|  |
| --- |
| SE3CN11 Computer networking |
| Networking Solution Specification for PrintMeNow |
| Group Coursework Report |
|  |
| **Mark Wells - 21008251** |
| **Ben Fitch - 21015439**  **Casey Singlehurst - 21011076**  **Tommy Bedford - 21009807**  **Luke Rickerby - 22009920**  **Max Loveday - 21012762** |

|  |
| --- |
| This report and the solution it presents is based on the specification as given for this assignment. It will present the networking problem as derived from the specification and highlight any assumptions such that it is clearly defined. It then describes the solutions as an overview and as an in-depth analysis of each of the key points. Finally, the solution will be verified against the initial problem by way of a conclusion. |

**17th March 2016**

**ABSTRACT**

Table of Contents

[1. Introduction 2](#_Toc445841950)

[2. The Solution Overview 3](#_Toc445841951)

[3. The Solution in Detail 5](#_Toc445841952)

[3.1. Point 1 5](#_Toc445841953)

[3.2. Point 2 8](#_Toc445841954)

[3.3. Point 3 13](#_Toc445841955)

[3.4. Point 4 16](#_Toc445841956)

[3.5. Point 5 19](#_Toc445841957)

[3.6. Point 6 21](#_Toc445841958)

[3.7. Point 7 23](#_Toc445841959)

[4. Conclusion 27](#_Toc445841960)

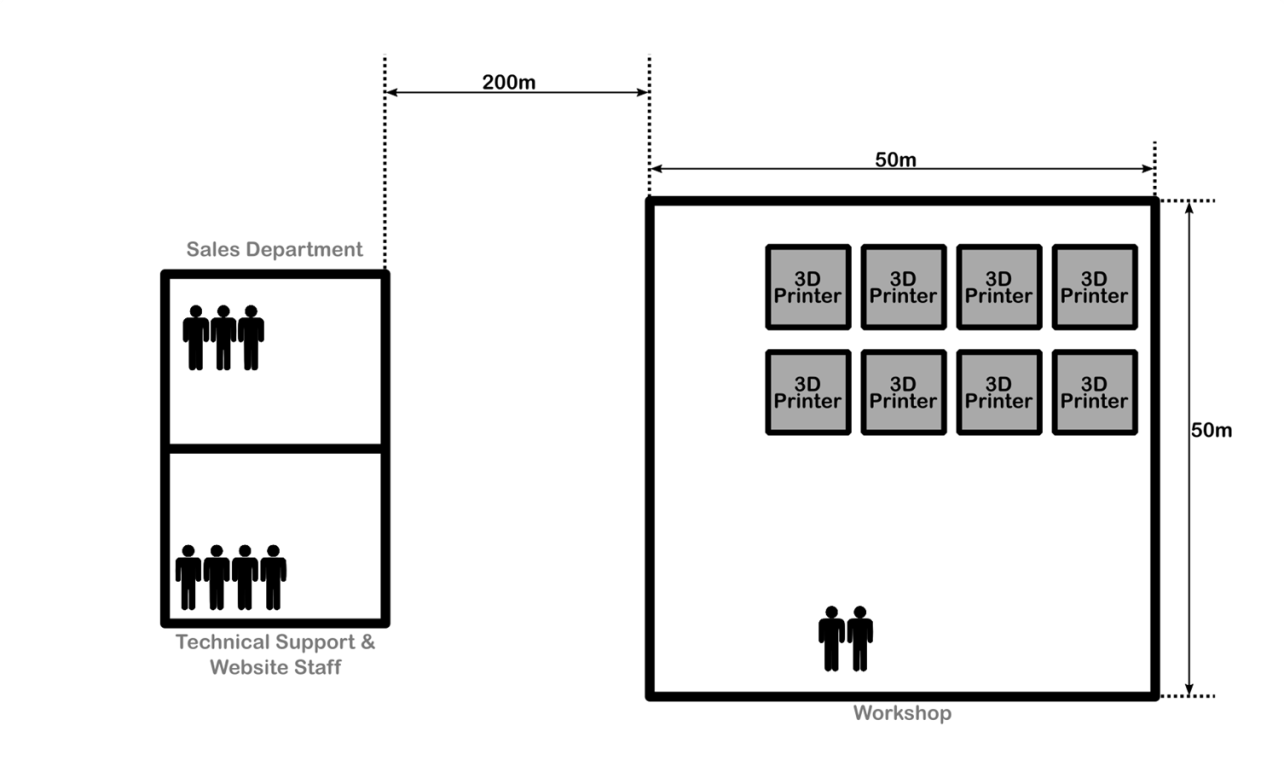
[5. References 28](#_Toc445841961)

# Introduction

This introduction will outline the problem as derived from the specification and outline the assumptions which have been made.

This project required the research and design of a complete networking solution for the start-up company “PrintMeNow”. The networking solution had to not only be suitable to meet the needs and arrangements of the company and each of its separate offices – comprised of the sales department, the technical department and the workshop – but also take the physical layout, security and external connections into account.

To ensure the requirements were met, a brief was supplied with all the relevant information in regards to the layout and needs of the company. The brief was then simplified down to the key components of the business with regards to the network, which can be seen below:

* Customer uploads 3D model files
* Printed objects will be posted back to customers
* Customers pay via on-line payment company ‘PayFriend’
* Sales and Technical offices next to each other, with 3 and 4 personnel respectively
* 50m x 50m Workshop situated 200m away, housing 2 personnel
* Host their website themselves
* 2 Databases (file stores) – Primary and Backup
* Start with 8 3D printers – Initially print 25 objects per day
* Expansion must be considered in every decision

The initial empty layout of the offices and personnel are shown below in figure 1.1.

Figure 1.1 - Layout of offices and workshop

With the layout of the problem and the key points of the brief determined, assumptions have to be made to fill any unknown knowledge. The general assumptions made about the design and layout have been listed below:

* All out-shipping will be handled from the workshop.
* The business is based in an industrial estate.
* The offices and workshop aren’t facing each other, or within line of sight.

# The Solution Overview

Using the brief and along with the assumptions made, a networking solution was design and developed; the final design can be seen below in figure 2.1.

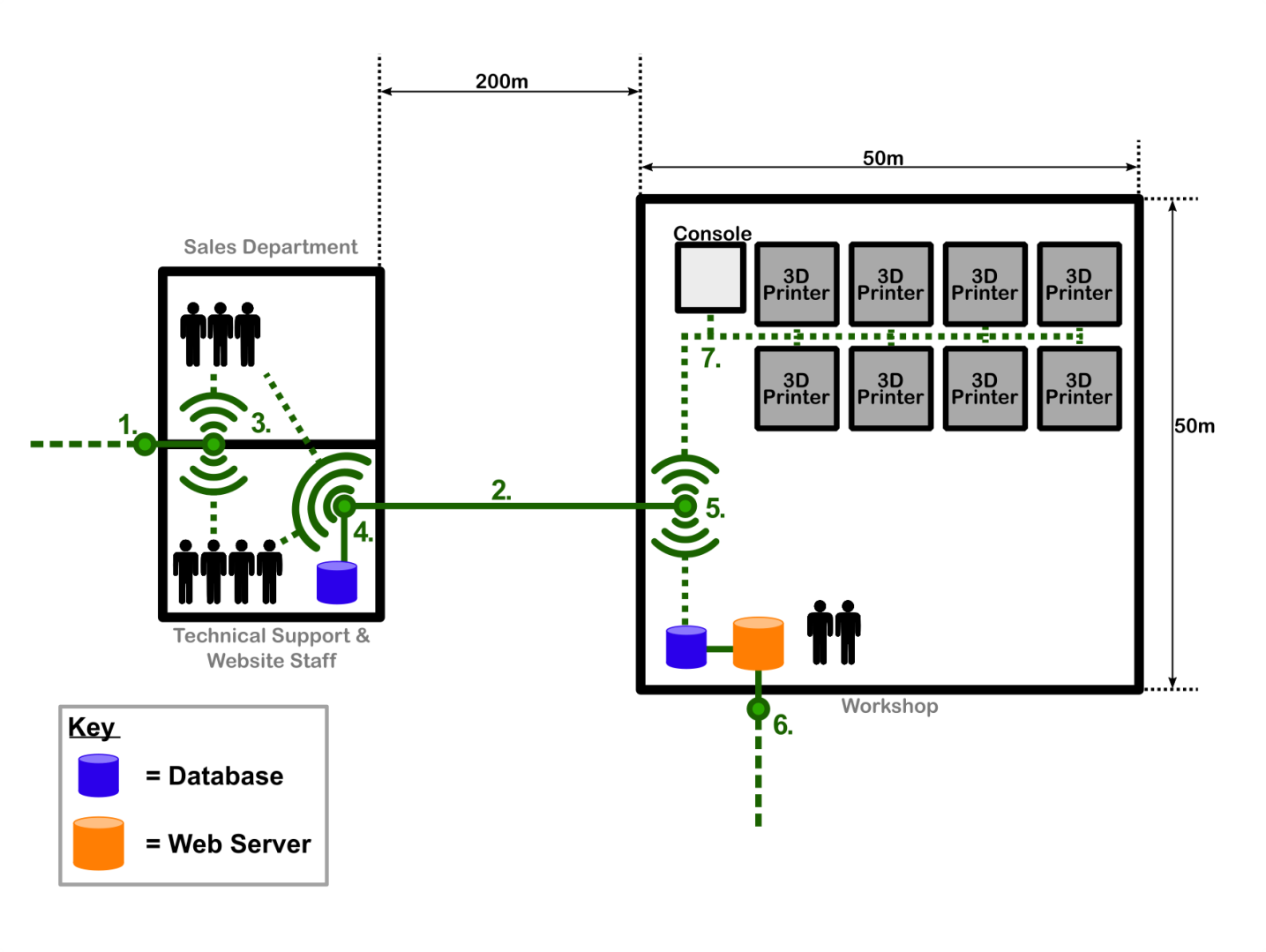


Figure 2.1 – Final Networking Design

The solution is comprised of 7 individual points/sections, with each point playing a different role in the network.

