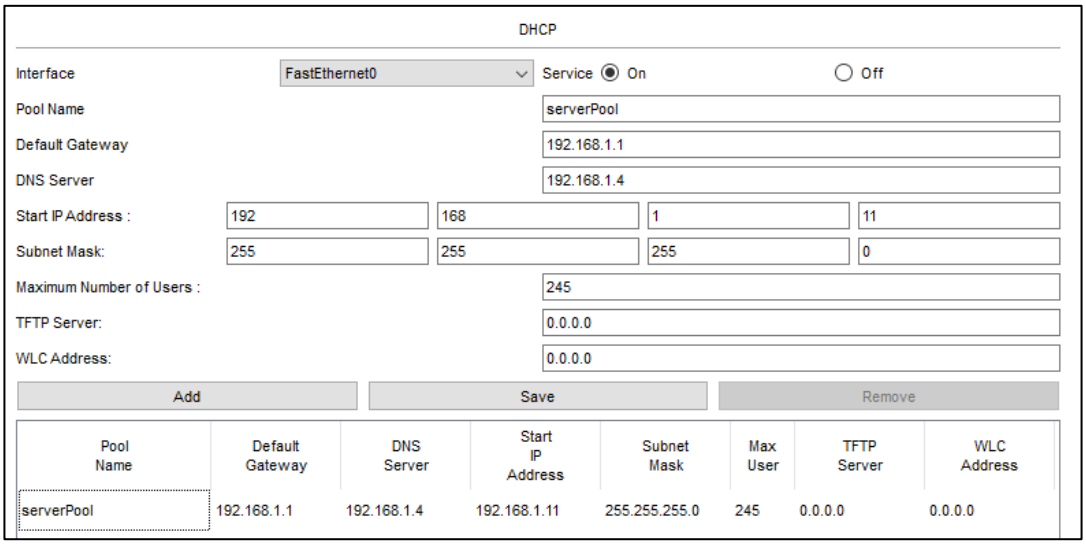
As there is only a small amount of networking equipment required and only a small number of users, an IP 192.168.1.0 with a subnet mask of 255.255.255.0 is more than suitable. It allows for the single network to have usable addresses. Some of these addresses will be statically assigned/reserved and a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

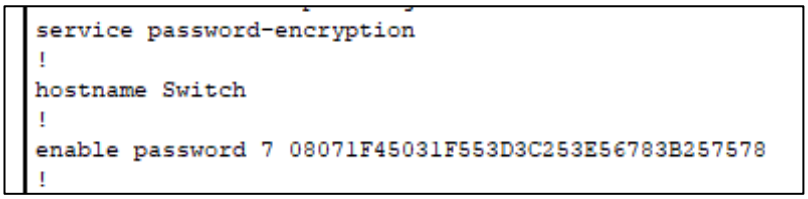
The network design demonstrates the connectivity of devices in the surgery:



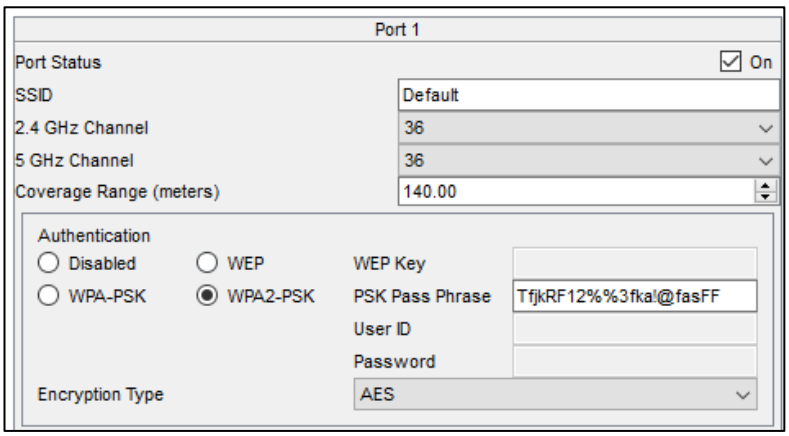
The server is configured as a DHCP server to complete DHCP requests made by devices on the network. All devices communicate via the switch unless access to resources outside of the network are required, then the router is utilised.



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.



