Network and Security Coursework 1: Configure and design a network

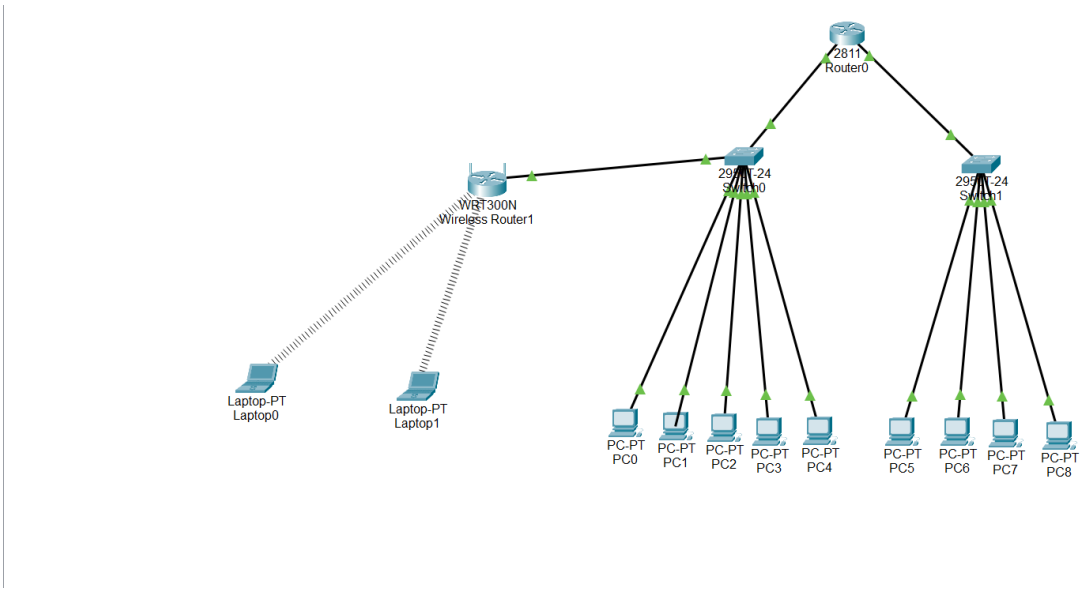
I have done the coursework 1 the second time, because the first time I didn't understand the coursework. I choose scenario 1:

Scenario 1

The company you are working with is a greenfield site, in that they have no existing network, but have been working with a simple wireless LAN supporting two laptops. The company has now employed 10 staff, who will require desktop machines and full networking capability. There will still be a requirement to support laptop machines locally within the organisation, but at this point everything will be run locally. You will need to consider the need to support local hardware and software tools and facilities, and these will need to be built in to your design.

Solution:

My design of the network



According to task and the scenario i have chosen, my network have an wireless LAN for the two computers, after that we know that we have 10 staff employee, the staff has be using the 10 machines desktops that will make the network full function.

We have used also a switch that will help us to connected to one of the LAN ports, after that we understand that the PCs are communication, and the laptop communicates through switches and routers.

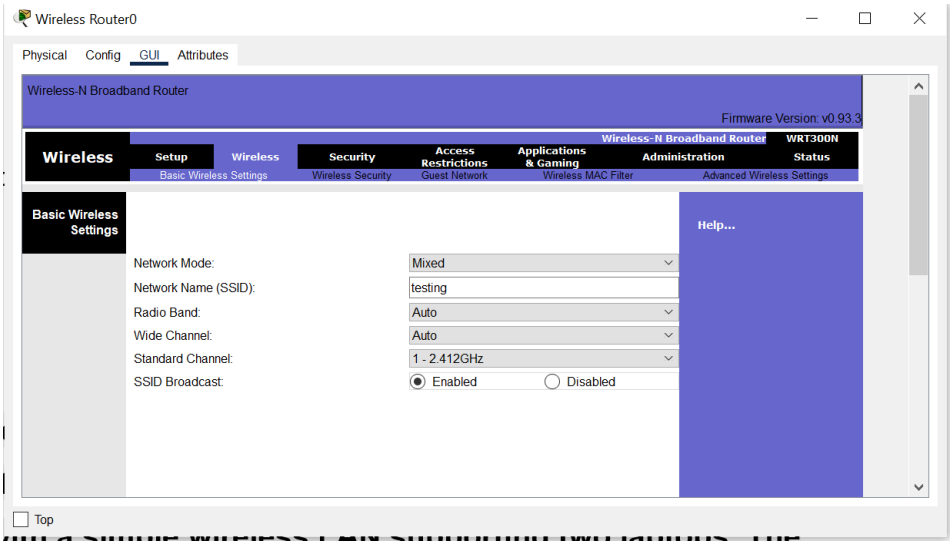
Network topology:

