Start Installing

Unit 32, Assignment 2

Thomas Robinson
rob21005043

2nd May 2023
Solihull College

Contents

1 Improving the Security of a Networked Device

To improve the security of a network, I have chosen to implement VLAN segregation and appropriate firewall rules to prevent traffic from one VLAN reaching the other. In this example, we will set up a guest network and a private network. The guest network will be able to access the internet, but not the private network. The private network will be able to access the internet and the guest network. This is a common setup in many businesses and homes, as it allows guests to access the internet without compromising the security of the private network.

The current layout of the network, without any changes, is shown in Figure 1.

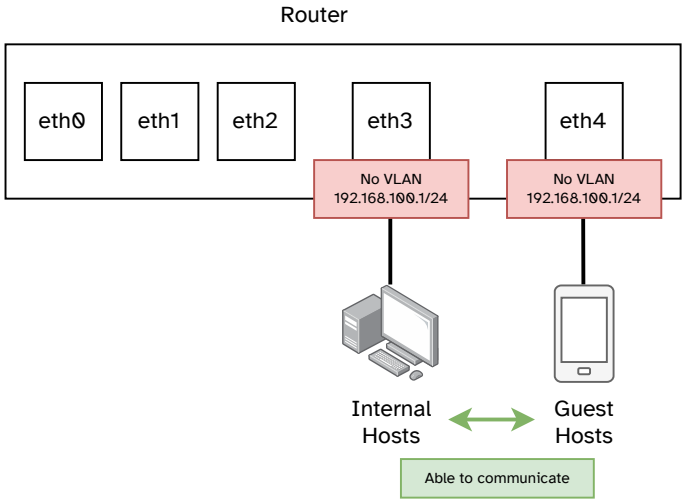

Figure 1: The network before any changes are made

1.1 Steps to Be Taken

1. Configure the router to have two VLANs, one for the private network and one for the guest network.
2. Assign the ports on the router to the appropriate VLANs.
3. Create firewall rules to prevent traffic from the guest network reaching the private network.

1.2 The Router

The router used in this example is a Ubiquiti EdgeRouter X. It is a small business router with a web interface and a command line interface. The web interface is used in this example, as it is easier to use and more accessible to those unfamiliar with the CLI (Figure 2).

1.3 Configuring the VLANs

On the 'Dashboard' page of the interface, it is easy to add a new VLAN from the 'Add Interface' dropdown. Here, I created two VLANs with IDs 240 and 250. These will be used as the Private and Guest networks respectively. Each VLAN was assigned to a port on the router, and a /24 address range given to each, allowing for 254 hosts on each network. This is shown in Figures 3 and 4.

