UNIVERSITY OF HERTFORDSHIRE
School of Computer Science

Modular BSc Honours in Computer Science

6COM1031 – Networks Project

Final Report
April 2023

Which devices offer the best performance and reliability and how do their price compare?

A. Hussain

Supervised by: Christopher Treglohan

Abstract

This study aims to compare the performance and reliability of various network devices across five distinct networks. At the core of this research lies the question, "Which devices offer the best performance and reliability, and how do the prices compare?" To address this question, the dissertation will begin by meticulously examining various network simulators and discussing their corresponding advantages and disadvantages. Ultimately, Cisco emerges as the preferred option. The dissertation then proceeds to discuss the five different network configurations, which range from basic setups comprising only a few devices to more intricate networks that incorporate multiple routers, switches, and servers. Subsequently, ping tests are conducted to quantify network speed and identify potential improvement areas. The results are scrutinized and compared, considering both device price and performance. Moreover, it will discuss how the project initially aimed to compare Cisco Packet Tracer and GNS3 which the literature review will be based on, but ultimately took a different course. Overall, this dissertation offers an exhaustive overview of network device performance, price, and reliability, and provides valuable insights for network design and implementation.

Acknowledgments

I would like to thank my supervisor Christopher Treglohan for guiding me the best he can and for always being available to help.

Table of Contents

Introduction

Background and motivation

With the current era of technology constantly expanding with the limit of technology being challenged, the question of "Which devices provide optimal performance and reliability, and how do their prices compare?" has always constantly been increasingly critical. It was stated in the Cisco annual internet report (2018-2023) white paper that "There will be 3.6 networked devices per capita by 2023, up from 2.4 networked devices per capita in 2018. There will be 29.3 billion networked devices by 2023, up from 18.4 billion in 2018" (Cisco, 2019) which in simpler terms means that it was predicted that by 2023, on average, 3.6 devices will be connected to a network by each person. This was an increase from the average number of devices connected to a network in 2018 which was 2.4 devices. Additionally, 29.3 billion total numbers of network devices, from 18.4 billion devices in 2018, were predicted worldwide when this report was made. With a predicted amount of "5.3 billion total internet users by 2023" (Cisco, 2019) and with the overwhelming number of available devices on the market, it can be a challenge for the average consumer to choose the best fit that meets their needs, budget, and lifestyle. This was the reasoning and motivation to find the best-performing device.

Moreover, as part of our daily routine technology has become an integral part ranging from entertainment and other activities to work and communication. So, would it not be logical to make sure the reliability is strong? Would you use a phone that consistently loses connection? Thus, reliability must be invested in, so it prevents disruptions and malfunctions. This was the motivation behind finding the most reliable device.

Furthermore, a lot of stuff can be overpriced, and some networks can end up costing hundreds of thousands of pounds which can lead to the cost being a particularly important decision-making process for many consumers. Thus, finding a device that is dependable and has a prominent level of performance at a reasonable price is one of the most crucial factors and that is why price will also be discussed in this report.

To summarize, determining the best devices that provide optimal performance and reliability and how they compare in price is the background of this project. Making an informed decision about technology investment, ensuring that the maximum value is received for the devices in question.

Research Question, objective, and hypothesis

The question that will be answered in this report is "Which devices offer the best performance and reliability and how do their prices compare?" As there is such a vast number of devices in the industry it would be virtually impossible to go through each device and speaking about every device is essentially worth the price. So, to make the goal and objective of this report more possible here will be a comparison of three areas. The First will be a bare minimum type of network where everything is aimed to be cheap this could aim to be less than $100. This network could be a remarkably simple and at-home network for someone who doesn't know about networking and just needs to get around. The second is the average type of spending on a network according to my research is "$1000 to $5000" (Abacus, 2020). This could be for a small company that needs to communicate over different networks. The final device will be looking for essentially the best on the market for a network that can aim to be well over $10,000. This could be for a big business or a business with its server farms etc. From each of these areas, two devices will be recommended along with an explanation for why. Finally, I hypothesize that Cisco Juniper will dominate the recommendations.

Project Journey

During this project, there have been numerous unexpected developments that have ultimately culminated in the outcome. Initially, the project was centered on an investigation of network intrusion detection systems (NIDS), where two commonly used NIDS tools were compared. Subsequently, the project shifted focus towards a comparison of two network simulators with minor alterations made to the topology. The journey then took yet another turn, resulting in two further minor modifications, before the project culminating in its current form. The present report will provide an account of the final project, which integrates the work carried out previously and addresses a specific set of objectives for all the changes and why they were made will be discussed in this section of the report.

Initial project plan

As previously mentioned, the very first project was to compare the NIDS of SNORT and SURICATA. Firstly, NIDS is a network intrusion detector and is a network security technology that is used to monitor traffic in real life. NIDS searches for any malicious activity signs or suspicious behavior. If the threat were detected it would notify the system administrator.

There are a lot of advantages of Snort, these include Flexibility, in which the system of Snort is highly configurable and allows the system to be customizable to meet the specifications of the security needs. Another is the community support to support with the documents and with add-ons and plugins and this is all because of the large supporting community. Finally, the ease of use for even non-experts is a big advantage because of the easy-to-understand rules and a user-friendly interface. There are a few disadvantages however for snort and they entail: limited scalability is a problem, and this could affect larger networks or high-speed traffic. Another is poor protocol support meaning that detecting attacks on certain protocols makes the system less effective. A final disadvantage is that there are limited detection capabilities which makes snort not as effective as detecting attacks like those using advanced evasion techniques and these are a few advantages and disadvantages of snort.

Suricata also holds many advantages when applied to a network. These include the suitability for large networks because of high-speed processing and Suricata is very scalable and can manage high-level high-speed traffic. The rich protocol support is also an advantage for Suricata as there is a wide range of support for protocols which leads to the effectiveness of detecting attacks on a variety of network protocols. A final positive for Suricata is that advanced detecting capabilities such as detecting advanced attacks even ones with evasion techniques used. Moving onto the disadvantages, the first disadvantage is that there is limited community support as there is only a small community of users compared to Snort and this is a problem because there are fewer add-ons and plugins and support in general. This would not be as bad of a problem if it were not for the complexity, which is my second disadvantage. The complexity of the system is harder to configure and use than Snort and tied with the lack of community help makes it harder to use. A final disadvantage that will be touched on is the limited syntax rule meaning that there are more limited rules compared to Snort and the customization challenge.

After learning the advantages and disadvantages of the NIDS it was then the challenge of how the NIDS can be evaluated. NIDS is a network intrusion detection system, so it is only logical to safely evaluate the NIDS by imitating an attack, so the question arises of which attacks can be used and how many attacks should take place. After countless hours of research, the number of attacks was decided at five common attacks which were: Denial of Service (Dos), SQL Injection, Cross-Site Scripting (XSS), Brute Force attack, and port scanning. Due to these attacks being common, the system was not challenged as such so there was also Distributed Denial of Service (DDoS) attack.

At this stage of the project planning it came to light that the level of understanding that was needed to produce the work that was needed for this type of project was not in my skill set and would leave the project half/not completed at all so as there was still more than enough time to change the project the choice was taken to move away from this idea and delve into a topic that I am confident in.

Second project plan

Looking at the last years of studying computer science, working in network simulator work is where I work best, and decided that the best option is to work around this kind of topic as there was a developing interest in network simulators. After only knowing about the Cisco pact tracer there was the question of which other simulators are in the field. Why are there different simulators? What makes them different? Finally, in my university why don't we study the other simulators? Why only the Cisco packet tracer? Research had shown that the Cisco packet tracer and Graphical network simulator-3 (GNS-3) are very similarly matched but what was the difference? The project originally started by just getting five different topologies and then comparing how easy it was to make and then comparing the functions and features.

The first obstacle to tackle was to choose which types of topologies to evaluate the simulators with. The project would start with a remarkably simple topology as a base, which will then increase the level of complexity with the addition of devices. However, I realized that this specific research question has already been done. So, to dive deeper into an existing research topic and try to challenge myself more, I decided I will deepen this topic by altering the topologies and making the network more complex.

A slight adjustment to the plan

From here the topology was rethought to have one vast network topology. The network topology was configured as a topology for a university consisting of five different departments over a hundred pcs, server rooms, printers, and numerous switches. The thought behind this kind of topology was that there was one extensive topology that could create a large amount of traffic and then evaluate to see how easy it was to create a large network and see how it will deal with extensive traffic.

The reason why the topology was moved on from this topology is because after making a visual representation of what the network will look like it became apparent that the network was extremely basic. Yes, the topology did reach its aim of being large and did that aspect very well. However, the devices that were used were very repetitive and did not expand my knowledge of network simulators or networking. So, from this, it was time to go back to the drawing board for another time to see what can be done.

Readjustment of plan

As I believed, I was looking too in depth at the situation at hand, and the approach that was taken needed to be altered so going back to the very basics the question that was concentrated on is what is a network simulator? Well, the job is simply to simulate networks so from this the next question is what devices are mainly used then is a simulator? Well after doing a little look around on the internet it was apparent that the main devices used are switches, routers, firewalls, access points, hubs, and servers. Now where to go from here? Well, now the devices that are needed are known it is now the challenge of implementing a working topology from these devices. So, to get an idea of what was needed the first step was getting all the devices on the simulator that was familiar to me so starting on the Cisco packet tracer the first step was to get a basic topology and add to the topology till all the devices that were mentioned was in the topology. This route the project took went well till the project moved on to working on GNS3.

The simple problem what was faced in this was that GNS3 was troublesome to me was that in GNS3 nothing comes pre-downloaded, and the figure below is demonstrating what I was met with when downloading GNS3.

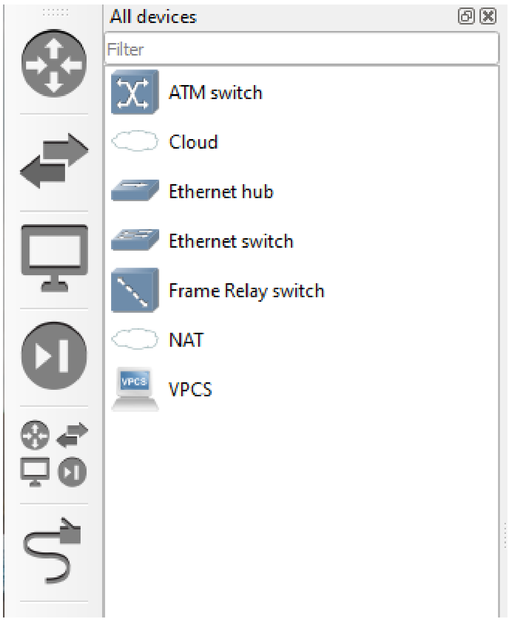


Fig 1. The devices are available when downloading GNS3.

Now as it is visible there are quite literally only switches and VPCs and that is considerably basic to what is needed. The solution that was attempted to try to get the devices needed was trying to find YouTube videos to find out how other users worked on GNS3 and looking for online resources to work out how to get all the devices. However, a lot of the links that people recommended to use were outdated and the links that did work the instructions to get them to work were impossible to understand. After spending countless hours working out how GNS3 works, and continuous dead ends, a rethink at the drawing board was to get this project back on track so what now?

Final project

Looking back at when the research was done for which devices were used in a network simulator there was an extensive number of available devices that all had different price ranges so this started to have me delve deeper into what devices were available and for small businesses which one would be the best to use? As pricing is a real-world problem the project took a final turn to look at the devices. So, what will the project look like? As stated, before the question that will be looked at is “Which devices offer the best performance and reliability, and how does their price compare?”. This will look at what are the best devices in switches, routers, wires, and servers to use for small, medium, and large companies looking at the ping between devices and comparing them to other devices.

Literature review

This section will focus on the Literature review. The Initial review will look at network simulators and the advantages and disadvantages of both. This literature review was done before working on the network simulators. The research was based on the different network simulators as the project was still incredibly open to change and the network simulator was a known backbone of the project so if the project changed, which it did, then the work in essence would not be for nothing.

The initial question that was researched was “What are the different simulators available?” The reason why this was researched was to make sure the most suitable simulator was used and to develop a better understanding of the simulators. Network simulators are used to create a virtual representation of a computer network. This is done to simulate and test different configurations, protocols, and scenarios of networks and evaluate the results. According to sources (Admin, 2020), the top two network simulators are the Cisco packet tracer and Graphical network simulator 3 which is also known as GNS3.

Cisco Packet Tracer

Cisco Packet Tracer is an exclusive application that facilitates the operation of Cisco platform devices. This software is pre-installed with a suite of Cisco devices and is compatible with Windows, Linux, and Mac OS operating systems. The software includes a Simulation mode that exhibits the flow of packets on each layer of the OSI model in a graphical representation. Although the user could customize routers and switches with additional modules, external device integration is not a feature. Furthermore, the software encompasses virtual servers that allow for the testing of various services, albeit with limited functionality.

