Project Report on

Judiciary System for Bangladesh

Course Code: CSE 310

Course Title: Data Communication and Networking Lab

Section: 01

Submission Date: January 15, 2022

Submitted by

Md. Mutasim Billah Abu Noman Akanda

(192 014 038)

Email: mutasim.billah.cse@ulab.edu.bd

Submitted to

Mahim Mahbub

Lecturer,

Department of CSE,

University of Liberal Arts Bangladesh

Email: mahim.mahbub@ulab.edu.bd

Table of Contents

Overview

The project entitled **"Judiciary System for Bangladesh"** is a networking-based project where our objective is to develop a server-based network system for the Judiciary of Bangladesh where case-related important documents of different courts can be stored in distributed servers. We know that there is a judicial hierarchy in Bangladesh and initially we have assumed that there are total 7 different courts in the existing hierarchy and they are:

1. Metropolitan Session Courts
2. Metropolitan Magistrates Courts
3. Civil Courts
4. Criminal Courts
5. High Court Division
6. Appellate Division and
7. Court of Chief Justice.

However, the network is designed using a simulator named **"Cisco Packet Tracer".**

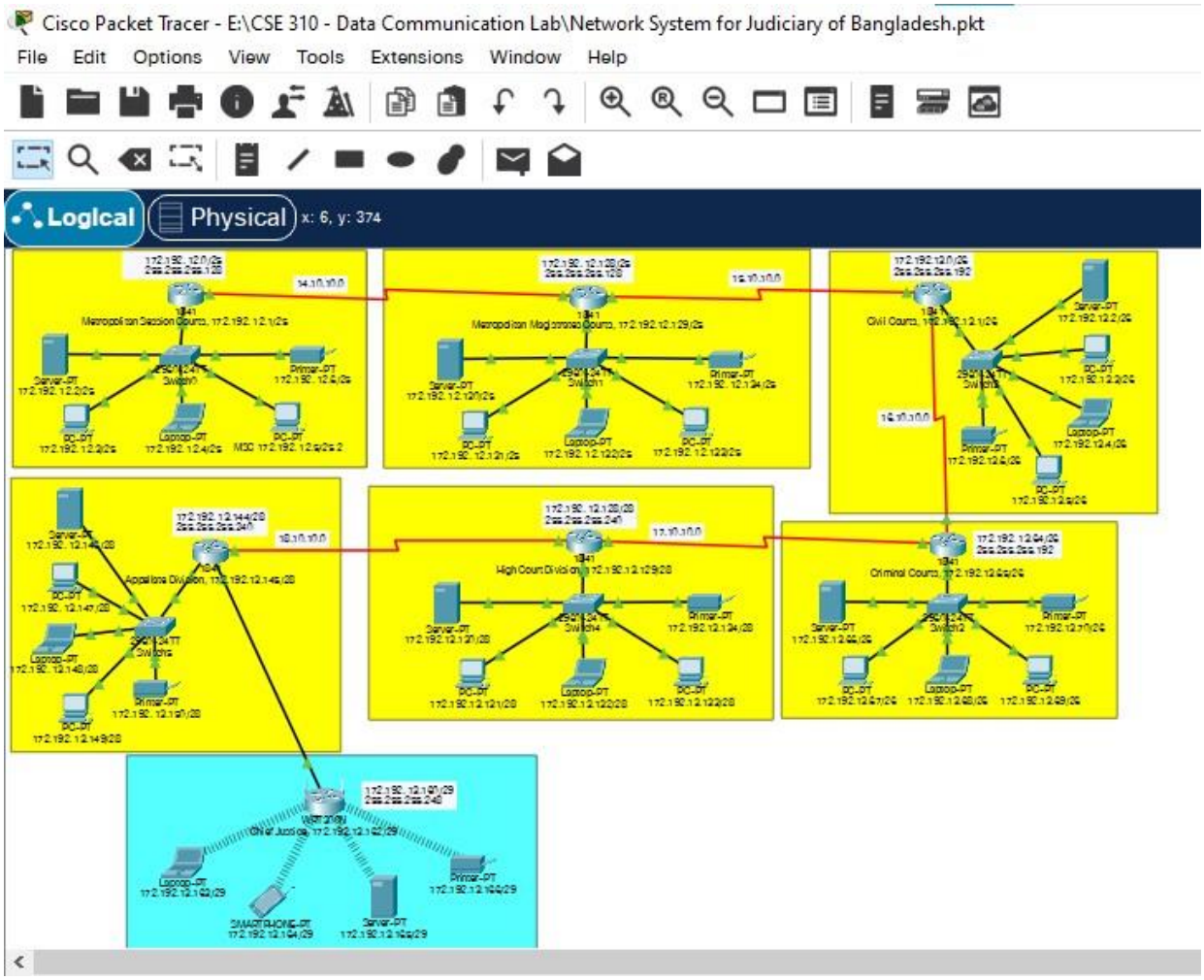


Figure 1: Judiciary System for Bangladesh

Cisco Packet Tracer

Cisco Packet Tracer is a tool built by Cisco. This tool provides a network simulation to practice simple and complex networks. The main purpose of Cisco Packet Tracer is to help students learn the principles of networking with hands-on experience as well as develop Cisco technology-specific skills. Since the protocols are implemented in a software-only method, this tool cannot replace the hardware Routers or Switches. Interestingly, this tool does not only include Cisco products but also many more networking devices. Using this tool is widely encouraged as it is part of the curriculum like CCNA, CCENT where Faculties use Packet Trace to demonstrate technical concepts and networking systems. Students complete assignments using this tool, working on their own or in teams. Engineers prefer to test any protocols on Cisco Packet Tracer before implementing them. Also, Engineers who would like to deploy any change in the production network prefer to use Cisco Packet Tracer to first test the required changes and proceed to deploy if and only if everything is working as expected. This makes the job easier for Engineers allowing them to add or remove simulated network devices, with a Command-line interface and a drag and drop user interface.

Motivation

Our team, ULAB Binary Soldiers, have visited The Supreme Court of Bangladesh and found out that there is no network system in the Judiciary system of Bangladesh and even still they store all the case related documents (hard copy) in the storerooms situated on the 4th floor of the high court in an unorganized way. As a result, if any lawyer needs any kind of document related to his client's case, he/she needs to go to the storerooms physically and searches for the documents which need a good amount of time to get his/her desired documents. And if any document of the case is in any court of another district, then there is no end to the suffering. It was also found that the case was lost or the court was adjourned due to failure to get the documents in time. So our motivation behind this project is to solve the problems given below:

1. Analog storeroom for storing case related documents
2. Overloaded storerooms for unorganized storing system
3. Requires much time to fetch case related documents from one district court to another
4. Postponed case hearing because of the unavailability of required documents

Network Model

Initially, we have taken into consideration that there are total 7 different courts in the existing hierarchy of the Judiciary system of Bangladesh and the number of hosts that will be used in different courts is given below:

1. **Metropolitan Session Courts:** 120 hosts
2. **Metropolitan Magistrates Courts:** 63 hosts

3. **Civil Courts:** 47 hosts
4. **Criminal Courts:** 31 hosts
5. **High Court Division:** 10 hosts
6. **Appellate Division:** 7 hosts and
7. **Court of Chief Justice:** 4 hosts.

We will consider each court as a single network. However, as we are designing the network system using a simulator named **"Cisco Packet Tracer",** we will practically show only 5 hosts (1 server, 1 printer, 2 desktops, and 1 laptop) in the networks which have more than 5 hosts.

Variable Length Subnet Mask

Variable Length Subnet Mask (VLSM) is a subnet, a segmented piece of a larger network, a design strategy where all subnet masks can have varying sizes. This process of "sub netting subnets" enables network engineers to use multiple masks for different subnets of a single class A, B or C network. With VLSM, an IP address space can be divided into a well-defined hierarchy of subnets with different sizes. This helps enhance the usability of subnets because subnets can include masks of varying sizes. A subnet mask helps define the size of the subnet and create subnets with very different host counts without wasting large numbers of addresses. However, in this project, we will develop our network using Variable Length Subnet Mask.