To summarise; the network is made up of two separate connections to the Internet, one made through point 1 for the sales and technical offices, and the other at point 6 to the workshop. The Internet connection for the offices is solely for the purpose of allowing them access to the Internet for uses such as checking email, research and the like. The connection made at point 6 is the main connection for the company as it is the direction connection for the webserver to the Internet, which is hosting their website. Connected directly to the webserver is the primary database; the reason for being connected so closely to the webserver is so that there is minimal delay and distance for saving of the customers uploaded files and information to the database.

The personnel in the sales and technical offices are able to access the primary database through the local area network (LAN) made up through points 2, 4 and 5. Having the connections locally allows for fast speeds and low congestion. The backup database is situated in the technical office, and is updated nightly. The reason for situating it apart from the primary is for security purposes, so in the case of a fire or break-in it is likely one of the databases will be safe.

In the section 3, each individual point is expanded upon; stating the requirements, potential solutions and proposed solution.

# The Solution in Detail

## Point 1

**Problem**

Connection Point 1 is required to connect the offices to the Internet. This needs to have one incoming and one outgoing connection for standard Internet use. It connects to Point 3 which will take care of distributing the connection appropriately to the two offices.

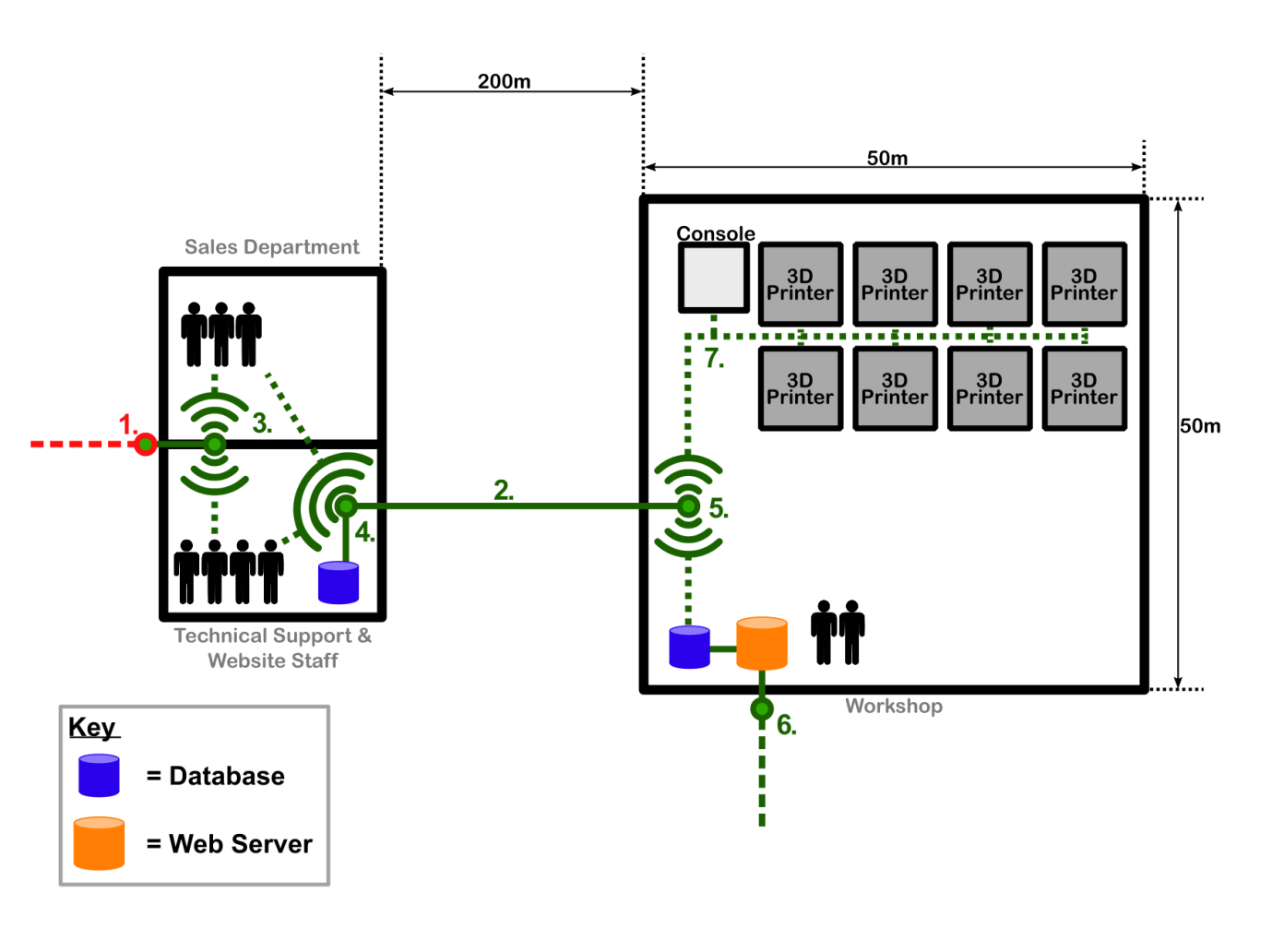


Figure 3.1.1 – Point 1 providing Internet access to the offices

**Considerations and Assumptions**

The solution for Point 1 must be able to cope with two way traffic at suitable speeds such that the office staff can carry out their day-to-day tasks. While the number of people in the offices is currently seven, Point 1 must consider the potential for expansion and thusly serving an increased number of staff.

It is only required that Point 1 handles Internet traffic for the offices and not for the web server, as this is handle by Point 6. The day-to-day tasks can, in most cases, be assumed to be fairly ordinary such as checking emails and providing support through forums. These tasks do not require much bandwidth, and so Point 1 does not need to be able to cope with large volumes of traffic.

Point 1 needs to be appropriately secure to protect transferred data (which may be sensitive, such as customer details) and to prevent hijacking of the connection. The security needs to be sufficient to prevent Point 1 being vulnerable for the office staff and their devices.

It must also be ensured that the connection is reliable. As most daily activities for all staff will require connection to the Internet, it is important that the connection is always available. Sustained problems with Point 1 would hinder the work that needed to be carried out by the office staff and have cascading effects on the operation of the business.

**Potential Solutions**

Providing an ISP provides an incoming connection, Internet connectivity can be supplied to the offices by a router. A router is a piece of hardware which can receive incoming packets of data and ‘route’ them on to their next destination [1]. A router is able to send and receive in multiple directions. In this case, it can receive packets from the Internet and route them on to Point 3 as well as receiving packets from Point 3 and sending them on to the Internet in the direction of their destination. A router sits at a gateway point [2] thus connecting two networks together.

Routers will attempt to optimise the path to a destination and learn routes rather than just randomly taking packets in and spitting them out on the other side. A router will usually have at least two Network Interface Cards [3] to connect to two separate networks. Just like a PC which uses the TCP/IP protocol, a router will also have a routing table. This is used to determine where to send data packets and to attempt to select the best possible route.

With IPv4 addresses having run out and ISPs transferring over to the new IPv6 address, it is important that any modern router is IPv6 compatible.

Routers can either be wired or wireless. This means that although the connection from the ISP will typically be wired to the building and to the location of the router, the connection between the router and Point 3 could be wired or wireless.

Wired

Wired routers will usually use an Ethernet cable to pass the connection to the next point (in this case Point 3). A standard Cat-5 Ethernet cable can provide speeds of up to 100 Mb/s which would be more than suitable for the employees in the offices [4]. Alternatives to Ethernet include using a phone line or power line, however Ethernet still offers a faster service than these.