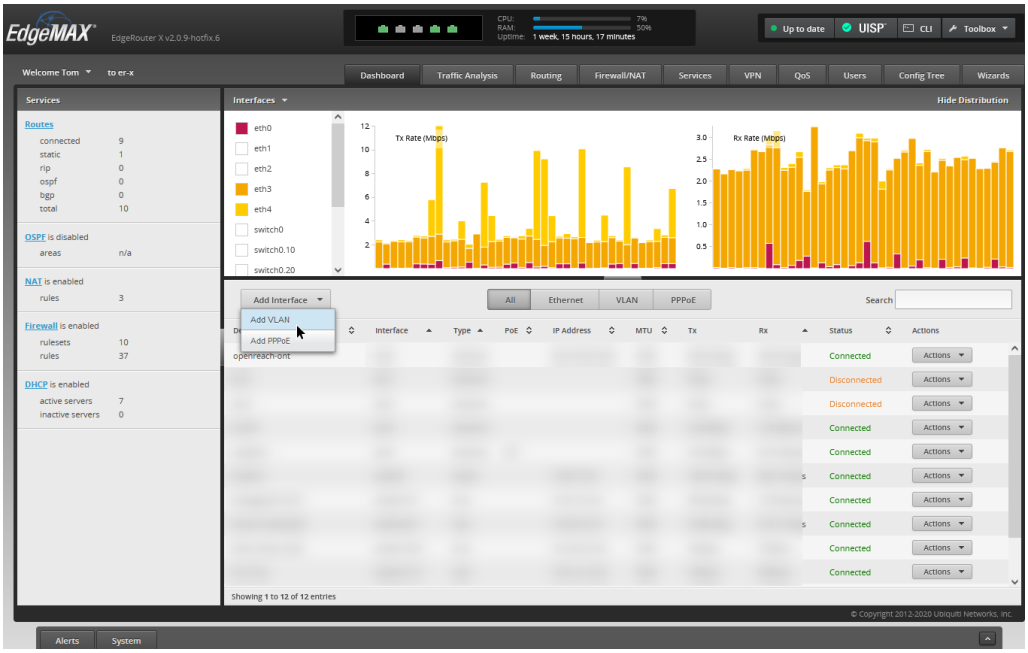

Figure 2: The web interface of the EdgeRouter, with the 'Add Interface' option expanded

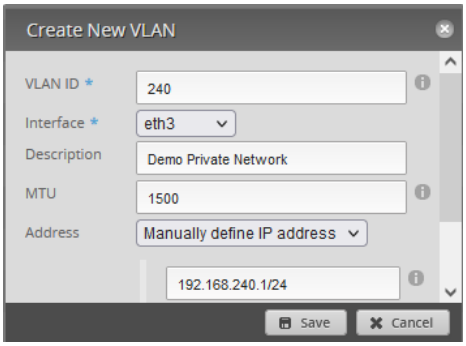

Figure 3: Creating the Private VLAN

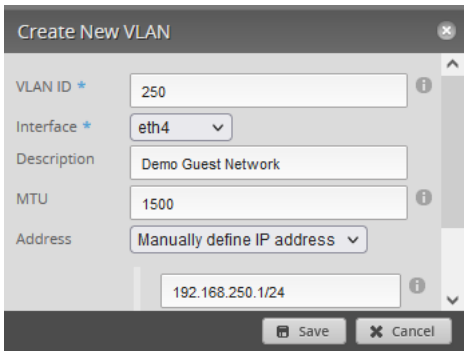

Figure 4: Creating the Guest VLAN

1.4 Configuring the Firewall

Firewall rules are managed from the 'Firewall/NAT' page of the interface. Here, two new rulesets were created, one for each VLAN, with the default action of 'allow' (Figures 5 and 6). Inside the ruleset for the guest network, a rule was created to disallow traffic from the guest network to the private network. This was done by setting the source address to the guest network's address range, and the destination address to the private network's address range. The action was set to 'Drop', and the rule was placed at the top of the ruleset to ensure that it was applied first (Figure 7). This means that the private network can access the guest network, but the guest network cannot access the private network. Since the default action is 'allow', the guest network can still access the internet and the private network can still access the guest network.