Looking into the Cisco packet tracer in more detail there are advantages and disadvantages to using the system. Starting from the side of the advantages the user interface allows for the design, configuration, and simulation of networks to be easy. Making the simulator easy to use for anyone no matter the skill level (Yousef & Al-Nabhan, 2019). The second advantage of Cisco is its versatility as the Cisco packet tracer supports a wide range of network protocols and technologies. (Yousef & Al-Nabhan, 2019). And finally, an advantage that the Cisco packet tracer has is that it is multi-platform supportive. The accessibility of Cisco is vast to the point it is available on Windows, Linux, and Mac OS.

With positives, there are always negatives to follow. Cisco packet tracer is no different from the research done. Three disadvantages are in the Cisco packet tracer. The most common disadvantage that was in almost every report was that there are limited devices supported as the devices that are only supported in the simulator are devices that are made by Cisco and external device integration is also not allowed. For the more complex designs, this is very limiting. The second disadvantage of Cisco is that along with the devices, features are also limited. However, this will once again only affect more complex network simulations (Yousef & Al-Nabhan, 2019). The final disadvantage of the research (Mudgal & Rawat, 2018) was that the simulator is not always realistic. The research states that the behavior of the network simulator may not reflect the behavior that a network in the real world would react to.

GNS3

Moving away from the Cisco packet tracer, the other network simulator that was analyzed in the research was GNS3. Graphical Network Simulator 3 Unlike the Cisco packet tracer this simulator is open source. The simulator is based on Dynamips and a Cisco emulator with the option available to the user to have the ability to run the Cisco IOS software. Just like the Cisco packet tracer this network simulator supports devices that include routers, switches, and firewalls. Along with offering this the platform also offers for testing and troubleshooting the networks that were configured in this virtual environment.

Developing deeper into the research of GNS3 the advantages there were highlighted included the use of Cisco IOS, a wide range of devices, and open source. Starting the use of Cisco IOS software images is an advantage because the environment that the user will be put in will be more realistic and will closely resemble a real-world network atmosphere (Yousef & Al-Nabhan, 2019). Moving on to the second advantage of a wide range of devices (Mudgal & Rawat, 2018) the software allows for testing and evaluating a large built complex network topology with multiple devices with numerous configurations. Finally, the last-mentioned positive is the open source. The advantage that open source brings is that it is free to use and easily assessable with constant improvements and updates. The system can also be altered by the users themselves to fit their own needs.

Although many advantages were displayed by GNS3. There is still, however, disadvantages that follow the simulator that could affect the users that should also be considered. The main problem that is dominant is the additional setup requirement. When GNS3 is downloaded it comes as a skeleton more than a ready-to-use simulator as the competitors have to offer so when the software is downloaded additional downloads must be done to add the systems desired (Mudgal & Rawat, 2018). The difficulty that the simulator brings is also another big disadvantage that the simulator brings to the table. In comparison to the other simulators from a learner's or beginner's perspective, GNS3 is a hard simulator to understand and use. The final disadvantage that was found in the research that was done was that the software does not support all network devices like certain switches and routers are not supported by the software and this limits the compatibility and scope.

To summarize this literature review, both the networking simulators of Cisco packet tracer and GNS3 are robust, and they both possess unique strengths and weaknesses. The straightforward and simplified experience and ready-made devices with easy-to-use functionality and interface that Cisco has to offer. GNS3 also offers a more adaptive, flexible experience. The support for a broader range of devices and protocols also not be overlooked.

The choice of GNS3 may not be the optimal choice for all users although the benefits are substantial. The newer networkers who are working on network simulators may find the use of GNS3 hard to use. The use of user-friendly interfaces with pre-configured devices sounds a lot more indulgent and a more excellent choice for newer users.

Therefore, based on the literature review conducted, the networking simulator that will be used in this project will be a Cisco packet tracer due to the user-friendly interface, and preloaded devices. Also, the support for various protocols chose this software to be a lot more open and suitable for my use.

Methodology

This section will discuss the research methodology that was used to investigate Which devices offer the best performance and reliability and how do their price compare? The research took a quantitative research approach as the research approach that was taken was to focus on measuring and quantifying network performances. Measurements such as ping testing to produce numerical data to work with.

As stated, in this report the method used to answer this question was to gather data on a network simulator. The network simulator that was used was a Cisco packet tracer to develop on small networks, ideally starting basic and adding on a device or more to a network and looking at the ping test. The ping test was done to measure the approximate round trip times in milli-seconds that were produced. This was done for the devices available in Cisco packet tracer and research was conducted to find the cheaper alternative and the best alternative.

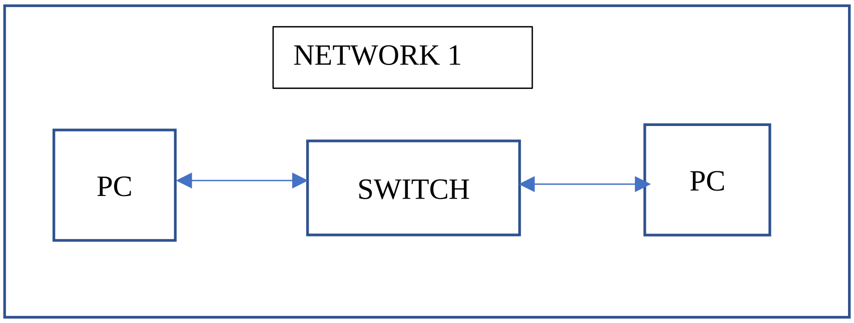
The data was analyzed by looking at what the research that was done before the test lined up with what was produced by the network simulator to see if the research was done correctly. The way that the research will be structured in the report will be that the artifact will be shown first, then the artifact and the device then the recommendations on other devices and how it will be better or worse depending on what will be spoken about.

Due to this methodology being used on a simulator, there are obvious limitations in that the devices could act differently in real-life scenarios. However, all the limitations and possible improvements will be discussed in the latter part of the report, and the possible solutions around how it could be fixed.

Design of networks

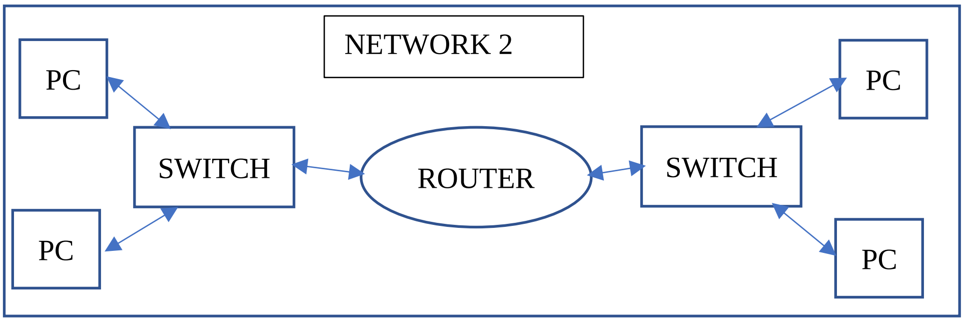
When designing a network there is a lot of involvement in developing the structure and communication pathways for devices within a system. Optimal functionality, scalability, and performance are essential when designing a network. In this section of the report, the design of a small, medium, and large network will be discussed.

Starting with the small business there will be two network topologies the first one being:



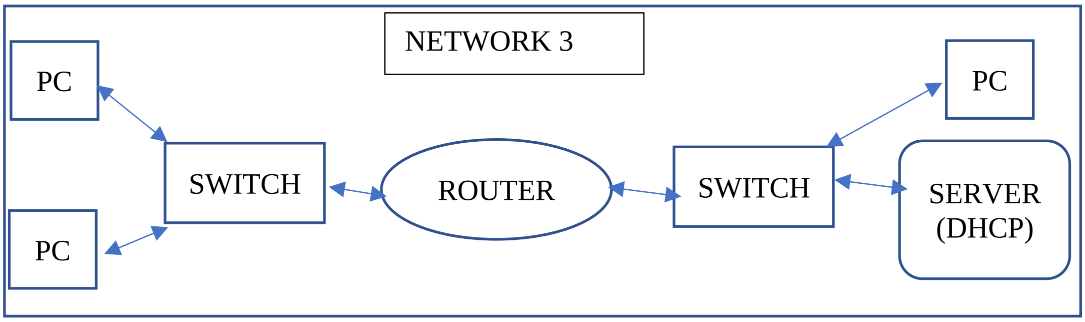
As shown in the diagram above the first network topology is a very simple topology consisting of two pcs and one switch to form a bridge for the two pcs. Connected with ethernet cables and the left pc will have a connection of 192.168.1.2/24 and the right side having 192.168.1.3/24 with static signing. This topology can be set up for a small office with only two employees with their desktops for example.

The second network topology that will be used for the showcase of the small network topology is:



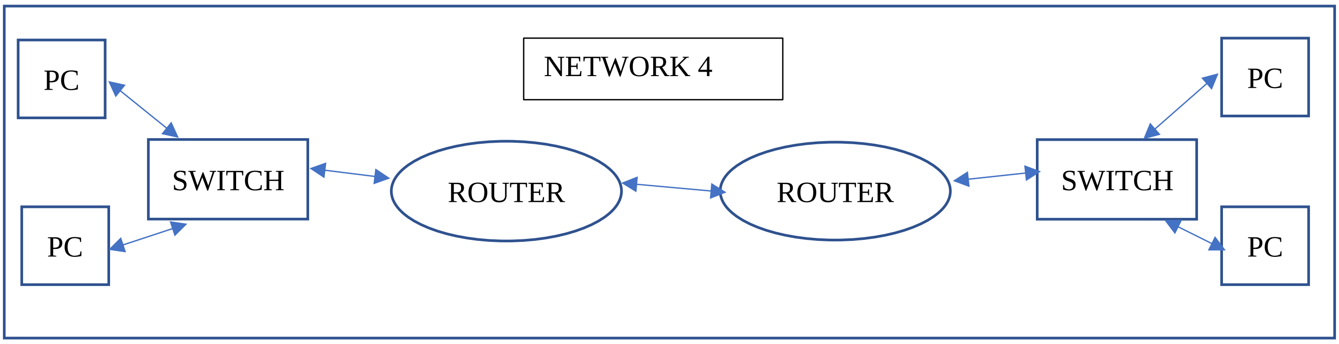
As shown in the diagram above the network topology is a little more complex with 2 networks bridged with a switch and a router and 2 pcs in each network but still would come under a small business. With all wires in the connection connected with ethernet cables with the first port on the left configured as 192.168.1.1/24 and the first pc configured as 192.168.1.2/24 and the second configured as 192.168.1.3/24. The first port for the right-hand side would be configured as 192.168.2.1/24 and the first pc on the left is configured as 192.168.2.2/24 and the final one configured as 192.168.2.3/24. Although this is a little more complex this topology is still for a small network like a small office or home office (SOHO) this could be for a network with limited devices that need to be connected to a network. Internet connectivity can be provided by the router and bridge the connection between the pcs and switches. The reason why this could be used is to segment the network into different areas. Improvements such as performance and security can be advanced by the reduction of the amount of broadcasting traffic on the network.