The disadvantage of using a wired router is the inconvenience of the wire itself. Depending on the office structure and the placement of Point 3, the wire could present a tripping hazard or require fixings and holes to the structure to keep it out of the way.

Wireless

Wireless routers do not need cables to transmit packets but the overall quality of a wireless signal has to be considered. The most common signal frequencies in Wi-Fi routers are 2.4 GHz and 5 GHz [5]. While 2.4 GHz routers have a higher range (around 46 metres indoors) than 5 GHz, this is not a concern as the distance to Point 3 will be much shorter. However, 5 GHz is more reliable than 2.4 GHz as it is not as much affected by interference [6]. While the support for 5 GHz from connecting devices may not be as available as that for 2.4 GHz, providing Point 3 accepts the frequency then this is not an issue. 5 GHz is more expensive, and considering that there will not be any interference from other networks, 2.4 GHz would be the better option.

Security has to be considered for any connection, in particular wireless. This is because data packets travelling through the air are easier to intercept than those travelling through a solid cable. WPA2 is currently the best and strongest encryption for wireless routers [7] and so it should be ensured that the router supports this. Although having security on a router does slow it down, it is vital for a small business to be using a secure connection and this importance will only increase through business expansion.

**Proposed Solution**

It is proposed that a wireless router is chosen for Point 1. It should:

* Have a 2.4 GHz frequency band
* Support WPA2 Security
* Be IPv6 compatible

As discussed above, the wireless router can provide sufficient speed and security without the inconvenience of using a physical wire. It will be able to handle personnel expansion and should not suffer from too much interference on the 2.4 GHz frequency band as there are no other networks supplied to the offices. This solution will minimise cost as well as meeting the requirements of supplying Internet connectivity to the offices.

## Point 2

**Problem**

Point 2 is the connective line between points 4 and 5, and is used by both the sales and technical departments for accessing the primary database for either the customer’s information or to fix/alter their 3D models. The basic customer information won’t be too large, as will primarily be address, order information etc. so won’t require much bandwidth as a result. But, the 3D models will range in size from 20MB up, with complex models being capable sizes over 50MB: As a results, if many models are being accessed at once it could create a large amount of traffic over the connection, causing congestion and slowing down the connection line. Overnight the connection will be used to update the backup database with any changed that occurred during the working day.

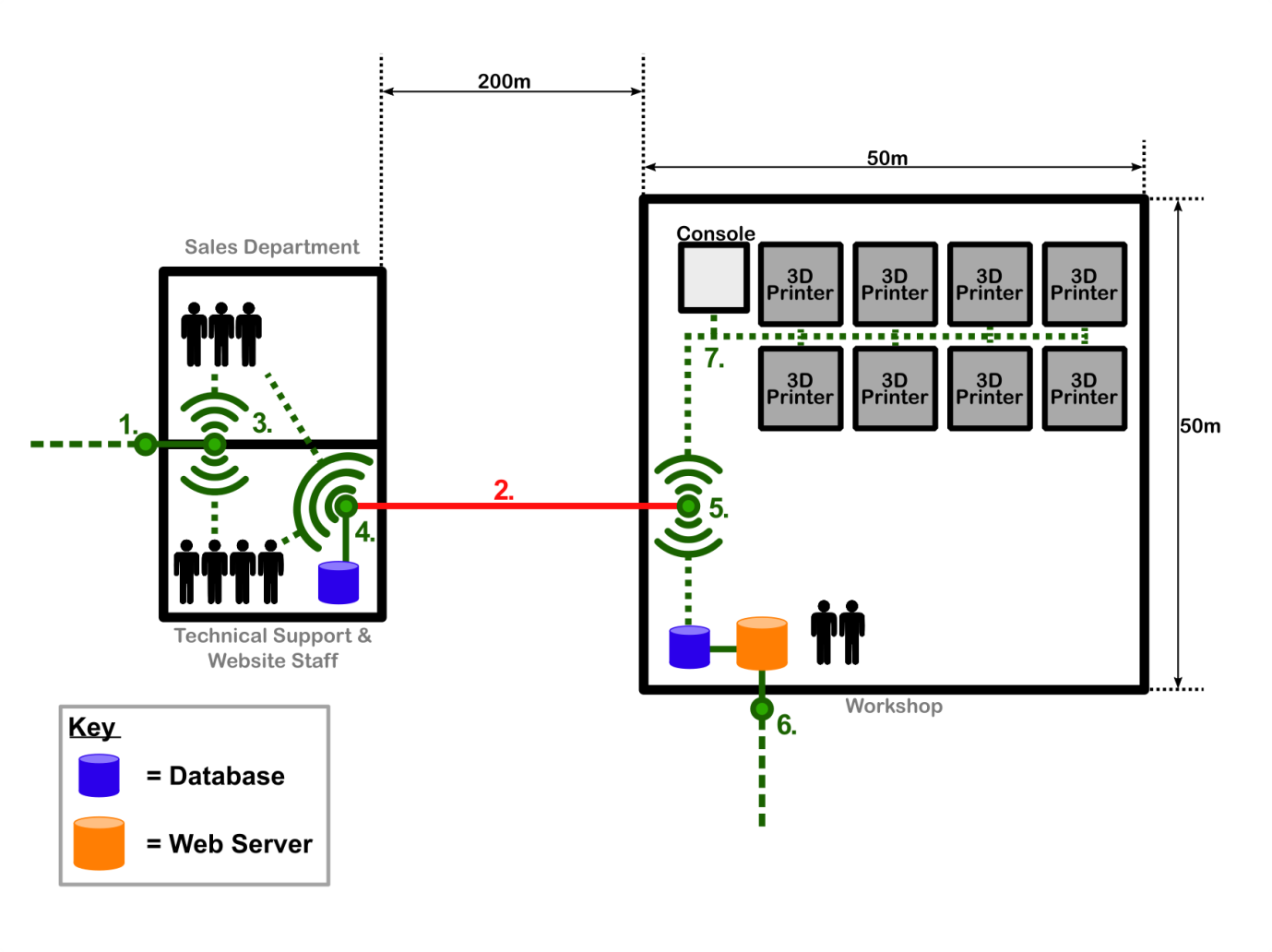


Figure 3.2.1 – Point 2 as the connecting line between points 4 and 5

**Considerations**

Due to the importance of the connection to the business with it being the lifeline between the warehouse and the offices, it is essential that the connection is not only reliable but suitably fast. A loss of connection could set the company back a great deal of time and money, with losses to orders as well as customer trust.

Security is of great importance, and with connection 2 being the main line for all sensitive data it must be ensured that the line is full secure no minimal risk of break-ins. The loss of leaking of customer information is not only potentially fatal for the company, but also risks the customers.

Regardless of the above the solution must still be feasible, there is no use in spending the companies budget in the setting up of a single connection line.

**Options**

This section will discuss the possible options for utilisation as the connection line - point 2. Four separate options were identified and are discussed below. The implementation as well as the Pros and Cons of each option will be explored.

Over internet

Over internet implies that the sales and technical departments access the primary database through the internet, removing the any physical link between points 4 and 5. This option would also require the backup database to be automated for backing up overnight. The consequences of such a decision would require some level of reorganising the layout of the overall network, this is due to there being a much larger throughput for both routers with the passing of files and data to and from the databases.

*Pros:*

Utilising over internet as an option is potentially costless. This is a result of the network layout having to be adjusted; though it would require more capable routers (point 1 and 6) there would be no need for point 4 as the backup database could be directly connected to the router at point 1, as well as the staff in both the technical and sales office accessing the primary database through the internet.

This option is also totally non-evasive in the sense that there would be no need to dig up roads or create extra holes in buildings: Both of which require outsources and dramatically increase the cost as well as damaging the leased building.

*Cons:*

With this option, all data will be passed over the internet from the database to the required department. The sending of data around the internet puts it a risk of potential interception and when the data is customer information such as name, address or other personal information this is not something that can be taken lightly. Even the models being stolen is an unacceptable risk, especially considering that the 3D part could be patented or of sensitive nature and being stolen and released into the public domain could have great repercussions. The risk of interception could be decreased by encrypting the data by either using SFTP or FTPS, but non the less it still leaves the data open to bruteforce attacks: There are even application that can be downloaded specifically for brute forcing SFTP and FTPS (Low and Slow Brute Force Scanner).

Another down side to the use of over internet is the slow speed that would ensue. Due to the internet being best effort there is no guarantee of the files ever making it to their destination, potentially requiring the resending of packets: This results in an inconsistent speed for the passing of data, and when large 3D model files are considered (ranging from 20MB) this could take time.

Wi-Fi

For this option it will be referring to point-to-point Wi-Fi, where the connection is bridged using two transceivers with one on each building.

*Pros:*

Point-to-point Wi-Fi is more than capable of covering the 200m distance between the two building, with some systems being able to reach distances of up to 5 miles. But for this network, a smaller option would be all that is necessary.

