



# SECURING THE NETWORK

Network Security of Small-scale Ltd (SS Ltd)

## ABSTRACT

“SS Ltd has a lot of confidential information on their network so security is also an issue and they would like to make sure that none of this sensitive information, such as accounts, and new construction designs and planning documentation get out into the public domain.”

Gheorghe Mitrea 1118495  
Tower Hamlets College 2016

## Table of Contents

INTRODUCTION .....	5
TASK 1 Understand the Impact on the Social and Commercial Environment of Network Security Design.....	6
1.1 Evaluate the Current Systems Network Security .....	6
1.2 Discuss the Potential Impact of a Proposed Network Design .....	7
1.3 Network Attacks and Their Impact .....	9
TASK 2 Design Network Security Solutions .....	14
2.1 Network Design for SS Ltd.....	14
2.1.1 The Firewall Configuration.....	15
2.1.2 Missing Patches .....	16
2.1.3 Access and Authentication.....	16
2.1.4 Wireless Connectivity .....	16
2.1.5 Disable the USB Ports .....	17
2.1.6 IP Address Allocation .....	17
2.1.7 Packet Filtering .....	18
2.1.8 Intrusion Detection Systems (IDS) .....	19
2.2 Evaluate Design and Analyse Feedback .....	19
TASK 3 Implement and Testing Network Security Solutions.....	22
3.1 Network Security Implementation of SS Ltd.....	22
3.1.1 Switch Configuration .....	23
3.1.2 Router Configuration .....	24
3.1.3 Disable USB from BIOS.....	26
3.1.4 Good Access and Authentication.....	27

3.1.5	Secure Wireless Network.....	27
3.1.6	Virtual Private Network (VPN) .....	31
3.1.7	The Physical Security of The Equipment .....	31
3.2	Testing of Network Security Implementation.....	34
3.2.1	Internal Tests.....	35
3.2.2	External Tests.....	37
3.3	Analysis of Test Results.....	43
TASK 4	Manage Network Security Solutions .....	47
4.1	General Maintenance.....	47
4.2	Security Audit .....	49
4.2.1	Security Assessment Services.....	49
4.2.2	Vulnerability Assessment .....	50
4.2.3	Penetration Testing Assessment .....	51
4.3	Recommend Potential Change Management .....	51
CONCLUSION	.....	54
Bibliography	.....	55

## **LIST OF FIGURES**

Figure 1: Process of DDoS attack	10
Figure 2: Eavesdropping attack	10
Figure 3: The man-in-the-middle attack with example	11
Figure 4 Network design proposal for SS Ltd.	15
Figure 5 Figure 23 Class C IP address	18
Figure 6 Router configuration	25
Figure 7 Disable the USB from BIOS	26
Figure 8 Implement the Wireless Isolation Option	28
Figure 9 Look for MAC address	29
Figure 10 Configure the MAC address	30
Figure 11 Hiding the SSID	30
Figure 12 Implementing a VPN solution	31
Figure 13 Secure the rack servers with locks	32
Figure 14 Intruder Alarms, CCTV and Fire Detection	33
Figure 15: Switch testing	34
Figure 16 Router configuration	35
Figure 17 Check if Wireless Isolation s enabled	36
Figure 18 Checking if the USB functionality is disabled	37
Figure 19 Results of the scan of ports	39
Figure 20 Internet Common Ports Probe attempts to establish standard TCP Internet connections	39
Figure 21 Verification of open ports through command prompt	40
Figure 22 Using command nslookup to find a IP address of SS Network	41
Figure 23 Spoofability Test	41
Figure 24 Results of Anti-spoofing test	42
Figure 25 File Sharing test	42
Figure 26 Check the visibility of SS router from outside of the network	43
Figure 27 Static IP configuration	53
Figure 28 VLAN configuration	53

## ***INTRODUCTION***

The security is the first demand in organisations to keep their communication and information safe from competitors and other outsiders. The report will discuss the pros and cons of the network design in SS Ltd. The report will also discuss in depth the various vulnerabilities on network security. Different types of attacks will be discussed in the context of network security. Later the report will design the new network system for the organisation and evaluate the changes in comparison to previous network design.

The report will discuss the implementation of the network in details for each step of implementation. The test will be conducted to analyse the network design effectiveness and documents will be prepared on network design. The report will also determine the practices and policies to maintain the network health and recommendations will be given to enhancing the structure of the network.

## TASK 1 Understand the Impact on the Social and Commercial Environment of Network Security Design

### 1.1 Evaluate the Current Systems Network Security

The network system needs to be robust and flexible to use in the organisation to meet the demands and requirements. The present network structure is somehow capable of bringing all the required functionality but still lacks the security and performance issues. There are still many points those should be identified to ensure the security of the network. The SS Network has the following *benefits* for the organisation:

- The network does not have a proper delimitation between the wired network and the wireless one, is it open to external sources by simply develop a bridge using a mobile phone.
- The network has two major parts: wired devices and wireless connections. Only a single switch is used to serve all the devices in the network and a single wireless router is used to provide the connectivity to wireless devices in the network. There is no segmentation of network according to departments and users
- The network design has a great combination of accessibility through the integration of wireless as well as wired connections. The most of the devices can be connected easily to the network
- The network is flexible enough to add and remove the components like switches and used to centralise the structure and to manage the connections effectively. Each department or user is served with the dedicated connection
- The web address filtering is done at HTTP server to block unauthorised users in the network. Henceforth the network is capable of securing the devices from being attempted by unknown users for access and information in the network (Ciccarelli, 2012).
- Fibre cable is used for high internet performance and to make the system secure from the interception attacks in the network. The cable is more secure and faster than a traditional Ethernet cable

- The network has dedicated file servers, HTTP server and DHCP server to simplify the effort to manage the network over time. It has enhanced the performance and reduced the maintenance (Robertazzi, 2011)

## 1.2 *Discuss the Potential Impact of a Proposed Network Design*

The network system has the following **risks** in this kind of implementation because network design does not address all standards and practices:

- The most import vulnerability is the possibility of having a bridging between wired network and wireless by using the mobile phones which are connected to the wireless network of the company. These can lead to a security vulnerability in the network by developing links between the wireless network and the local network, which can result in various threats such as data theft or taking pictures of sensitive data.
- 
- The network system has no security against the failure. All the channels are connected to a central switch. If the switch gets fails, the network will go down. The dependency of the network on the single point of service is not enough to meet the organisational demands under abnormal load and use of the network.
- Wired SS Ltd network is not properly divided regarding its subnets, users or groups, where it can find the Surveyors, Architects and Managers using the same subnet which contains level access for Directors, Network Engineers, Receptionist, Account Officers. Also, another issue is that the Contractors are part of the internal network of the company.
- Wireless connections are not secured with an adequate amount of range and encryption. Also, it is difficult to manage the wireless connections under the control of the server.
- Using optical media like USB, CD, DVD, by employees, contractors or visitors of the company in the network can lead to a major vulnerability network.

- There is no user-based authentication system to use the network and the firewall is not present to control the incoming and outgoing packages in the network.
- The network is prone to attacks from the users also because there is no segmentation of network for different users as their activities in the network may interrupt the entire network for performance and security.
- Wireless networks do not benefit from physical security as wired networks incorporeal, so are more prone to attack. Once obtained access to the network, an intruder can easily use the resources within it.
- Removal and mobile devices - The vulnerabilities are also seen in the use of mobile devices like mobile phones and laptops in the network because the devices can be used to connect with the network without many difficulties. It also becomes difficult to track the wireless devices and their operations in the network. The security should be governed with browsing and emailing in the network via the mobile devices. Addition to it, the removal drives and devices may introduce the risk to system and information through virus and other attacks.
- The mobile connectivity in the network may be influenced by external factors for the speed and signalling. Also, the mobile devices are cohesive to pull down the performance in the network. The connectivity of mobile devices through USB may influence the security of system and information in the network. The mobile devices and their connectivity may bridge the network as they can independently form the network and interact with organisational network security system. Hence, the improper management of mobile devices in the network may lead the issues in network security implementation.

The following points also must be noted to analyse the security of the network:

- There is no encrypted communication with private contractors such as Virtual Private Network (VPN);
- Also, the segments are not properly managed because the devices are used interchangeable in the network. Employees are using wired connections to computers and preferring the wireless connectivity for mobile phones and laptops. The segments have no clear management for security and performance in the network.



- The network lacks the firewall, authentication and traffic management to secure the network against the failure and attacks.
- Software failures of any kind can lead to errors in the proper functioning of the system may open gaps in protection, or can do so uncertain in operation that can no longer work properly and efficiently. The security features of computer errors can open gateways intruders or accidents. Even if each software and hardware in hand are sure, all of them may be compromised if the hardware components are connected wrong or if the software is not installed and configured correctly.

### **1.3 Network Attacks and Their Impact**

Hackers use the attacks to read the information or to prevent the users from the access to assets and information so that own benefits can be made during that time. The attacks can be protected through the proper treatment of practices on network policies. The following are major network security attacks:

***DDoS attacks:*** In distributed denial of service attacks, the intruder prevents the authenticated users to have access to the server as the server is bottlenecked with many requests from attackers. Finally, the server may take too long to respond or may fail to serve the original requests. Different IP addresses are used to target the server as a result; it becomes difficult to detect the original and intentional requests in the network (Futoransky, 2010).

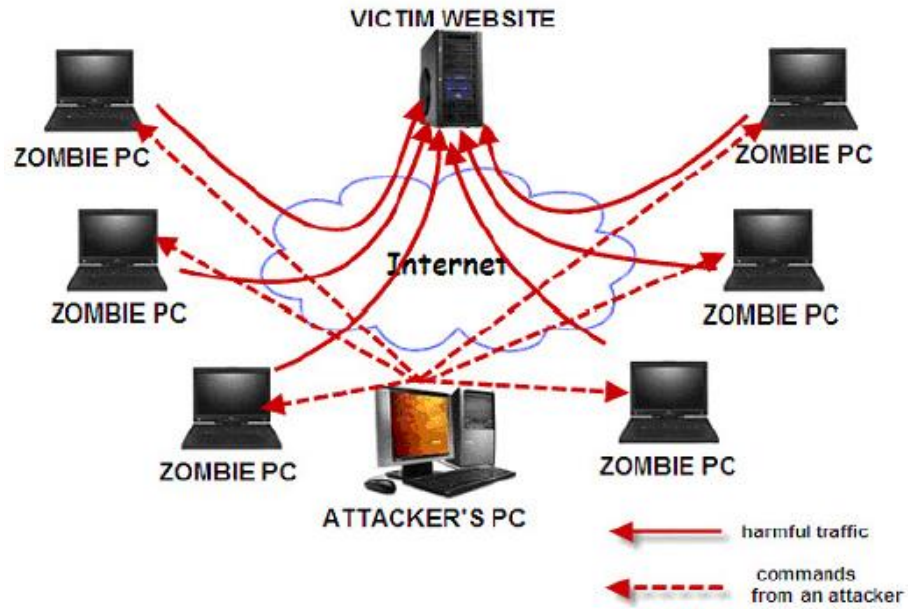


Figure 1: Process of DDoS attack  
(Source: DDoS attack, 2016)

**Eavesdropping:** The lack of encryption and security on the data transmission may result into eavesdropping or sniffing attack in which intruders get the access to the plain text of information without the knowledge of sender and receivers. The transparent acting of intruders to listen to the information through insecure data paths may lead to the disclosure of information in the network.