Contract to the small network, the medium-sized network as this report is concentrating on the devices and not the actual topology itself these topologies will look basic but have the devices in the network available to be able to scale up into a complex network. The first of these two networks are:



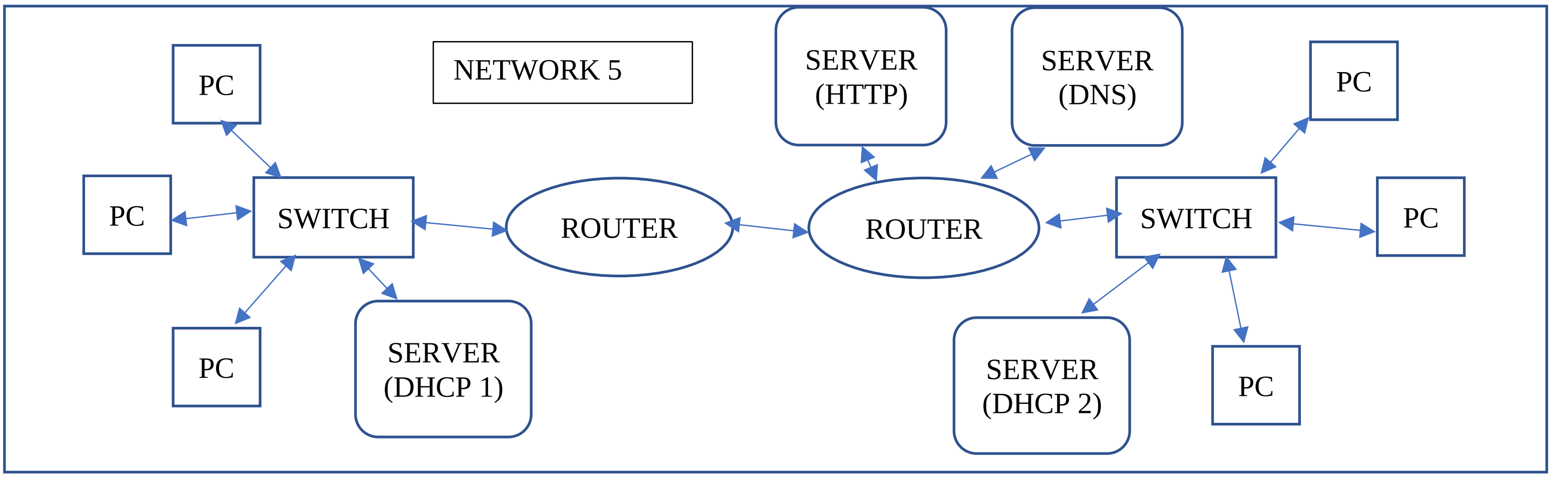
The topology shown above has a connection to a DHCP server which will automatically give out the addresses to the pcs connected to the network. So, on the right-hand side, the IP address will automatically be given to the pc which should be 192.168.2.3/24 and the IP address of the DHCP server should be 192.168.2.2/24. As the DHCP server is on only one side of the network topology it cannot hand out IP addresses to all the pc users so on the left-hand side the IP address 192.168.1.3/24 will be given to the pc on top and 192.168.1.4/24 will be given to the pc below. The port connecting the left-hand side will have the port address 192.168.1.1/24 and the port connecting the right-hand side will have the port number 192.168.2.1/24. All the connections will be ethernet connections, and the router will be RIP so that it can communicate with both sides of the network.

The second topology used in the medium-sized business will be:



In this topology, the reason why there are two routers is that they have the possibility of bringing redundancy and failover, load balancing, and security. The IP addresses that will be used on the end devices on the left-hand side are 192.168.1.2/24 for the top left and 192.168.1.3/24 for the bottom left. Moving to the right-hand side the top right of the end device will have the connection 192.168.2.2/24 and the bottom right will have the connection 192.168.2.3/24. For the port connecting to the left-hand side of the left router the connection to the port will be 192.168.1.1/24 is used and to bridge the connection between the two routers the connection 10.0.0.2/24 will be used. For the right-hand side of the connection looking at the right router, the connection to the port will be 192.168.2.1/24 and the same connection of 10.0.0.2/24 will be used to bridge the connection between routers. RIP will be done between the routers so the networks can communicate with each other and once again ethernet cables will be used with a serial connection between the routers. These topologies could be used in a slightly larger network, possibly a small business or large office, an example of this could be a small law firm, one with multiple floors or quite a few employees.

Finally moving on to the large topology there is only one topology that was used and that is:



The purpose of the DNS and the HTTP servers is that it could manage the possible website that the company has and its internal network system. Just like in the last network topology, the DHCPs will give the pcs IP addresses. For the left-hand side top left pc, the IP address that the pc is meant to get is 192.168.10.4/24 and the one in the middle should get 192.168.10.3/24, and the bottom one should get 192.168.10.5/24. Moving over to the right-hand side of the topology the DHCP should also distribute the IP address for the pcs in the topology starting from the top the IP address should be 192.168.20.4/24 the middle pc should be 192.168.20.2/24 and the bottom one should be 192.168.20.3/24. The DHCP on the left will be able to configure up to 192.168.10.253/24 and the IP address of the DHCP will be 192.168.10.10/24 and the DHCP on the right will have the configuration 192.168.20.254/24 and the configuration of the server will be 192.168.20.10/24. The DNS will have the IP address 192.168.30.10/24 and the HHTPS will have the IP address 192.168.40.10/24. Moving on to the ports, the connection to the left-hand side of the topology of the router will have the IP address of 192.168.10.1/24 and the right-hand side of that connection that connects to the other router will be 10.0.0.1/24. Moving to the left-hand side router the IP address for the connection to the routers will be 10.0.0.1/24 and the connection to the other network will be 192.168.20.1/24. Connecting to the DNS server the IP address will be 192.168.30.1/24 and the connection to the HTTP website the IP address will be 192.168.40.1/24.

Wires in networks

Before indulging in the networks and devices wires need to be discussed first. Selecting the right cables is one of the most essential processes when developing a reliable network infrastructure. The correct cables for the network might make a distinction between an efficient, smooth connection and one that is sluggish, unreliable, and unsafe. A quick review of the various cable kinds, their functionality, cost, and dependability, as well as the benefits of using the best cable possible.

For ethernet networking the cables used are called Cat or category cables. The cables come in different categories and capabilities starting with the oldest type of cable that is available, the Cat 5 cable with 100 MHz for the maximum frequency and 100 Mbps for the maximum bandwidth. For the slightly improved speed of 350 MHz frequency and 1Gbps bandwidth as a maximum, the cable Cat 5e is the cable. Cables Cat 6 and Cat 7 have the same bandwidth at 10 Gbps but Cat 6 has a max frequency of 550 MHz whereas Cat 7 has a slightly higher max frequency at 600 MHz.

Looking at the cables from the viewpoint of speed, the cables can vary when it comes to bandwidth and frequency. The higher that the cat goes the faster the cables and the transmission becomes. An example of this is evident by looking at cat 5 and comparing it to cat 6, cat 5 has a maximum speed of 100 Mbps whereas cat 6 has 10 Gbps. The resistance to interference and noise can also be influenced by the frequency and bandwidth with the impact being on reliability and performance.

Looking at it from the aspect of cost, the cheapest cables are the cables with the lowest frequency and bandwidth which is cat 5 at the bottom and cat 7 at the top. However, in the viewpoint of the short distance for the wire, the price is negligible.

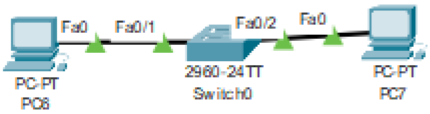
Looking at specific types of wires that can be used at the top of the list for the best wire are fiber optics cables. With transmission rates at 10Gbps + and since light is used to transmit the data. With no interference from electromagnetics and high bandwidth making fiber optics long-distance ideal. However, it is not all perfect as the price of fiber optics per foot can be found at $0.50 to $5. The price difference is because the quality of the cable can change the value of the cable. As this cable uses light to communicate it does not come under cat.

Looking into a cable that is a little cheaper than the fiber optic cables is the twisted pair cables that can also be found as shielded and unshielded. But what is the difference? For better protection from electromagnetic interference the shielded twisted pair, which is also known as STP, are either wrapped in metallic foil or braid. Therefore, the unshielded twisted pair, also known as UTP, is unsurprisingly not covered in anything. The problem that it causes is that UTP is more prone to interference but both cables offer good performance, at 10 Mbps to 10 Gbps, at a good price, at $0.20 to $0.50 per foot, and are at cat 5.

In conclusion, the best cable that is available is the fiber optical cables if the budget for the topology allows for such cable however the twisted pair of cables are very good as well and a lot cheaper.

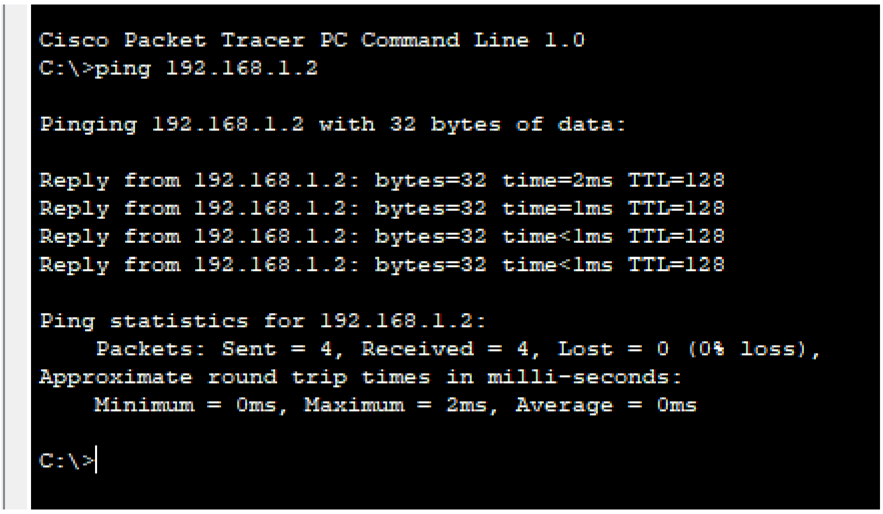
Topologies

Starting with the network one switch used in the artifact made is the 2960-24TT.



Looking into the Cisco catalyst 2960-24TT the device is a commonly used switch in the market of small and medium-sized businesses and is a mid-range switch. The fat travel speed of 32 Gbps allows for the backplane speed of the device to transfer data fast within the network and supports 24 ports with 2-gigabit uplink ports. The advantages that are in the switch has to offer are that features such as quality of service and virtual local area networks have been built into the system and the device is made to last long. However, the disadvantage this can bring is that layer 3 protocols are not built in. However, if the device is not being used for larger more complex buildings, then it is not an issue.

Looking into the pings:

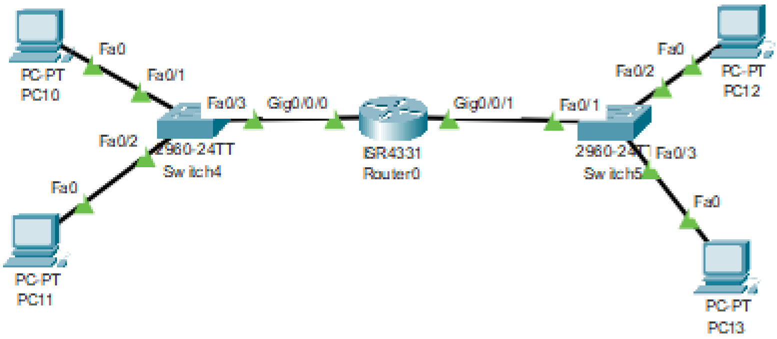


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=2ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>
```

For this ping test, the results are nothing that can be improved as the speed of this device is already very fast. However, for a price range of $300 to $900, it is an expensive device for a company that is starting up. Even because for $20 to $30 the TP-Link TL-SF1005D with an average local speed of 1-10ms for the ping. Looking at the best switch that is on the market, however, for a switch the Cisco Nexus 9000 series priced at $20,000 to $200,000 is an overkill in my opinion for this type of network.

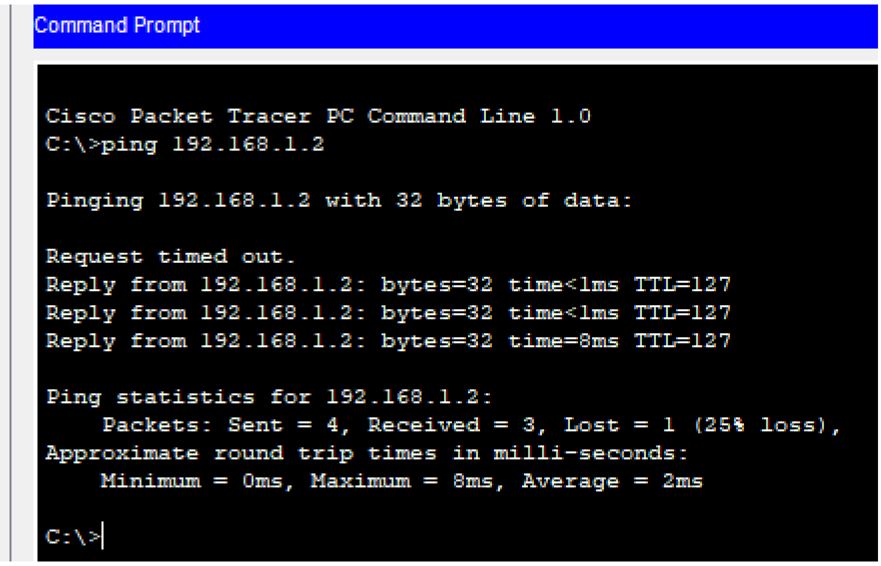
Looking at the rough price range for networks, at a basic level the price is from $50 to $200. From this, the basic level of TP-Link TL-SF1005D is a perfect switch for this setting as the price is the very bare minimum for a bare minimum topology.

Moving on to the second network the router ISR4331 was used with the same switch from network 1.



The switches have already been discussed in the last topology. So, looking at the ISR4331 router in this topology the price for this router starts at $1,500 to $3,000 and for that price, the router can include support for multiple types of WAN connections. VPN and firewalls are also available and capable by this router with included T1 and T3, which is digital transmission used for voice and data communication, and ethernet. And a limitation that this router brings with all the positive points is that the ports are very limited to 10/100/1000.

Ping test results from the second topology



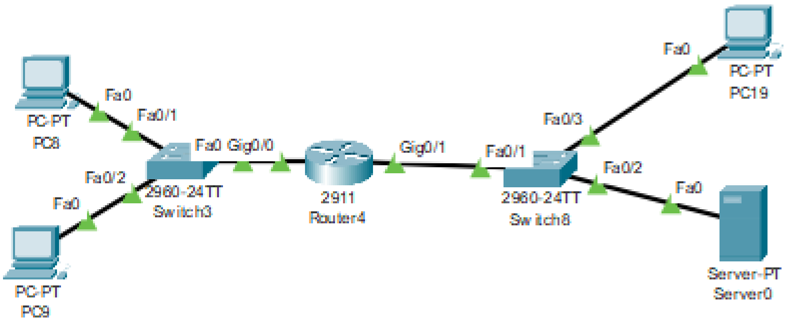
Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time=8ms TTL=127

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 8ms, Average = 2ms

C:\>
```

Looking at the ping test ones again there is very little room for improvement as the ms are all as best as they could be. By looking at the average prices of the router used and comparing it to the average amount spent on a network by a small business the amount the router costs is worth too much. For a small network, this router is very good but for the average price range a TP-Link Archer C50 at a price range from $20 to $50. On the other hand, the top-of-the-range router that is available is a Cisco ASR9000. However, this router could range from thousands to hundreds of thousands of pounds. But for this topology, the TP-Link Archer C50 is recommended.