VLSM calculation of Judiciary System for Bangladesh

We will be using the network address 172.192.12.0/22 and show the following items for each court:

1. Network Address
2. Subnet Mask (in AAA.BBB.CCC.DDD format)
3. Broadcast Address
4. Number of Usable Hosts
5. Usable Hosts IP Address Range

For VLSM, first of all, we will create a table in descending order based on **"Number of Hosts"** in which we will put all the answers after doing all the necessary calculations:

Courts	Number of Hosts	Network Address	Subnet Mask	Broadcast Address	Number of Usable Hosts	Usable Hosts IP Address Range
Metropolitan Session Courts	120	172.192.12.0/25	255.255.255.128	172.192.12.127/25	126	172.192.12.1/25 to 172.192.12.126/25

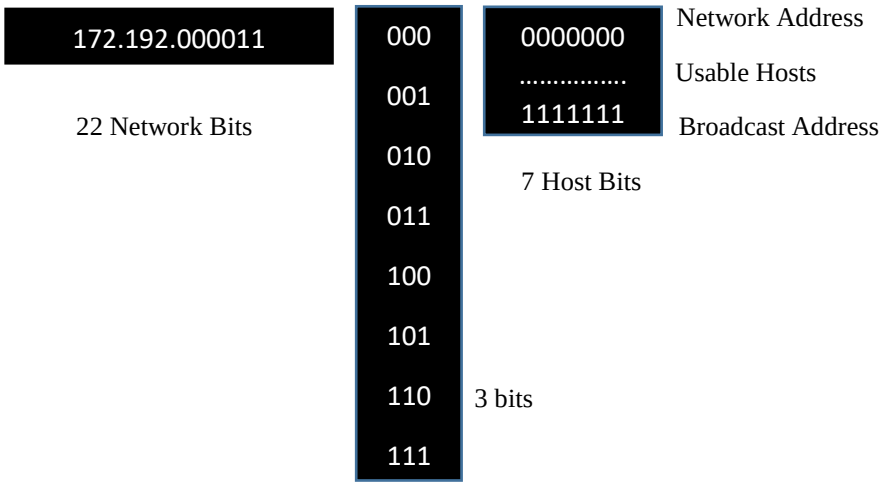
Metropolitan Magistrates Courts	63	172.192. 12.128/25	255.255. 255.128	172.192.12. 255/25	126	172.192.12.129/25 to 172.192.12.254/25
Civil Courts	47	172.192. 13.0/26	255.255. 255.192	172.192.13. 63/26	62	172.192.13.1/26 to 172.192.13.62/26
Criminal Courts	31	172.192. 13.64/26	255.255. 255.192	172.192.13. 127/26	62	172.192.13.65/26 to 172.192.13.126/26
High Court Division	10	172.192. 13.128/28	255.255. 255.240	172.192.13. 143/28	14	172.192.13.129/28 to 172.192.13.142/28
Appellate Division	7	172.192. 13.144/28	255.255. 255.240	172.192.13. 159/28	14	172.192.13.145/28 to 172.192.13.158/28
Chief Justice	4	172.192. 13.160/29	255.255. 255.248	172.192.13. 167/29	6	172.192.13.161/29 to 172.192.13.166/29

Table 1: Variable Length Subnet Mask Outputs

We will start sub netting from that court which is consist of the maximum number of hosts and then we will continue sub netting accordingly in descending order.

VLSM for Metropolitan Session Courts

Number of Hosts in Metropolitan Session Courts is 120. So, we need minimum of 7 bits to represent 120 hosts because $2^7 = 128 - 2$ (excluding Network and Broadcast ID) = 126 will be usable hosts which is the closest value of 120. Since the given network address is 172.192.12.0/22, if we expand the network address then we will get:



Remember, the mid 3 bits here is 000

So, subnet = /25

Network Address = 172.192.00001100.00000000/25 = 172.192.12.0/25

Broadcast Address = 172.192.00001100.01111111/25 = 172.192.12.127/25

Subnet mask = 11111111.11111111.11111111.10000000 = 255.255.255.128

Usable hosts IP address range = 172.192.12.1/25 to 172.192.12.126/25

Number of usable hosts = 126 – 1 + 1 = 126

VLSM for Metropolitan Magistrates Courts

Number of hosts in Metropolitan Magistrates Courts is 63. If we take 6 bits to represent 63 hosts, then the usable hosts will be 2^6 = 64 – 2 (excluding Network and Broadcast ID) = 62 which is less than required hosts 63. So, we have to take 7 bits where usable hosts will be 2^7 = 128 – 2 (excluding Network and Broadcast ID) = 126. If we expand the network address then we will get:

172.192.00001100.10000000, where network bits are red colored and hosts bits are green colored.

Remember, the mid 3 bits here is 001

So, subnet = /25

Network Address = 172.192.00001100.10000000/25 = 172.192.12.128/25

Broadcast Address = 172.192.00001100.11111111/25 = 172.192.12.255/25

Subnet mask = 11111111.11111111.11111111.10000000 = 255.255.255.128

Usable hosts IP address range = 172.192.12.129/25 to 172.192.12.254/25

Number of usable hosts = 254 – 129 + 1 = 126

VLSM for Civil Courts

Number of hosts in Civil Courts is 47 so we have to take 6 bits to represent 47 hosts because 2^6 = 64 – 2 (excluding Network and Broadcast ID) = 62 which is closest to the 47. If we expand the network address then we will get:

172.192.00001101.00000000, where network bits are red colored and hosts bits are green colored. Here, the mid 3 bits are 010 which I have divided into 2 parts, one is 0100 and the other is 0101. This is basically the variable length sub netting concept because I will only use 47 hosts among 128 / 2 = 64 – 2 = 62 hosts. So, I need not to waste the remaining 64 – 2 = 62 hosts unnecessarily.

Remember, the mid 4 bits here is 0100

So, subnet = /26

Network Address = 172.192.00001101.00000000/26 = 172.192.13.0/26

Broadcast Address = 172.192.00001101.00111111/26 = 172.192.13.63/26

Subnet mask = 11111111.11111111.11111111.11000000 = 255.255.255.192

Usable hosts IP address range = 172.192.13.1/26 to 172.192.13.62/26

Number of usable hosts = 62 – 1 + 1 = 62

VLSM for Criminal Courts

Number of hosts in Criminal Courts is 31 so we have to take 6 bits to represent 31 hosts because 2^6 = 64 – 2 (excluding Network and Broadcast ID) = 62 which is closest to the 31. If we expand the network address then we will get:

172.192.00001101.01000000, where network bits are red colored and hosts bits are green colored. Here, we have used the other part of the previously divided network which is 0101.

Remember, the mid 4 bits here is 0101

So, subnet = /26

Network Address = 172.192.00001101.01000000/26 = 172.192.13.64/26

Broadcast Address = 172.192.00001101.01111111/26 = 172.192.13.127/26

Subnet mask = 11111111.11111111.11111111.11000000 = 255.255.255.192

Usable hosts IP address range = 172.192.13.65/26 to 172.192.13.126/26

Number of usable hosts = 126 – 65 + 1 = 62

VLSM for High Court Division

Number of hosts in High Court Division is 10 so we have to take 4 bits to represent 10 hosts because 2^4 = 16 – 2 (excluding Network and Broadcast ID) = 14 which is closest to the 10. If we expand the network address then we will get:

172.192.00001101.10000000, where network bits are red colored and hosts bits are green colored. Here, the mid 3 bits are 011 which we have divided into 2 parts 3 times. Firstly, we have divided 128 / 2 = 64 (in bits 0110 and 0111), then again 64 / 2 = 32 (in bits 01100 and 01101) and finally 32 / 2 = 16 (in bits 011000 and 011001). So systematically the mid bits here are 011000.