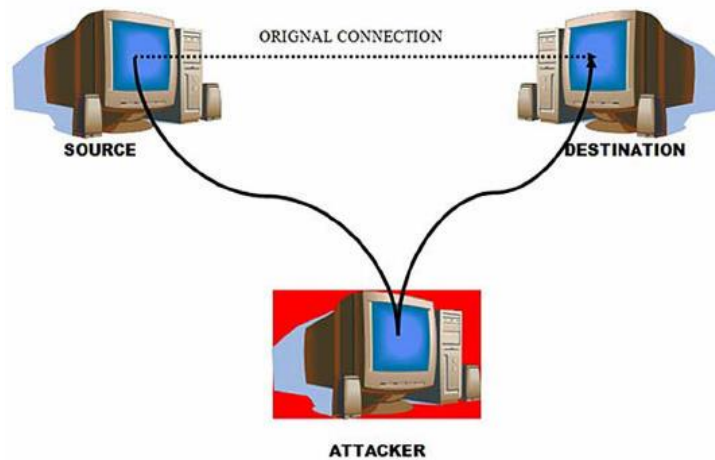


Figure 2: Eavesdropping attack  
(Source: Eavesdropping attack, 2016)

**Man-in-middle:** The attack in which an intruder is in between the communication path to listen and modify the information. The intruder has the full control of the communication and interprets as

the source of information so that receiver assumes the information from authenticated user. The man-in-middle can read and write the information for the receiver to misguide and make benefits with authentication identity.

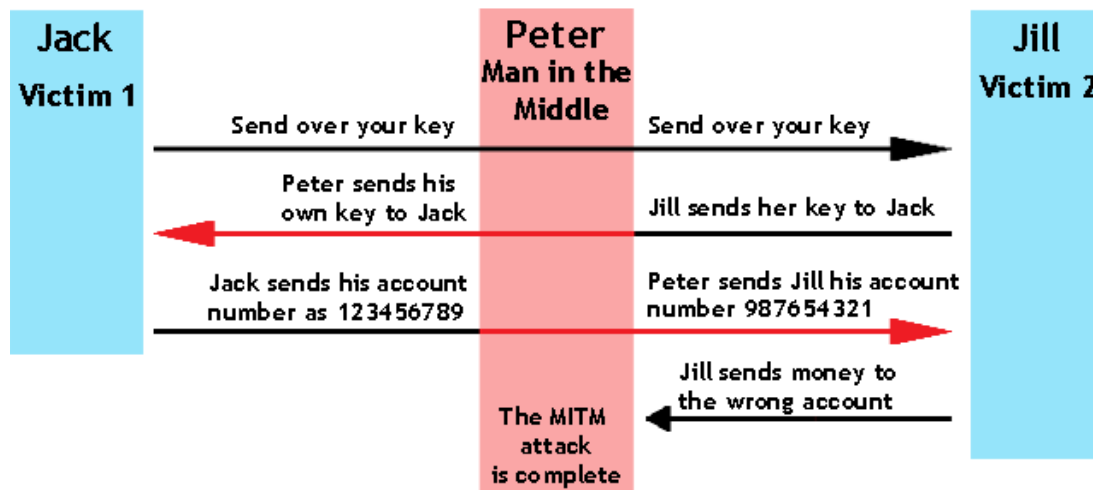


Figure 3: The man-in-the-middle attack with example  
(Source: The man-in-the-middle attack, 2016)

**Compromised key:** In this kind of attack, it is possible that the intruder may stall the authentication of the user and behaves like authenticated users in the network. In this manner, the intruder gets the control and access to network security (Casas, 2011).

**Phishing** - is an attack, which simulates a legitimate organisation that requires confidential information from the user, for example, e-mail the victim comes to a message which contains a site emulated an organisation's real with its emblem, and in case the user tries to log in, it sends the password to the attacker.

**SMTP attacks** - These attacks are usually based on vulnerability of buffer overflow, inserted in the text message content too high. The sequence does not fit the e-mail included orders for the e-mail server, so after sending the message, the error will execute malicious code message, giving the hacker opportunity to break the server (Hoffman, 2002).

**Password cracking** - This represents a hacker attack that carried him to be able to authorise and authenticate a system to get them resources.

**Flooding site** - can flood a server or host with an unusual number of packages, aimed at overloading the server. Flooding sites distinguish two types:

- SYN Flood
- ICMP Ping Flood

**Spoofing** - is not always an attack but is usually accompanied by an attack. It is hiding information about the attacker computer, for example, IP address, MAC address, DHCP server, DNS, User Agent. It is used to hide the identity of the hacker and make them harder to find computer attacker. Spoofing is achieved through proxy servers, vulnerabilities in TCP / IP or secret services on the Internet.

**Sniffing** - It represents sniffing process of capturing and analysing traffic. Utilities used for sniffing are called sniffers and protocol analysers. They analyse packets transmitted over the network, capturing passwords or other sensitive data transmitted in plain text. Usually, protocol analysers are used in local area networks, but can also be used in WANs.

**Wireless attacks** - As radio waves are difficult to control, Wi-Fi networks are often subject to security attacks.

**A virus** - is usually self-replicating programs designed to spread and infect as many computers without users realising this. Viruses spread by attaching itself to other programs, EXE or COM files, and more recently, and documents WORD, EXCEL, even HLP files, or some may infect the boot sector of the disk (Balthrop, 2004).

**Trojans** - are programs disguised trying to create gaps in the operating system to allow a user to access the system. Trojans do not have the facility to self-multiply as computer viruses.

**Worms** - are programs with destructive effects that use communication between computers to spread. Worms have common features with both viruses and Trojans. Worms can multiply like viruses but do not locally but on other computers.

**A physical risk** - is a potential reason for an occurrence that may bring about misfortune or physical harm of the PC frameworks. It accompanying rundown orders the physical dangers into three fundamental classifications;

- Human: These dangers incorporate robbery, vandalism of the framework and additionally equipment, disturbance, unintentional or purposeful blunders.
- External: These dangers incorporate helping, surges, seismic tremors.
- Internal: The dangers incorporate fire, insecure power supply, moistness in the rooms lodging the equipment and so forth.

After discussing possible threats on a network, the next step is to come with the new network security solutions.

## **TASK 2     Design Network Security Solutions**

### **2.1 Network Design for SS Ltd**

For the security purpose, it becomes necessary to design the new network with robustness and full proof against the security issues.

The organisation can use packet filtering services in the firewall to prevent the network from being damage from unknown and harmful packages. Packet filtering works on the source and destination IP addresses to filter the packets through the firewall. Also, the routers in the network can use network address translation techniques in which one IP address space is remapped to another address during the routing in the network. It is simple to address the new destination in comparison of readdressing at a device level. With NAT technology, the organisation can save public addresses as each client needs a single address to communicate on the internet. Besides to use the software level security, it is also necessary to secure the network and its components with a physical arrangement. For instance, servers and workstations can be monitored with surveillance camera and secured with locks on server room. It is somehow effective to prevent the access and reach to the system.

Technical staff in the network can prepare the single access point for the users to access the resource in the network as a single access point, which is effective to monitor the user activities and to control the user permissions on resources. To handle the power failure, the organisation can use UPS system to support the server up running. In this manner, the organisation can ensure the maximum uptime of servers and other network types of equipment. The cabling can be made tight along with proper positioning of equipment in a rack so that connection and devices can be secured.

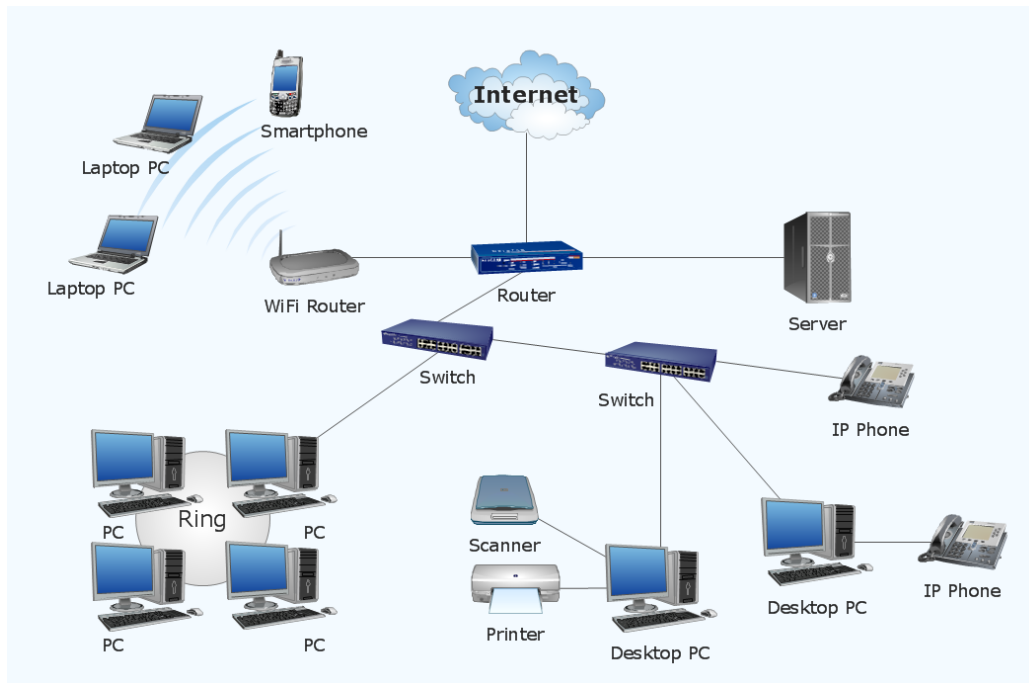


Figure 4 Network design proposal for SS Ltd.

The network design needs to meet the business requirements and to cover the following vulnerabilities in network security:

### ***2.1.1 The Firewall Configuration***

The firewall should be configured well according to devices in the network. The proper configuration of access control list and packets helps the organisation to achieve the security from outside intruders in the network. The network design must be implemented through the configuration of the firewall for incoming and outgoing requests. The routers, switches and internet interface, must be included under the supervision of firewall to offer the security. Security policies and rules need the attention to protecting the system from unauthorised access and requests in the network.

### ***2.1.2 Missing Patches***

The network system must be configured and updated to the latest stable release. The equipment in the network like router and switches must be according to latest technology so that patches can be fixed to improve the security (Kavitha, 2010). The software in router and computer firewall also needs the same treatment to deliver the security in the network. The patches help to reduce the risk and close the security holes in network security. The regular monitoring of network performance and health contributes to achieving the security practices towards the patches.

### ***2.1.3 Access and Authentication***

The new network must need to include the password protection in the network so that one's files cannot be disclosed to others. The network security should be strengthened with security at each end in the network.