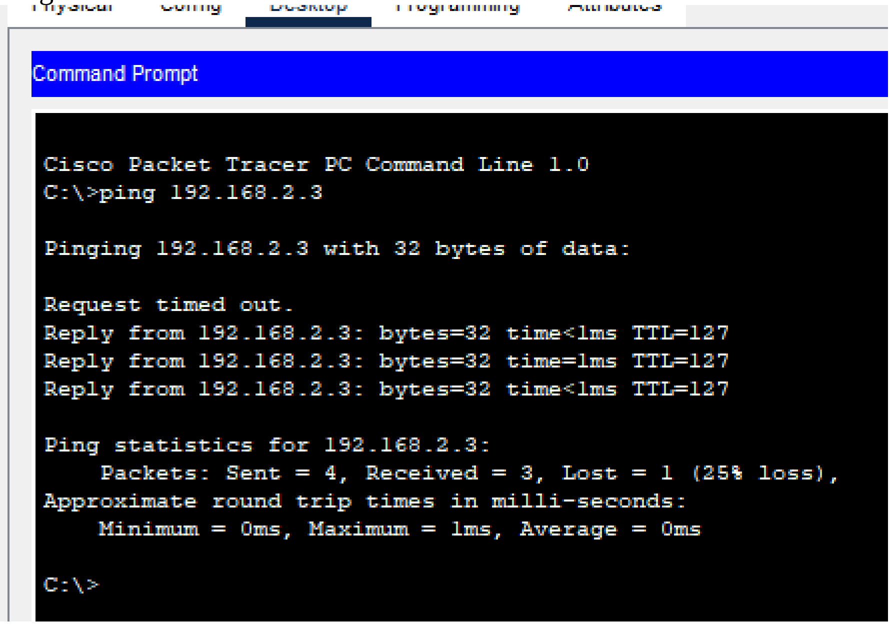
So as a quick summary, the switches and routers that are recommended for the average amount spent on a network simulator are the basic unmanaged TP-Link TL-SF1005D for the switch and the TP-Link Archer C50 for the router. Even though the switch is known as unmanaged with basic features the mean time before failure is still aimed at around 3 years if not longer if used in its capabilities. Moving onto the router with also a mean time before failure also 3 years it has a built-in firewall to have some protection on the network. But like all routers, factors such as the load on the router can affect the reliability and performance of the router. Also, the speed of the network will be from 1 ms to 10 ms.

Moving on to the third topology that looked like this when configured:



Based on the information that was found from the last network the best switch to use is the 290-24TT as it is best for a mid-ranging network and as money is less of a problem for this network topology the switch fits perfectly in the topology. In this topology, there was another router 2911 used with high performance with 180 Mbps, advanced security features, modern design, easy upgrades, and scalability. However, the disadvantage of the router is that it is expensive at $1,000 to $3,000. And may require additional licenses for certain features. Looking at servers, the cheapest server available starts at $300 to $600 and the mid-price is $2.500 to $5,00, and the highest one is,00 to $15,000.

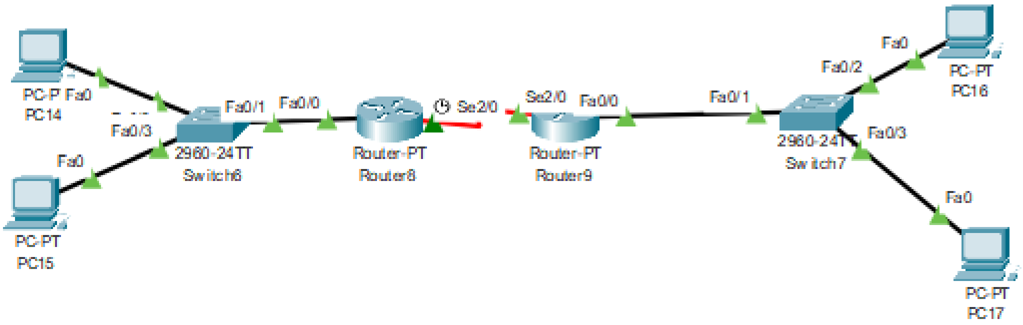
Ping test



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.3: bytes=32 time<1ms TTL=127
Reply from 192.168.2.3: bytes=32 time=1ms TTL=127
Reply from 192.168.2.3: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

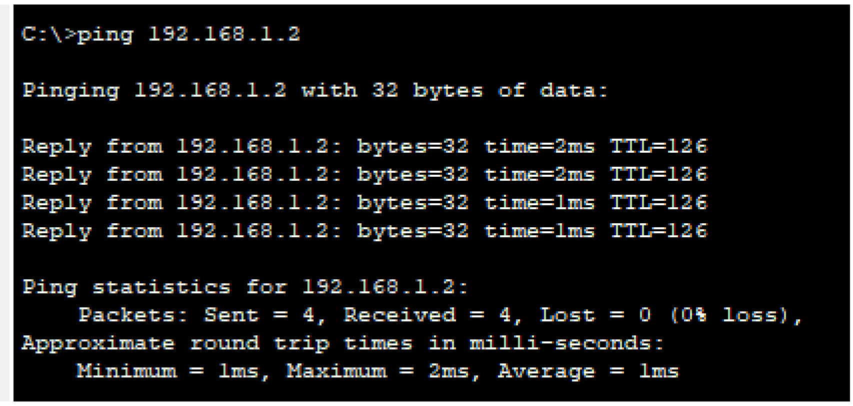
The test done with this ping test showed that the current routers and switches used are as best as they could get with times as low as 1 ms. Keeping the same switches and changing the routers and servers. According to the research done the best mid-range router that is out right now is the Asus RT-AC68U and the pro of the router is that router is high-performance hardware making the routers fast and efficient with good security features and good range and coverage. The range of the price of the router is $50 to $400. Also, Asus is known for its good reliability. Moving on to the server and fitting this topology the HPE ProLiant DL360 Gen10 server priced at $2,500 to $5,000 is the best device to fit the topology. The pro of this server is that it has high performance with 56 threads per processor and 28 cores. The server can also hold up to 3TB of memory.

Looking at the fourth topology that looked like this when configured:



The devices that could be exchanged in the topology have already been discussed so in this section of the report the discussion will be on using 2 routers in the network topology. With a dual router setup, several positives develop. Firstly, the redundancy of the system Is improved this is because the system is not reliant on just one router holding up the network so there is leeway essentially that if a router is to go down the system can still be running. The load between both routers can be distributed evenly meaning that there is less pressure on a singular device. This could bring the benefit of lasting longer and saving money in the long run, however, it would be expensive in the short term, and busting performance as the system can tackle the job faster. Of course, the final point is that the system is a lot more scalable due to the possible empty ports. It will save money and time when a business wants to expand the business even further. One of the biggest drawbacks to the dual router is that the compatibility of the devices could be an issue. The impact this could bring could ruin the improvement of performance and reliability. In an overall view, however, the idea of having a dual router setup is better, because of the load balancing, redundancy, quality of service, security, and monitoring, for the company in the long run.

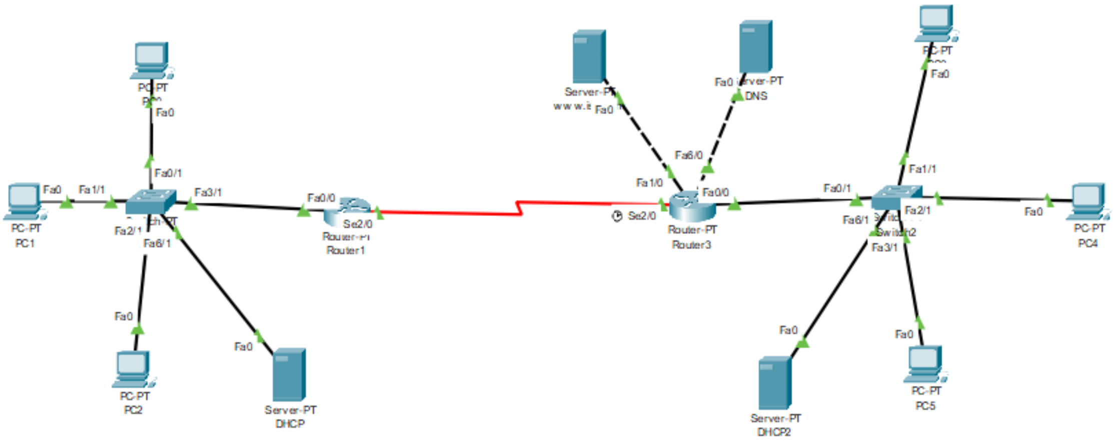
Ping test:



```
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=2ms TTL=126
Reply from 192.168.1.2: bytes=32 time=2ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms 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 = 1ms, Maximum = 2ms, Average = 1ms
```

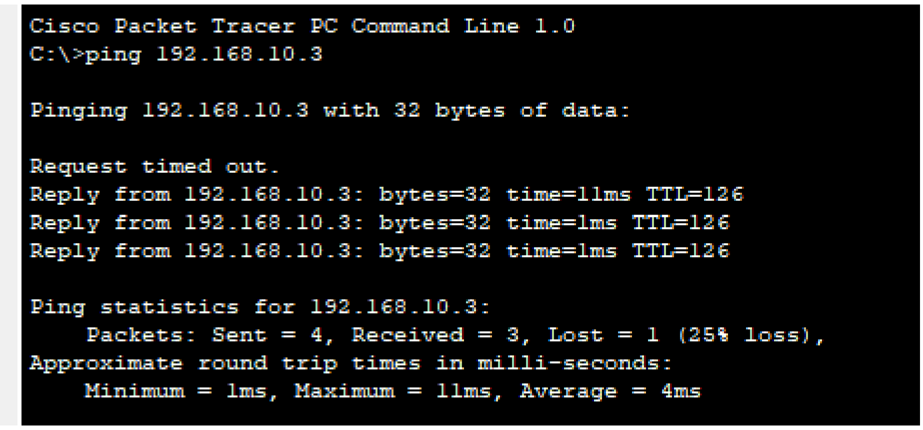
From the ping test that was conducted the system does look to be a little bit slower but with the right functions put in I believe it could be even faster than a single router.

Finally looking at the last topology of the report



Looking at this topology the best devices that would fit in this are the best of the best devices. Starting with the routers the Cisco ASR 1000 Series is a good router to use with a price of $10,000 to $50,000. The network connectivity is managed by this router with traffic management. This is done for efficient use of resources and when having your website up you will want the system to be as efficient and well-run as possible. Also, WAN connectivity so that the business will have an easy trying to contact other companies and not have to worry about where the company is located. The switch that is to be recommended is the Cisco Nexus 9000 Series. The high-speed low latency, with virtualization, automation, and security. The price of a switch like this could vary from $10,000 to$50,000. Finally, the Dell PowerEdge R940 with the offering of performance, scalability, and reliability the server is all that is needed to run a website with the price of the server starting at $10,000 to $50,000. The server also provides centralized storage and processing capabilities. The hosting of applications and servers is the most important.