Remember, the mid 6 bits here is 011000

So, subnet = /28

Network Address = 172.192.00001101.10000000/28 = 172.192.13.128/28

Broadcast Address = 172.192.00001101.10001111/28 = 172.192.13.143/28

Subnet mask = 11111111.11111111.11111111.11110000 = 255.255.255.240

Usable hosts IP address range = 172.192.13.129/28 to 172.192.13.142/28

Number of usable hosts = 142 – 129 + 1 = 14

VLSM for Appellate Division

Number of hosts in Appellate Division is 7 so we have to take 4 bits to represent 7 hosts because 2^4 = 16 – 2 (excluding Network and Broadcast ID) = 14 which is closest to the 7. If we expand the network address then we will get:

172.192.00001101.10010000, where network bits are red colored and hosts bits are green colored. Here, we have used the other part of the previously divided network which is 011001.

Remember, the mid 6 bits here is 011001

So, subnet = /28

Network Address = 172.192.00001101.10010000/28 = 172.192.13.144/28

Broadcast Address = 172.192.00001101.10011111/28 = 172.192.13.159/28

Subnet mask = 11111111.11111111.11111111.11110000 = 255.255.255.240

Usable hosts IP address range = 172.192.13.145/28 to 172.192.13.158/28

Number of usable hosts = 158 – 145 + 1 = 14

VLSM for Chief Justice

Number of hosts in Chief Justice is 4 so I have to take 3 bits to represent 4 hosts because 2^3 = 8 – 2 (excluding Network and Broadcast ID) = 6 which is closest to the 4. If we expand the network address then we will get:

172.192.00001101.10100000, where network bits are red colored and hosts bits are green colored. Here, the mid 5 bits are 01101 which is already a divided part previously. Again, we have divided this network into 2 parts 2 times. Firstly, we have divided 32 / 2 = 16 (in bits 011010 and 011011), then again 16 / 2 = 8 (in bits 0110100 and 0110101. So systematically the mid bits here are 0110100.

Remember, the mid 7 bits here is 0110100

So, subnet = /29

Network Address = 172.192.00001101.10100000/29 = 172.192.13.160/29

Broadcast Address = 172.192.00001101.10100111/29 = 172.192.13.167/29

Subnet mask = 11111111.11111111.11111111.11111000 = 255.255.255.248

Usable hosts IP address range = 172.192.13.161/29 to 172.192.13.166/29

Number of usable hosts = 166 – 161 + 1 = 6

The tree diagram of variable length subnet mask for this project is given below:

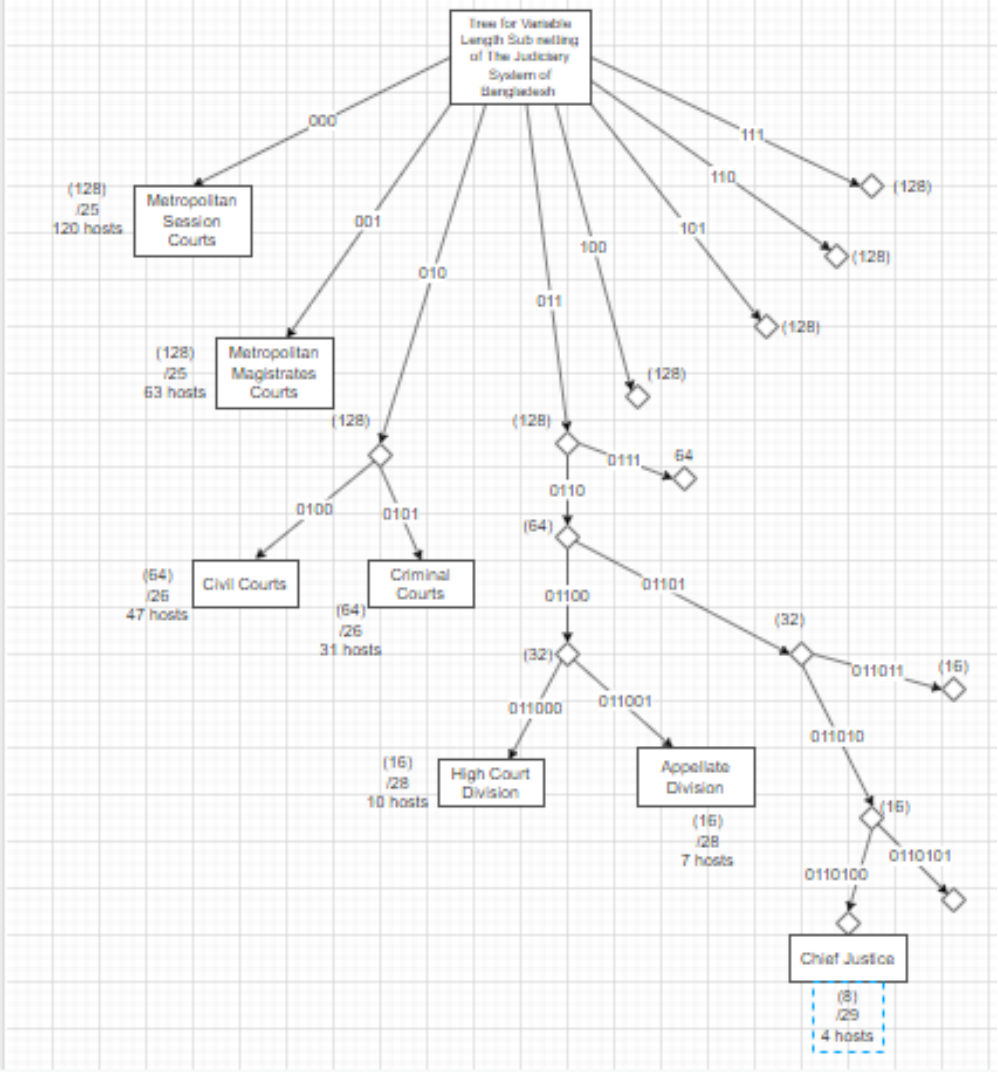


Figure 2: Tree Diagram for VLSM

Networks Development

We have used Static method both for end device to router configuration and router to router configuration. We have designed our Chief Justice network as wireless and rest of the networks as wired. Let us discuss the development procedure of our individual 7 networks first and then we will discuss about court to court router configuration.

Metropolitan Session Courts

Steps:

1. We have taken a router of 1841 model, switched off the router, added a serial port WIC-2T and turned on the router.

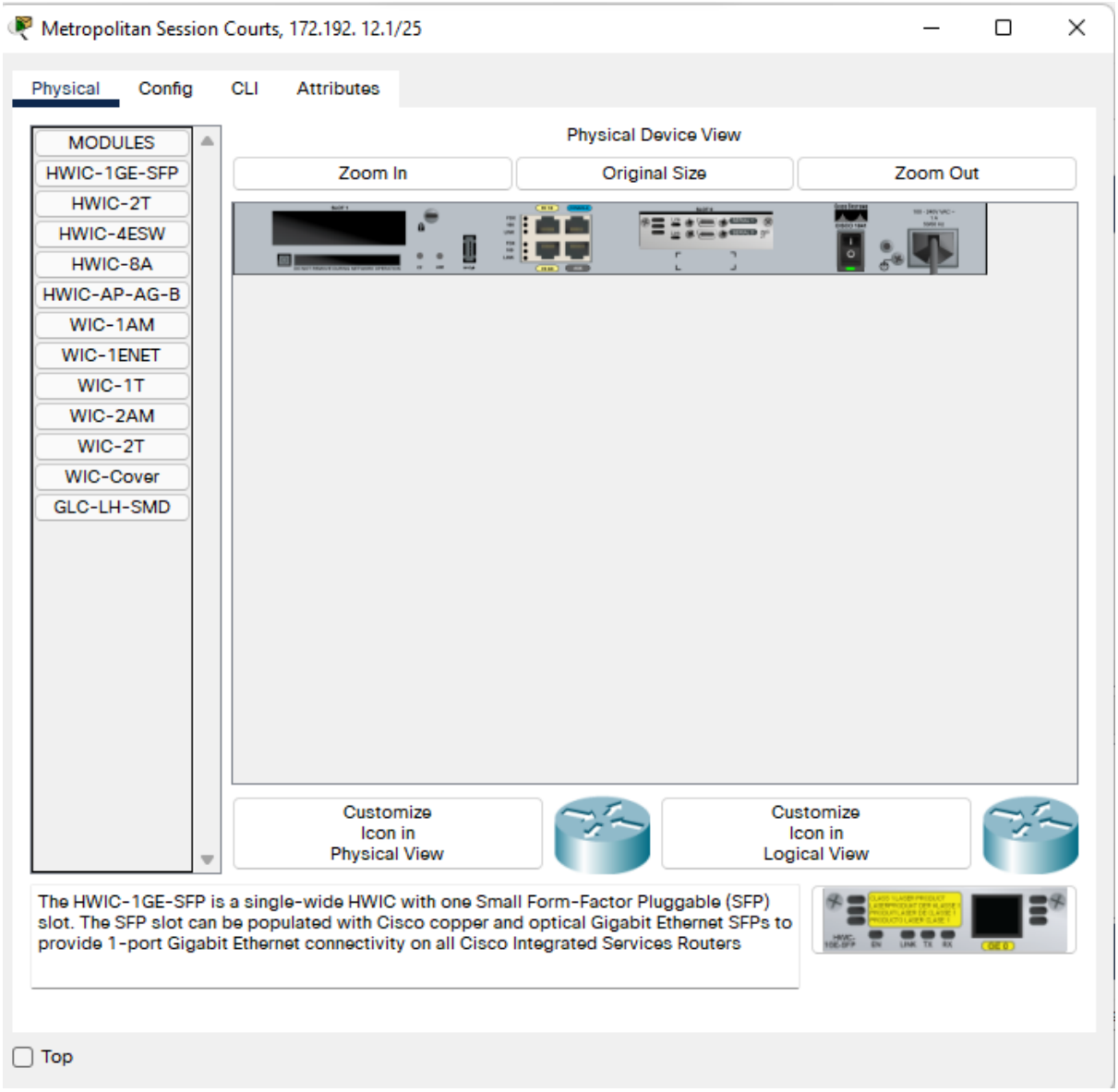


Figure 3: Adding serial port WIC-2T to Metropolitan Session Courts router

2. As the network address for Metropolitan Session Courts is 172.192.12.0/25, so we have assigned 172.192.12.1 as IPV4 address and 255.255.255.128 as subnet mask in FastEthernet0/0 interface of this router, hop address 14.10.10.1 in Serial0/0/0 and turned on the port status.

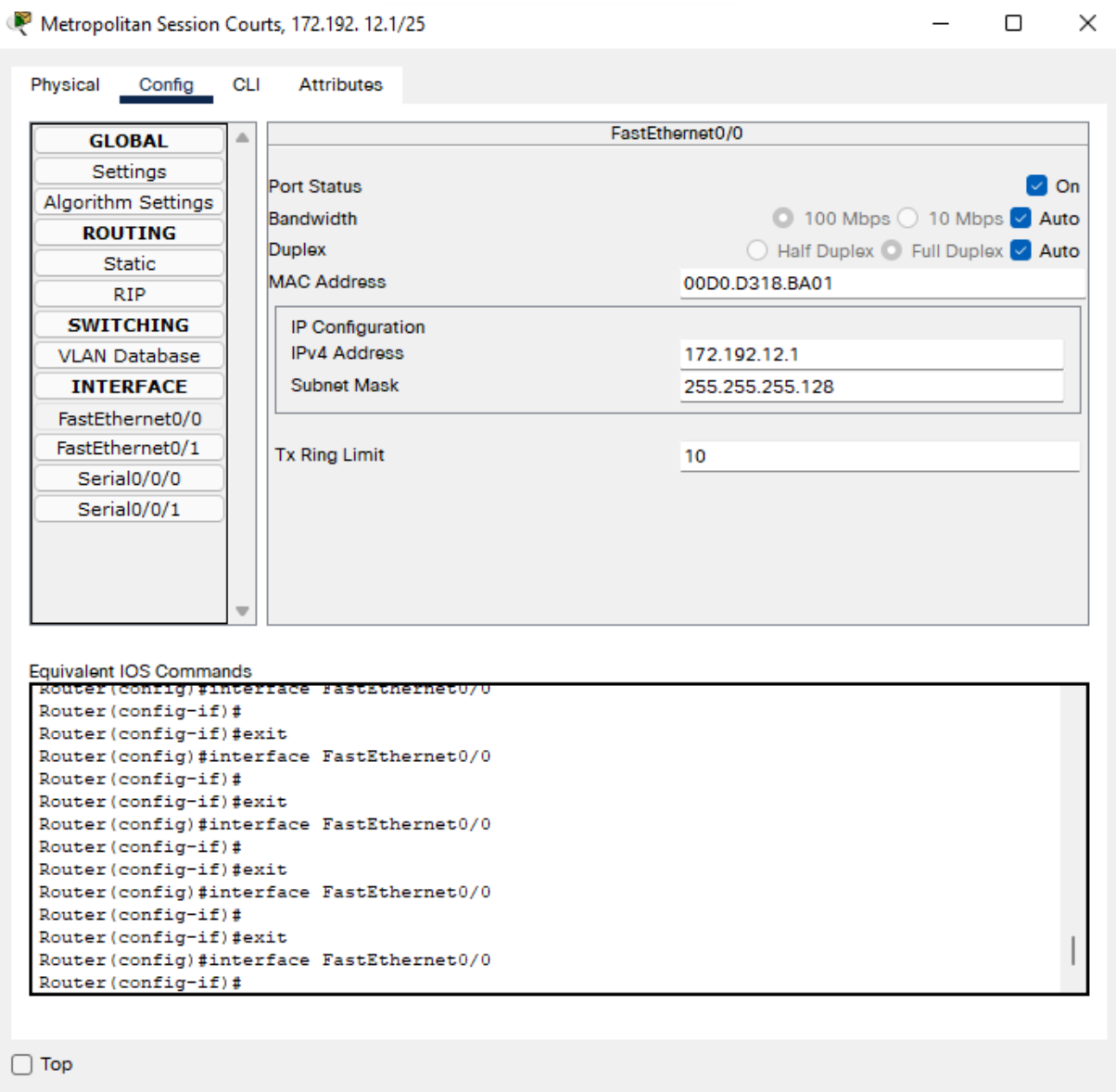


Figure 4: Assigning IPV4 address and Subnet Mask to Metropolitan Session Courts router

3. Then, we have taken a server for this network, assigned 172.192.12.2 as IPV4 address and 255.255.255.128 as subnet mask in FastEthernet0 interface of this server, default gateway 172.192.12.1 and turned on the port status.
4. In the same way, we have taken two PC, 1 laptop and 1 printer for this network, assigned 172.192.12.3, 172.192.12.5, 172.192.12.4 and 172.192.12.6 respectively as IPV4 address and 255.255.255.128 as subnet mask in FastEthernet0 interface of these hosts, default gateway 172.192.12.1 and turned on the port status.
5. After that, we have taken a switch of 2960 model and connected all the hosts with the switch using copper straight-through and then connected the switch with the router of Metropolitan Session Courts.