### ***2.1.4 Wireless Connectivity***

The network design has integration of wireless connectivity under the same ISP. The network will implement the firewall and filtering services between the router and internet so that network can be protected against the attacks and vulnerabilities (Nagurney, 2010). Proper use of switches and routers helps to achieve high security and easy maintenance in the network.

Also, as a good prevention for the network security of the company, it must take into consideration that the Wi-Fi router should have an option of isolation for the wireless network by lock down the Wi-Fi network on computers connected to the wired network. This solution is ideal for the business of the company to avoid possible intruders from public Wi-Fi networks. This solution limits and confines clients associated with the wireless network. They cannot interface with the computers related to the more secure wired system; they can use only the Internet.



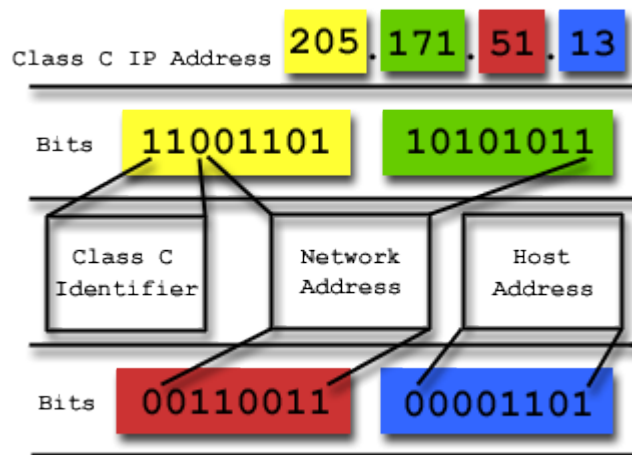
### 2.1.5 Disable the USB Ports

Also, the security solution must include exclusion or block the use of USB ports and other external drivers, to remove any risk of theft data or to avoid a bridge between the wired network and wireless network. The access to this configuration must be made by using a password known only by those responsible for the administration of the network.

### 2.1.6 IP Address Allocation

It is possible that devices in the network may be added and removed so that we need to manage the addressing of each device. IP addressing is required to identify the device in the internet to send the packets or to receive the response back. The IP address can be allocated in two ways: static and dynamic. The static means the IP address will be same for the device each time it will appear in the network as an online device.

The below diagram shows how class C IP addresses are in the structure.



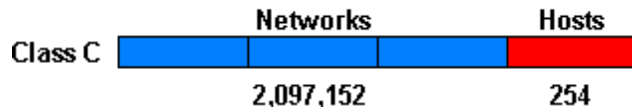


Figure 5 Figure 23 Class C IP address

### 2.1.7 Packet Filtering

Restricting IP packet consists of blocking packages, depending on:

- source and destination IP address,
- interface (NIC) input and output,
- the physical address of the source (e.g., Ethernet),
- protocol (TCP, UDP, ICMP),
- source and destination port,
- connection status (TCP),
- 

Rejected packets, network administrator of SS Ltd. can configure actions:

- recording in a log file (and possible packages admitted)
- ignoring package (as if it had not been received)
- sending back a packet of information (ICMP destination unreachable or TCP reset)

Restricting IP packets aims:

- preventing impersonation computers on the local network by outside intruders
- Denial of access to certain services externally.

- Thus, in the case of a burglary, being inside burglar can be found easily and punished.

### ***2.1.8 Intrusion Detection Systems (IDS)***

It will use an HIDS (Host based IDS) or Intrusion Detection System station. It records both operations performed and system resource usage.

The security audit in the network needs to be focused on the durability of the network in various attack conditions. The focus also should be given to the authentication process, transfer load and filtering of packets. SS Organisation can audit the policies to segment the network and to secure the user data during transmission (Forouzan & Mukhopadhyay, 2011).

## **2.2 Evaluate Design and Analyse Feedback**

The new network design is differing than the older design of network in many terms to offer high security and accessibility in network operations. The network design has added the additional switches to segment the various users and departments in the network so that network errors and faulty positions can be determined effectively. The organisation has better security with the addition of switches and there is no single point to control the network and fewer possibilities of failures. Each switch in the network represents the group of devices in the network so that organisation has better management of devices and associated addresses in the network. Addition to it, the firewall is used to filter the incoming network requests and control the unauthenticated packets in the network. The firewall implementation is done to protect the access to servers and assets in the network through the internet. Firewall applications are also used in each computer to provide the dual end security in the network (Natarajan, 2012). The computers have own authentication system to connect to the network, so it reduces the chances of key compromise in

the network. The authentication is required to block the unwanted users and to safeguard the information inside the network.

The users are also grouped according to their role and responsibility in the network so that information and assets can be used in an efficient manner. For instance, the printing service is only offered to the users those are from the group of printer users. The remaining users in the network cannot access the printer although they are connected to the same network. The network structure is also changed for the addressing as switches are used to use the same internet address to all other devices under the switch. For instance, the introduction of DHCP and subnet masking has reduced the requirements for the demand of IP addresses in the network (Wu, 2005).

The design of the system prevents the user from connecting the external devices like USB and other drives with the system so that information can be safeguarded against the theft and misuse. The SB drives and software becomes the reason of security breach in the network. BIOS can be safeguarded to prevent the USB connections. The new network also supports the software level authentication in the network so that users need username and password each time to login into the network to access the information and assets. The network design supports the WPA authentication system for wireless connections and open access points are removed for network security. Proper traffic management and MAC address filtering are implemented in the network through software to secure the network design.

VLAN solution could be useful to implement in the network as it can group the end station when the network is dispersed. Also, the routers can be reduced with the help of VLAN. The solution of VLAN is not yet implemented due to business constraints but can be in future improvements to meet the market changes and requirements. Segmentation is helpful to boost the network performance and to offer the security. Also, the failures in the system can be limited to a specific set of computers and visitors can be controlled effectively with segmentation.

Also, as a feedback for this solution is to design a segmentation plan of the network system. The network system could have added the additional switches to segment the various users and departments in the network so that network errors and faulty positions can be determined effectively. The organisation could have better security with the addition of switches and there could be no single point to control the network and fewer possibilities of failures. Each switch in

the network might represent the group of devices in the network so that organisation can have better management of devices and associated addresses in the network.

Now as it was designed the security solutions for the company is time to concentrate on the next task on implementation and testing steps.

## TASK 3     Implement and Testing Network Security Solutions

### 3.1 Network Security Implementation of SS Ltd.

The propose of this new network security solution is to protect the next issues:

#### *Sensitive data of the company*

List of intellectual property, trade secrets, identity information, data cards, medical information, databases of partners and any other data that can be retrieved from the compromised wireless network.

#### *Network Services of the company*

The list covers the e-mails accounts, files, databases, directories, user's application service, Internet connectivity, applications, web services viruses and intrusion detection that can be compromised by infiltrating the network.

The *advantages* of this implementation consist of:

- The best segmentation of the network
- The project requires a less financial investment
- A better authentication and access through Active Directory by better securing the wireless network
- Block potential risks to the wired network using mobile phones as a bridge to the outside network
- Also, an advantage is the use of VPN, which allows secure access to the company's internal network from any location
- Not least, the development of security hampers physically stealing of company data.

The disadvantages of implementing the new security are:

- The time of the implementation is longer
- Limit the use of USB and other storage devices, saving all passwords used within the network,
- Limit the access only to authorised persons, darkening process work among the employees and the contractors.

To ensure network security is important to implement specific mechanisms from the physical (Physical Protection of transmission lines), continuing with procedures to block access to the network (firewall), to the application of coding techniques data (encryption), or by protecting a specific method for communication between processes running on different application type network computers.

The network can be implemented to ensure the better security and availability of resources. The design can be carried out in more steps. The first phase of implementation is dedicated to configuring all the devices for the IP address allocation. Later Virtual Local Area Network will be implemented. The implementation will be done for the switches and routers configuration in the network, followed by MAC address filtering, disable the USB ports, good authentication and secure wireless network.

### ***3.1.1 Switch Configuration***

The switch configuration can be done in the following manner. First look at the switch configuration.

- Enter command to configure the switch  
S1# configure terminal
- Enter into interface configuration mode.  
S1(config)# interface fastethernet 0/1
- Now configure the interface duplex mode via the command.  
S1(config-if)# duplex full

- Configure the interface speed.  
S1(config-if)# speed 100
- Then return to EXEC mode.  
S1(config-if)# end
- These are three basic commands to verify the setting (Garg, 2010)  
S1# show interfaces[*interface-id*]  
S1# show startup-config  
S1# show running-config

### **3.1.2 Router Configuration**

- Configure terminal in the router with the following command:  
Router> enable  
Router# configure terminal
- Set the hostname  
Router(config)# hostname Router
- Enable password to secure the access to router  
Router(config)# enable secret qr1dy5ho
- Disable the router so that it cannot translate the unknown words in IP address.  
Router(config)# no ip domain-lookup
- Set interface for local Ethernet connection  
Router(config)# interface gigabitethernet 0/1
- Now set IP address and subnet marking through router configuration  
IP address 192.168.0.0 255.255.255.0
- Enhance administrative privileges to control the router shutdown status  
Router(config-if)# no shutdown  
Router(config-if)# exit