It is relatively fast, with most point-to-point set ups having a minimum of 1000Mbps full-duplex capabilities, but with more expensive options obtaining speeds of up to 10Gbps. The obtainable speed is very much dependant on the budget for the connection.

Much like the over internet there would be a minimal set up cost, this is due to Wi-Fi being non-evasive and not requiring large contracting operation for digging up roads or the like. But because of the requirement for the transceivers having be pointed to each other within the line of sight; contractors may be required for the installing for masts to mount the system to, as well as requiring holes through the building to connect to points 4 and 5.

*Cons:*

As mentioned above, the transceivers are required to be connected through line of sight, but one of the assumptions made is that the buildings are in an industrial estate meaning they aren’t. This causes a problem, as to ensure the line of sight is maintained they would require being mounted on tall masts, which could in turn cause planning issues depending on the necessary height of the mast ([8] Schedule 2, Part 16 – Class A).

Even taking into account that most modern point-to-point systems now make us of narrow beamwidth antennas as well as encryption, there is still the risk for security failures resulting in the loss of confidential customer information and property; raising the same issues as with the over internet solution. Many antennas make use of RADIUS authentication, but the protocol is by no means totally secure and still poses a risk for break-ins.

Even with the a relatively good reliability offered by point-to-point Wi-Fi, they are still susceptible to environmental factors. Many of the available antennas come with an optimal humidity range for operation which can be exceed with recent rainfall (“5 to 95% Noncondensing” [9]). As well as having a maximum wind load, which is potentially at risk of being exceeded while fixed atop a mast without any buildings to protect it.

Ethernet

This option requires the laying of a physical copper connection to span the 200m distance between the buildings; this has its own strengths and weakness’ that are explained below.

*Pros:*

Due to the nature of having the physical connection buried in the ground it solves many of the security risks associated with Wi-Fi and over internet. For someone to gain access to the connection they would be required to locate the line and dig quite deeply into the ground in order to even gain access; making it much safer in terms of security than the above options.

As the line is a physical connection spanning points 4 and 5, it would be inherently more reliable than non-physical connections that are capable of being blocked or slowed for various reasons.

*Cons:*

As the line is physical there is a very real risk of a possible break or cut to the line. This could be accidental people conducting roadwork and cut through the line by mistake, or even for sabotage purposes. This also includes the risk of someone cutting the line and intercepting all the data passing though it; though the means necessary to facilitate this are quite extensive.

Because of the need to bury the line, external contractors will be necessary for the burying on the line. This will require specialist work to ensure the line is laid in a watertight conduit to prevent moisture from damaging the connection terminals due to corrosion: This is worsened by the need for a repeater halfway through the line. Specialist waterproof cable is also available – known as flooded cable – but is move expensive than its counterpart.

Ethernet connection are not suitable for distances over 100m [10], therefore to bridge this connection a repeater would have to be placed halfway along the buried cable to clean and boost the signal. This alone causes many problems: Including the need for a special watertight connection point buried with the conduit, creating another point for moisture to enter in the case of a failure. Also the repeater itself is another point capable of failure, as well as a perfect spot for someone to have an easy connection point to make into the network and breaching security.

As briefly mentioned above, water damage is a real possibility. This would not only degrade the copper line itself, but potentially destroy the repeater which would cause a whole lot of problems; potentially requiring the ground to be dug up again depending on how it was set up.

The main problem with a solid copper connection between the two building is the likelihood of differing ground potentials between the buildings [11]. This would mean in the instance of a lightning strike there is a very real risk of it traveling down the line and destroying all the electronics as well as potentially killing an employee. Though this is a remote risk, it is far from an acceptable one, which completely strikes through the possibility for Ethernet and a means of connection.

Fibre Optic

Fibre optic is the process of passing the data down a glass cable in the form of light, this comes with its own unique set of advantages and disadvantages.

*Pros:*

As a result of the data transition being conducted via the sending of light, fibre optic is incredibly fast, capable for reaching speeds of over 30Gbps in the most expensive options. Though those speeds aren’t necessary a fast connection is useful when possible expansion is considered along with the general files sizes of the models ranging from 20MB.

As with Ethernet the security risk is minimal due to the cable being buried. Not only that, but if someone were to try and gain access by digging up the cable it would require very specialist equipment for them to cut and intercept the connection without permanently destroying it. Unlike Ethernet there is no need for any sort of repeater, meaning the 200m can be spanned using a single cable over the entirety of it. The main plus over Ethernet is that is doesn’t pass an electric current over the line, meaning it isn’t susceptible to the same ground potential problems as Ethernet.

*Cons:*

Much like Ethernet and all physical line connections, there is the risk of the line being cut or broken, and requiring specialist contractors to lay the cable – at a great expense. But, fibre optic isn’t prone to moisture induced damage meaning it will have a small chance of needing to be replaced.

One major consideration with fibre optic is that it requires specialist equipment in order to integrate it into Ethernet/Wi-Fi based networks. This will need to be done with either a specialist switch which comes with a fibre converter, a media converter or a SFP/XFP transceiver. The drawback with these, is that in order to make full use of the potential speeds of the cable more expensive converters must be used.

The major downside to fibre optic is the overall cost of the whole system. This is a result of not only the cable being very expensive, but also the cost for laying it into the ground as well as the means of integrating into the network at both ends.

**Proposed Solution**

The option deemed most suitable is Fibre Optic. Despite being the most expensive option in regards to set up and installing, it was chosen because it not only offers the safest option in regards to the customer’s sensitive information, but has the fastest speeds. The proposed cable is OM3 grade, this is capable of delivering over 10Gbps between the 200m buildings: With suitable transceivers. Though this sounds excessive, it allows for the technical department to down and upload the 3D models in fractions of a second with room for plenty of expansion while still delivering good speeds. OM4 cable is available and offers even greater speeds, but is much more expensive, as well as requiring even more expensive equipment to make use of the full capabilities while integrating it into the network. Despite all this, there is still a real risk of the connection being broken, but with the cable being buried this risk is small.

## Point 3

Connection point 3 is the key connection point within the office of the business. It supplies both the Support staff, who troubleshoot errors and ensure the continuity of the 3d printing businesses website and services and it supports the sales team as they go about their daily activities of promoting and selling the businesses products.

