

Assignment 3

PLAN PROCEDURES TO SECURE A NETWORK (P4)

**CONFIGURE A NETWORKED DEVICE OR SPECIALIST SOFTWARE TO
IMPROVE THE SECURITY OF A NETWORK (P5)**

**REPORT ON THE SIMILARITIES AND DIFFERENCES BETWEEN SECURING
WIRELESS AND WIRELESS AND WIRED NETWORKED SYSTEMS (M3)**

NADIM UDDIN 14100462

Plan procedures to secure a network (P4)

Introduction: In this criteria I will be showing a plan procedure which includes all the equipment needed to secure a network

This is a check list of all the equipment needed to have a secure network.

Equipment	In possession
PC	✓
Network Cable	✓
Router	✓
Desktop firewall	✓
Anti-virus software	✓
Username	✓
Password	✓
	✓

Configure a networked device or specialist software to improve the security of a network (P5)

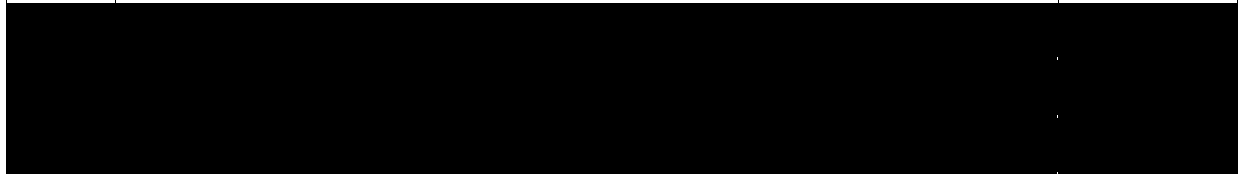
Introduction: In this criteria I will be configuring a networked device or specialist software to improve the security of a network

Observation record

Learner Name:	Nadim Uddin
Qualification:	BTEC Diploma/Extended Diploma - IT Practitioners
Unit Number & Title:	Unit 32: Network Security

No	Description of activity undertaken	
P5	Configure a networked device or specialist software to improve the security of a network.	✓
	Installed a Wireless Network Card	✓
	Add and cable the following devices together: a Router and one PC	✓
	Configure the following for the Linksys router: DHCP "Start IP Address": 192.168.1.150	✓
	Maximum number of DHCP users: 1	✓
	SSID: CiscoSBA	✓

	Network Mode: Mixed	✓
	Channel: 6	✓
	Security Mode: WPA2 Personal (or PSK2 Personal)	✓
	Passphrase: ITE5.0SBA	✓
	Add a wireless Computer	✓
	Configure the Computer with a static IP address and connect to the router	✓
	Verify connectivity between all devices	✓
	Ping the gateway address	✓
	Configure the Linksys router to block the computer's wireless NIC	✓
	Ping the gateway address	✓
	Install McAfee Antivirus Security Software on the computer	✓
	Configure the Windows Firewall to block ping requests	✓
	Ping the PC	✓
		✓



The screenshot shows the 'Basic Setup' web interface for a Linksys WRT150N router. The browser address bar shows 'http://192.168.1.1/index.asp'. The interface is divided into three main sections: Internet Setup, Network Setup, and Time Settings.

Internet Setup

Internet Connection Type: Automatic Configuration - DHCP

Optional Settings (required by some Internet Service Providers)

Host Name:

Domain Name:

MTU: Auto Size: 1500

Network Setup

Router IP

IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255.255.255.0

DHCP Server: ☒ Enabled ☐ Disabled [DHCP Reservation](#)

Start IP Address: 192 . 168 . 1 . 150

Maximum Number of Users: 1

IP Address Range: 192.168.1.150 to 150

Client Lease Time: 0 minutes (0 means one day)

Static DNS 1: 0 . 0 . 0 . 0

Static DNS 2: 0 . 0 . 0 . 0

Static DNS 3: 0 . 0 . 0 . 0

WINS: 0 . 0 . 0 . 0

Time Settings

Time Zone: (GMT-08:00) Pacific Time (USA & Canada)

☒ Automatically adjust clock for daylight saving changes.

Buttons: Save Settings, Cancel Changes

Help...

CISCO SYSTEMS

The screenshot shows the 'Basic Wireless Settings' web interface for a Linksys WRT150N router. The browser address bar shows 'http://192.168.1.1/Wireless_Basic.asp'. The interface is divided into two main sections: Wireless and Basic Wireless Settings.

LINKSYS
A Division of Cisco Systems, Inc.