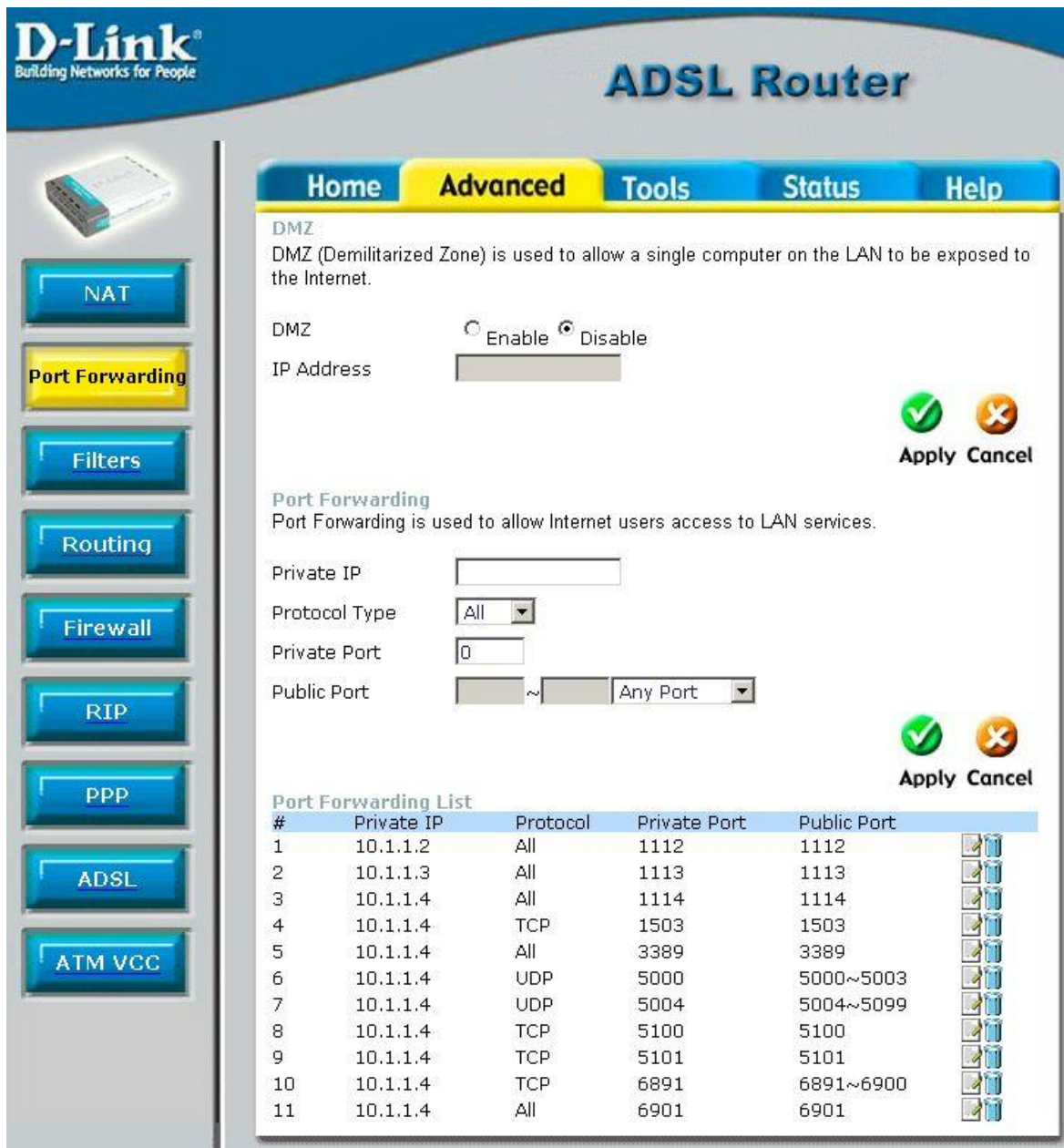


Figure 6 Router configuration

*Source Internet*

Static IP address can be used to handle the limited number of computer in devices as it is secure to prevent the external devices in the network due to lack of extra availability of IP addresses in the network. A firewall can be implemented on computers as well for the network to filter the

packages and to control the communication among internal devices and outer devices. Contractors in the wired network can be closed to prevent the addition of mobile devices in the network.

### 3.1.3 Disable USB from BIOS

To avoid a bridge between the wired network and wireless network it is recommended to disable USB ports from the BIOS, it can prevent unauthorised persons to enter the company network to steal data or to use the network system. To disable the USB ports to be accessed must follow the next steps:

- Enter BIOS and select the option to enable or disable onboard USB ports
- Save and exit with F10

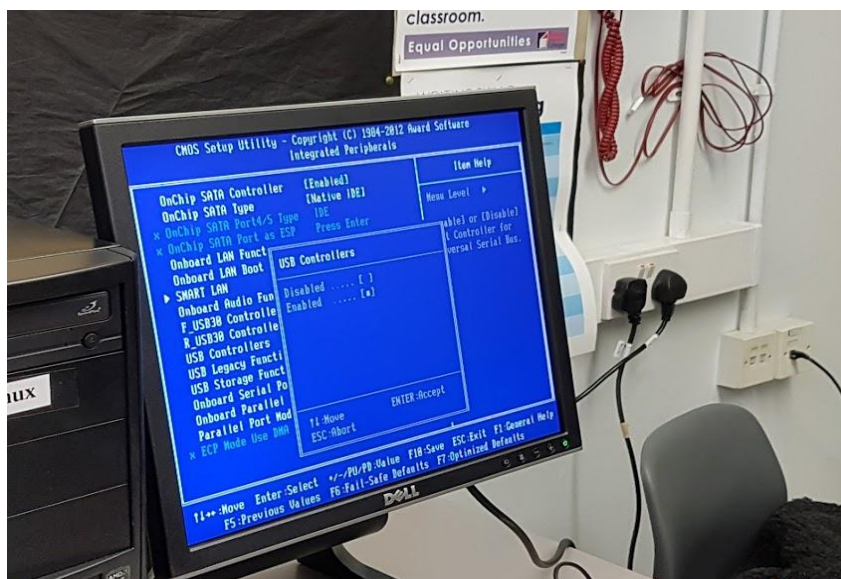


Figure 7 Disable the USB from BIOS

- Setting a password to enter the BIOS setup configurations that prevent changes by unauthorised persons.

### ***3.1.4 Good Access and Authentication***

At the level of Active Directory is implemented the security policies, is the level of authentication and authorization. Users of SS Network can use their password information to access the network resources and data. The security on the database server and data servers should be reviewed to enhance the security of the network (Hoque, 2014).

A proper authentication means:

- Selecting the passwords with a combination of alphanumeric characters along with special symbols.
- Make the password longer than 8 characters.

The password should regularly be changed to reduce the chances of assumptions and hacks.

### ***3.1.5 Secure Wireless Network***

#### ***Change the router password management***

The easiest step to secure the wireless network router password is by changing the provider password with a new password. Choose a unique password composed of at least 15 characters (uppercase and lowercase letters, numbers and signs).

#### ***Firmware updates for the router***

Whenever bugs are discovered at a particular router manufacturer, the router provider comes with a new firmware that these security holes are solved (like updates Windows Security Updates). Before the new firmware update, it should have a backup of the current settings directly from the router.

### *Having Wireless Isolation Option*

The company will use wireless isolation feature by enabling the isolation option for Wi-Fi clients of SS Ltd. This implementation will lock down the communications with other devices on the local network. Through a configuration of firewall tenets, customers associated with the Wi-Fi may have the capacity to speak with the Internet, not each other or any other computers from the wired system.

To implement this option generally, the settings are under Wireless > Advanced Wireless Settings > AP Isolation:

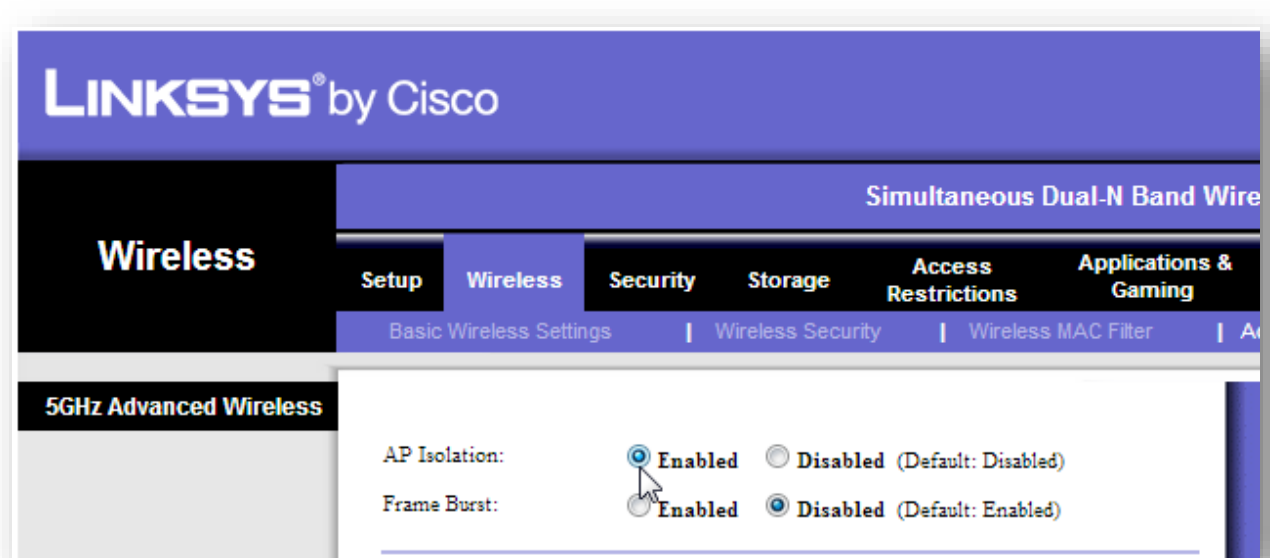


Figure 8 Implement the Wireless Isolation Option

### *Use encryption at wireless router login*

It is creating a password for SS's wireless network and set WPA2 as standard encryption/authentication for a password to be better protected from hackers. It is recommended to use WPA2 because WEP has been proven to be extremely easy to decode/broken. Using WPA2 encryption, there is a guarantee that whenever a network device (PC, laptop, mobile phone.) is connected to the router, the password is sent encrypted. Typically, WPA2 mode setting is

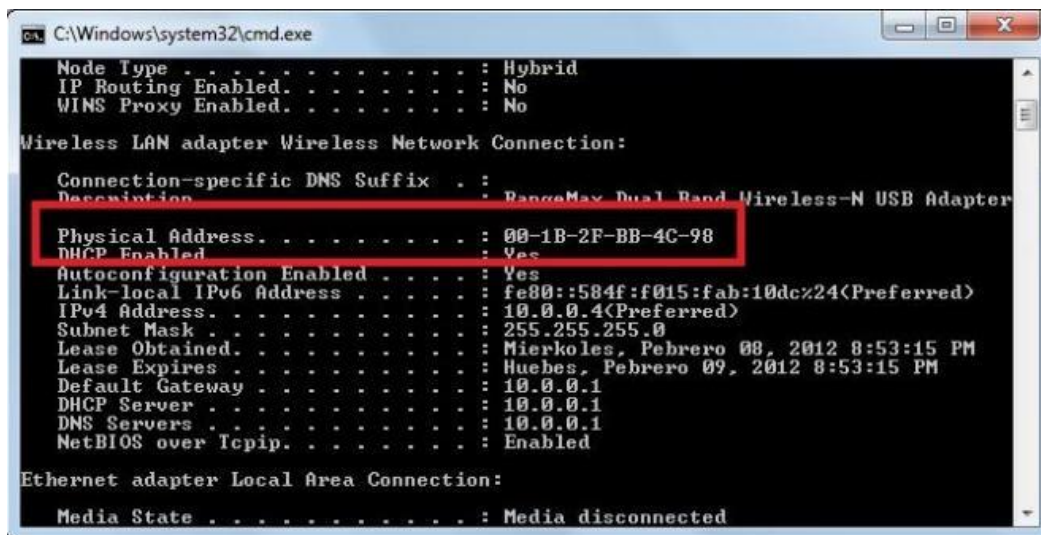
performed directly within walking distance from the router's management interface, here is a quick example:

- look for wireless security settings menu
- Choose WPA 2 and AES encryption (Advanced Encryption Standards)
- Pre-Shared Key Enter a combination of 8-63 alphanumeric characters
- Selecting a password authentication (a unique combination of alphanumeric characters, it is well to remember easily because it will be required when somebody wants to connect to the wireless network)

### *MAC address filtering*

Once the password was changed for the SS Ltd. wireless, now it can ensure that the device used by an unwanted guest will not come again. Even if the unauthorised user is managing to find the new wireless password, he cannot access the router because his MAC address is blocked by the router, after his MAC address was added to the blocked devices list.