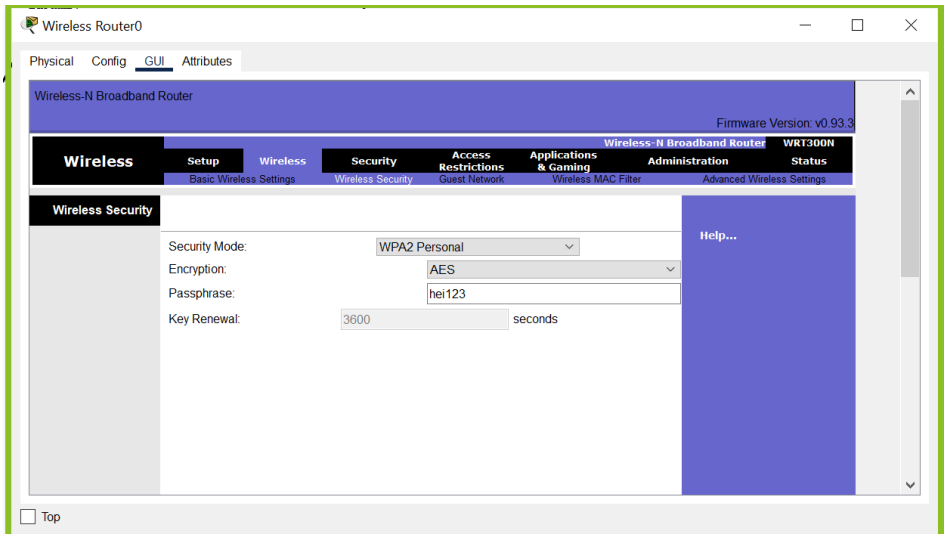
I have chosen the network topology, **Star Topology.** Star topology is a type of network topology in which each of the network's component is physically connected to central router. The main reason I didn't choose the bus topology is that the star can take more cables than the bus, if one component or a cable fail, only one component will be brought down.

In our firm the advantage can be that we have centralized management of the network trough use of the central computers.

Back to my network design, I have provided IP-Address. I have chosen to use Cisco Packet Tracer and the routers I have used **DHCP**, that mean Dynamic Host Configuration Protocol. With the help of DHCP server you can automatically give IP-Addresses. This can make the different users of the network to communicate more efficiently

Configuration of Wireless and password:

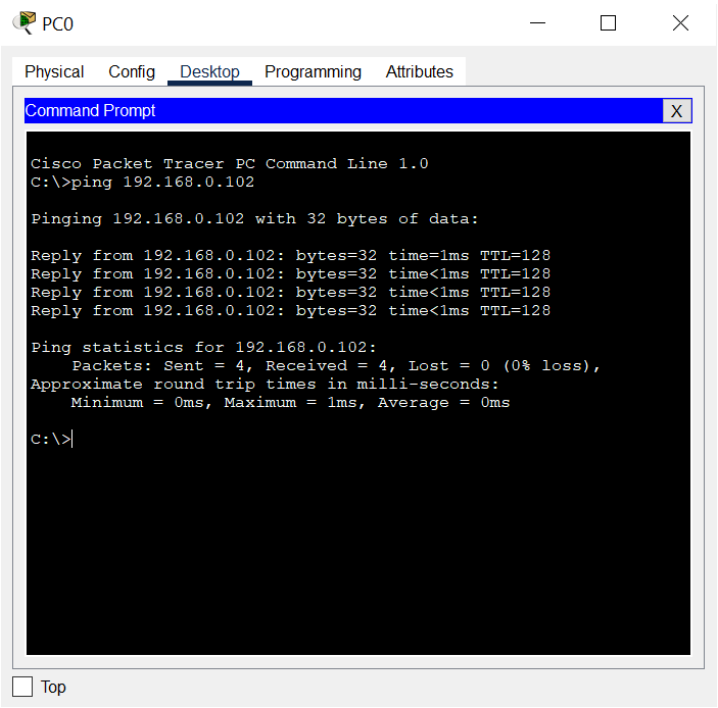




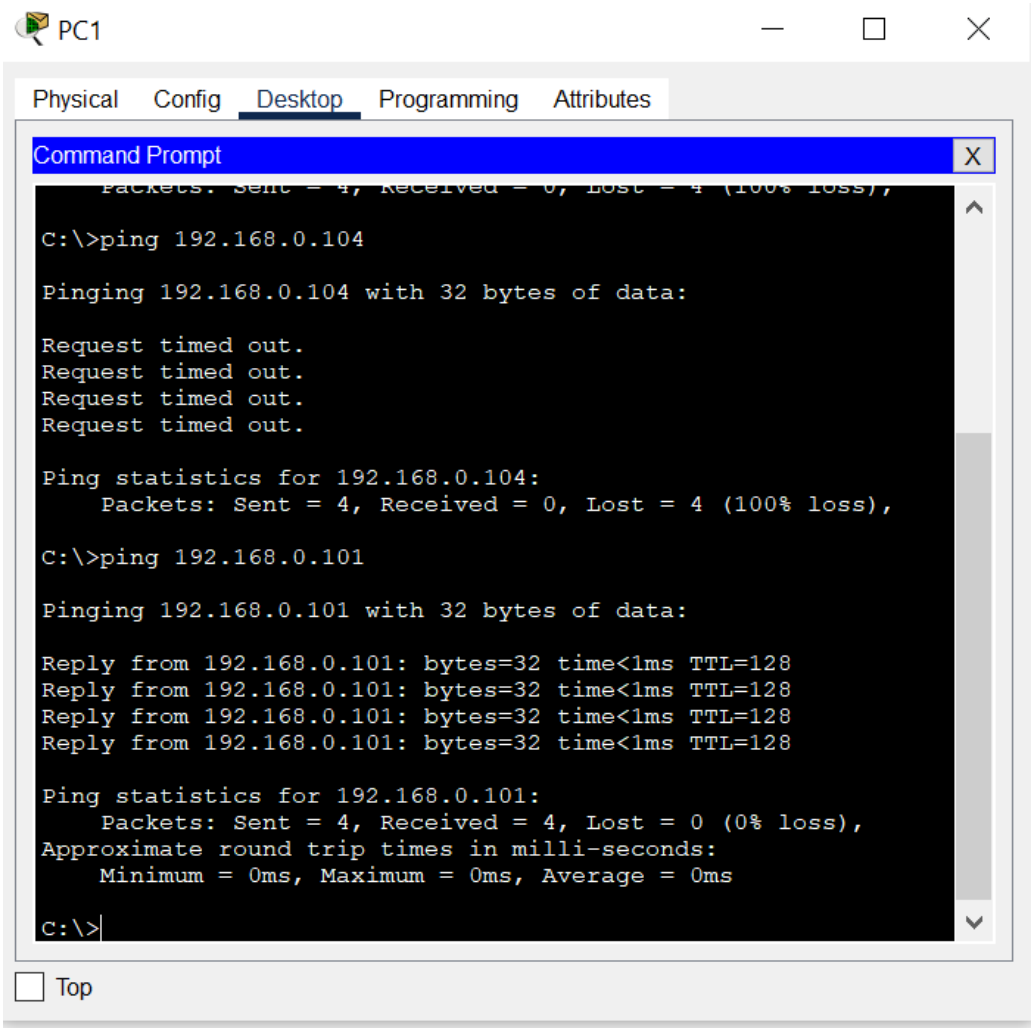
This to screenschot from Cisco packet tracer, choose that I have made configuration of the wifi router, with name and password.

Testing of the network:

In this section I will test different part of the network. I will first start with one of the desktops PC and and laptop 1 (or 0). We start from PC 0 - Laptop 1.



Communation PC0 to Laptop 1, we use the ping command with the IP-Adress, and see that is sucessfull.



In the next example, I have first written IP-Address. We write in the command prompt ping and see that from PC1 – to Laptop 1 is successful.

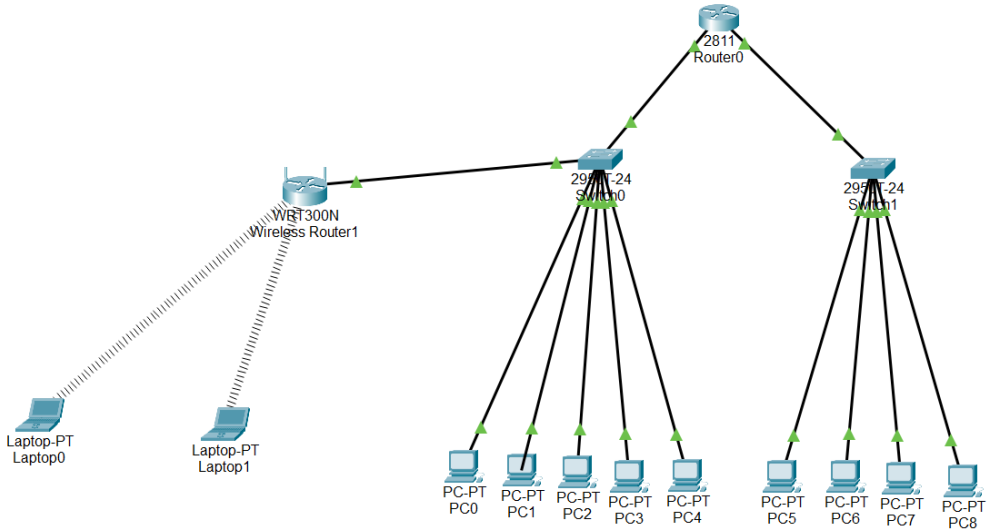
Coursework 2 – Design security controls of your network

So, for this task you should describe how you would establish the perimeter security for your network. Obviously, if you are working on scenario 2 or 3, you should assume there is an existing perimeter security, so you should describe what it is and how you would change/extend it to accommodate your new network design. You should be able to describe how you would setup firewalls, IDS/IPS, anti-virus, and authentication controls. You should also be able to describe the threats to your system and how those would be addressed by your perimeter security controls.