Firmware Version: v1.01.8

Wireless-N Home Router WRT150N

Wireless

Setup | **Wireless** | Security | Access Restrictions | Applications & Gaming | Administration | Status

Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings

Basic Wireless Settings

Network Mode: Mixed

Network Name (SSID): CiscoSBA

Radio Band: Auto

Wide Channel: Auto

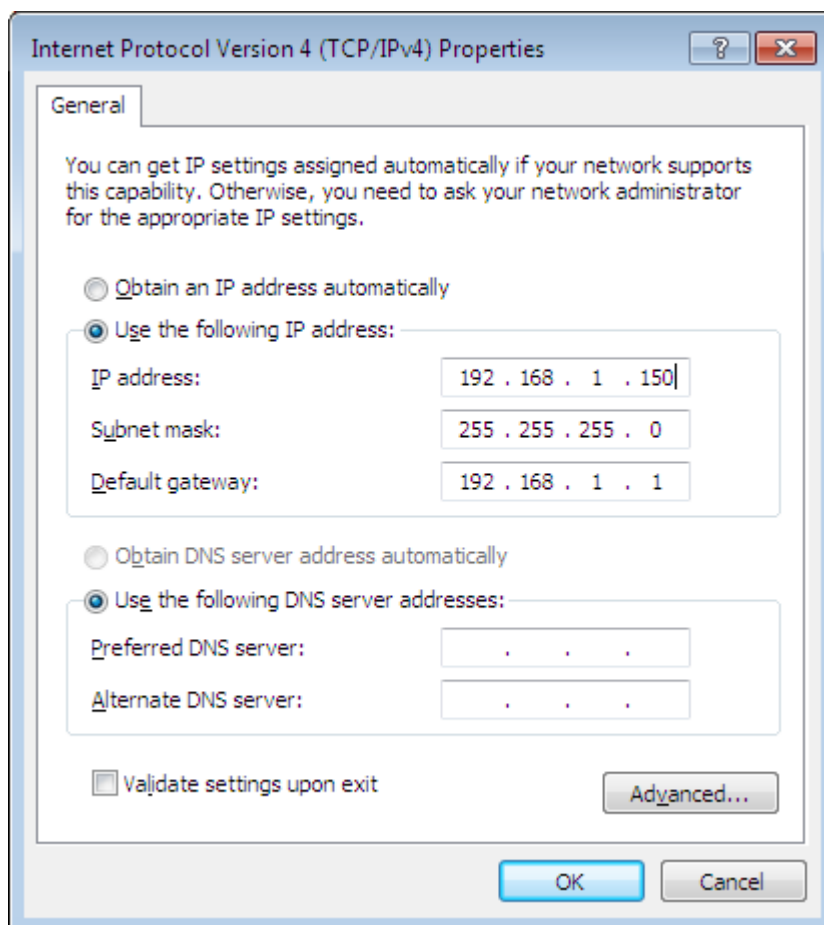
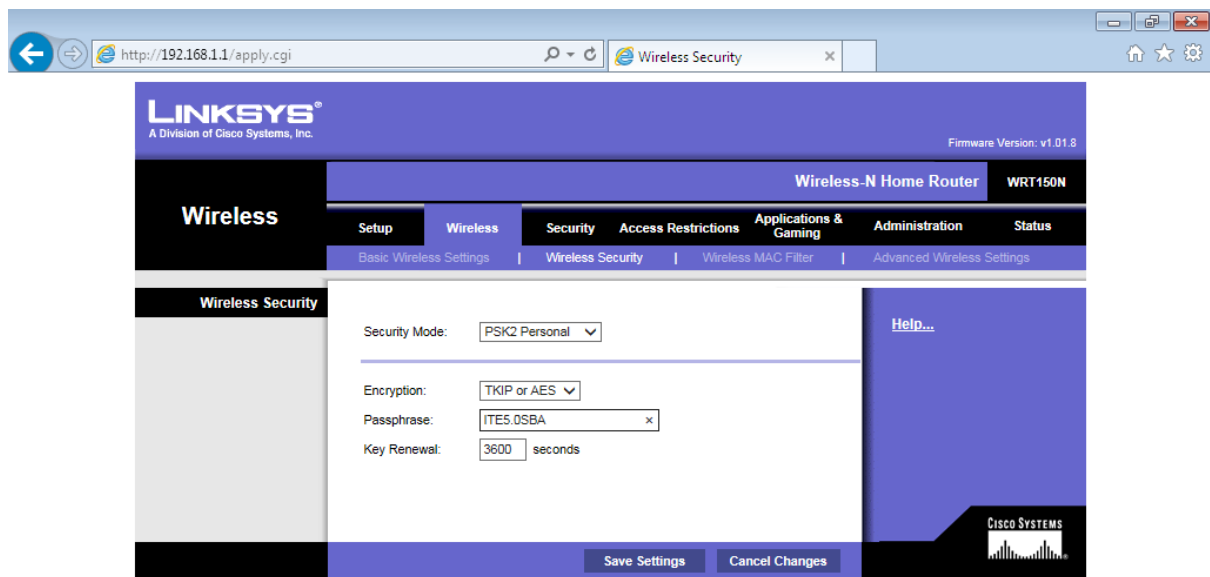
Standard Channel: Auto