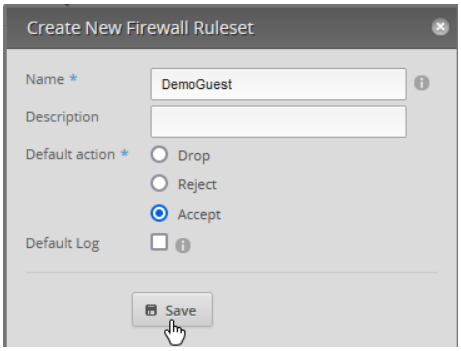

Figure 5: Creating the Guest firewall ruleset

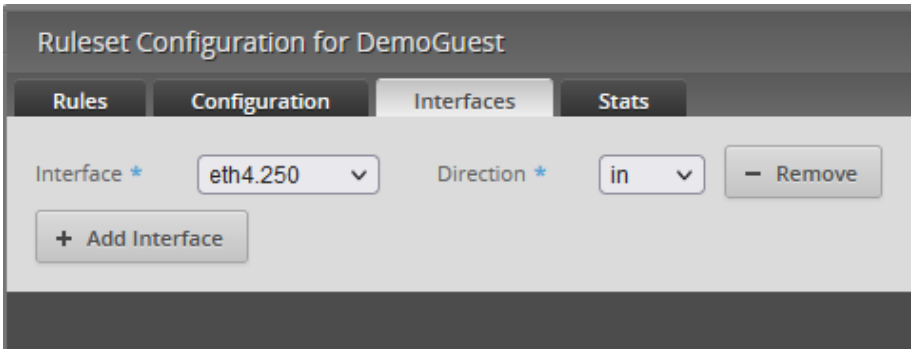

Figure 6: Applying the firewall ruleset to the Guest interface

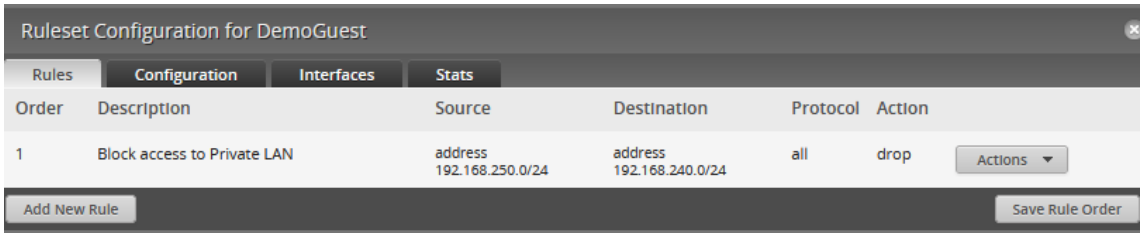

Figure 7: The Guest firewall rules

1.5 Testing the Configuration

To test the configuration, two computers were connected to the router, one to each configured port. They were assigned IP addresses in the appropriate ranges, and the inter-network firewall rules were tested by attempting to ping and run tracert between the two computers. The results are shown in Figures 8 and 9. In Figure 8, the tracert is unable to reach the destination computer, as the firewall rules disallow traffic from the guest network to the private network; the same applies to the ping. In Figure 9, the first hop is the router, and the second hop is the other computer. Though the firewall rules were tested using ICMP, they apply to all traffic, including TCP and UDP.

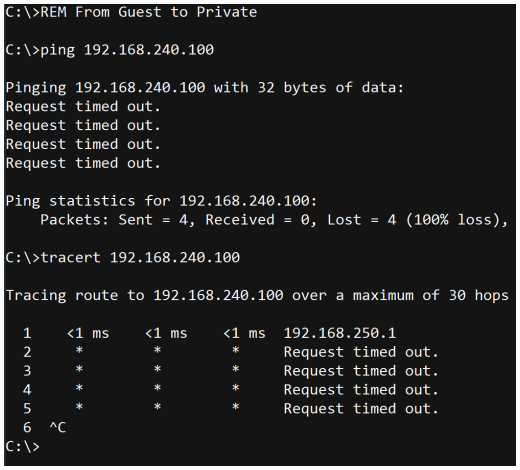

Figure 8: Showing that a device on the guest network cannot communicate with devices on the private network

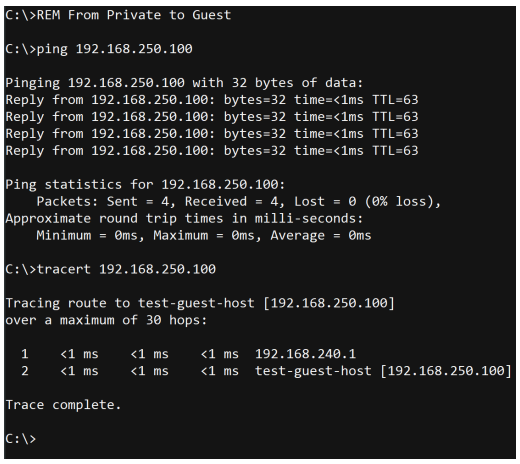

Figure 9: Showing that a device on the internal network is able to communicate with devices on the guest network

The network after the changes were made is shown below, in Figure 10.

