Unit 32, Assignment 2

Start Installing

George Hotten

April 26, 2023

Planning Procedures to Secure a Networked Device

To secure a networked device, I will be implementing the use of Generic Routing Encapsulation. GRE creates a tunnel between two routers to send and receive GRE packets directly. All data sent through a GRE tunnel is encapsulated. This ensures that when the data is travelling between other routers, they will not access the encapsulated data. Most networks do not support this type of data, therefore a GRE tunnel creates a way for the unsupported, encapsulated, data to reach the required network.

Because of this encapsulation and tunnelling, it ensures that the data being sent cannot be intercepted and read by any unauthorized third party. This allows for secure traffic to be sent between two networks.

To implement this, I will set up the GRE tunnel on the two routers of the networks I want to be able to securely communicate. This will include doing the following:

- Set up an IP address for Tunnel 0.
- Add the source and destination endpoints for Tunnel 0.
- Configure Tunnel 0 to send IP traffic over GRE.
- Repeat for both networks, changing the IP addresses as appropriate
- On both routers, configure a route for the private IP traffic

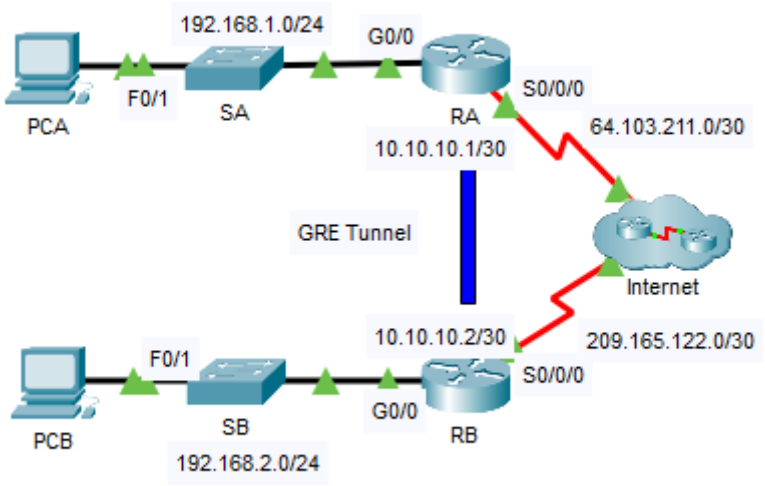

Figure 1: Diagram of the two networks I will be connecting via a GRE.

Upgrading the Security of a Networked Device

I will start by setting up the GRE tunnel on the first router, Router A.

```
RA(config)#
RA(config)#interface tunnel 0
RA(config-if)#ip address 10.10.10.1 255.255.255.252
RA(config-if)#
```

Figure 2: RA: Setting an IP address for Tunnel 0.

```
RA(config-if)#
RA(config-if)#tunnel source s0/0/0
RA(config-if)#tunnel destination 209.165.122.2
RA(config-if)#
```

Figure 3: RA: Settings the source and destination endpoints for Tunnel 0.

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

Figure 4: RA: Configuring Tunnel 0 to send traffic over GRE and enabling the interface.

```
RB(config)#
RB(config)#interface tunnel 0
RB(config-if)#ip address 10.10.10.2 255.255.255.252
RB(config-if)#tunnel source s0/0/0
RB(config-if)#tunnel destination 64.103.211.2
RB(config-if)#tunnel mode gre ip
RB(config-if)#no shutdown
RB(config-if)#
```

Figure 5: RB: Repeating the steps from RA, changing the IP address as appropriate.

```
RA(config)#
RA(config)#ip route 192.168.2.0 255.255.255.0 10.10.10.2
RA(config)#
 RB(config)#
 RB(config)#ip route 129.168.1.0 255.255.255.0 10.10.10.1
 RB(config)#
```

Figure 6: Adding the IP routes for each router.

After running those commands, a GRE tunnel should be fully setup. To test the tunnel, I will perform a `ping` and `tracert` between the PCs on the different networks. If they can communicate and no public IPs are shown, then we have successfully set up the GRE tunnel.

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=70ms TTL=126
Reply from 192.168.1.2: bytes=32 time=83ms TTL=126
Reply from 192.168.1.2: bytes=32 time=38ms TTL=126
Reply from 192.168.1.2: bytes=32 time=66ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 38ms, Maximum = 83ms, Average = 64ms

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    53 ms     34 ms     39 ms     10.10.10.1
  3    63 ms     47 ms     50 ms     192.168.1.2