The ping test:



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.10.3: bytes=32 time=11ms TTL=126
Reply from 192.168.10.3: bytes=32 time=1ms TTL=126
Reply from 192.168.10.3: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 11ms, Average = 4ms
```

As clearly visible from the piing test the system is very slow and could be improved drastically so that is why the devices above have been suggested.

Evaluation

As for the hypothesis that was made at the start of the project, I came to find out that it was very broad, and that juniper did not even come up hardly in the report. To improve, if I was to do this project again, I would try to get a network in real life to see how they compare. However, if I was to do another project, I believe I would set out a task and not change the project often.

Conclusion

In conclusion, there were a lot of different devices, and researching them has told me that there is more to networking than meets the eye. There are so many devices that have so many different possible outcomes and ways that they work. In conclusion, there was a lot learned and a lot to improve on.

References

Mudgal, N., & Rawat, P. (2018). Comparative analysis of network simulators: GNS3, Cisco Packet Tracer, and NS2. International Journal of Computer Science and Mobile Computing, 7(5), 112-118. Retrieved from http://www.ijcsmc.com/docs/papers/May2018/V7I5201841.pdf
Yousef, S., & Al-Nabhan, N. (2019). Evaluation of network simulators: Cisco Packet Tracer vs. GNS3. International Journal of Computer Science and Information Security, 17(9), 166-174. Retrieved from https://arxiv.org/ftp/arxiv/papers/1910/1910.02102.pdf
Mudgal, N., & Rawat, P. (2018). Comparative analysis of network simulators: GNS3, Cisco Packet Tracer, and NS2. International Journal of Computer Science and Mobile Computing, 7(5), 112-118. Retrieved from http://www.ijcsmc.com/docs/papers/May2018/V7I5201841.pdf.

Yousef, S., & Al-Nabhan, N. (2019). Evaluation of network simulators: Cisco Packet Tracer vs. GNS3. International Journal of Computer Science and Information Security, 17(9), 166-174. Retrieved from https://arxiv.org/ftp/arxiv/papers/1910/1910.02102.pdf

Abacus. "How Much Does It Cost to Set up a Small Business Network - Abacus." *Goabacus.com*, 25 June 2020, goabacus.com/how-much-does-it-cost-to-set-up-a-small-business-network/#:~:text=So%20how%20much%20will%20it%20cost%20you%20to. Accessed 18 Apr. 2023.

Admin. “Best Network Simulation Tools for Network and Network Security [2020].” *GNS3 Network*, 28 July 2020, www.gns3network.com/best-network-simulation-tools/#:~:text=Best%20Simulation%20Tools%20for%20Computer%20Networking%201%201. Accessed 29 Feb. 2023.

Cisco. “Cisco Annual Internet Report (2018–2023) White Paper.” *Cisco*, 9 Mar. 2020, www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html. Accessed 10 Apr. 2023.

Jeong, Jiwoong, et al. *Radiomics in Cancer Radiotherapy: A Review*. 2018.

Bibliography

Electrical & Computer Engineering Project. “Static Routing with Connecting 4 Routers with Explanation | Cisco Packet Tracer Tutorial 3.” *Www.youtube.com*, 21 July 2019, www.youtube.com/watch?v=rZw_b0wpQ00&t=298s. Accessed 18 Mar. 2023.

GeeksforGeeks. “Network Devices (Hub, Repeater, Bridge, Switch, Router, Gateways, and Brouter) - GeeksforGeeks.” *GeeksforGeeks*, 5 Sept. 2018, www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/. Accessed 16 Feb. 2023.

Mann, Terry. “The Most Common Types of Network Devices.” *Lepide Blog: A Guide to IT Security, Compliance and IT Operations*, 11 July 2022, www.lepide.com/blog/the-most-common-types-of-network-devices/. Accessed 10 Jan. 2023.

Melnick, Jeff. “Network Devices Explained.” *Netwrix.com*, 8 Jan. 2019, blog.netwrix.com/2019/01/08/network-devices-explained/. Accessed 15 Jan. 2023.

Rifat, Unique. “Web Server in Cisco Packet Tracer || How to Configure a Web Server.” *Www.youtube.com*, 26 July 2020, www.youtube.com/watch?v=XDvQWQW0SCo&t=5s. Accessed 18 Mar. 2023.

Shock, Code. “Configuring Two Routers with Switch Using CLI in Cisco Packet Tracer.” *Www.youtube.com*, 8 May 2016, www.youtube.com/watch?v=q5dzTH2bHX8&t=403s. Accessed 18 Feb. 2023.

Tagliacane, S. V, et al. “Network Simulations and Future Technologies in Teaching Networking Courses: Development of a Laboratory Model with Cisco Virtual Internet Routing Lab (Virl).” *IEEE Xplore*, 1 Mar. 2016, ieeexplore.ieee.org/abstract/document/7566212. Accessed 28 Dec. 2022.

Technical Xpress. “GNS3 Tutorial - Full Setup Guide for Beginners - a to Z.” *Www.youtube.com*, 2021, www.youtube.com/watch?v=AuokrRQVTEw. Accessed 11 Jan. 2023.

Roshan Kandel. “How to Create a Simple Network in GNS3 with 1 Router, 1 Switch & Multiple End Devices (VPCs).” *Www.youtube.com*, 2022, www.youtube.com/watch?v=Xt0M0VgMBBU&t=75s. Accessed 2 Jan 2023.

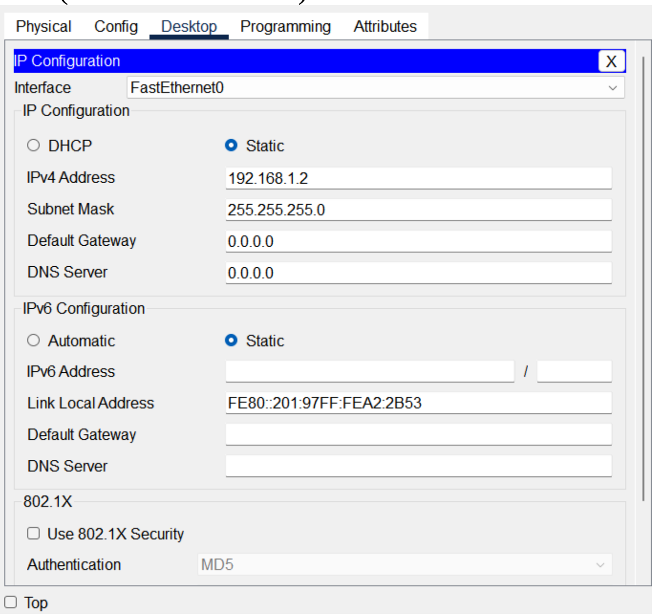
Rajganesh Pandurangan. “GNS3 - Basic Routing, ARP, ICMP, Wireshark Demo.” *Www.youtube.com*, 2016, www.youtube.com/watch?v=MfDLeqiCM8c&t=2s. Accessed 2 Jan 2023.

Appendix

The appendix will consist of the configuration screenshots of all the networks that were created.

Network 1:

Pc 1 (left virtual machine)



IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.1.2

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::201:97FF:FEA2:2B53

Default Gateway:

DNS Server:

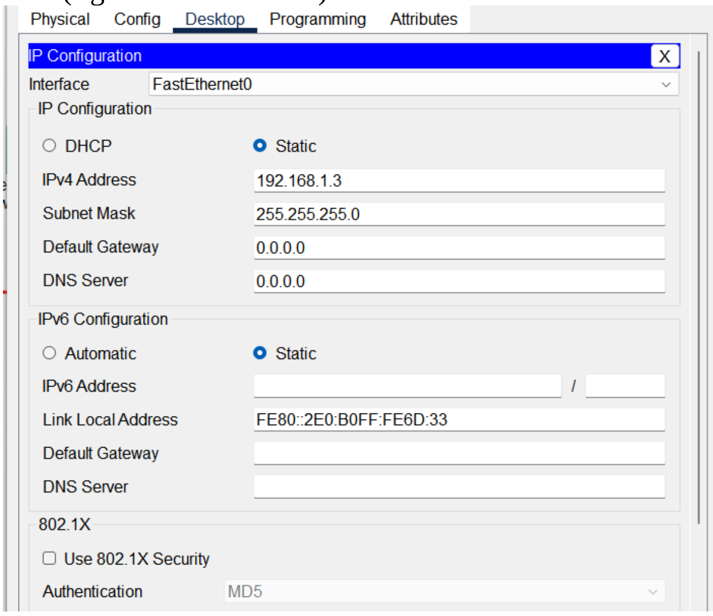
802.1X

□ Use 802.1X Security

Authentication: MD5

□ Top

Pc 2 (right virtual machine)



IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.1.3

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::2E0:B0FF:FE6D:33

Default Gateway:

DNS Server:

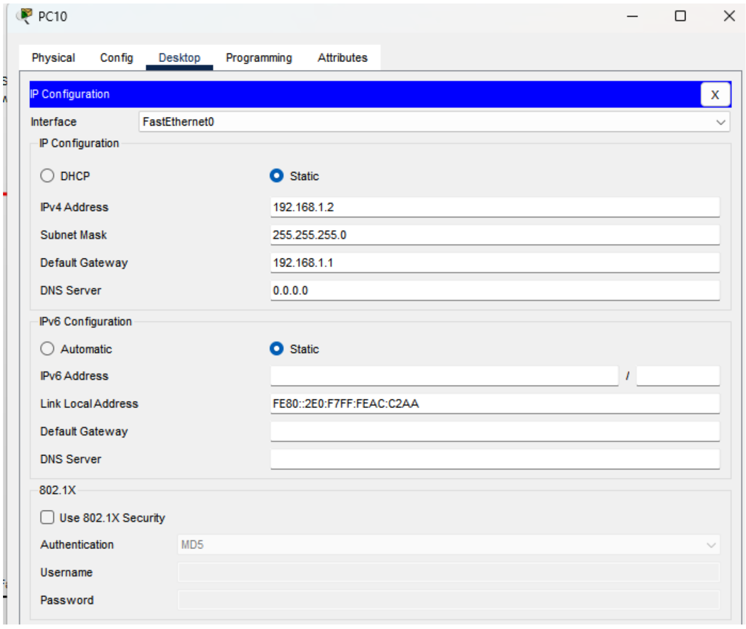
802.1X

□ Use 802.1X Security

Authentication: MD5

Network 2:

Pc for the top left configuration



Interface FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address 192.168.1.2

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address /

Link Local Address FE80::2E0:F7FF:FEAC:C2AA

Default Gateway

DNS Server

802.1X

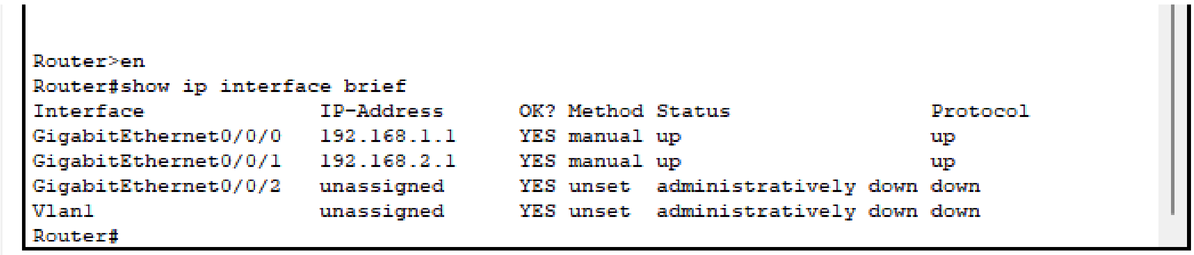
□ Use 802.1X Security

Authentication MD5

Username

Password

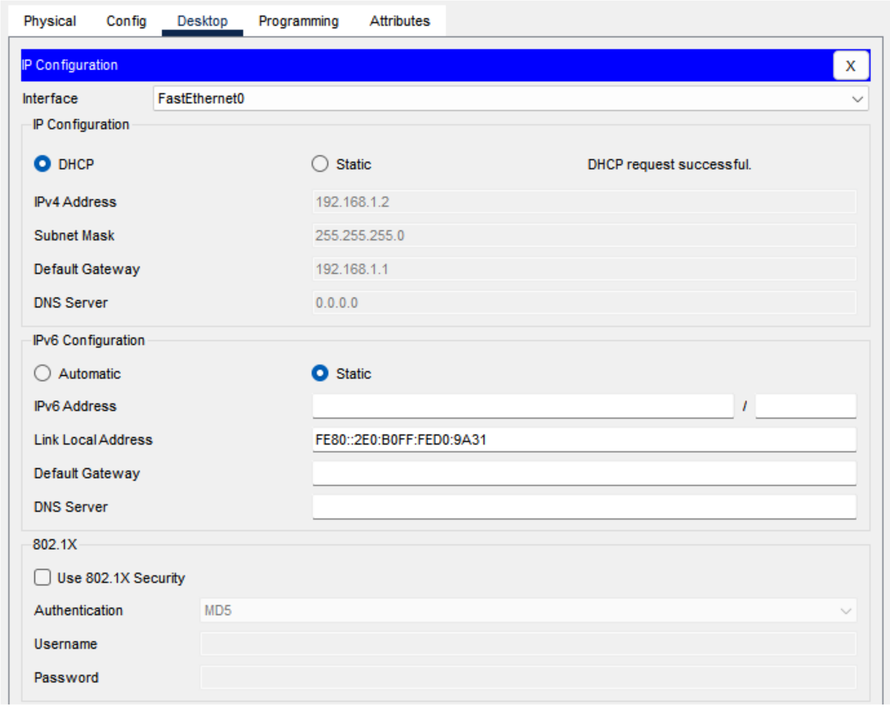
The router configuration for all the ports was.