If we first start to explain the meaning of Perimeter Security. The perimeter security is the philosophy of the setup the functional apparatus or it can be the different techniques at the perimeter of the network that can secure the different data and other resources. To explain furthermore the perimeter security is also about the part to preventing unauthorised access, by the help of then securing the boundaries of the system or the network.

The reason for why we use perimeter security for our network is that the Perimeter security of the network is a technology that can help us to provide a range of security services from a basic firewall protection and it can also be through end-to-end security for your network or business. If we go back to our design of the network. We have ensured that our employees are safe when they are browsing around the internet. Perimeter security can also be a defence system around your network designed to help stop unwelcome user to enter our internet.

Draw of the network Design:



This the network design I choose to make from coursework 1, if we look further, we can see that our design not got any security protocols or information that help to hold the network safe.

Why is perimeter network security important?

It is important question to ask yourself why network security is important, one of the main point is that in the technology world today one main thing its hackers. According to study from Clark School study, **hackers attack every 39 second** [1]. If we look furthermore, we can also see that 43% of all the cyberattacks often target small businesses while 64% of companies have also experienced web-based attacks [2]. To conclude after we look at the stats you can say its quite alarming. The main reason for the attacks happened it's because most the companies do not defend their networks appropriately.

To secure network design:

To start in the beginning the perimeter security begin with secure network design, in the start we can start by using firewalls.

Firewalls:

Firewall always plays a vital role in network security that help us to supporting the internal networks. We start with the first thing that is to secure the firewall, the securing a firewall is most vital step to first ensure only the authorized administrators to have access to it, in our case it is the ten employees for the greenfield site. The next part is to then establish firewall Zones and then a IP Address Structure, we have to remember that is important to then identify the network assets and resources that must be protected. After that we have to configure Access Control list, configure other firewall services, then to test the Firewall configuration and then in the end to manage firewall continually.

Network firewalls are also used to protect the entrance to a network and then to block packets based after the IP-Address and then port numbers in the head.

IPS/IPS:

We first start to IPS, Intrusion prevention systems that help us to comprise one of the elements in comprehensive cybersecurity portfolio, this helps us to proactively neutralize the cyberthreats before they enter the infrastructure and our network. We also have IDS, intrusion detection system that is a passive system that scans internal network traffic and then report back about potential threats. We also know that it also operates outside of the traffic flow, it also not affect the network performance.

How I want to setup the IDS/IPS

Before we start, you need to understand a few things about our network and the traffic. What kind of traffic do we see? How complex is our network, How many different connections are between our network?. After you have asked yourself this question, by this information that will help you to decide how many IDS or IPS devices you then will need and what kind of hardware you will need. IDS/IPS is strategically placed in an entrance of an organisation. We also know that modern fully featured routers contain within them all firewall and IPD/IPS functions, which then can be configured to perform the specified functions. To conclude its very important to remember that an IPS is not same thing as the IDS, therefor is important to see that the technology that you use to give a detect security problems in an IDS can be very similar to the technology in IDS. In our network if I had to choose, I had chosen the IDS because it not does change the network packet in any way of form, but instead if we have firewalls they can then block traffic by the use of an IP-Address.

Web treats:

Example to different treats to a network, often depend on the design of the actual network we got. If we talk about today one of the main treats to a network can be hacking, when you hack a network you can use various type to treat the network.

- Poor network policy
- Employees in our firm
- Viruses
- Spyware

When we talk about poor network policy in our company its important to remember where a network does not have a security rule in place to the employee to follow, therefor it's really important that the employee in our firm have a common set of rules or policy to follow. Employee can also be a big web treats to our network, when we got users of the network that can be the employee that does not adhere to the network policy it can be a big treat. Often it can be employees that do not follow or obey the rules, they can work without a firewall against viruses.

Setup Web Server:

The task is to setup a webserver the most important thing to remember when we are setting up a webserver is to have computers available, but since we are working in a firm that have the chance to allow their employees to have a laptop or a computer in the job. After that we can choose to be running the webserver by the help by running Windows, or Linux or a Mac computer running macOS

Abdirahman Aden Osman Network Coursework 1 & Coursework 2

Sources:

[1]: https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds

[2]: https://www.elitegroup.com/news-and-insights/what-is-perimeter-security-the-basics-and-why-we-need-it/

https://www.computerhope.com/jargon/s/startopo.htm from Coursework 1