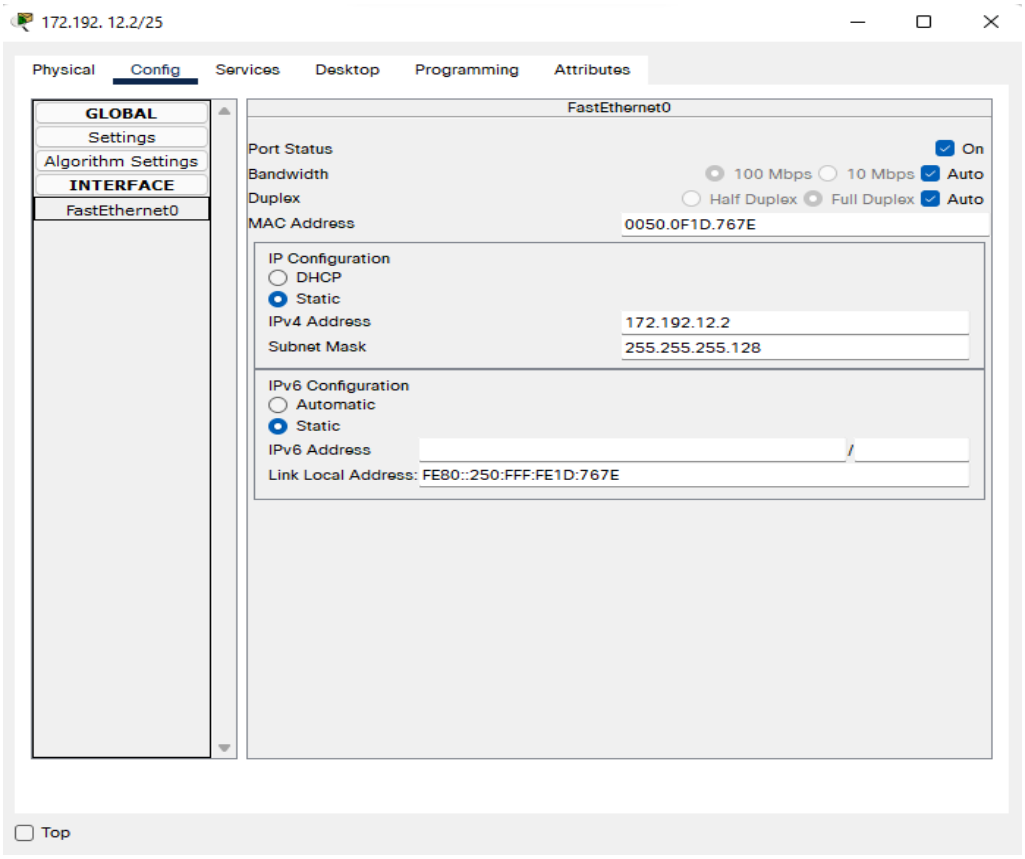


Figure 5: Assigning IPV4 address and Subnet Mask to Metropolitan Session Courts server