```
Router>en
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   192.168.1.1     YES manual up                    up
GigabitEthernet0/0/1   192.168.2.1     YES manual up                    up
GigabitEthernet0/0/2   unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
Router#
```

Network 3:

In the third network, the pc connected to the DHCP had the connection.



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static DHCP request successful.

IPv4 Address: 192.168.1.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::2E0:B0FF:FED0:9A31

Default Gateway:

DNS Server:

802.1X

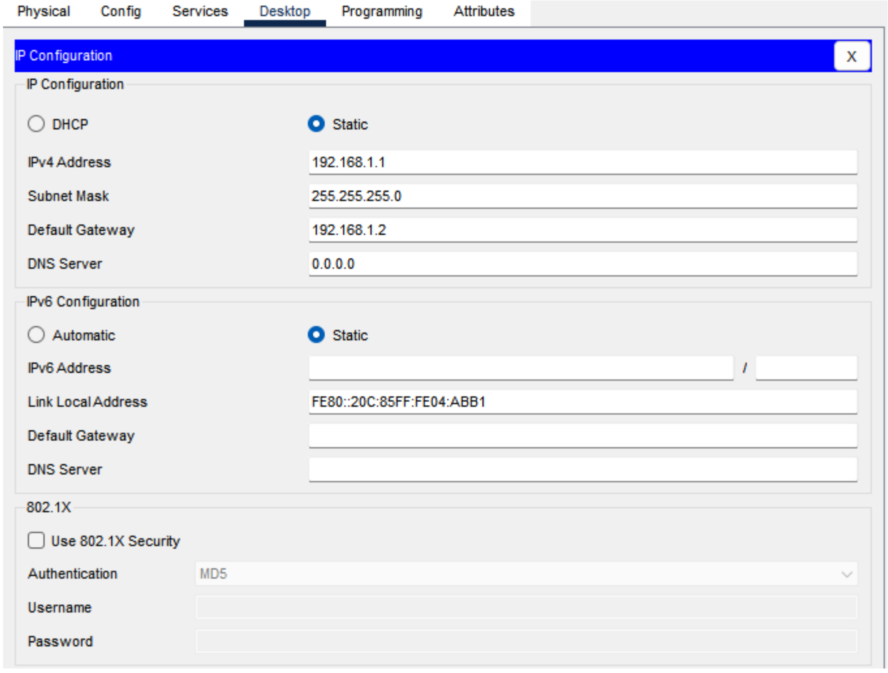
□ Use 802.1X Security

Authentication: MD5

Username:

Password:

The DHCP has the static IP configuration of



IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.2

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::20C:85FF:FE04:ABB1

Default Gateway:

DNS Server:

802.1X

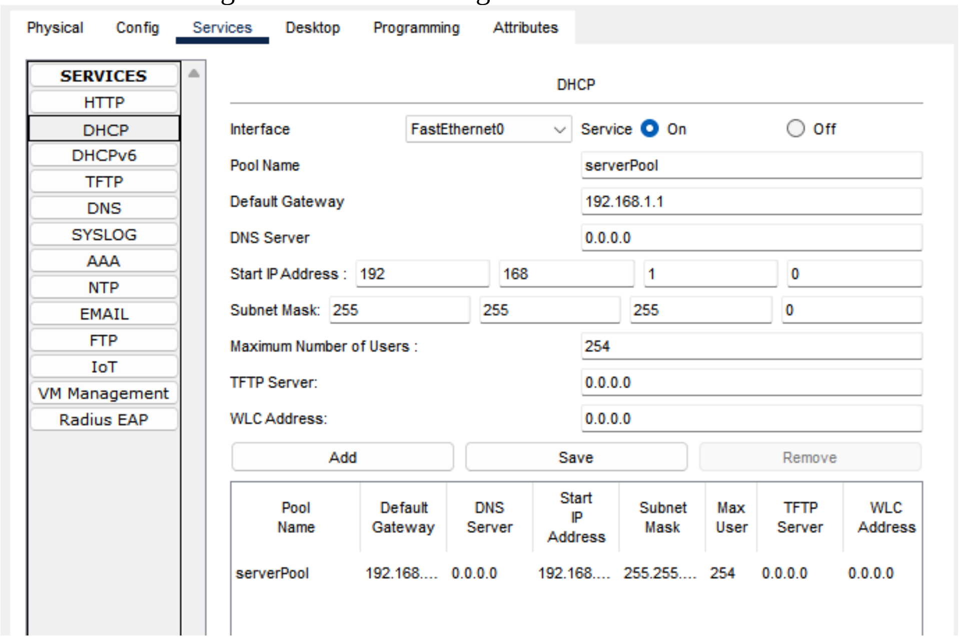
□ Use 802.1X Security

Authentication: MD5

Username:

Password:

The connection to get the DHCP working is in the next screenshot.



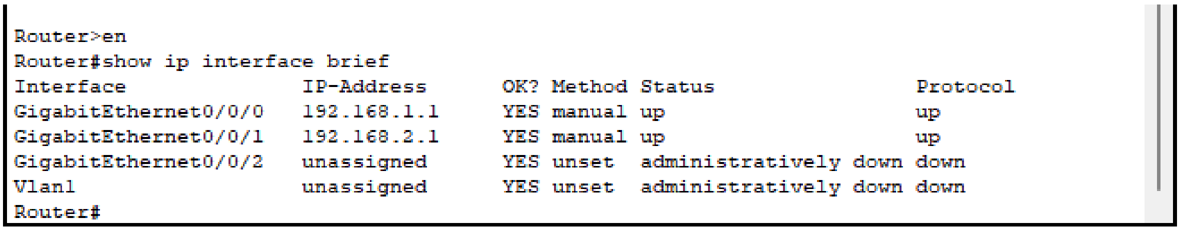
DHCP

Interface: FastEthernet0 Service ● On ○ Off

Pool Name	serverPool
Default Gateway	192.168.1.1
DNS Server	0.0.0.0
Start IP Address :	192 . 168 . 1 . 0
Subnet Mask:	255 . 255 . 255 . 0
Maximum Number of Users :	254
TFTP Server:	0.0.0.0
WLC Address:	0.0.0.0

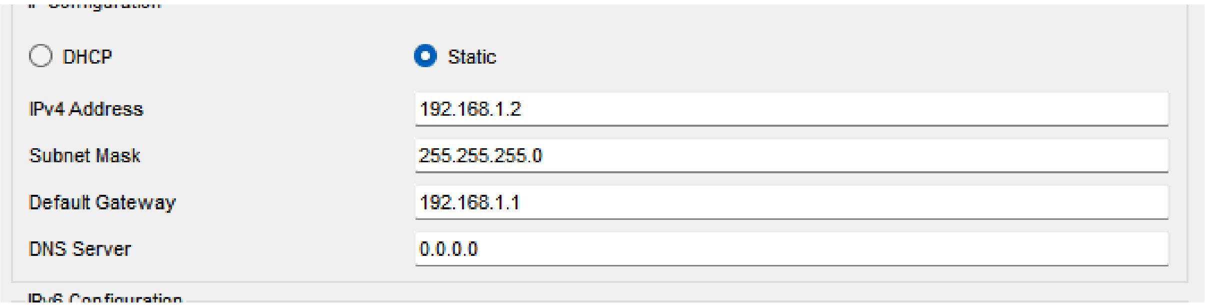
Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168....	0.0.0.0	192.168....	255.255....	254	0.0.0.0	0.0.0.0

The router in this network has the connections of



```
Router>en
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   192.168.1.1     YES manual up                    up
GigabitEthernet0/0/1   192.168.2.1     YES manual up                    up
GigabitEthernet0/0/2   unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
Router#
```

One of the static connections of the pcs in this connection is the next screenshot.

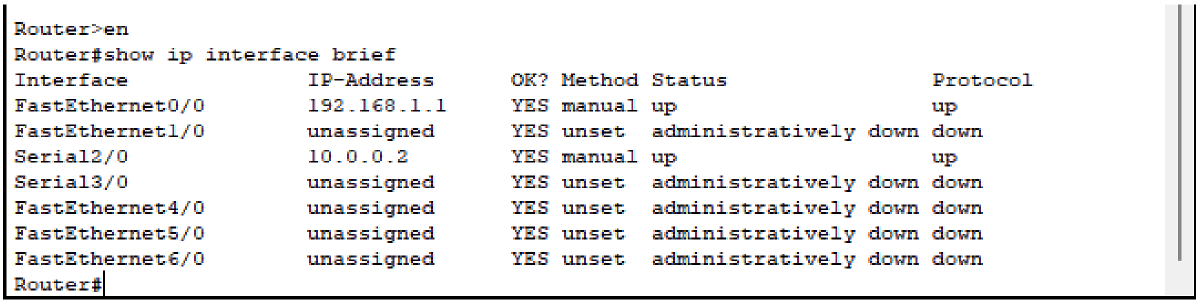


○ DHCP ● Static

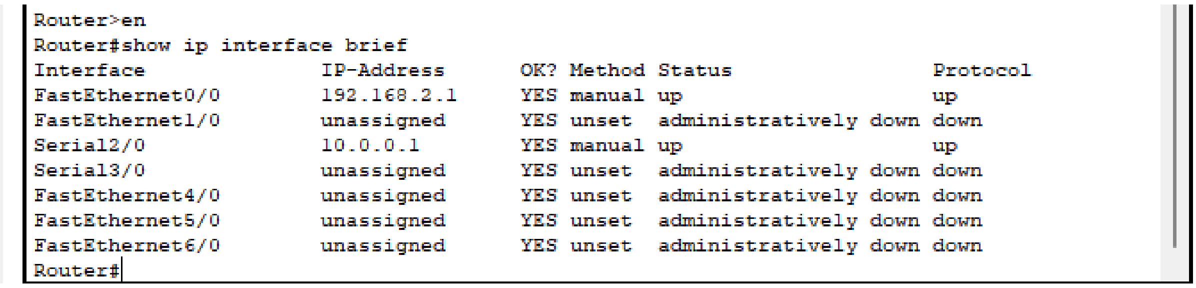
IPv4 Address	192.168.1.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	0.0.0.0

Network 4:

Starting with the routers first the configuration looks like this.



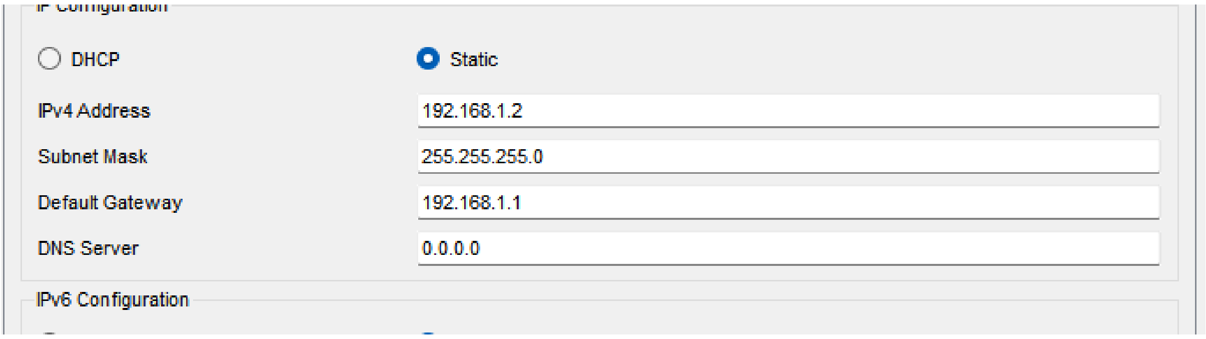
```
Router>en
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.1.1     YES manual up                    up
FastEthernet1/0        unassigned      YES unset  administratively down down
Serial2/0              10.0.0.2        YES manual up                    up
Serial3/0              unassigned      YES unset  administratively down down
FastEthernet4/0        unassigned      YES unset  administratively down down
FastEthernet5/0        unassigned      YES unset  administratively down down
FastEthernet6/0        unassigned      YES unset  administratively down down
Router#
```