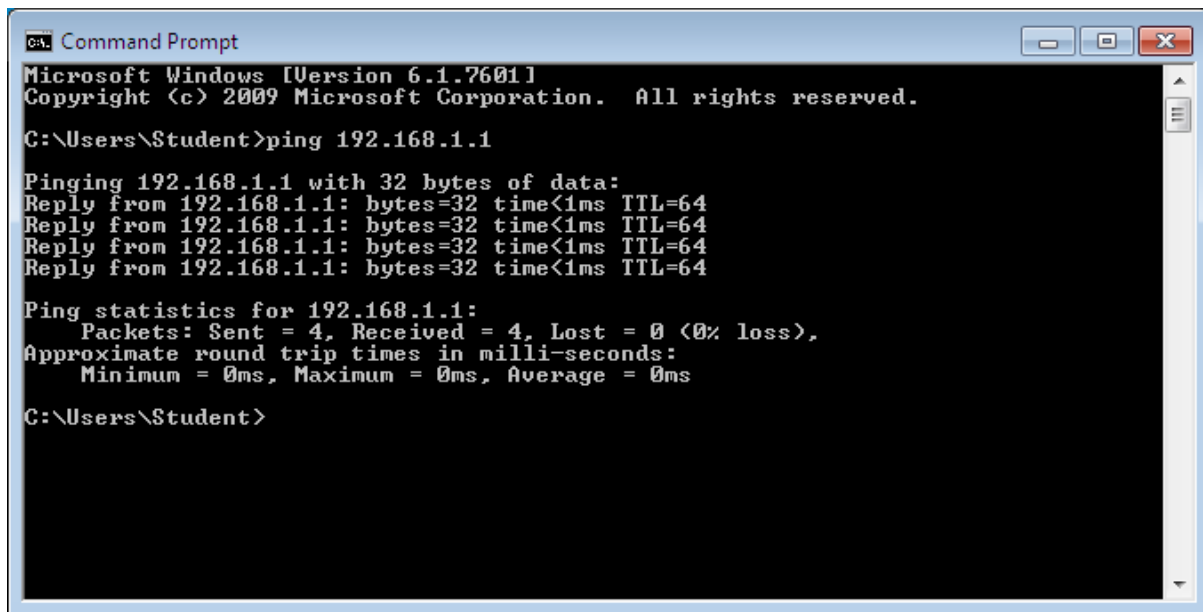
SSID Broadcast: ☒ Enabled ☐ Disabled

Buttons: Save Settings, Cancel Changes

Help...

CISCO SYSTEMS



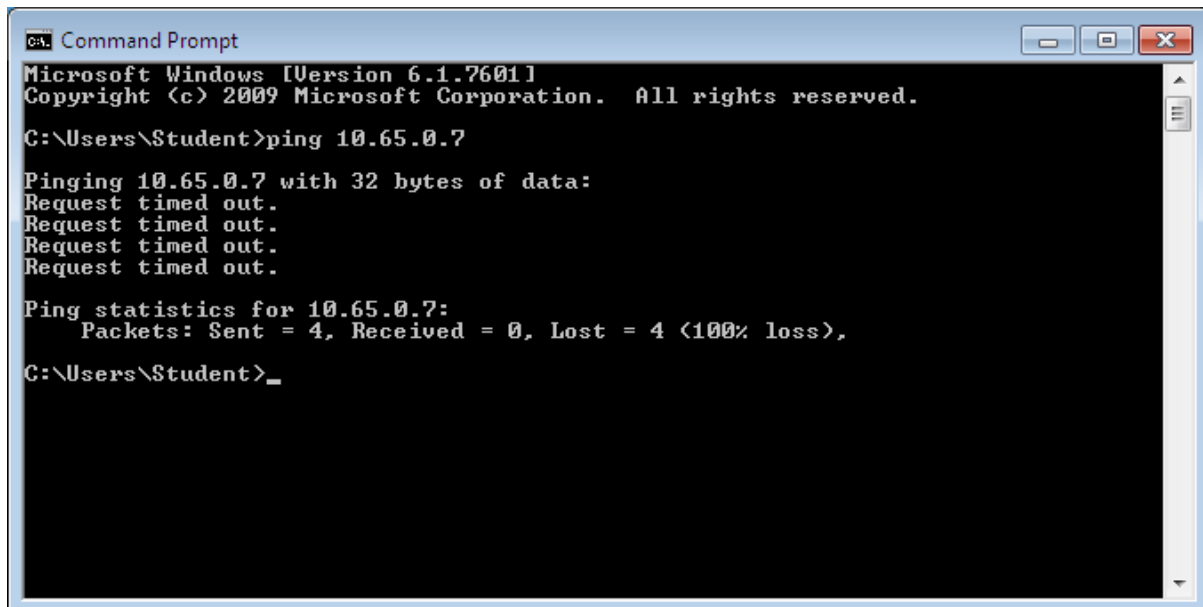


```
C:\Users\Student>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Student>
```



```
C:\Users\Student>ping 10.65.0.7

Pinging 10.65.0.7 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.65.0.7:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Student>
```