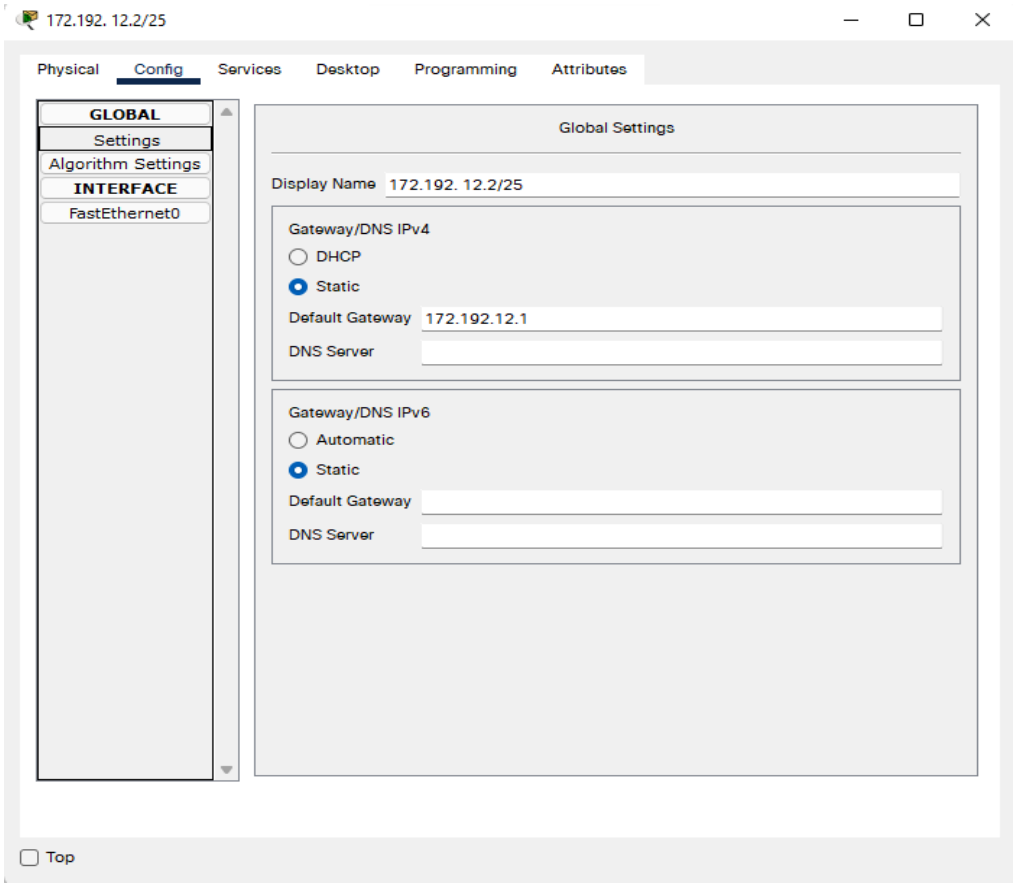


Figure 6: Assigning default gateway to Metropolitan Session Courts server

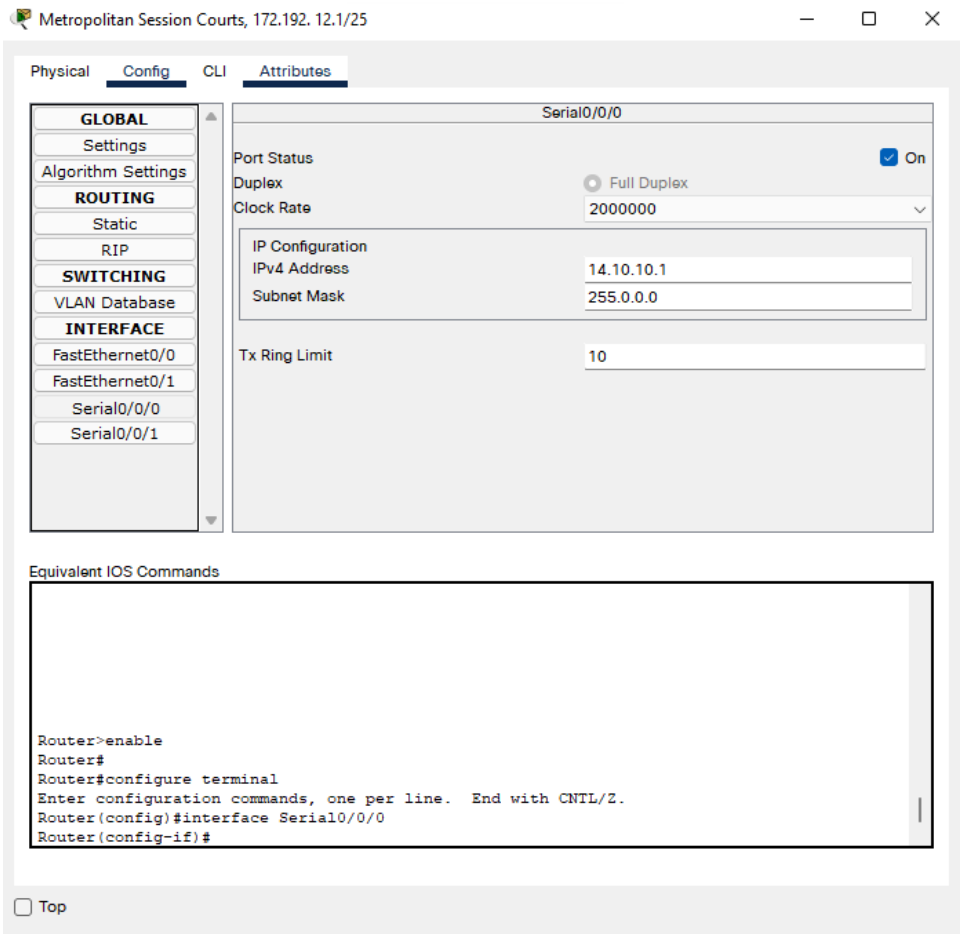


Figure 7: Assigning hop address to Metropolitan Session Courts router

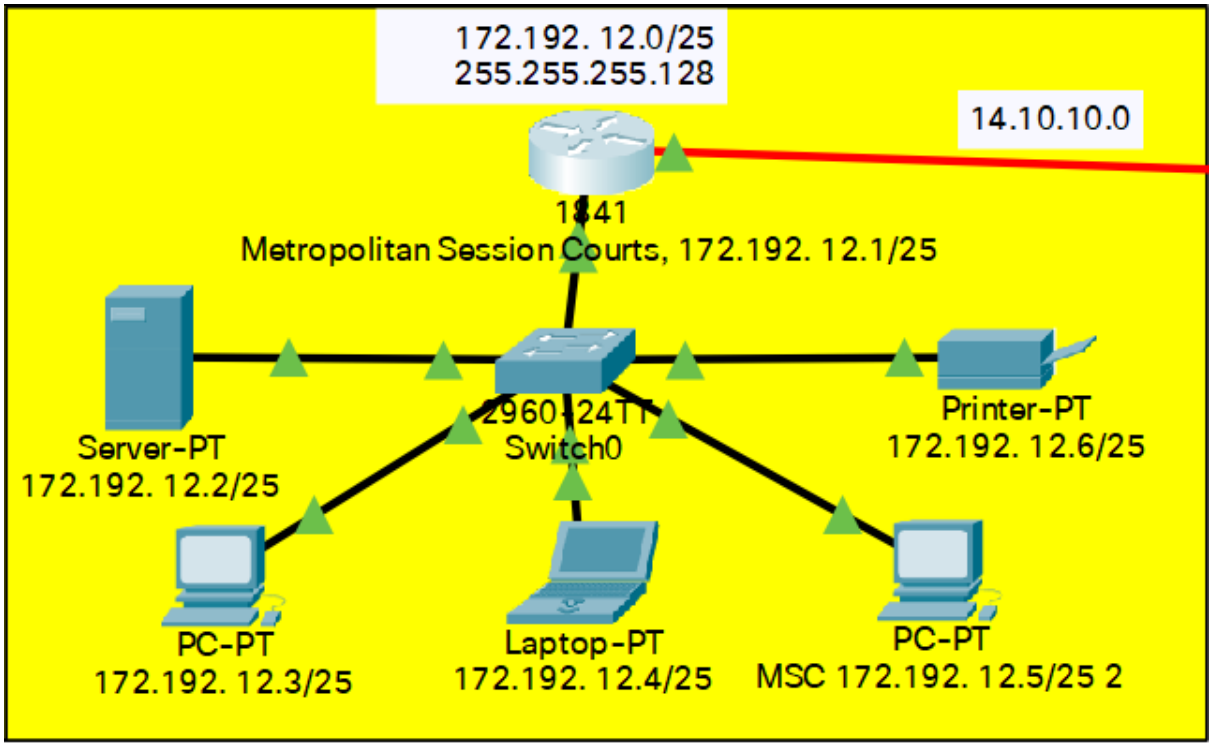


Figure 8: Metropolitan Session Courts Network

Metropolitan Magistrates Courts

Steps:

1. Just like the previous network, we have taken a router of 1841 model, switched off the router, added a serial port WIC-2T and turned on the router.
2. As the network address for Metropolitan Magistrates Courts is 172.192.12.128/25, so we have assigned 172.192.12.129 as IPV4 address and 255.255.255.128 as subnet mask in FastEthernet0/0 interface of this router, hop address 14.10.10.2 and 15.10.10.1 respectively in Serial0/1/0 and Serial0/1/1 and turned on the port status.
3. Then, we have taken a server for this network, assigned 172.192.12.130 as IPV4 address and 255.255.255.128 as subnet mask in FastEthernet0 interface of this server, default gateway 172.192.12.129 and turned on the port status.
4. In the same way, we have taken two PC, 1 laptop and 1 printer for this network, assigned 172.192.12.131, 172.192.12.33, 172.192.12.32 and 172.192.12.34 respectively as IPV4 address and 255.255.255.128 as subnet mask in FastEthernet0 interface of these hosts, default gateway 172.192.12.129 and turned on the port status.
5. After that, we have taken a switch of 2960 model and connected all the hosts with the switch using copper straight-through and then connected the switch with the router of Metropolitan Magistrates Courts.

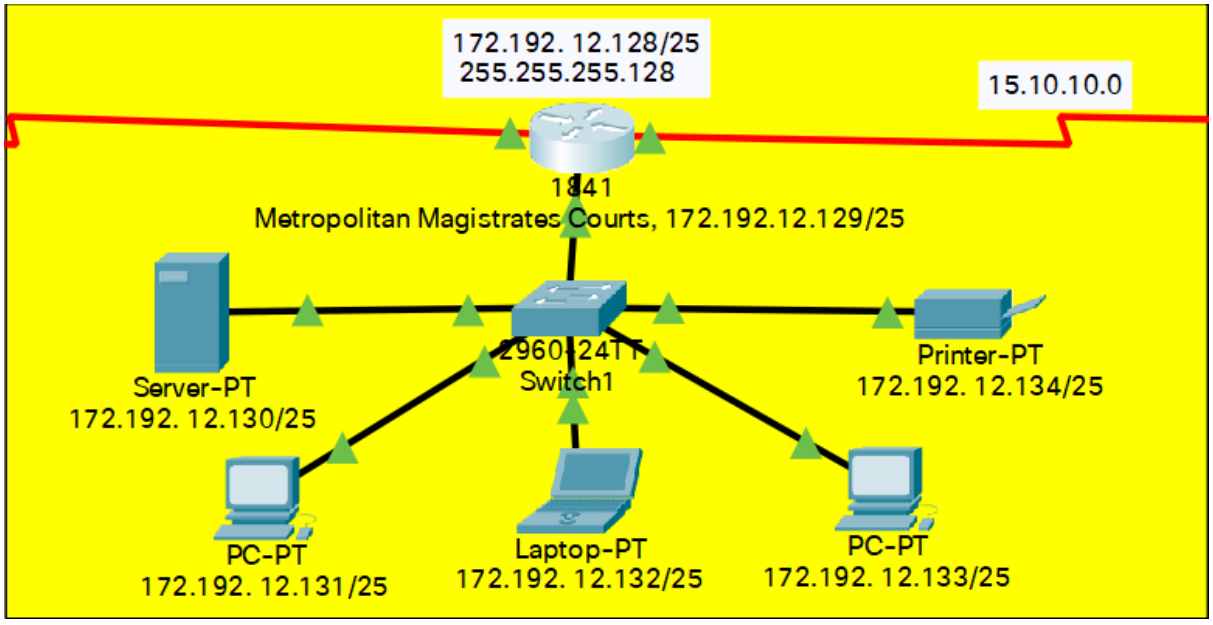


Figure 9: Metropolitan Magistrates Courts Network

Civil Courts

Steps:

1. Just like the previous network, we have taken a router of 1841 model, switched off the router, added a serial port WIC-2T and turned on the router.
2. As the network address for Civil Courts is 172.192.13.0/26, so we have assigned 172.192.13.1 as IPV4 address and 255.255.255.192 as subnet mask in FastEthernet0/0 interface of this router, hop address 15.10.10.2 and 16.10.10.1 respectively in Serial0/1/0 and Serial0/1/1 and turned on the port status.
3. Then, we have taken a server for this network, assigned 172.192.13.2 as IPV4 address and 255.255.255.192 as subnet mask in FastEthernet0 interface of this server, default gateway 172.192.13.1 and turned on the port status.
4. In the same way, we have taken two PC, 1 laptop and 1 printer for this network, assigned 172.192.13.3, 172.192.13.5, 172.192.13.4 and 172.192.13.6 respectively as IPV4 address and 255.255.255.192 as subnet mask in FastEthernet0 interface of these hosts, default gateway 172.192.13.1 and turned on the port status.
5. After that, we have taken a switch of 2960 model and connected all the hosts with the switch using copper straight-through and then connected the switch with the router of Civil Courts.