```
Router>en
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.2.1     YES manual up                    up
FastEthernet1/0        unassigned      YES unset  administratively down down
Serial2/0              10.0.0.1        YES manual up                    up
Serial3/0              unassigned      YES unset  administratively down down
FastEthernet4/0        unassigned      YES unset  administratively down down
FastEthernet5/0        unassigned      YES unset  administratively down down
FastEthernet6/0        unassigned      YES unset  administratively down down
Router#
```

With the proof of the RIP configuration is the ping as if it was not done the two networks would not communicate with each other

As the pcs are all static connections only one screenshot will be provided of the top left pc



IP Configuration

○ DHCP ● Static

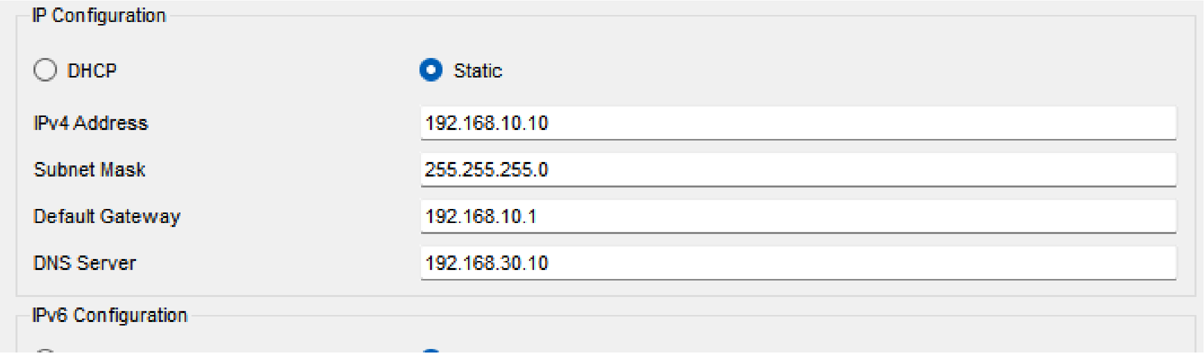
IPv4 Address	192.168.1.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	0.0.0.0

IPv6 Configuration

Network 5:

First looking at the DHCPS the first screenshot will be the static IP address of the DHCP and the second being the actual connection for the DHCP to work.

DHCP 1

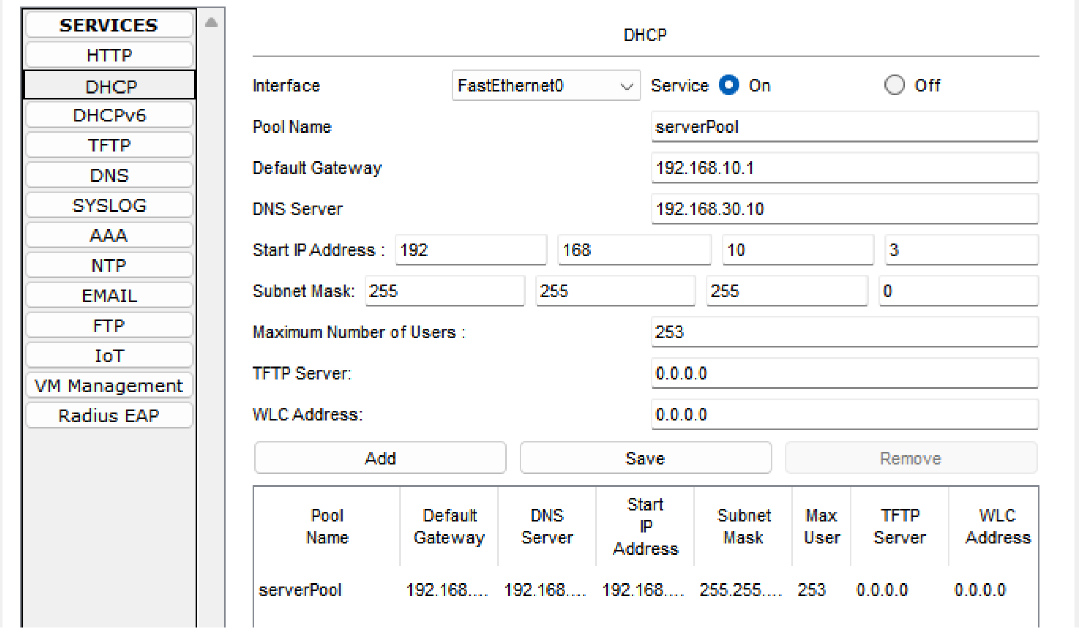


IP Configuration

○ DHCP ● Static

IPv4 Address	192.168.10.10
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
DNS Server	192.168.30.10

IPv6 Configuration



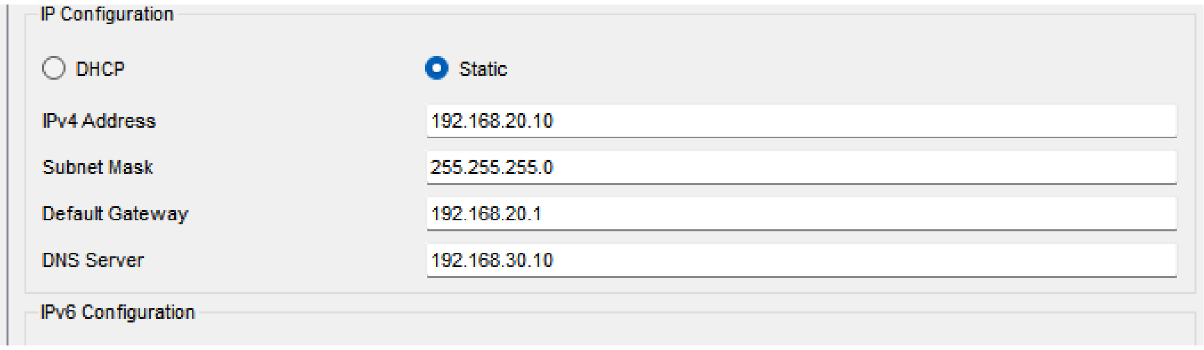
DHCP

Interface FastEthernet0 Service ● On ○ Off

Pool Name	serverPool
Default Gateway	192.168.10.1
DNS Server	192.168.30.10
Start IP Address :	192 168 10 3
Subnet Mask:	255 255 255 0
Maximum Number of Users :	253
TFTP Server:	0.0.0.0
WLC Address:	0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168....	192.168....	192.168....	255.255....	253	0.0.0.0	0.0.0.0

DHCP 2

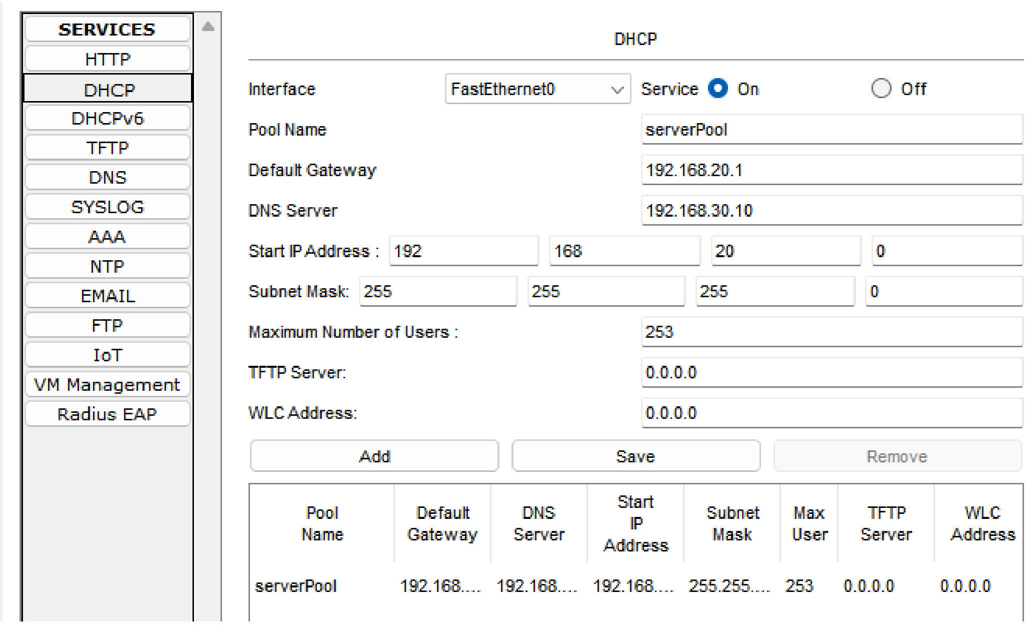


IP Configuration

○ DHCP ● Static

IPv4 Address	192.168.20.10
Subnet Mask	255.255.255.0
Default Gateway	192.168.20.1
DNS Server	192.168.30.10

IPv6 Configuration



DHCP

Interface: FastEthernet0 — Service ● On ○ Off

Pool Name: serverPool

Default Gateway: 192.168.20.1

DNS Server: 192.168.30.10

Start IP Address : 192 168 20 0

Subnet Mask: 255 255 255 0

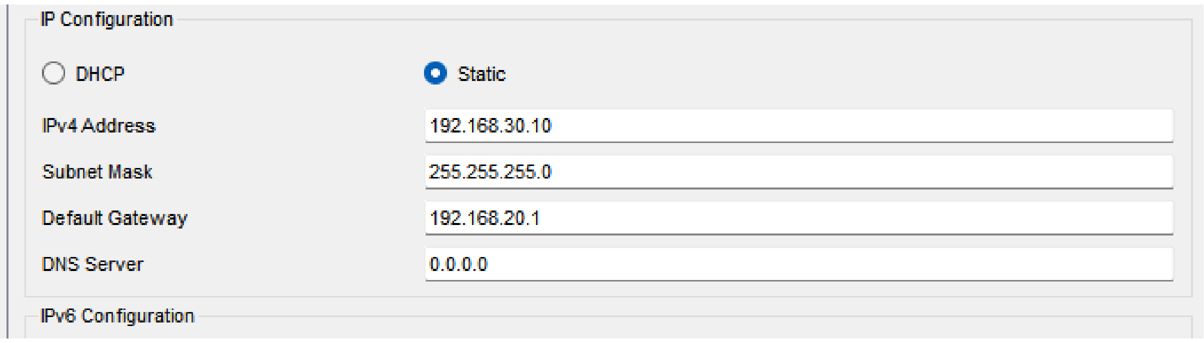
Maximum Number of Users : 253

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168....	192.168....	192.168....	255.255....	253	0.0.0.0	0.0.0.0

Now looking at the DNS server in the same format.



IP Configuration

○ DHCP ● Static

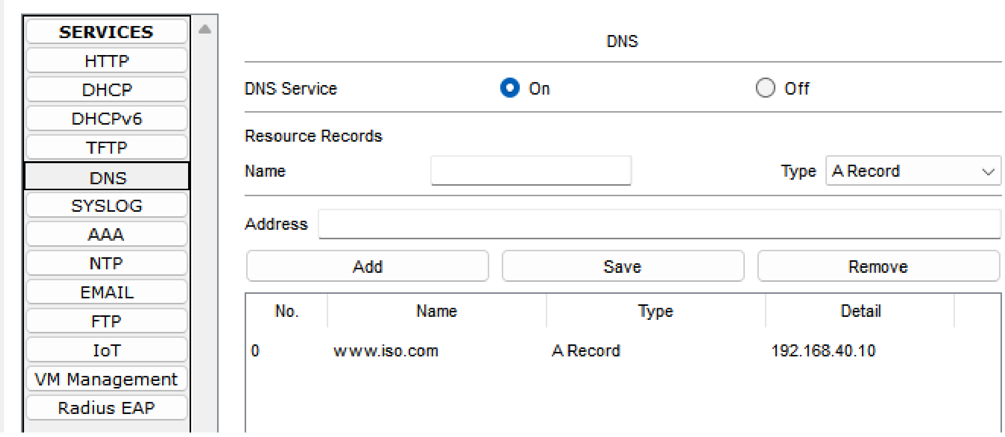
IPv4 Address: 192.168.30.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.20.1

DNS Server: 0.0.0.0

IPv6 Configuration



DNS

DNS Service ● On ○ Off

Resource Records

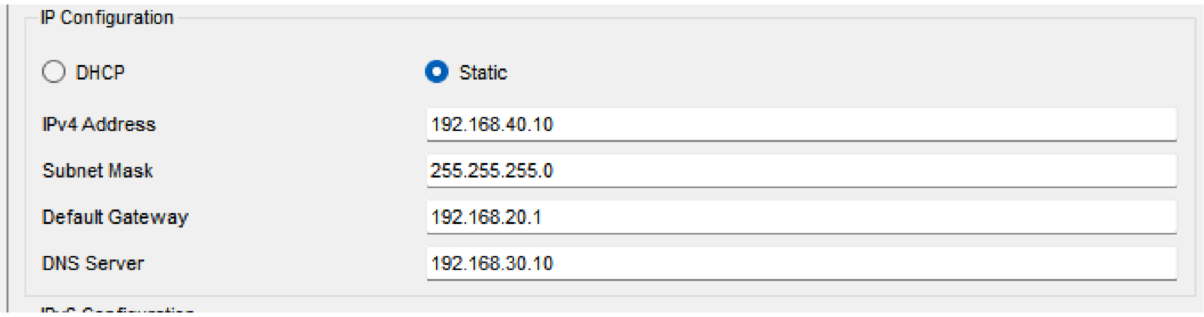
Name: — Type: A Record

Address:

No.	Name	Type	Detail
0	www.iso.com	A Record	192.168.40.10

Now looking at HTTP the first will be the static connection and the second will be the code for the website and the last will be the working website on a virtual machine.

Static screenshots



IP Configuration

○ DHCP ● Static

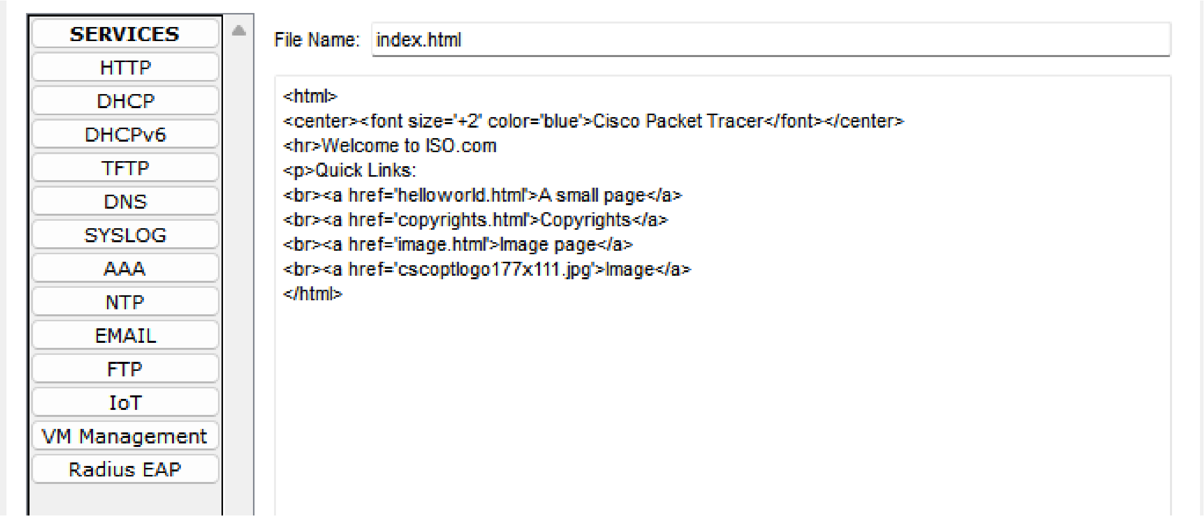
IPv4 Address: 192.168.40.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.20.1

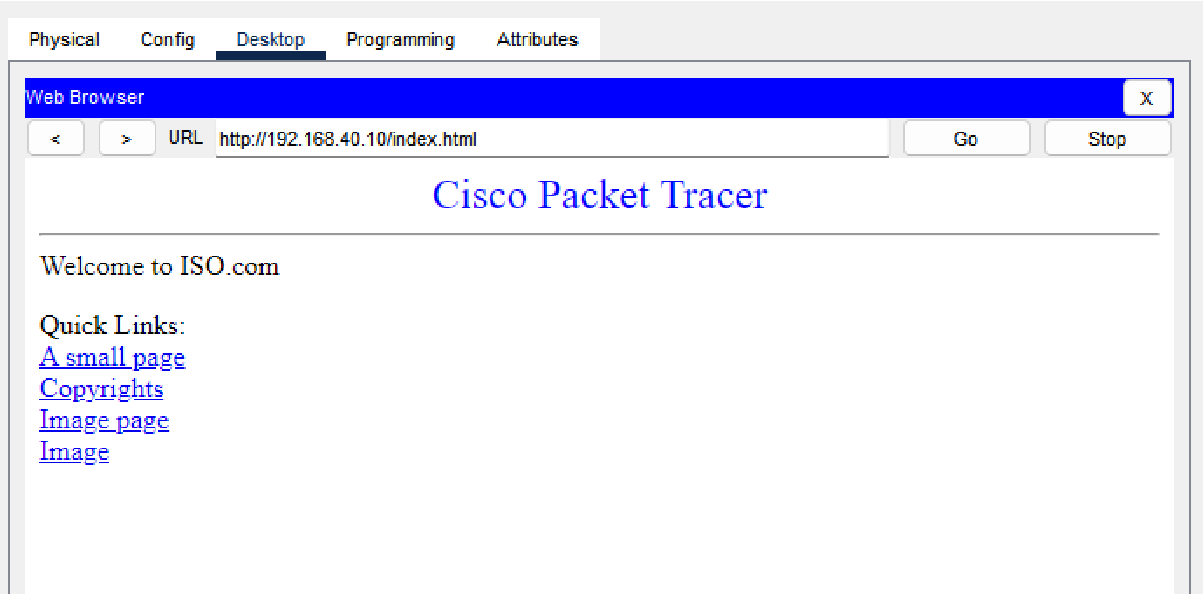
DNS Server: 192.168.30.10

This is the front-end code for the website.



File Name: index.html