Report on the similarities and differences between securing wireless and wired networked systems (M3)

Introduction: In this area of the document I will be explaining the differences and similarities between securing wireless and wired network systems.

Differences between wired vs wireless

Wired network consists on you connecting wires to each computer in order for the devices to connect to the network. Wireless network can be configured in two different ways which is either Adhoc or infrasture mode. The cost of a wired connection is much cheaper than a wireless network because acquiring switches, cables and Ethernets are expensive. Wired network have a higher bandwidth which can offer 100mbps bandwidth with the use of fast

Ethernet technology. For wired connection the maximum bandwidth which is provided by a wireless network is around 11mbps. Wired connections with the use of Ethernet cables and switches are known to be more reliable in comparison to wireless connections. For wireless connections laptop devices can be moved around freely within the wireless network based on the type of wireless network it is for example PAN, WAN, LAN MAN. This benefits users with mobility. Most secure wireless connections require passwords whereas wired connection don't. Wired connections can be messy because of all the cabling that may be needed for your devices. If you are using a desktop computer, it is more recommended to use a wired connection however if you use mobile devices and laptops a lot wireless connections may be more suited for you. Sharing data can be much easier on wireless connections because of the range of options such as blue tooth and being able to connect to other devices such as network printers.

Similarities between wired vs wireless

Security measures can be done to both devices connection to wireless and wired for example having a firewall on to stop unauthorised access and installing an antivirus software to stop any malware from infecting your computing system. They both allow a network connection which depends on your range on how far you are from your network it may not matter which connection you choose for example if you sit around your wireless network, you will still receive a fast connection which shouldn't have much interference.

Wired vs wireless

Wired network consists on you connecting wires to each computer in order for the devices to connect to the network. Wireless network can be configured in two different ways which is either Adhoc or infrasture mode. Using wired connection can be seen as the best option for the best network connection since they offer a faster connection and it is more reliable. It can also be the most secured connection in comparison to wireless connections. The reason why wired connections are much for secure and stable, this is because for wireless connections others can see and be potentially be able to access your wireless network which can be done in seconds and enable them to steal your bandwidth and steal information that is shared over the network.

Although wired connections are more secure wireless can be configured for example WLANS use a wired equivalent privacy encryption to protect data. Another way is to change the name of your network and the purpose of doing this is so the hacker who is trying to gain access doesn't know the type of network it is for example if your network was BT, Talk Talk or virgin media. This is known to help wireless networks to be as secure as wired connections. In terms of protection within a certain radius such as a business anyone can connect to the network with the right cables however with most wireless networks, they require you to access with a password. You can also make your wireless network more secure by positioning it in an area where people within the building can only gain access for example having it in the centre of the building so people outside the building can't gain access. Other barriers can also be made onto devices by having an anti-virus software and

having a firewall on. Although anyone can connect using the right cables for a wired connection, it can easily be observed on who's using the network with a wired connection.

In conclusion wired connections are for users who just use a desktop computer to access the internet and wireless connections are made for multiple users connecting or portable devices on a wider radius which helps make it convenient for users to gain access of a network from a location or a Wi-Fi hotspot. Wireless networks help give users more mobility, easy setup, expandable and cost sine wireless network reduce the costs on buying wires. The securest option out of the two connections is the wired connection since people can't try to access your network unless they are wired which prevents hackers who are trying to crack the password to your network however there are many security measures that can be done on wireless networks by having a strong secure passwords and having protection software on devices such as firewall and a anti-virus software.

Unit 32 references

<http://www.cisco.com/c/en/us/solutions/small-business/resource-center/work-anywhere/wireless-network.html> 20/02/17 13:45PM