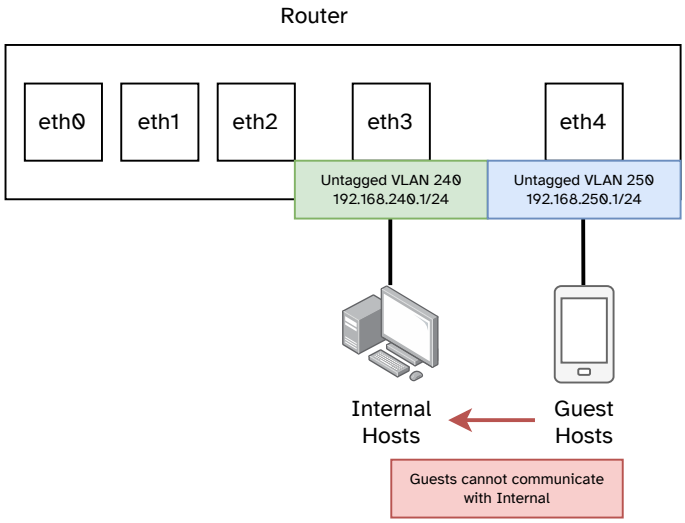

Figure 10: The network after the changes were made

2 GRE Tunnel Packet Tracer Exercise

In this exercise, a GRE tunnel was configured between Cisco routers with WAN IPs on the internet. Routing rules were then configured to allow traffic between the two networks, and the tunnel was tested by pinging a computer on the other network, as well as running a traceroute to the other network.

It is important to note that in this configuration, a GRE tunnel adds no security to a network. In fact, it could be argued that security is reduced. This is because GRE is an encapsulation protocol that does not employ any encryption of its own. When sent over the GRE tunnel, the packets are being sent over the internet in plain text, meaning at any point along the route the packets could be intercepted and read. It is possible to encrypt the packets before they are sent over the GRE tunnel, but this is not part of the GRE protocol itself. This is not part of the given exercise, but would be accomplished by using a VPN protocol such as IPsec.

```
RA>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     192.168.1.1     YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Serial0/0/0            64.103.211.2    YES manual up                    up
Serial0/0/1            unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
RA>
```

Figure 11: The IP addresses of Router A

```
RB>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     192.168.2.1     YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Serial0/0/0            209.165.122.2   YES manual up                    up
Serial0/0/1            unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
RB>
```

Figure 12: The IP addresses of Router B

```
RB>ping 64.103.211.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 64.103.211.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 11/16/19 ms

RB>
```

Figure 13: Ensuring the connectivity between the two routers over the ‘internet’

```
RA>en
RA#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
RA(config)#interface tunnel 0

RA(config-if)#
%LINK-5-CHANGED: Interface Tunnel0, changed state to up

RA(config-if)#ip address 10.10.10.1 255.255.255.252
RA(config-if)#tunnel source s0/0/0
RA(config-if)#tunnel destination 209.165.122.2
RA(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up

RA(config-if)#tunnel mode gre ip
RA(config-if)#no shutdown
RA(config-if)#
```

Figure 14: Configuring the tunnel on Router A

```
RB>en
RB#config term
Enter configuration commands, one per line.  End with CNTL/Z.
RB(config)#if tunnel 0
                  ^
% Invalid input detected at '^' marker.

RB(config)#interface tunnel 0

RB(config-if)#
%LINK-5-CHANGED: Interface Tunnel0, changed state to up

RB(config-if)#ip address 10.0.10.2 255.255.255.252
RB(config-if)#tunnel source s0/0/0
RB(config-if)#tunnel destination 64.103.211.2
RB(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up

RB(config-if)#tunnel mode gre ip
RB(config-if)#no shutdown
RB(config-if)#
```

Figure 15: Configuring the tunnel on Router B

```
RA(config-if)#ip route 192.168.2.0 255.255.255.0 10.10.10.2
RA(config)#
```

Figure 16: Configuring the routing of private traffic over the tunnel on Router A

```
RB(config-if)#no shutdown
RB(config-if)#ip route 192.168.1.0 255.255.255.0 10.10.10.1
RB(config)#
```

Figure 17: Configuring the routing of private traffic over the tunnel on Router B