Trace complete.
```

Figure 7: The two PCs are able to communicate, and no public IPs are shown.

This shows we have successfully set up a GRE tunnel, securing the traffic between the two networked devices.

Securing a Network: Wired vs Wireless

Wired Networks

What is a Wired Network? A wired network is connected via cables, most commonly using twisted coper pairs. However, in more demanding environments, fibre-optic cables can be used for their higher speeds.

What equipment is required? Typically, devices on a wired network are connected together via a Switch. Using MAC address, the switch is able to appropriately route data the required device. In larger networks, there are often multiple switches connected together. The switches then connect to a router, which provides access to the internet. This creates a 'star' network topology.

What does the installation involve? When setting up a wired network, a design must be created and validated to ensure the best possible performance and reliability on the network. This can often include having multiple links between each switch on the network, and multiple links to the router per switch. This helps reduce the change of the network going down to a single point of failure. However, in smaller networks, this isn't always needed.

Once a physical connection is made between the end devices, switch and router, the network will just require a DHCP server (which can often be found within the router's settings) and devices will be able to communicate.

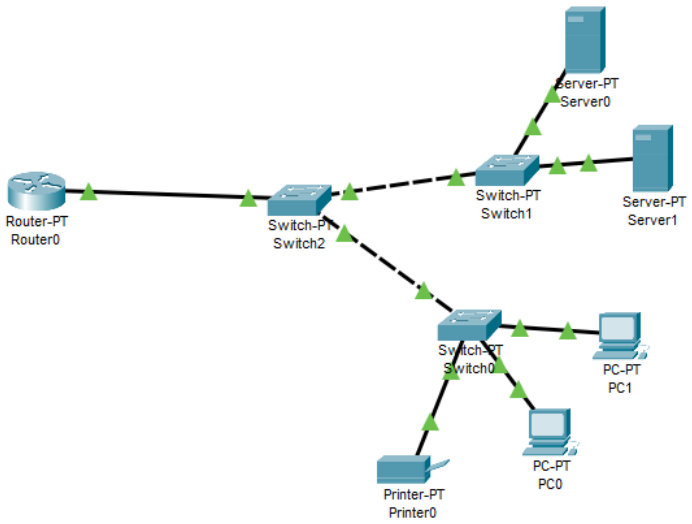

Figure 8: Example setup of a wired network.

Wireless Networks

What is a Wireless Network? A wireless network is connected via radio waves on the 2.4GHz and 5GHz spectrum. Wireless networks can sometimes require no cables at all, with the expection of a cable between your router and your ISP.

What equipment is required? To operate a wireless network, you would need a Wireless Access Point and a router. In larger networks, you may connect your WAP to a switch, especially when multiple access points are required. In small networks, such as ones found in homes, an access point is often built into your router, making the only required equipment to run the network a router.

What does the installation involve? To set up a wireless network, you should ensure that your access point(s) are in an adequate location within your building to ensure maximum coverage. If you have multiple access-points, you must position them to ensure minimal signal overlapping. If you are using a router combo box, DHCP and other required services are often pre-configured and do not require any user action. However, if you are using a separate router and access point, you will need to configure the access points with IPs and set up a DHCP server on the router.

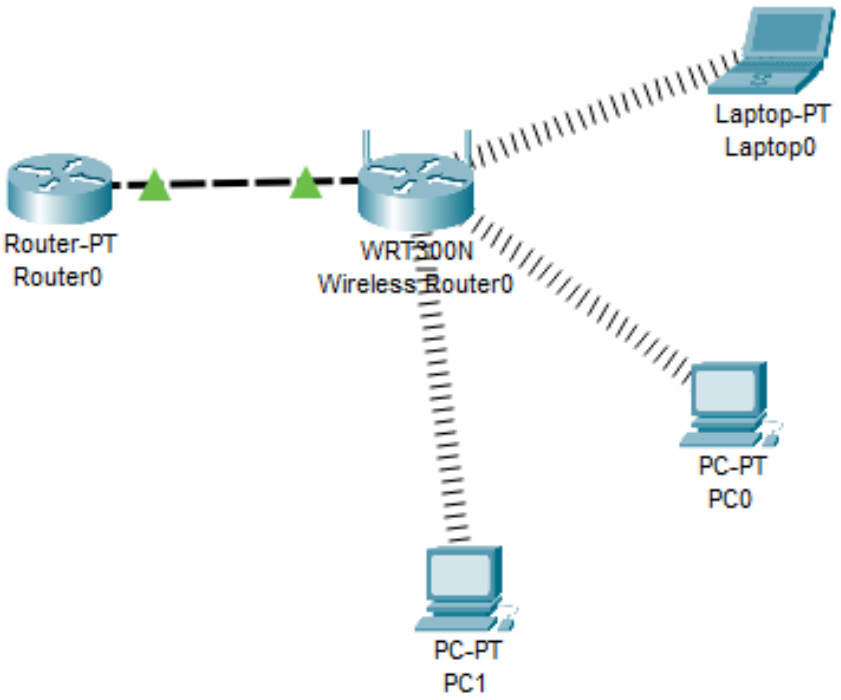

Figure 9: Example setup of a wireless network.

Securing the Networks

Wired Networks

Wired networks by design are more secure from outsiders than a wireless network. This is because to sniff and intercept data from a wired network, you need physical access to the infrastructure and equipment to insert a sniffing device.

To combat this, modern switches and routers often have a feature known as MAC Address Binding / Port Locking. Port Locking monitors the MAC address of the device it is connected to. Once it knows the MAC address, it will lock that port the device's MAC address. If another MAC address is detected, all traffic is dropped to and from the device. This helps combat someone unplugging a device and plugging a new device in. To further stop someone from plugging their malicious device into your network, any unused ports should be disabled in your switches and router's configuration.

Wireless Networks

Wireless networks often have worse security then wired networks as all data is transmitted over radio waves where anyone can attempt to sniff and intercept them. On public Wi-Fi networks, this can be especially dangerous as there is little to no encryption.

To protect a wireless network from sniffing attacks, it is important that you set up your network to use the proper encryption and security. Wi-Fi Protected Access 3 is the latest and strongest security that can be used. WPA3 uses the latest encryption standards such as GCMP-256, 256-bit Galois/Counter Mode Protocol. Elliptic Curve Cryptography is also used for key exchange, making cracking and intercept data from a wireless network harder.

WPA3 also uses Forward Secret, which means that if an attacker is able to intercept traffic, they will not be able to decrypt it as WPA3 uses unique session tokens for each connection.