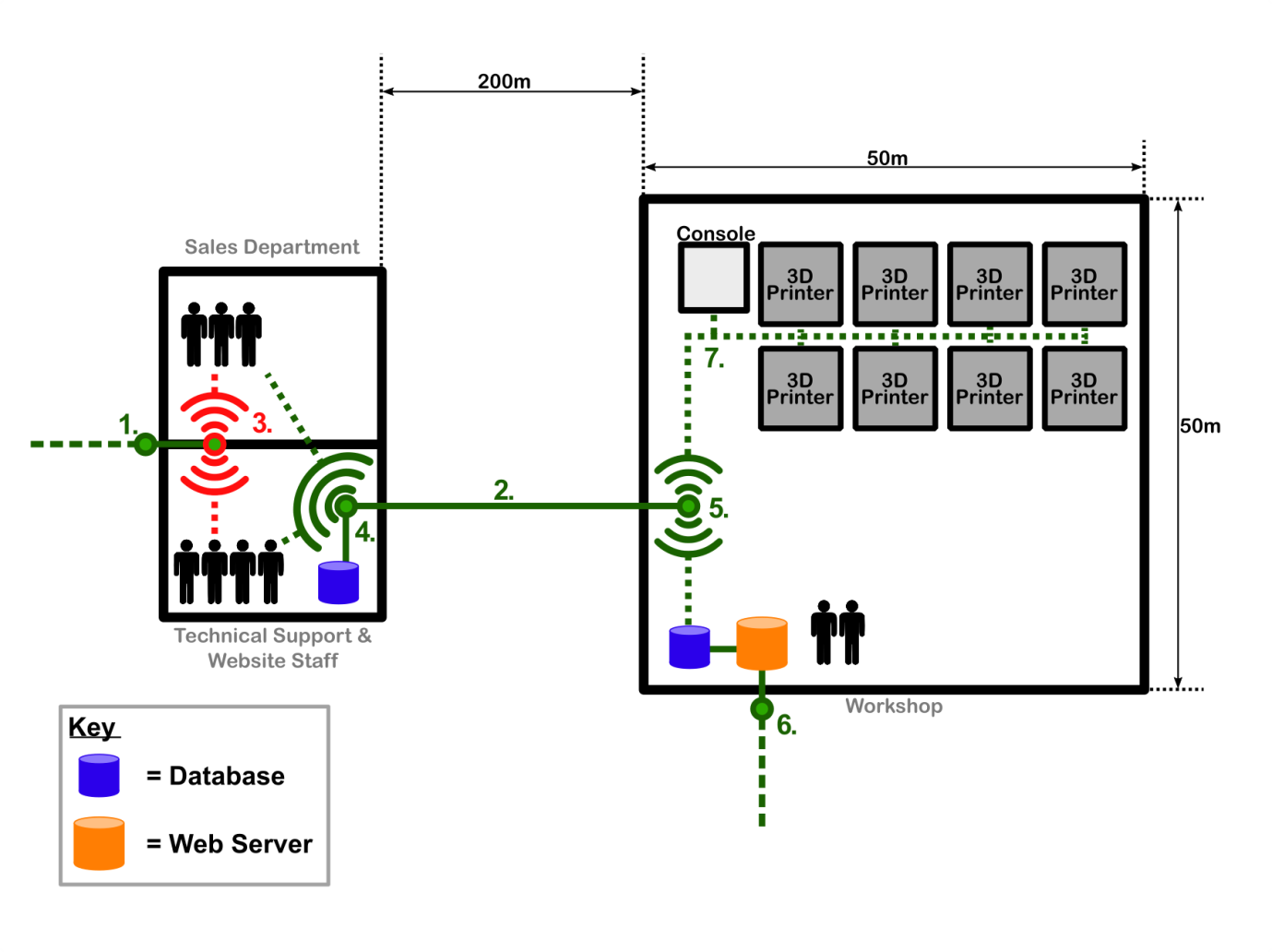


Figure 3.3.1 – Point 3 supplies both offices

**Considerations and Assumptions**

The solution for point 3 must be able to handle the load of all the current staff within the office accessing the internet through point 3 into point 1 at any one time. It must provide appropriate speeds, not slowing the network down so that the tasks can be completed at the same time as the request comes in, this is important for both the support staff, who will have service level agreements with customers, and the sales staff will need a connection that can allow them to make and process sales on the spot.

The solution needs to be suitable for rapid expansion, currently only 7 employees reside within the office, but should the business take off at an alarming rate, it will be assumed that more employee’s will be needed meaning more hardware/devices will be added and a suitable standard of equipment will be needed to ensure that this is not a problematic transition.

The solution needs to be secure to ensure no outside access can be gained to the network; it needs to ensure that it is protected to internal and external threats whilst still allowing the employees to access the internet at will.

The solution must not fail unless the parts it relies on, namely point 1 fails, this will ensure a constant connection for the workplace, should the connection fail it would mean no access for the workplace, this would result in a loss of sales and being unable to sort out any customer problems and items such as service level agreements between the workplace and the company could be jeopardised.

**Potential solutions**

Wireless router

A wireless router would allow the company to fulfil the needs of both the sales and support departments; at current rates it would be able to sustain the current needs regarding traffic through the router, a wireless router can theoretically hold 255 connections, however after 45 devices have been connected the device can start to struggle to hold connections and maintain speed. This would allow for some expansion but would limit it, if you assume that each person has between 2 to 3 devices this would soon stop after growth up to 15 people and soon slow the network down [12].

The latest IEEE standards 802.11ensure that networks are protected by WPA and WPA2 protection, this protects the network from outside access and only people who know the key can access it. Any router that is bought is compliant with the new standard and therefore protects the network, however WPA and WPA2 are not unbreakable and still leave a small vulnerability within the network [13].

The router will need to be business grade and not consumer grade in order to cope with the changing demands of the business, consumer or household items will not be able to cope with the influx of data being transferred or rapid expansion that may occur [14].

Hub

A hub would also allow fulfil the needs of the company. It would be able to withstand the current rates of flow of data, it would ensure solid connections that would only break in the event of a cable being cut or loss of power and it would also allow for rapid expansion has hubs come with anything from 12 to 48 ports for connection. Security would however be an issue, no security is available on a hub and anyone who has access to the hub can simply plug in a wire and have access to the network.

Switch

A switch would allow for security to be put in place in the form of a Vlan as it would partian parts of the networks in the case of point 3 the support team and the sales team in order to keep the network safe [15].

Purchasing business grade switches with in-line power will ensure a constant and sufficient connection for the workplace; this would ensure the connection is constantly available as the switch would have its own power source and will save on costs further down the road as you will not have to install power outlets for extra switches [14].

Business grade switches will allow for rapid expansion as they often come with anywhere up to 48 ports which will allow for multiple connections and allow the staff forces to expand if needed. The only problem with this would be that the VLANs will need to be configured.

**Proposed solution**

The proposed solution would be a switch connected to a wireless access point. The switch will provide safe connections within the workplace through the use of VLANs whilst the wireless access point will allow the members of staff in the sales section to be connected on the move which can always be useful for items such as mobile phones and tablets.

A Virtual local area network will be set up by running a single Ethernet cable from the switch to a router, this router will be located within the sales office and allow the employees there to access the internet wirelessly, it is assumed that 2.4ghz frequency will be used as this is the most common frequency in use and use IPV6 to connect the devices in the sales office.

The Support staff will be connected directly from the switch via Ethernet cables/ Ethernet ports located around the office area to connect the support staff computers to the switch allowing them to access the internet/network.

The devices will connect to the web server via the wireless device at point 4, the connection is wireless and using a router management interface will allow the staff to connect to the webserver when needed.

The switch wireless access point will ensure that expansion can happen at any point with spare ports being available to those wishing to connect new hardware to the switch whilst new sales employees can access the hub to get to work as soon as possible. The hub should be protected with a WPA2 key to ensure the safety and integrity of the network at all times.

This low cost but effective solution will ensure that the business is ready to meet the demands of its customers whilst ensuring a solution is in place for any unforeseen events. This will increase the longevity of the business.

## Point 4

**Problem**

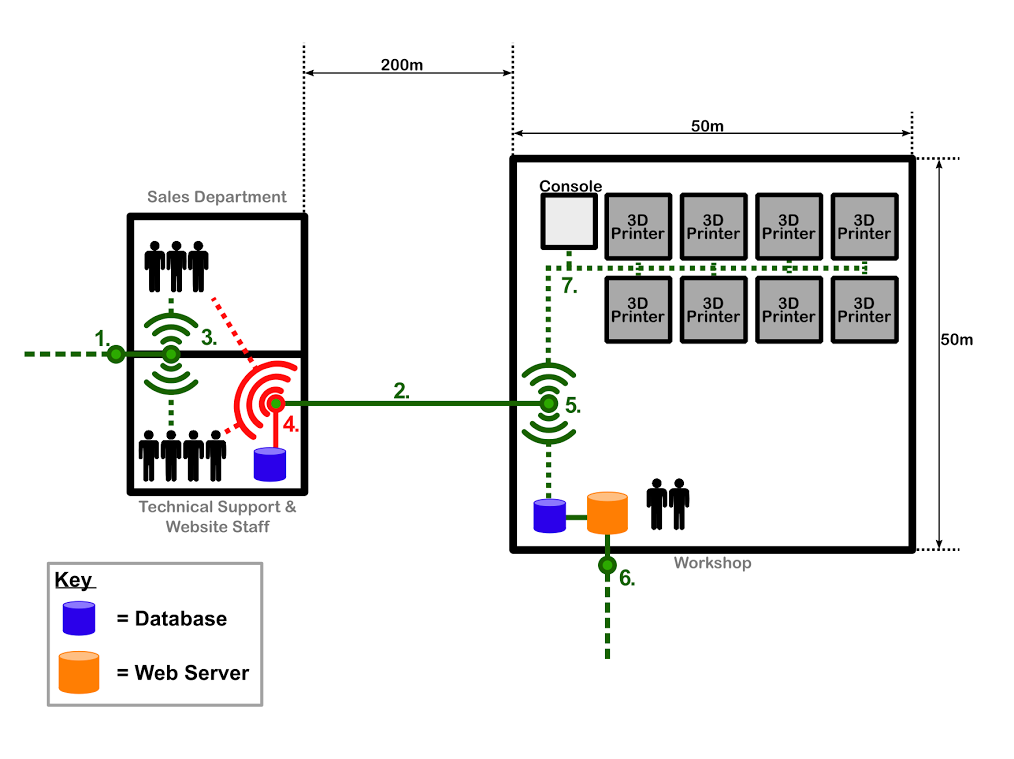
Connection point 4 is a device responsible for linking the connection between the offices and the warehouse. It will be responsible for connecting to the secondary database, which is backed up with the data from the primary database each night. Additionally, it will allow the sales workers and technical support to access the primary database so that they can access any project/customer information that they may need at the time. Both of these functions will require fast, reliable data access.

Figure 3.4.1 – Point 4 links the offices to the warehouse and the backup server

**Considerations and Assumptions**

The backing up of the data will only occur at night, so the connection will need to be reliable, as if it fails it is likely no-one will be around to fix the issue until the morning.

Sensitive data will also be backed-up, such as customer names and addresses, therefore the security should be as robust as possible.

Connection point 4 will only provide a connection to the project/customer information for the office/support workers, the general internet connection will be handled by connection point 1.

Although customer information would require very little bandwidth, the 3D-model files can reach 50mb in size [16], and could cause slow-down if multiple people are accessing/modifying these files at the same time.