Find the MAC address of the computer devices by running the command: `ipconfig /all`



```
C:\Windows\system32\cmd.exe
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Wireless LAN adapter Wireless Network Connection:

Connection-specific DNS Suffix . : 
Description . . . . . : RangeMax Dual Band Wireless-N USB Adapter
Physical Address. . . . . : 00-1B-2F-BB-4C-98
DHCP Enabled . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::584f:f015:fab:10dc%24(Preferred)
IPv4 Address. . . . . : 10.0.0.4(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Mierkoles, Pebrero 08, 2012 8:53:15 PM
Lease Expires . . . . . : Huebes, Pebrero 09, 2012 8:53:15 PM
Default Gateway . . . . . : 10.0.0.1
DHCP Server . . . . . : 10.0.0.1
DNS Servers . . . . . : 10.0.0.1
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Local Area Connection:

Media State . . . . . : Media disconnected
```

Figure 9 Look for MAC address

Now configuring the MAC address in router setting and update the router for MAC filtering to allow only the authorised devices to use the network of SS Ltd.

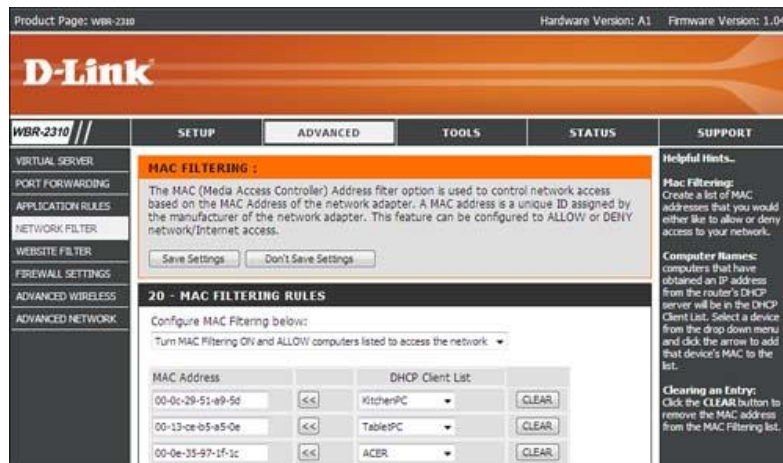


Figure 10 Configure the MAC address

**Hide SSID** - Open the web page of the router chose advance configuration to hide the SSID from the outer side.

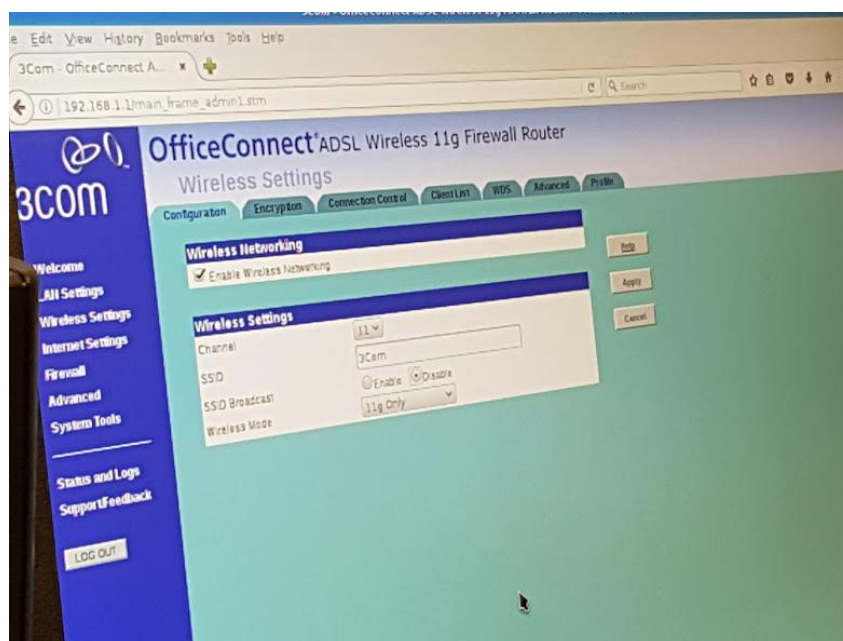


Figure 11 Hiding the SSID



### 3.1.6 Virtual Private Network (VPN)

Implementing Virtual Private Network (VPN) establishes a link per-to-per (point to point) with other shareholders of the company others then the staff, this communication is safe, encrypted, cannot be intercepted by a Man in the Middle, but there are others that can communicate through HTTPS but less safe.

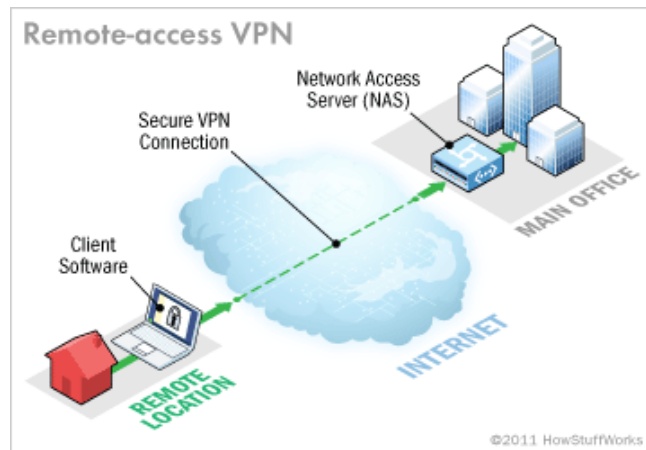


Figure 12 Implementing a VPN solution

source: <http://computer.howstuffworks.com/vpn3.htm>

### 3.1.7 The Physical Security of The Equipment

Physical security is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to SS Ltd network. This involves protection from natural disasters, flood, fire, theft, burglary, vandalism and terrorism.

- **Ensure security servers:** The servers will be closed in a server room, to avoid any intentional damage or accidental damage. The server's rack will be located in a room in which the access is limited and this server rack will have a lock on it.



Figure 13 Secure the rack servers with locks

- **Cable Protection:** The network cable can interfere with a device for an interception and in this case, the data can be stolen directly. In this context, in the design phase, the cables are routed laid down in such a way as to not allow the access of unauthorised persons.
- **Save backups of data and programs:** safety carry out the operations to save data and programs will be made on both the magnetic supports and through the cloud. The procedures for conducting backups of data are included in the security. Data can be lost or damaged in the circumstances such as theft, equipment failure or natural disasters such as a fire or flood. Backing up data is one of the most effective ways of protecting against data loss. Backup data will be carried out daily, weekly and monthly.
- **To protect the network area** of the company must always be security measures such as fencing building, locks, get to control cards and fire concealment frameworks. Physical areas ought to be observed utilising security cameras and notice frameworks, for example, interruption location sensors, warm sensors and smoke finders.





Figure 14 Intruder Alarms, CCTV and Fire Detection

Source Internet: <http://www.dragonfs.co.uk/>

- **Disaster recovery** policies and procedures should be tested on a regular basis to ensure safety and to reduce the time it takes to recover from disruptive human-made or natural disasters.

The network has been implemented with desired functions and features through the configuration of all devices in term of their addresses and settings to connect with other devices. The network has efficient use of switches and routers to perform the business objectives. The next step is to see if the implemented security solutions are working by testing differently implemented solutions.

### 3.2 Testing of Network Security Implementation

The network has been tested in the following manner:

#### *Switch testing:*

In switch testing, the switch is made connected to some of the devices in the network. The packet tracer tool is used to check the setting of the switch to connect with six computers. The switch configuration and functioning are tested and shown below:

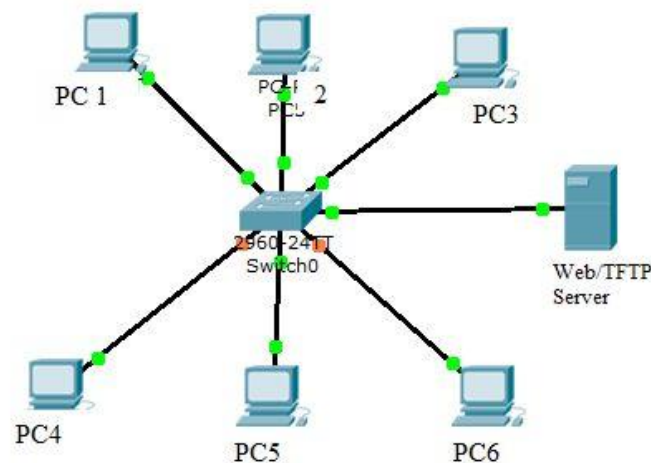


Figure 15: Switch testing  
(Source: switch testing, 2016)

#### *Router testing*

The router setting is also simulated with network packet tracer tools. The tool shows that the configuration is effective to serve the devices with performance and security (Lam, 2011). The router configuration is tested along with switches to ensure the integrated functionality delivered by them to the network. The router has security against the unknown packets and requested. The router has effective functioning and performance as measured by the tool.

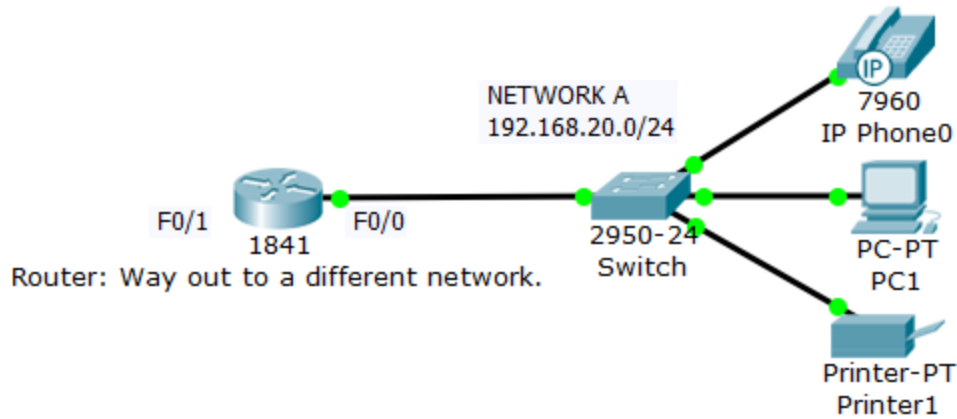


Figure 16 Router configuration

What kind of network vulnerability tests does testing?

Proposed are two kinds of testing: internal and external tests.

### 3.2.1 Internal Tests

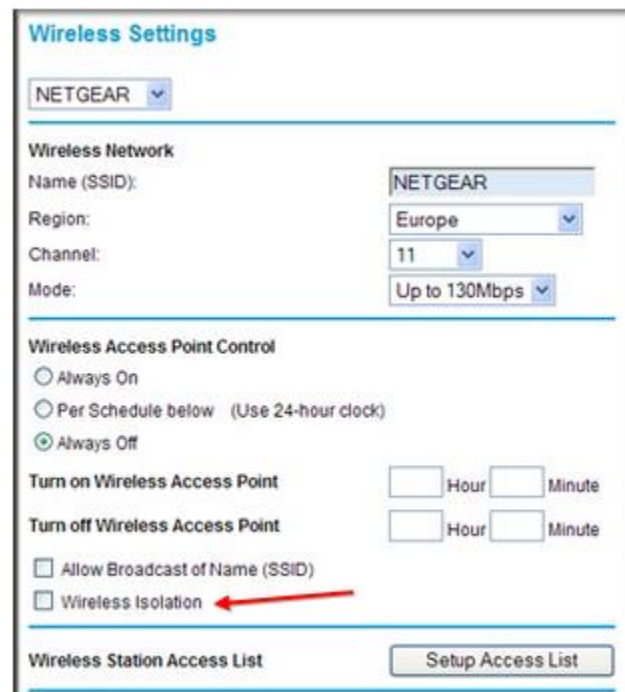
Internal Tests are the tests that assess security within the network, related to the staff and clients of the company.