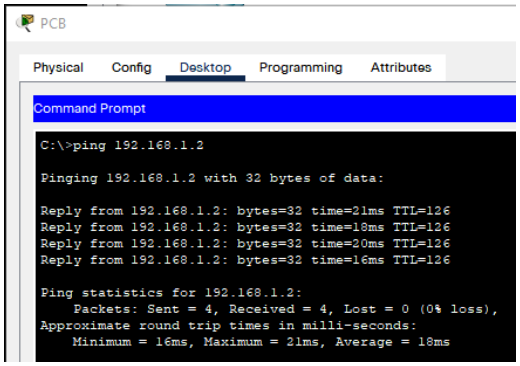

Figure 18: Pinging PC A from PC B over the tunnel

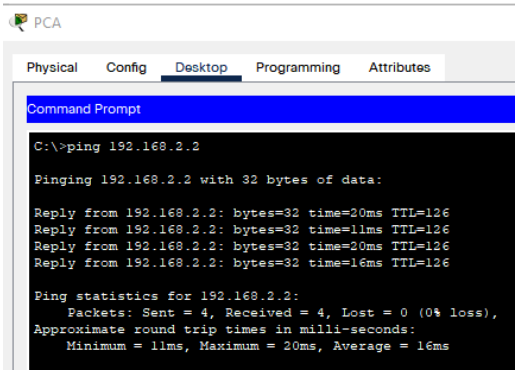

Figure 19: Pinging PC B from PC A over the tunnel

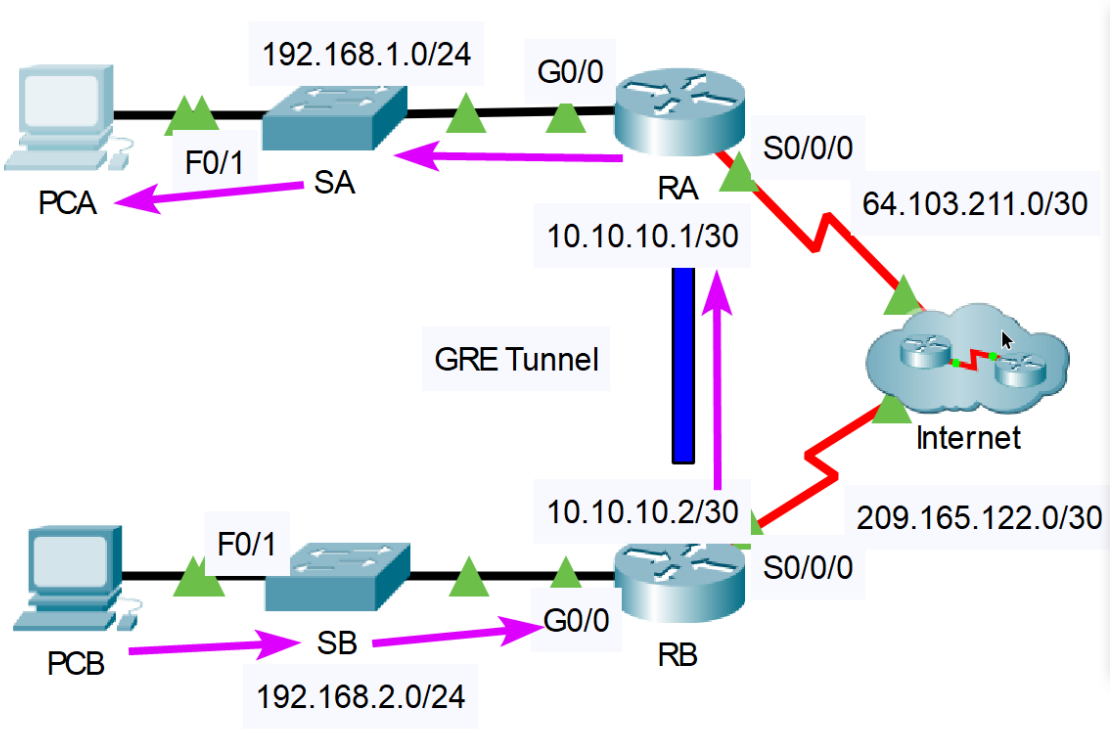

Figure 20: The path of a packet sent from PC B to PC A, shown in pink

```
C:\>tracert 192.168.1.2

Tracing route to 192.168.1.2 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      192.168.2.1
  2    14 ms     19 ms     19 ms     10.10.10.1
  3    *         11 ms     19 ms     192.168.1.2

Trace complete.

C:\>
```

Figure 21: Running traceroute to demonstrate the path of a packet from PC B to PC A, over the GRE tunnel. Note that the 2nd hop is the router on the other network.