This model assumes that there will be no major obstacles to wireless reception, and that there are few/no conflicting networks nearby to cause Wi-Fi interference.

**Potential Solution**

Switch vs Hub

Both a switch and a hub could be used to provide the required connection. However, there are some features that make a switch more desirable than a hub for this situation [17]. The network is set up in a way where connections to the primary database are only requested by individual computers, where an employee needs access to customer or project information. With a hub, the information would be sent to all devices on the network, regardless of which it was requested by. This can cause security issues when dealing with sensitive data, and can also result in data collisions.

A switch on the other hand, thanks to its full-duplex communication, can identify the MAC address of the requesting device, and forward the information on to only that device, resulting in a more efficient, secure data transfer. For example, when the database is being backed up overnight, the data to be stored would only be sent to the backup database, and not to all the other connected devices in the office as would be the case if a hub was used.

Wireless vs Wired

Another decision to make is whether the connection from the switch to the office employees should be wired or wireless. The benefits of a wireless connection in this situation is that it would be a cheap way to allow all the office employees to access the network. The office is small enough that a wireless connection could cover the entire area quite easily, allowing them to access the information they need wherever they are on, on any device, such as a phone or netbook. Additionally, a wireless solution would make it very easy to expand in the future, as new employees could simply have a computer set up, without any new wiring to be done.

There are some issues with a wireless connection, which could result in problems in this scenario. For example, wireless connection speeds are slower than wired [18], although due to the relatively small file size, the speeds should still be more than sufficient. Connection reliability is also a potential problem, but with the relatively small size of the office and staff, it would be easy and inexpensive to find a product capable of fully covering the offices, and eliminate any blind spots.

Another issue to consider though is security. With a wired connection you have much more control over who can access your network [19], which when dealing with customer information, and valuable project files is very important. However, as long as a wireless network is set up correctly, using security such as WPA2 encryption [20], it can be very secure as well. Overall, the convenience and added benefits of wireless, greatly outweigh the potential issues it could have.

**Proposed Solution**

Overall, in this scenario, the most suitable solution would be a switch connecting the connection from the warehouse to the offices. A switch provides the most efficient way of routing connections between different devices so that bandwidth isn’t wasted, and collisions prevented. To connect the office employees to the network, a wireless connection will be set up to allow employees as quick and easy access to the information they need as possible, so that the business can run to maximum efficiency.

The backup database however will be connected through an Ethernet cable to the switch at connection point 4. This is due to the database requiring a reliable connection for the overnight backups, and also due to its close proximity to the connection point, would be cheap and easy to set up.

## Point 5

**Problem**

Connection point 5 is located in the warehouse. This point has several main features of use. It is the point that connects the 3d printers to the server and print terminal. This point is also one end of the connection bridging the office and the warehouse. The connection from point 5 to the offices 200 meters away will be a wired OM3 connection that will be used mostly for overnight backup, with the possibility for technical support staff and sales staff to access the main server via this connection during the day. Point 5 will need to connect all 8 printers to the same network such that a terminal can house a print request program to control the printing. This terminal should also collect and show diagnostic data about the printers, such as amount of material left in the printer, so the workshop staff can easily take care of any matters involving the printer, such as refilling plastics. The same network will need to incorporate the main server where the print files are located. With all of the criteria met for point 5, the terminal will be able to take unprinted jobs from the server, and queue them to print to any available printer automatically.

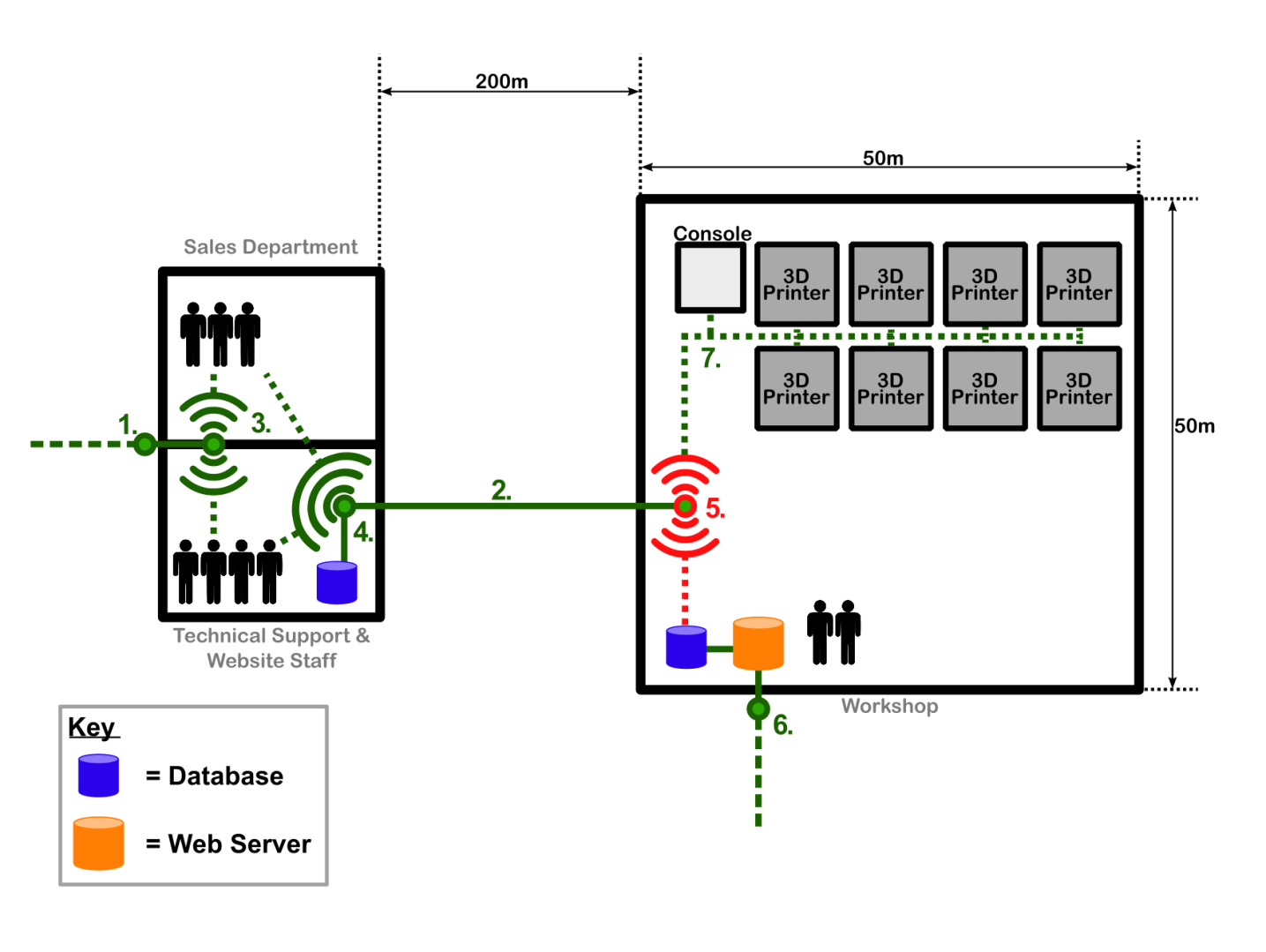


Figure 3.5.1 – Point 5 is the primary connection point for the warehouse

**Assumptions**

* The OM3 cable enters the warehouse in roughly the middle of the room with ample cabling to spare, so no special care has to be taken over the installation of connection point 5 provided it is placed close to the middle of the left wall.
* The building and layout is set up in such a way that both cables can be easily run just below the surface, and any wireless signal can reach its full range without any impediment.
* Connection point 5 is placed in such a way that any vertical measurements are not taken into account (i.e. a wireless signal with 50m range will reach exactly from one end of the warehouse to the other)
* Backup of the server is done exclusively at night. If the backup fails on any particular night, the backup then waits until the next night before retrying.

**Considerations**

This connection point will be one end of the bridge between the offices and the warehouse. As the warehouse stores the main server, traffic from the offices will route through this point during the day, and the backup will route through this point at night. Because of this, this connection point will need to have as close to 100% uptime as possible. The connection will also need to handle a server backup unsupervised.

This connection point also serves as the network connector between the main server and the printers. This network will also have a terminal connected to serve as a printer controller. This terminal will collect print jobs from the main server, and send them to free printers. The terminal will also collect data about the printers, such as the amount of plastic currently left in the printer, and display them to the workshop employees.

The connection point will be connected to the offices using an optical wire. Because of this, connection point 5 will have to allow a wired connection to it. The workshop is small enough that either wired or wireless options are feasible to connect the server to the printers without any wired or wireless repeater technology used.

The connection will need to be suitably fast to keep up with the optical fibre’s speed, and to be able to backup a server potentially up to terabytes in size.