These tests are aimed at finding vulnerabilities and access methods that lead to unauthorised access to staff, or elevation of privilege in an unauthorised manner.

It will test, among other things, security policies, the effectiveness of antivirus and system susceptibility to complex attacks, such as MIT/ARP spoofing/Window/Downgrade Authentication and others.

### *Test the Wi-Fi Isolation Option*

To ensure that the wireless network is isolated from the wired network of the company  
It is recommended to go to advanced settings of the router configuration and check if Wireless Isolation is enabled or not, to prevent possible intruders on the wired network of the firm:



The screenshot shows the 'Wireless Settings' page for a Netgear router. The 'Wireless Network' section includes fields for Name (SSID) set to 'NETGEAR', Region set to 'Europe', Channel set to '11', and Mode set to 'Up to 130Mbps'. The 'Wireless Access Point Control' section has three radio buttons: 'Always On', 'Per Schedule below (Use 24-hour clock)', and 'Always Off' (which is selected). Below these are fields for 'Turn on Wireless Access Point' and 'Turn off Wireless Access Point', each with 'Hour' and 'Minute' sub-fields. There are two checkboxes: 'Allow Broadcast of Name (SSID)' and 'Wireless Isolation'. A red arrow points to the 'Wireless Isolation' checkbox, which is currently unchecked. At the bottom, there is a 'Wireless Station Access List' section with a 'Setup Access List' button.

Figure 17 Check if Wireless Isolation is enabled

### *Test of disabled functionality of USB on wired computers*

Another option to test the implemented network security solution for SS Ltd. is to check if the USB functionality is disabled from the BIOS. This test comes to counteracting any bridges with the wired network, and corporate data theft.



Among the tools used in penetration testing programs are listed following categories:

- a) ***Firewall test*** - Firewall is effective to filter the internal and external request in the network. Access control list prevents the internal users to access only the granted portion of the network and also filters the external requests. The internal users also need to go through the firewall before the file server and HTTP server so that their permissions and rights are examined to grant their requests. The external requests are blocked though the ACL in the firewall.

To see if SS Network has a good security there are some tests which can be done through Shields Up from Gibson Research Corporation's website.

### ***Common Ports Tests***

The below image come with results regarding open ports test, in which Solicited TCP Packets and Unsolicited Packets both have PASSED and Ping Reply has been RECEIVED which means that SS network system replied to ICMP Echo Ping.

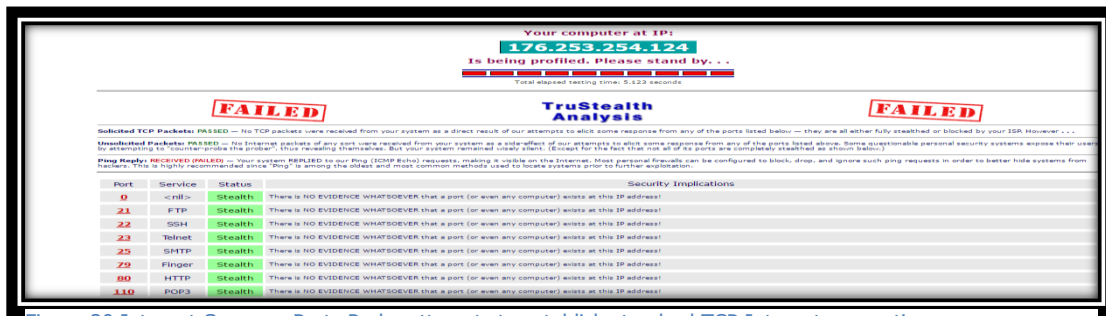


Figure 20 Internet Common Ports Probe attempts to establish standard TCP Internet connections

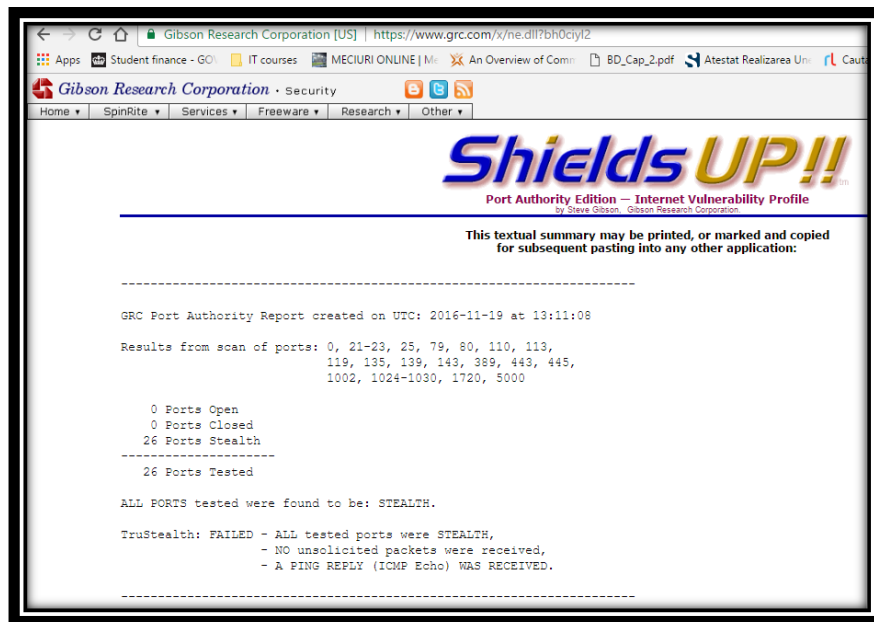


Figure 19 Results of the scan of ports

Also, the verification of the open ports can be done with command prompt using command netstat -an, Start -> Run -> cmd -> netstat -an:

```

C:\Windows\system32\cmd.exe

Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\mitrea>netstat -an

Active Connections

Proto Local Address           Foreign Address         State
TCP    0.0.0.0:135              0.0.0.0:0               LISTENING
TCP    0.0.0.0:445              0.0.0.0:0               LISTENING
TCP    0.0.0.0:2869             0.0.0.0:0               LISTENING
TCP    0.0.0.0:5357             0.0.0.0:0               LISTENING
TCP    0.0.0.0:6783             0.0.0.0:0               LISTENING
TCP    0.0.0.0:6783             0.0.0.0:0               LISTENING
TCP    0.0.0.0:49152            0.0.0.0:0               LISTENING
TCP    0.0.0.0:49153            0.0.0.0:0               LISTENING
TCP    0.0.0.0:49154            0.0.0.0:0               LISTENING
TCP    0.0.0.0:49155            0.0.0.0:0               LISTENING
TCP    0.0.0.0:49165            0.0.0.0:0               LISTENING
TCP    0.0.0.0:49169            0.0.0.0:0               LISTENING
TCP    127.0.0.1:5939           0.0.0.0:0               LISTENING
TCP    127.0.0.1:9527           0.0.0.0:0               LISTENING
TCP    127.0.0.1:30000          0.0.0.0:0               LISTENING
TCP    127.0.0.1:49954          0.0.0.0:0               LISTENING
TCP    127.0.0.1:50911          0.0.0.0:0               LISTENING
TCP    192.168.0.3:139          0.0.0.0:0               LISTENING
TCP    192.168.0.3:49209        40.77.229.28:443        ESTABLISHED
TCP    192.168.0.3:49212        52.209.33.66:443        ESTABLISHED
TCP    192.168.0.3:49435        64.233.166.188:5228     ESTABLISHED
TCP    192.168.0.3:49469        31.13.90.36:443         ESTABLISHED
TCP    192.168.0.3:49624        31.13.90.2:443          ESTABLISHED
TCP    192.168.0.3:50419        52.48.63.69:443         ESTABLISHED
TCP    192.168.0.3:50537        104.20.66.90:443        ESTABLISHED
TCP    192.168.0.3:50551        54.77.253.102:3050      ESTABLISHED
TCP    192.168.0.3:50582        52.21.184.191:443       ESTABLISHED
TCP    192.168.0.3:50585        52.48.63.71:443         ESTABLISHED
TCP    192.168.0.3:50592        52.21.184.191:443       ESTABLISHED
TCP    192.168.0.3:50606        216.58.214.3:443        TIME_WAIT
TCP    192.168.0.3:50607        172.217.17.67:443       TIME_WAIT
TCP    192.168.0.3:50609        216.58.198.174:443      TIME_WAIT
TCP    192.168.0.3:50625        74.125.206.154:443      TIME_WAIT
TCP    192.168.0.3:50658        192.168.0.1:5431        TIME_WAIT
TCP    192.168.0.3:50667        104.18.63.176:443       TIME_WAIT
TCP    192.168.0.3:50668        216.58.214.3:80         TIME_WAIT
TCP    192.168.0.3:50671        104.25.3.34:443         TIME_WAIT
TCP    192.168.0.3:50675        104.198.49.0:443        TIME_WAIT
TCP    192.168.0.3:50676        104.198.49.0:443        ESTABLISHED
TCP    192.168.0.3:50689        136.243.63.184:80       TIME_WAIT
TCP    192.168.0.3:50696        216.58.212.110:443      TIME_WAIT
TCP    192.168.0.3:50698        216.58.212.110:443      TIME_WAIT
TCP    192.168.0.3:50699        52.54.2.72:80           CLOSE_WAIT
TCP    192.168.0.3:50700        52.54.2.72:80           TIME_WAIT
TCP    192.168.0.3:50701        52.59.77.252:80         ESTABLISHED
TCP    192.168.0.3:50702        54.165.242.147:80       CLOSE_WAIT
TCP    192.168.0.3:50703        23.64.16.151:80         TIME_WAIT
TCP    192.168.0.3:50704        90.223.204.24:80        ESTABLISHED
TCP    192.168.0.3:50705        23.64.16.151:80         TIME_WAIT

```

Figure 21 Verification of open ports through command prompt



- b) *Query DNS (nslookup)* - To find the IP address of a host on the domain name or IP address corresponding to a domain name nslookup command. It queries the DNS server whose IP address is set on the local computer. For example, finding the IP server:

```
C:\Users\mitrea>bslookup
'bslookup' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\mitrea>nslookup
Default Server:  Unknown
Address:  fd64:555a:f26b:0:9221:6ff:fe93:ca0c
```

Figure 22 Using command nslookup to find a IP address of SS Network

c) *Spoofing ability test:*

In the below pictures, external ping and query are ignored, DNSSEC security server has good security standards, that means a good anti-spoofing configuration.