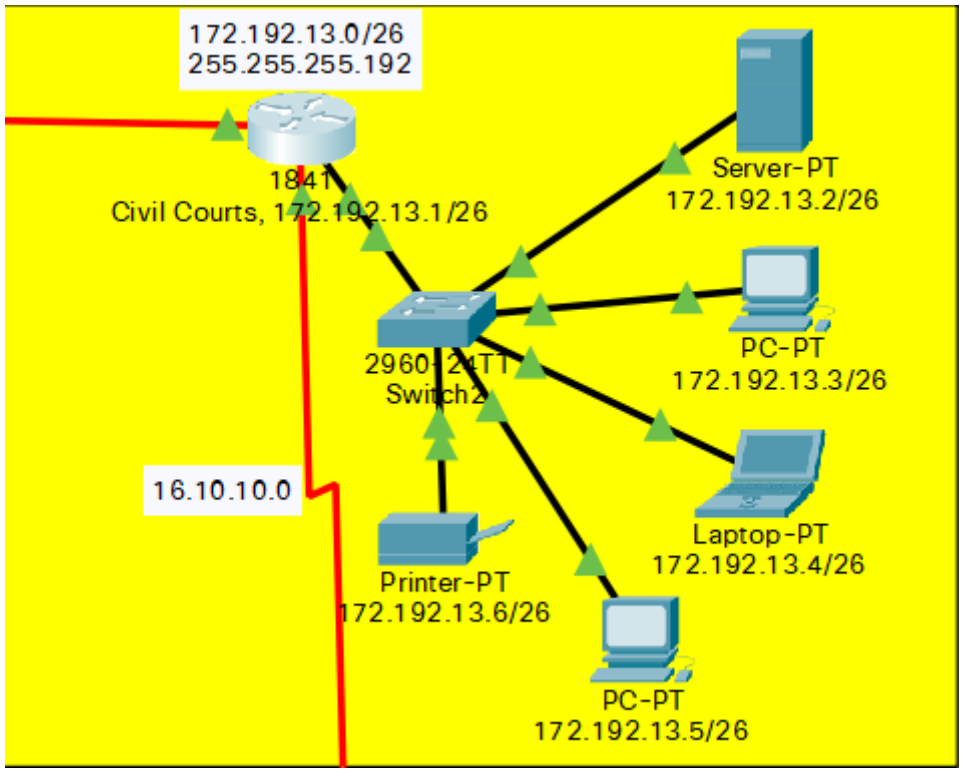


Figure 10: Civil Courts Network

Criminal Courts

Steps:

1. Just like the previous network, we have taken a router of 1841 model, switched off the router, added a serial port WIC-2T and turned on the router.
2. As the network address for Criminal Courts is 172.192.13.64/26, so we have assigned 172.192.13.65 as IPV4 address and 255.255.255.192 as subnet mask in FastEthernet0/0 interface of this router, hop address 16.10.10.2 and 17.10.10.2 respectively in Serial0/1/0 and Serial0/1/1 and turned on the port status.
3. Then, we have taken a server for this network, assigned 172.192.13.66 as IPV4 address and 255.255.255.192 as subnet mask in FastEthernet0 interface of this server, default gateway 172.192.13.65 and turned on the port status.
4. In the same way, we have taken two PC, 1 laptop and 1 printer for this network, assigned 172.192.13.67, 172.192.13.69, 172.192.13.68 and 172.192.13.70 respectively as IPV4 address and 255.255.255.192 as subnet mask in FastEthernet0 interface of these hosts, default gateway 172.192.13.65 and turned on the port status.
5. After that, we have taken a switch of 2960 model and connected all the hosts with the switch using copper straight-through and then connected the switch with the router of Criminal Courts.

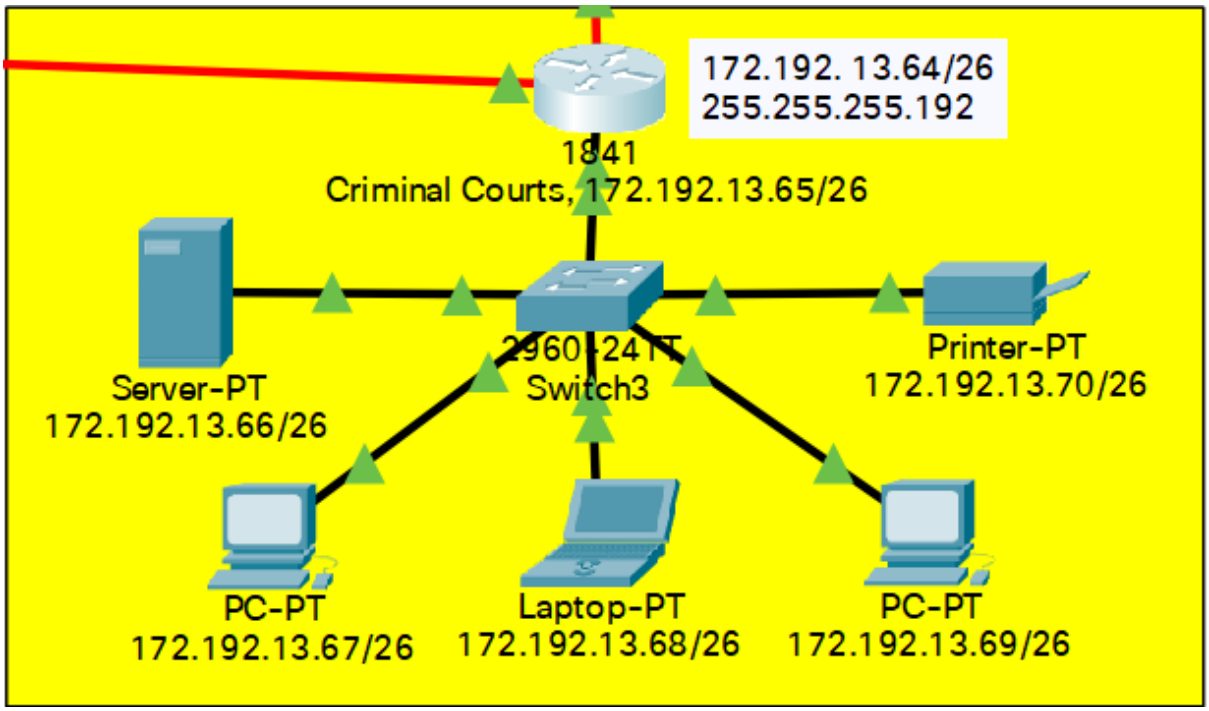


Figure 11: Criminal Courts Network

High Court Division

Steps:

1. Just like the previous network, we have taken a router of 1841 model, switched off the router, added a serial port WIC-2T and turned on the router.
2. As the network address for High Court Division is 172.192.13.128/28, so we have assigned 172.192.13.129 as IPV4 address and 255.255.255.240 as subnet mask in FastEthernet0/0 interface of this router, hop address 17.10.10.1 and 18.10.10.2 respectively in Serial0/1/0 and Serial0/1/1 and turned on the port status.
3. Then, we have taken a server for this network, assigned 172.192.13.130 as IPV4 address and 255.255.255.240 as subnet mask in FastEthernet0 interface of this server, default gateway 172.192.13.129 and turned on the port status.
4. In the same way, we have taken two PC, 1 laptop and 1 printer for this network, assigned 172.192.13.131, 172.192.13.133, 172.192.13.132 and 172.192.13.134 respectively as IPV4 address and 255.255.255.240 as subnet mask in FastEthernet0 interface of these hosts, default gateway 172.192.13.129 and turned on the port status.
5. After that, we have taken a switch of 2960 model and connected all the hosts with the switch using copper straight-through and then connected the switch with the router of High Court Division.