```
<html>
<center><font size='+2' color='blue'>Cisco Packet Tracer</font></center>
<hr>Welcome to ISO.com
<p>Quick Links:
<br><a href='helloworld.html'>A small page</a>
<br><a href='copyrights.html'>Copyrights</a>
<br><a href='image.html'>Image page</a>
<br><a href='cscoptlogo177x111.jpg'>Image</a>
</html>
```



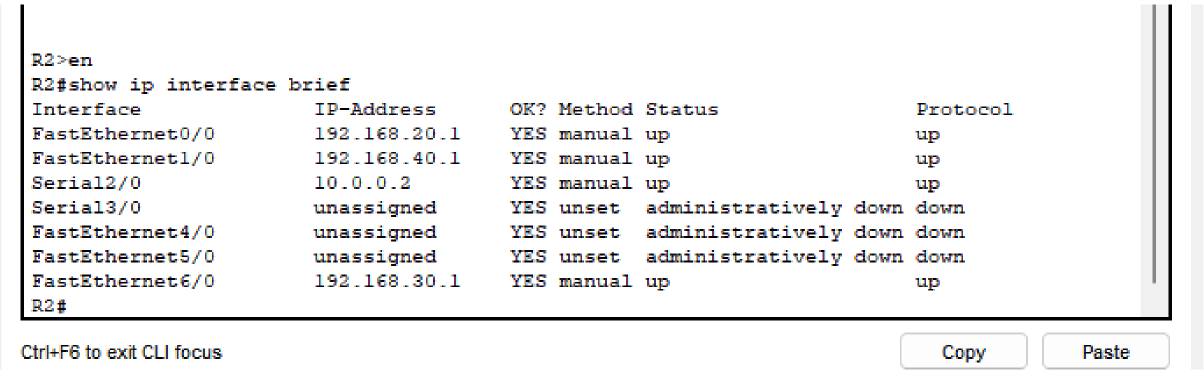
URL: http://192.168.40.10/index.html

Cisco Packet Tracer

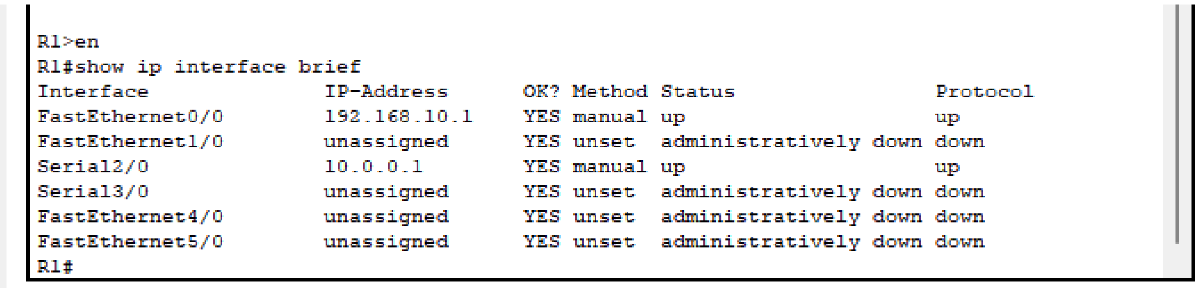
Welcome to ISO.com

Quick Links:
A small page
Copyrights
Image page
Image

Moving on to the routers now both routers will show the port connections.



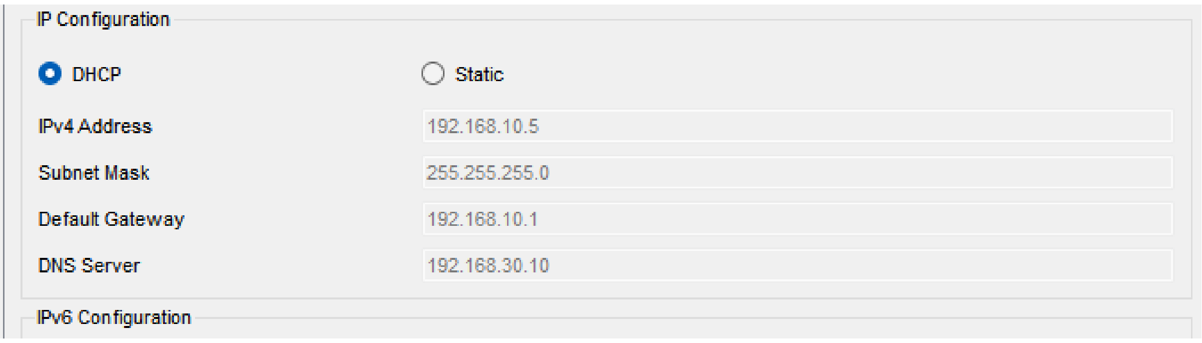
```
R2>en
R2#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.20.1    YES manual up                    up
FastEthernet1/0        192.168.40.1    YES manual up                    up
Serial2/0              10.0.0.2        YES manual up                    up
Serial3/0              unassigned      YES unset  administratively down down
FastEthernet4/0        unassigned      YES unset  administratively down down
FastEthernet5/0        unassigned      YES unset  administratively down down
FastEthernet6/0        192.168.30.1    YES manual up                    up
R2#
```



```
R1>en
R1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.10.1    YES manual up                    up
FastEthernet1/0        unassigned      YES unset  administratively down down
Serial2/0              10.0.0.1        YES manual up                    up
Serial3/0              unassigned      YES unset  administratively down down
FastEthernet4/0        unassigned      YES unset  administratively down down
FastEthernet5/0        unassigned      YES unset  administratively down down
R1#
```

The next screenshot will be the DHCP connection from both ends of the network.

Pc connection to DHCP from the left side of the network



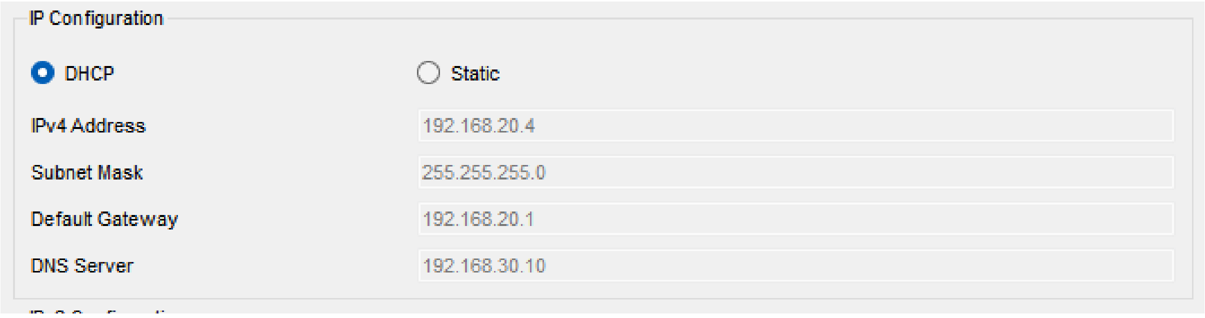
IP Configuration

● DHCP ○ Static

IPv4 Address	192.168.10.5
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
DNS Server	192.168.30.10

IPv6 Configuration

Pc connection to the second DHCP to the right side of the network



IP Configuration

● DHCP ○ Static

IPv4 Address	192.168.20.4
Subnet Mask	255.255.255.0
Default Gateway	192.168.20.1
DNS Server	192.168.30.10