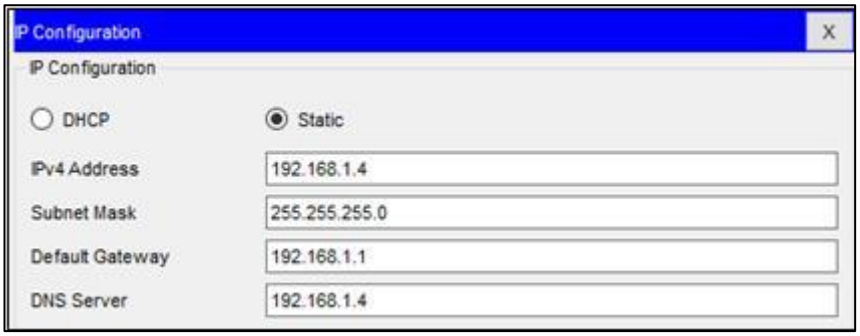
The access point has been configured with WPA2-PSK security with a complex password. This is to ensure the secure communication with wireless devices and is far more secure than the other options for securing the wireless connection that are available on this access point. The key has also been made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



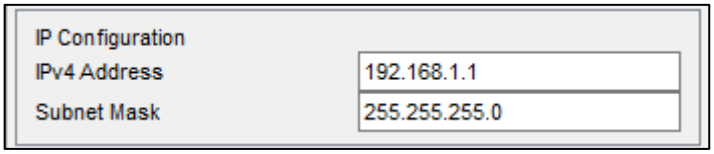
Whilst WPA2/PSK is not completely secure, it gives a good balance of security against disadvantages. Due to its limitations, if someone has got access to the key, they could share it with someone, or if a staff member leaves then they could continue to access the network. One option to consider would 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.

Server static IP address configuration



Router static IP address configuration



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 made recommendations for the hardware they have chosen and justified why they recommended each piece. The hardware that they have recommended is not only fit for choice, but in many cases is also suitable for upgradability in the future.

The student has gone further and identified the use of one potential supplier and justified their reason for this. They have also included a realistic approximate price range table (low and high range) that meets the scenario requirements whilst allowing for future expansion. This demonstrate a wide range of excellent knowledge and skills that are required for this real-world scenario.

One area for improvement would be to consider the language used and identify if this needs to be in a format that a non-technical person would easily understand. For example, in many instances the document highlights the features of a product that is recommended but does not clearly explain, in a non-technical manner, why this would be beneficial to the business. An example of this is when they state that no devices will be located within the demilitarized zone (DMZ), so all devices will be protected by the firewall, but they do not explain what a DMZ is and what this means for the business.

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
Pass	The network diagrams are logical and display sufficient knowledge in response to the demands of the brief.

	The student makes some use of relevant knowledge and understanding of network cabling theories and practices but demonstrates adequate understanding of perspectives or approaches associated with industry best practice.
	The student makes adequate use of facts/theories/approaches/concepts and attempts to demonstrate breadth and depth of knowledge and understanding in their designs and implementation, as well as in their testing and documentation.
	The student is able to identify some information from appropriate sources and makes use of appropriate information/appraise relevancy of information and can combine information to support decision making.
	The student makes sufficient judgements/takes some appropriate action/seeks clarification with guidance and is able to make adequate progress towards solving faults with network cables or resolving faults found in testing.
	The student attempts to demonstrate skills and knowledge of the relevant concepts and techniques reflected in network cabling, design and implementation and generally applies this across different contexts.
	The student shows adequate understanding of unstructured problems that have not been seen before, using sufficient knowledge to find solutions to problems and make some justification for strategies for solving problems.
Distinction	The network designed and developed is precise, logical and provides a detailed and informative resolution to the demands of the brief.
	The student makes extensive use of relevant knowledge and has extensive understanding of the network cabling practices and demonstrates an understanding of the different perspectives/approaches associated with designing, installing and testing networks.
	The student makes decisive use of facts/theories/approaches/concepts in their designs, demonstrating extensive breadth and depth of knowledge and understands and selects highly appropriate skills/techniques/methods to build and test their networks.
	The student is able to comprehensively identify information from a range of suitable sources and makes exceptional use of appropriate information/appraises relevancy of information and can combine information to make coherent decisions.
	The student makes well-founded judgements/takes appropriate action/seeks clarification and guidance and is able to use that to reflect on real life situations in resolving network cabling faults and network configuration.
	The student demonstrates extensive knowledge of relevant concepts and techniques reflected in network cabling, design and implementation and precisely applies this across a variety of contexts and tackles unstructured problems that have not been seen before, using their knowledge to analyse and find suitable solutions to the problems.

	The student can thoroughly examine network requirements in context and apply appropriate analysis in confirming or refuting conclusions and carrying out further work to justify strategies for solving problems, giving concise 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.

NCFE is authorised by the Institute for Apprenticeships and Technical Education to develop and deliver this Technical Qualification.

Owner: Head of Assessment Solutions.

Change History Record

Version	Description of change	Approval	Date of Issue
v1.0	Published final version.		May 2021
v1.1	NCFE rebrand		September 2021
v2.0	Annual review 2023: Amends to grade descriptors to ensure clarity	June 2023	19 June 2023
v2.1	Removal of direct internet references / images in task 1	November 2024	12 December 2024