3 Securing Wired & Wireless Networks

Both wired and wireless protocols are used in most networks, be it a small business, large organization, or home environment. Securing access to a network is integral to the privacy of users and the data they communicate. There are similar and differing methods to applying access control and security to either type of network.

The most common wired network technology is Ethernet, so further references to a wired network will be to wired Ethernet LANs. Wi-Fi is a similar story; it is the prevailing set of standards used for wireless local area networks, so future mentions of wireless networks will be referring to Wi-Fi LANs specifically. Other standards do exist, such as those used for cellular mobile data communication.

A simple Ethernet network would consist of a switch and a number of end-devices connected to it using Ethernet cables. The switch would be connected to (or be a part of) a router, which would be connected to the internet. A simple Wi-Fi network would consist of a wireless access point (WAP) and a number of devices connected to it. This WAP would be connected to (or be a part of) a router, which would be connected to the internet.

3.1 Commonalities

Both Ethernet and Wi-Fi are described in the IEEE 802 set of standards and make use of a 48-bit MAC addresses to identify interfaces at Layer 2. These MAC addresses can be used for access control. An example of this would be specifying that only a certain MAC address is permitted to send traffic on a specific port on a switch. In a wireless network, an explicit allow-list may be kept to limit the devices that are permitted to connect by their MAC address. Access control using MAC addresses can prove effective, though once a would-be intruder discovers an allowed address, it is trivial to spoof this on a different device to gain access to a network. This is where physical security can play a part in securing a network.

Firewalls can be used with either technology. They can be used to limit traffic depending on its origin, destination, type, or even the time of day. This can increase security by blocking access to devices, networks or content. For example, one department may be on a VLAN with firewall rules configured to disallow communication with other department networks.

Physical security can play an integral role in wired and wireless networks. Securing access to a networking closet, or network devices in general, can prevent an attacker from plugging arbitrary devices into a network or the hardware on which it runs. In the case of a wired network, an attacker may be able to connect to a poorly configured router or switch and directly issue commands to tweak their configuration, or plug their device into the network to cause harm that way. A wireless network is harder to secure physically, since the signal is broadcast over a wide area. The strength of a wireless signal, however, can be controlled to cover only the area within which it is needed. This proves some layer of physical security by requiring an attacker to be nearby—hopefully within range of CCTV, guards or other security measures—to connect to the wireless network.

3.2 Wi-Fi Encryption & Authentication

Wi-Fi networks can be secured using encryption. The most common encryption standard used is WPA2, which uses AES-CCMP to encrypt traffic. This is a symmetric encryption algorithm, meaning that the same key is used to encrypt and decrypt traffic. WPA3 is a newer standard that uses AES-GCMP, which is a more secure encryption algorithm. WPA3 also introduces a new handshake protocol that is more secure than the one used in WPA2. Both methods can make use of a pre-shared key (PSK) or a RADIUS server to authenticate users. A PSK is a shared secret that is used to authenticate users. This is a simple method of authentication, but it is not very secure. A RADIUS server is a more secure method of authentication, since it uses a username and password combination to authenticate users. This is more secure since the password is not shared between users. These methods of authentication help to prevent unauthorized users from connecting to a wireless network.

3.3 Wi-Fi Network Spoofing

Wireless networks are able to be spoofed by an attacker. If not configured correctly, an attacker can set up a rogue access point that mimics a legitimate one. This can be used to trick users into connecting to the rogue access point, which can be used to intercept traffic or steal credentials. This can be mitigated by using a strong password for the wireless network that is difficult to guess or brute-force.

3.4 Comparing Their Security

Generally, a wired network is more secure than a wireless network. This is because an attacker would have to be physically present in order to connect to it. Depending on the physical security measures in place, this may be difficult or impossible. A wireless network, on the other hand, is broadcast over-the-air to a wide area, making it easier to target and connect to. This is why appropriate encryption and authentication methods should be used to secure a wireless network.