## Point 6

**Problem**

Connection Point 6 is required to connect the web server to the Internet. It must be able to receive and pass requests for web pages to the web server and return the appropriate content. It must also receive and pass 3D model data uploaded by the user to the server.

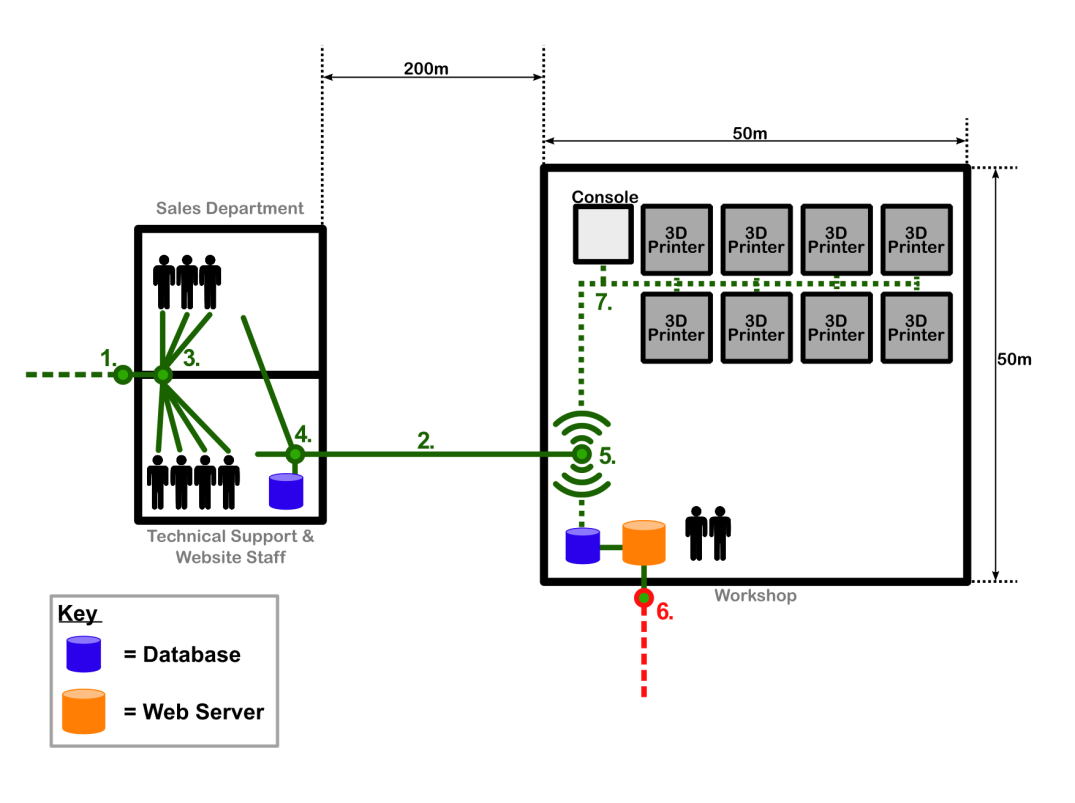


Figure 3.6.1 – Point 6 provides Internet connectivity to the web server

**Considerations and Assumptions**

The solution for Point 6 must primarily be able to handle appropriate web traffic. As well as return web pages to the user with the potential for gaining new customers, it must also be able to handle the uploading of 3D model data files passing through the router and reaching the server. To recognise company expansion and increased exposure, this may be a significant volume of web traffic.

For any web server there are security vulnerabilities and it would be a target for anyone wishing to attack the company. The device at Point 6 is the first line of defence and so it must be as secure as possible, as well as being robust and resistant to attack.

It is necessary for the connection to be as reliable as possible, as failure at this point could be very costly for the business. Failure to connect the web server to the Internet and maintain a connection would mean that it would inaccessible to users and customers, and thusly put the business at risk.

**Potential Solutions**

Internet access can be supplied to the web server with a router. An analysis of routers is provided in section 3.1 for Point 1, however whereas that was for office Internet connectivity, this is for the web server itself. Therefore the considerations made above need to be taken into account when searching for solutions.

Wired vs Wireless

A wired connection is capable of handling high speeds over Ethernet cable. Above Cat-5 Ethernet cable there is Cat-5e and Cat 6 which can handle 1 Gb/s and 10 Gb/s respectively. These will be more suitable for handling large volumes of traffic and maintaining consistent access to the web server. Security and reliability is even more important when supplying an Internet connection to a web server than and a wired connection is easier to ensure this [21]. The router should have firewall features of its own, along with standard security, to provide the outer layer of defence for the web server.

**Proposed Solution**

A wired router will be chosen for Point 6. It will be connected to the web server using a Cat 6 Ethernet cable for high data rates to handle web traffic and the uploading of 3D models. The router will be more costly than that chosen for Point 1, but it will be essential that it is to ensure that it is secure, robust, reliable and highly configurable to ensure efficiency and security.

## Point 7

**Problem**

Point 7 will manage the link of the 3D printers to the PrintMeNow business network. The network will be expected to manage initially 8 printers producing 25 models a day with the capacity for suitable expansion. The network must provide access for 2 technical staff members manning the warehouse. Below, figure 3.7.1 illustrates the 3D printers and a management console connecting via wireless router seen in point 5.

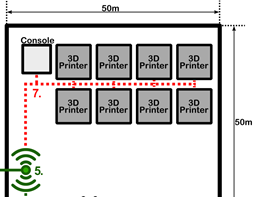


Figure 3.7.1 – Point 7 connects the 3D printers and management console

**Considerations and Assumptions**

The majority of current 3D printers and technologies commonly connect via USB or Wi-Fi [22].

Whilst extending the connection from network point 5 to the printers and staff using wired or wireless [23] technologies the printers demands on network resources, the size of network coverage in the warehouse and its accessibility need to be consider. Hardware such as a wired and wireless repeaters to filter and rebroadcast signals over long distances are usually good practice for distances in excess of 100m. As the warehouse dimensions are only 50x50m the network would not benefit from this hardware [24].

Printers on the network will occupy more network resources whilst transferring data from network to printer. The connection between the network and printer only need be maintained whilst data is transmitted. A loss to the network connection during data transfer to the printers can corrupt a print job which will waste time, materials and money. The average 3D print time for a model is roughly between 3 and 4 hours based on typical large model sizes of 200x200x150mm. 3D model average data sizes are determined by scale, detail, print colour and material. It is assumed that the printers will support common model print sizes such as the dimensions in the example above. The link between the network and printer needs to support reasonable download speeds and less concerned with upload speed. Much more data will need to be sent to the printers than received and once the data is uploaded printers will still be vacant for the remainder of the print job.

Network connection security is less of an issue inside the warehouse than external connections between the warehouse and business offices. Accessing the network could then be managed by controlling personnel access to the warehouse.

The cost of instalment, maintenance and reusability must be affordable and practical. The network will need to Catering for expansion and instalment of new devices.

**Potential Solutions**

Solution 1: USB Hub

Displayed in figure 3.7.2 is the installation of a USB Hub to a management console located at point 7 which would allow the 3D printers to be connected physically using USB2.0/3.0 cabling to the Hub as seen in red. The management console then connects via Ethernet cat5 cabling fed from point 5 as displayed in green. The management console located at point 7 is the access point for the technical staff situated within warehouse.

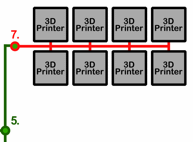


Figure 3.7.2 – The installation of a USB Hub to a management console at Point 7

*Pros:*

Connecting the 3D printers using USB cabling and a USB Hub would provide a more secure network.

Physical cabling is more reliable than wireless at is not susceptible to weather conditions or signal interference from obstructing materials like dense metal objects.

Wired networks offer faster data rates than wireless. They can support network speeds up to a gigabyte per second.

Hubs can be interlinked with one another to join together clusters of connected USB devices. Although there are some limitations to this method it does however provide a simple method for potential expansion.

*Cons:*

USB hubs will need an independent power supply (self-powered) so that the number of downstream ports is not limited to just 4. Self-powered USB hubs are slightly more in cost than bus-powered or dynamic but not a substantial gap in cost [25].

There would be potential hazard risks of physical cabling all over the warehouse or an extra cost to store them more practically.

In order to achieve USB2.0 or 3.0 data rates all connections from the USB device (printer) to the computer (management console) must be of the same USB version else data rates are capped at the lowest hardware version connected.

Extended the network would require another Hub, USB cabling and separate power supplies. Apart from the greater cost there is would be more hardware to maintain.

Solution 2: Wireless Router

Installing a wireless router at point 5 of as seen in figure 3.7.3 would provide network coverage for the entire warehouse allowing more flexibility of location when installing printers, management consoles and devices. As there is a fibre OM3 cable running directly into the warehouse security within the building is less of a concern making wireless a versatile and cheap option here.