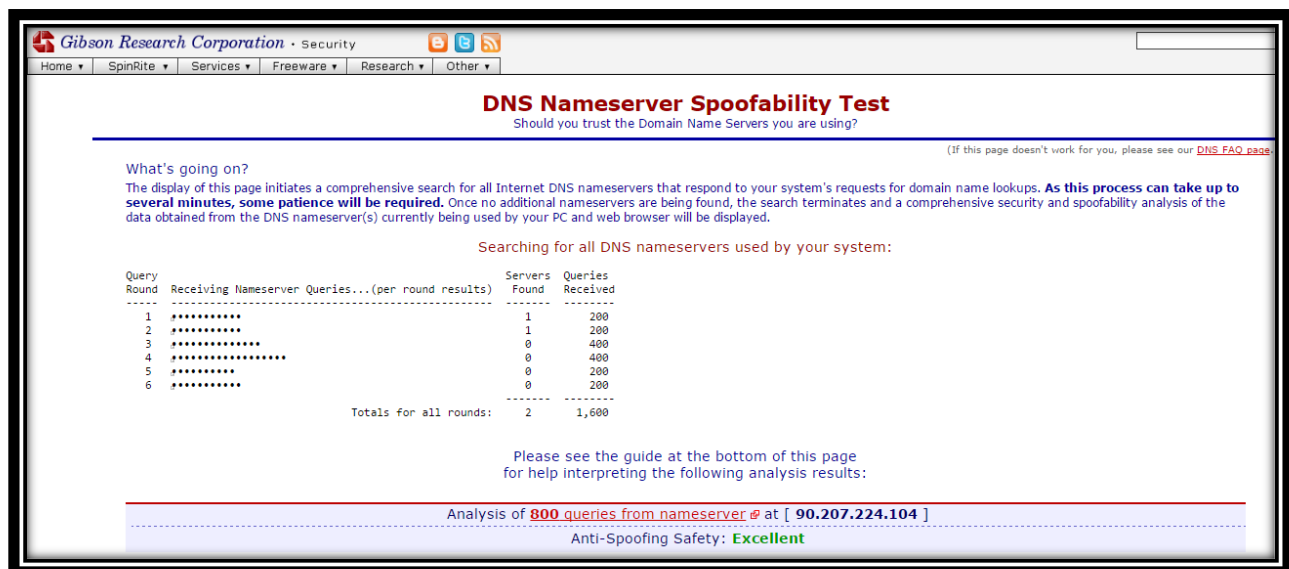


Figure 23 Spoofability Test

Query Source Port Analysis (worst case)				Query Transaction ID Analysis (worst case)			
Max Entropy:	15.92	Excellent		Dir Bias:	1.13%	Excellent	
Lost Entropy:	0.01	Excellent		Stuck Bits:	0	Excellent	

DNS Nameserver Access Details	
External Ping:	ignored (Nice, as it's preferable for it to be less visible.)
External Query:	ignored (This means the nameserver is more spoof resistant.)
DNSSEC Security:	supported (This server supports improved security standards.)
Alphabetic Case:	all lower (An improvement could be created by mixing case.)
Extra Anti-Spoofing:	unknown (Unable to obtain server fingerprint.)

Figure 24 Results of Anti-spoofing test

d) *Windows File Sharing testing:*

In the below figure, SS network computers are in full stealth mode and are not showing any information over the internal NetBIOS networking protocol.



Figure 25 File Sharing test

e) *Router security testing:*

As is shown in the next image, the router has a good firewall configuration to do not be visible from outside of SS Network.

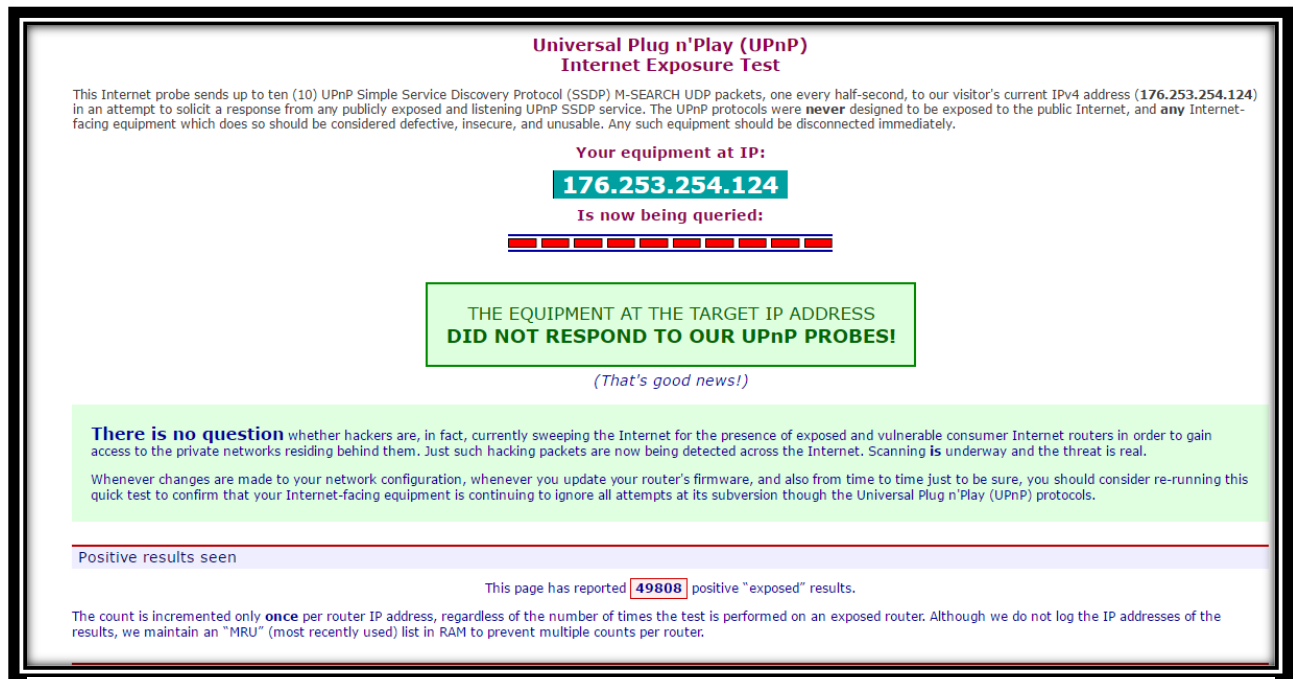


Figure 26 Check the visibility of SS router from outside of the network

### 3.3 Analysis of Test Results

The network design is effective than the older design and delivers the demands of the organisation for a secure and robust network. The network has high security using firewall and filtering services. All connections are directed towards the network firewall to check their packets for proper encryption and authentication. In the same manner, the incoming packets are being checked at the firewall for their authentication and destination in the network. It helps to achieve the security. Also, the routers and switches are configured to eliminate the attacks of the unwanted request and access to them. The network is effective to close all the open holes in security. Following test results are achieved with network implementation.

- Security is achieved through proper configuration of firewall, equipments and software.
- Firewall is effective to filter the internal and external request in the network. Access control list prevents the internal users to access only the granted portion of the network and also filters the external requests. The internal users also need to go through the firewall before the file server and HTTP server so that their permissions and rights are examined to grant their requests. The external requests are blocked though the ACL in the firewall.
- MAC addresses are used to support the lower level Ethernet network. The devices use the MAC addresses to reach the right destination in the network. Unique MAC address is implemented to segment the network and to identify the device in Ethernet.
- Efficiency is achieved to manage the traffic and congestion in a network through software so that network has high performance to serve the devices (Krutz, 2010).
- Proper segmentation of network helps to manage the network issues effectively with reduced effort and analysis. MAC addresses are used to support the lower level Ethernet network. The devices use the MAC addresses to reach the right destination in the network. Unique MAC address is implemented to segment the network and to identify the device in Ethernet.
- Security is achieved through proper configuration of disabling the USB functionality inside the wired network of the company for possible vulnerabilities as data theft or forming bridges with public Wi-Fi networks.
- Wi-Fi access is limited to known users only as WPA encryption is strong enough to prevent the assumptions and brute force cracking to penetrate the network. Intruders also need to know Wi-Fi SSID to connect with the hidden network. Internal mobile users know the SSID and WPA security so that they can connect safely. Encryption helps to prevent the data during transmission, access and sharing.
- Efficiency is achieved by using the option to lock down the access to computers from the wired network of the company to use the possible public wireless networks, through the use of Wireless Isolation option.
- Antivirus programs are updated in every computing system so that the entry of virus can be prevented and users can be alarmed with notifications on system health and security. In

this manner, the network is effective to secure the data and assets in the network. The performance is effective under the present load of data transmission in channels and requests to the server. However, the design is still supposed to have some changes to meet future risk and demands.

- It has proven effective on a physical level using surveillance cameras, securing the offices and hardware network by using locks to prevent unwanted person access and also planning backups of corporate data in the event of natural disasters or malicious actions.
- Regarding Penetration Test, it demonstrated effective implementation of the proposed solutions:
  - ✓ web vulnerability scanner
  - ✓ web proxy
  - ✓ web crawlers
  - ✓ tools used for information gathering
  - ✓ operating tools
  - ✓ wireless attacks

Parameter	Old design	New Design
<b>Bridging over the company network</b>	No	Yes, the wireless network has been isolated from the wired network
<b>Segmentation</b>	No	Perfectly
<b>DHCP</b>	No	Yes
<b>Firewall</b>	No	Dual firewall- in internet router and computers

<b>Control</b>	To single switch	More switches to control network
<b>Authentication</b>	Not at user side	Yes. With 128-bit encryption
<b>Cost to design</b>	High	Reduced
<b>Packet filtering</b>	Less security	High against inside users and outsiders.
<b>Wireless connectivity</b>	Low and less controllable	Yes, with better integration in network
<b>Blocking using USB</b>	No	Yes
<b>The physical security of the equipment</b>	No	Yes

The next step after the implementation and testing of the proposed security of SS Ltd.'s Network it will be presented the methods of maintenance of the proposed solution, the audit company's network security and possible improvements of the proposed solution.

## **TASK 4    Manage Network Security Solutions**

Managing the network for its continuous performance and security is necessary. A proper audit of policies and rules needs attention to secure the network under the increased number of users and wireless connectivity. The organisation needs to maintain the services over time in the following areas:

### ***4.1    General Maintenance***

Periodic maintenance is essential to maintain the safety and reliability of equipment, machinery and the environment. Maintenance works are carried out in all sectors of the company. Maintain security and reliability of equipment, machinery and working environment of the company.

It is recommended to have periodic updates of the accounts passwords and also router password, to change them monthly, for example, to avoid possible risks of intruders, data thefts or data leaks from the interior of the network to the external sources. In the same way, it is recommended to change periodically the codes of keypads of each office which has one.