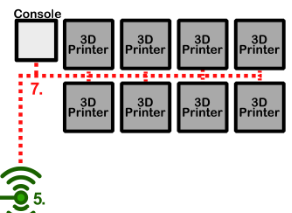


Figure 3.7.3 – With the user of a wireless router at Point 5

*Pros:*

A wireless router provides ease of accessibilty from anywhere within the warehouse.

Relocating and connecting new devices to the network can been easier with no extra hardware.

Installment is cheaper than a physical connection , easy to manage and non-invasive around the work place and the potential for reusing the network hardware if relocating business location is better than that of a physical line.

*Cons:*

With a wirelss router installed the wireless network types such as 802.11g or 802.11b that the router supports should match that of the printers as a difference could slow data transfer rates [26].

Wireless has limitations in range. The average wireless router frequenciy transmittion range is tens of metres. It also can be unreliable as the tramsmittion is subject to environmental aspects as dicussed earlier in this report .

Solution 3: Wireless network Hub

This solution would have an Ethernet connection via cat5 cabling from point 5 directly to point 7 a static management console. A wireless network hub is then used to connect the Wi-Fi enabled printers to the management console.

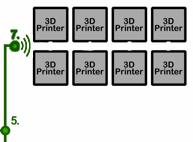


Figure 3.7.4 – Wireless Network Hub

*Pros:*

The network will be less secure as it can be accessed from anywhere in the warehouse. Security then has to be controlled by personnel access to the building.

Linking the printers to the network would require less cabling saving cost and reducing physical hazards in the workplace. This would allow more manoeuvrability when installing the printers.

*Cons:*

This wireless solution would be subject to the same disadvantages as the previous wireless solution.

Wireless networks have limited bandwidth. They are also limited to expansion due to the demand of wireless spectrum [27].

**Proposed Solution**

The proposed solution is a wireless setup. As seen in Figure.1 connection point 5 which hosts a wireless router. As mentioned earlier in the document a repeater is not necessary due to the dimensions of the warehouse. This option would reduce the initial cost of instalment, maintenance and expansion of warehouses operations. With a direct line being fed into the warehouse security is less of a concern in the building as personnel access can be controlled. With considerations to the pros and cons of the solutions to connection point 7 a wireless setup will provide more than enough speed and reliability necessary for the network demands. It also provides mobility and convenience whilst installing and expanding the system. This solution is a safer, cheaper and sufficient option.

# Conclusion

* Summarise the solution very briefly
* State how the solution satisfies the brief

# References

[1] "What is router?," in Computer Hope, Computer Hope, 2016. [Online]. Available: http://www.computerhope.com/jargon/r/router.htm. Accessed: Mar. 6, 2016.

[2] M. Rouse and D. Rhodes, "Router," in SearchNetworking, SearchNetworking, 2006. [Online]. Available: http://searchnetworking.techtarget.com/definition/router. Accessed: Mar. 3, 2016.

[3] D. A. R. Y. L, "How does A Router work?," in Think Like a Computer, Think Like A Computer, 2011. [Online]. Available: https://www.think-like-a-computer.com/2011/07/18/how-routing-works/. Accessed: Mar. 3, 2016.

[4] "What kind of Ethernet (cat-5/e/6/a) cable should I use?," in HowToGeek, 2015. [Online]. Available: http://www.howtogeek.com/70494/what-kind-of-ethernet-cat-5e6a-cable-should-i-use/. Accessed: Feb. 28, 2016.

[5] B. Mitchell, "What is the range of a typical Wi-Fi network?," in About.com, About.com Tech, 2014. [Online]. Available: http://compnetworking.about.com/cs/wirelessproducts/f/wifirange.htm. Accessed: Mar. 5, 2016.

[6] J. Moran, "5 pros and cons to 5 GHz Wi-Fi Routers," in Wi-Fi Planet, 2011. [Online]. Available: http://www.wi-fiplanet.com/tutorials/5-pros-and-cons-to-5-ghz-wi-fi-routers.html. Accessed: Mar. 1, 2016.

[7] "How to choose a wireless Router for your small business," in small-bizsense.com, Small Business Sense. [Online]. Available: http://small-bizsense.com/how-to-choose-a-wireless-router-for-your-small-business/. Accessed: Mar. 4, 2016.

[8] "The Town and Country Planning (General Permitted Development) (England) Order 2015," ed. legislation.gov.uk, 2015.

[9] Ubiquiti Networks, "NanoBean ac Datasheet." [Online]. Available: https://dl.ubnt.com/datasheets/NanoBeam\_ac/NanoBeam\_ac\_DS.pdf

[10] Panduit, "The Evolution of Copper Cabling Systems from Cat5 to Cat5e to Cat6," 27/02/2004.

[11] C. Ground, "Out in a flash: networks, power surges and lightning strikes," in Industrial Ethernet Book vol. Issue 65 / 33, ed. [Online]. Available: http://www.iebmedia.com/index.php?id=8089&parentid=63&themeid=255&hft=65&showdetail=true&bb=1&PHPSESSID=6c2m8qjcfoleblfdg3k1e6adg4

[12] "Wireless network Capacity…How many devices can connect to my WiFi network?," in ac. [Online]. Available: http://wifi.actiontec.com/learn-more/wifi-wireless-networking/wireless-network-capacity-how-many-devices-can-connect-to-my-wifi-network/. Accessed: Feb. 29, 2016.

[13] "TechLibrary," in juniper.com, 2013. [Online]. Available: http://www.juniper.net/techpubs/en\_US/network-director1.1/topics/concept/wireless-80211.html. Accessed: Mar. 7, 2016.

[14] "Building a small office network," in cisco.com, Cisco. [Online]. Available: http://www.cisco.com/cisco/web/solutions/small\_business/resource\_center/articles/connect\_employees\_and\_offices/primer\_building\_a\_small\_office\_network/index.html. Accessed: Mar. 5, 2016.

[15] "Virtual LAN," in Wikipedia, Wikimedia Foundation, 2016. [Online]. Available: https://en.wikipedia.org/wiki/Virtual\_LAN. Accessed: Mar. 2, 2016.

[16] "Frequently asked questions," in sculpteo.com, 2009. [Online]. Available: http://www.sculpteo.com/en/help/#maximum-file-size. Accessed: Mar. 9, 2016.

[17] "Hub vs switch - difference and comparison," in diffen.com. [Online]. Available: http://www.diffen.com/difference/Hub\_vs\_Switch. Accessed: Mar. 8, 2016.

[18] "Should I use a wireless or a wired connection?," in virginmedia.com. [Online]. Available: http://help.virginmedia.com/system/selfservice.controller?CMD=VIEW\_ARTICLE&ARTICLE\_ID=3675&CURRENT\_CMD=SEARCH&CONFIGURATION=1001&PARTITION\_ID=1&USERTYPE=1&LANGUAGE=en&COUNTY=us&VM\_CUSTOMER\_TYPE=Cable. Accessed: Mar. 11, 2016.

[19] S. Evans, "Wired vs wireless in the enterprise," in computerweekly.com, ComputerWeekly, 2013. [Online]. Available: http://www.computerweekly.com/feature/Wired-vs-wireless-in-the-enterprise. Accessed: Mar. 4, 2016.

[20] "Wi-Fi security," in ico.org.uk, ICO. [Online]. Available: https://ico.org.uk/for-the-public/online/wifi-security/. Accessed: Mar. 16, 2016.

[21] "Wired Routers," in firewallguide.com. [Online]. Available: http://www.firewallguide.com/hardware.htm. Accessed: Mar. 2, 2016.

[22] R. C. Ltd, "RS components,". [Online]. Available: http://uk.rs-online.com/web/c/computing-peripherals/3d-printing-scanning/3d-printers/. Accessed: Mar. 13, 2016.

[23] M. Kazmeyer, "Explanation of wireless vs. Wired printers," Small Business Chron. [Online]. Available: http://smallbusiness.chron.com/explanation-wireless-vs-wired-printers-58672.html. Accessed: Mar. 7, 2016.

[24] N. Randall and B. Sosinsky, "Extending wired & wireless networks," in pcmag.com, PCMAG, 2006. [Online]. Available: http://www.pcmag.com/article2/0,2817,1940078,00.asp. Accessed: Mar. 9, 2016.

[25] "USB hub," in Wikipedia, Wikimedia Foundation, 2016. [Online]. Available: https://en.wikipedia.org/wiki/USB\_hub. Accessed: Mar. 10, 2016.

[26] "Wireless network advantages and disadvantages," in ukessays.com, UKEssays, 2015. [Online]. Available: http://www.ukessays.com/essays/information-technology/wireless-network.php. Accessed: Mar. 2, 2016.

[27] M. Reardon, "Wireless spectrum: What it is, and why you should care," in cnet.com, CNET, 2012. [Online]. Available: http://www.cnet.com/news/wireless-spectrum-what-it-is-and-why-you-should-care/#! Accessed: Mar. 8, 2016.