Some maintenance operations for SS network security include:

- Installation and configuration of switches and routers
- Network management by authorised personnel
- Managing user access network by authorised personnel
- Configuring workstations to access files on the network
- Managing, restricting and monitoring access to the Internet
- Server and network monitoring to prevent incidents

- Configuration, management and security field; Active Directory, Group Policies, scripts
- DNS server configuration
- Network monitoring to prevent incidents
- Server configuration files; managing user access
- Setup router/ firewall
- Email server configuration; managing user access
- Web server configuration
- Installation and maintenance of email servers, manage email addresses

Maintenance management is responsible for:

- Operating safety equipment (reliability, availability, security, maintainability)
- Tracking maintenance costs and use of fixed assets
- Operational risk management
- Human resources management of maintenance

***The usage of channels:*** the organisation needs to determine the utilization of the channel. If the channel is not effective to meet the performance criteria, then bandwidth can be enhanced and alternatives can be used to enhance the user network experience. The bandwidth management is necessary to bring the control on congestions and packet dropping. The network needs to be analysed for the proper distribution of channel and bandwidth through switches and routers. The organisation may also need to expand or reduce the coverage of routers in wireless connectivity.



## **4.2 Security Audit**

The audit work examines in detail the activities on network security of SS Ltd. or its products and services to determine or estimate the extent that activities and results are consistent with a statement assumed and with some specific objectives agreed or applicable regulations. The audit activity of the company has some key moments in time. These include the conclusion of those identified in several deliverables types, such as audit opinion, audit report, action plan, plan actions corrective/preventive.

### **4.2.1 Security Assessment Services**

#### ***a) Network security assessment and data communications, traffic, wireless, access control and OS platforms.***

The evaluation shall identify all the ways of access to the network and their safety, both from inside and outside of the network. It shall also assess the presence of the services needed, vulnerabilities specific to each platform, errors of configuration and no security patches.

The final report shall result in the following evaluation which will contain considered information about each vulnerability and remediation recommended by the specialists. These recommended solutions are directly arising out of the best practices of vendors, best practices of security, as well as on the extensive experience gained around the area of technologies, concepts and security techniques.

#### ***b) Security Assessment Software***

The company wants a firm assurance on the fact that a business application works 100% for the purpose it was created; the organisation needs to guarantee that the business application is stable and meets minimum security parameters imposed.

#### ***c) Physical Security Assessment***

Physical security assessment of the working environment has become a critical issue for information security and aimed to identify shortcomings in the implementation of security policies.

Analysis of security databases is an essential process because it identifies weaknesses, threats and security breaches that could be exploited at a time of malicious hackers to get access to crucial information for everyday work of the organisation. Exploited vulnerabilities can lead to loss of vital information, major financial losses and not least the dramatic drop in the company's image to investors and partners, so by default to reduce the market share.

- Security evaluation of facilities: security access, security Data-centre activities, work spaces with limited access
- Evaluation of the implementation of security policies on company staff/visitors/contractors: use of equipment; monitoring access between the wired network and the Wi-Fi area network, to avoid to prevent the bridges between them; alignment with internal security policies; awareness; the use of recreational facilities and access roads
- Physical security evaluation of IT equipment: Computer; servers; Backup media; PDAs; Access Points
- Safety assessment of detailed data: document control; store confidential data; the destruction of confidential documents

The final report, drafted by analysing goods, hazards and vulnerabilities discovered, not only contains a list of recommendations but a prioritisation of exposure depending on the degree of risk. Therefore, the company can apply the right level of security for each service.

#### **4.2.2 Vulnerability Assessment**

Vulnerability Assessment is less viable than penetration testing. Therefore, it is recommended that vulnerability assessment be made on less critical systems or workstations and penetration tests to be done on the vital systems of the company. Also, it is recommended a periodic assessment of vulnerabilities be implemented alongside, prompt capping on new ones, thus avoiding their exploitation.

### 4.2.3 Penetration Testing Assessment

The main objective of a penetration test is to identify any security vulnerability of a system; from the perspective of a hacker. The tests are carried out to determine if vulnerabilities that could exploit the system are discovered and if so, their impact on the smooth running of the organisation.

Risk analysis includes penetration testing at the network level, whose objective is to test network infrastructure and servers and application penetration tests and also, is to check the active application services.

Alongside this, tests can be conducted both inside the organisation and outside (the Internet).

Penetration tests provide the company with a clear picture of vulnerabilities through superior system scalability and thus to develop a management strategy that will aim to finally remedy existing security problems and avoid the appearance of others.

### 4.3 Recommend Potential Change Management

For further changes, it is important keeping updated the new technologies of the network security, which will bring more protection for SS Ltd. network and these changes should be followed by implemented them as soon as possible, to avoid potential risks. Also, together with new updates of the network security must come with the necessary training for the staff.

The legislation related to the network security is one of the most developed from day to day and it is strong recommended keeping an eye on the news related to this domain.

For the future changes the company can have an *IP address allocation and a virtual local area network(VLAN)*.

### *a) IP address allocation*

It is possible that devices in the network may be added and removed so that the addressing of each device needs to be managed. IP addressing is required to identify the device on the internet to send the packets or to receive the response back. (Donlin, 2011).

It is possible that devices in the network may be added and removed so that the addressing of each device can be managed. IP addressing is required to identify the device on the internet to send the packets or to receive the response back. The IP address can be allocated in two ways: static and dynamic. The static means the IP address will be same for the device each time it will appear on the network as an online device. However, there may be an issue when a large number of devices needs to be managed and it becomes difficult to remember the IP address of each device. Thus, the network is implemented with DHCP in which there is no need to remember and assign the IP addresses of devices. The effort can be reduced to manage the IP addresses and to assign them to devices each time they are online (Donlin, 2011).

The class C IP address is effective to meet the organisational demands because it has enough number of hosts and devices in the network. Within class C addressing, an organisation can add up to 254 devices under the same network Identification. Also, it helps to meet the future demands. The organisation can use 3 to 4 subnets in the network: one for the management team, the second for contractors and third for rest of employees. The basic IP address can be 192.168.0.1; then the subnet can be created with a subnet mask 255.255.255.192 in which the host address range could be 192.168.0.1-192.168.0.62. The network will have a subnet ID 192.168.0.0.

- Management addresses: 192.168.0.0/10
- Contractor address: 192.168.0.0/20
- Rest to employees with wired connection: 192.168.0.0/20
- Employees with wireless networking: 192.168.0.0/12

The organisation can use following addressing scheme for routers and major devices in the network. Other devices will be addressed through Static IP configuration.

Device	IP	Subnet Mask
Srv0	192.168.3.1	255.255.255.0
WAP0	192.168.2.1	255.255.255.0
Router	192.168.1.0	255.255.255.0
Srv1	192.168.3.2	255.255.255.0
PC	192.168.4.1/30	255.255.255.0

Figure 27 Static IP configuration

#### *b) Virtual local area network*

The network address allocation can be broadcast with partitioning and domain based isolation so that the address can be enhanced to meet the organisational requirements. The basic domain address in the network can be split into some subnet addresses in organisations (Opricovic, 2003). The virtual networking helps to subdivide the LAN and to achieve the high usability of addresses.

<b>Vlan ID: 15-20 IPs: 192.168.20.10/35</b>
<b>Vlan ID: 1-18 IPs: 1192.168.10.38/52</b>
<b>Vlan ID: 21-24 IPs: wireless/DHCP assigned</b>

Figure 28 VLAN configuration

Devices in the network must be analysed over time for performance in the network. Software and hardware tools should be updated accordingly to a stable release to use the new technology and to achieve performance. A better routing algorithm, faster encryption and decryption, can help to achieve improved performance. The wireless connections are most vulnerable to performance and security issues, so that organisation needs to arrange the resources to enhance their coverage. The performance also can be improved by monitoring the network usage by specific users (Ciccarelli,

2012). Connections can be rearranged to meet the requirements of expansion and addition of new devices in the network.

## **CONCLUSION**

The report has discussed the advantages and disadvantages associated with existing network security design of SS Ltd., as well as identifying the vulnerabilities on network security. Also, the various attacks on network security have been recognised, along with their impact on the network. Recommendations about a new network security design for the organisation with proper positioning and use of resources has been made. The new design of network has been evaluated with the previous network design to fulfil the organisational demands and expectations. A discussion of in-depth steps of implementation of the network in the organisation has been completed. The testing has been done for the effectiveness of the network. The documents have been prepared for testing of the design. The final section of the report has suggested the maintenance and recommendations in network improvements.

## Bibliography

- Balthrop, J. F. S. N. M. a. W. M., 2004. *Echnological networks and the spread of computer viruses*, s.l.: Science.
- Carrasco, J. D. S. a. E. F. O. S., 2004. *System and method for rapid completion of data processing tasks distributed on a network*. s.l.: U.S. Patent 6,775,831.
- Casas, P. M. J. a. O. P., 2011. *Steps towards autonomous network security: unsupervised detection of network attacks*. s.l.:In New Technologies, Mobility and Security (NTMS), 2011 4th IFIP International Conference on (pp. 1-5). IEEE..
- Ciccarelli, P. F. C. F. J. D. A. G. D. a. S. T., 2012. *Introduction to Networking Basics*. s.l.:John Wiley & Sons.
- Ciccarelli, P. F. C. F. J. D. A. G. D. a. S. T., 2012. *Introduction to Networking Basics*. s.l.:John Wiley & Sons.
- Donlin, A. S. P. a. N. B. X., 2011. *Secure exchange of IP cores*. s.l.:s.n.
- Forouzan, B. A. & Mukhopadhyay, D., 2011. *Cryptography and network security*. s.l.:Tata Mcgraw Hill Education Private Ltd..
- Futoransky, A. N. L. R. G. a. S. C., 2010. *Building computer network attacks*. s.l.: arXiv preprint arXiv:1006.1916.
- Hoffman, P., 2002. *Smtip service extension for secure SMTP over trsansport layer security*, s.l.: tools.ietf.org.
- Hoque, N. B. M. B. R. B. D. a. K. J., 2014. *Network attacks: Taxonomy, tools and systems*. s.l.:Journal of Network and Computer Applications, 40, pp.307-324..
- Kavitha, T. a. S., 2010. *Security vulnerabilities in wireless sensor networks: A survey*. s.l.:Journal of information Assurance and Security, 5(1), pp.31-44.

Krutz, R. a. V. R., 2010. *Cloud security: A comprehensive guide to secure cloud computing*. s.l.:Wiley Publishing.

Lam, C., 2011. *Passive optical networks: principles and practice*. s.l.: Academic Press.

Nagurney, A., 2010. *Optimal supply chain network design and redesign at minimal total cost and with demand satisfaction..* s.l.:International Journal of Production Economics, 128(1), pp.200-208..

Natarajan, S. a. W. T., 2012. *January. Security issues in network virtualization for the future Internet*. s.l.: In Computing, Networking and Communications (ICNC), 2012 international conference on (pp. 537-543). IEEE..

Opricovic, S. a. T. G., 2003. *Defuzzification within a multicriteria decision model*. s.l.: International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 11(05), pp.635-652..

Robertazzi, T., 2011. *Basics of Computer Networking*. s.l.:Springer Science & Business Media.

Wu, J. a. T. Y., 2005. *Study on measure of complex network invulnerability*. s.l.:Journal of Systems Engineering, 2, p.003..