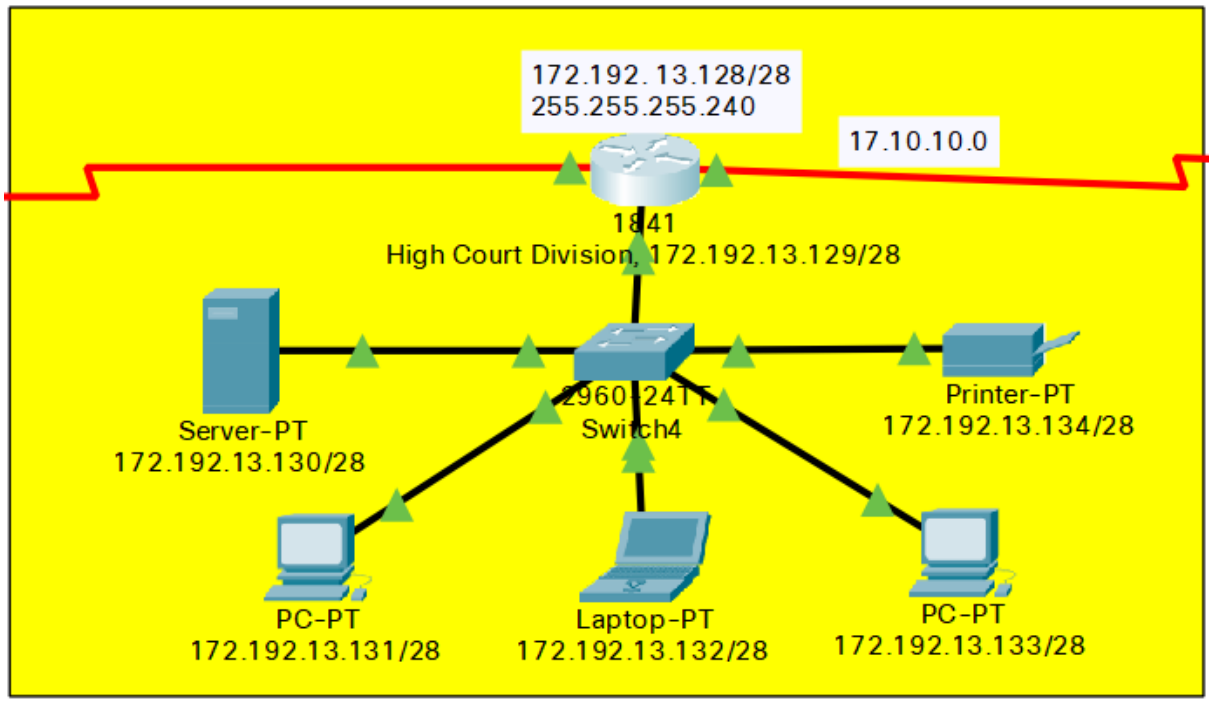


Figure 12: High Court Division Network

Appellate Division

Steps:

1. Just like the previous network, we have taken a router of 1841 model, switched off the router, added a serial port WIC-2T and turned on the router.
2. As the network address for Appellate Division is 172.192.13.144/28, so we have assigned 172.192.13.145 as IPV4 address and 255.255.255.240 as subnet mask in FastEthernet0/0 interface of this router, hop address 18.10.10.1 in Serial0/1/0 and turned on the port status.
3. Then, we have taken a server for this network, assigned 172.192.13.146 as IPV4 address and 255.255.255.240 as subnet mask in FastEthernet0 interface of this server, default gateway 172.192.13.145 and turned on the port status.
4. In the same way, we have taken two PC, 1 laptop and 1 printer for this network, assigned 172.192.13.147, 172.192.13.149, 172.192.13.148 and 172.192.13.150 respectively as IPV4 address and 255.255.255.240 as subnet mask in FastEthernet0 interface of these hosts, default gateway 172.192.13.145 and turned on the port status.
5. After that, we have taken a switch of 2960 model and connected all the hosts with the switch using copper straight-through and then connected the switch with the router of High Court Division.

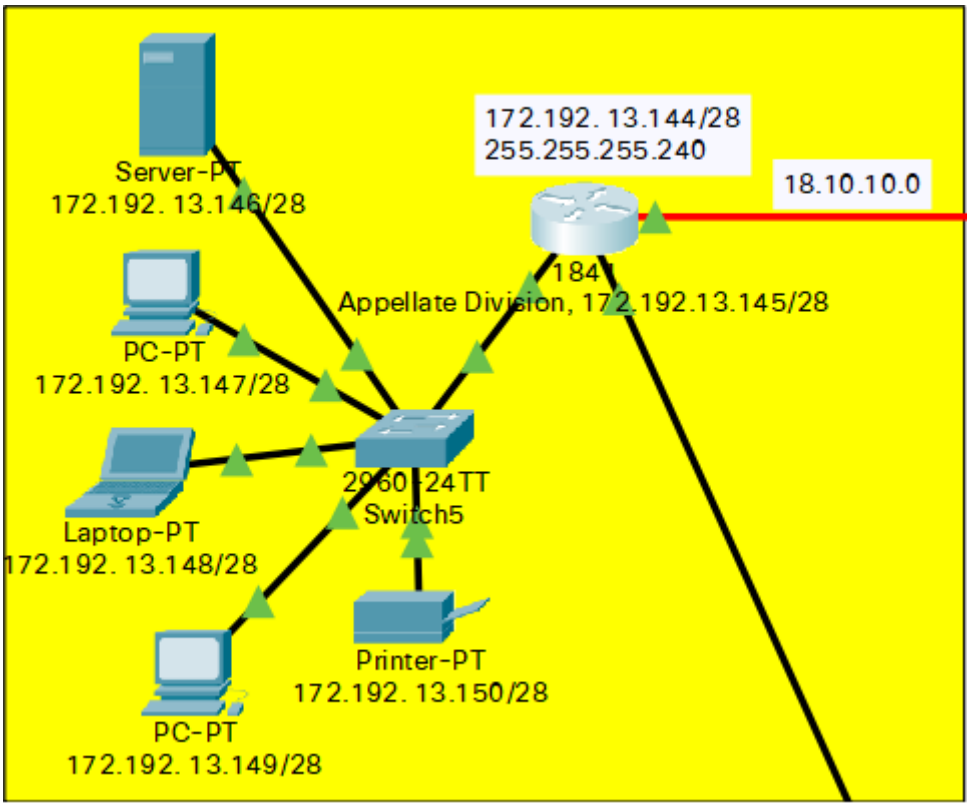


Figure 13: Appellate Division Network

All these 6 networks have been designed as wired, but the last network which is Chief Justice, has been designed as wireless.

Chief Justice

Steps:

1. First of all, we have taken a router of WRT300N model.
2. As the network address for Chief Justice is 172.192.13.160/29, so we have assigned 172.192.13.161 as default gateway in Internet, 172.192.13.162 as IPV4 address and 255.255.255.248 as subnet mask in LAN interface.

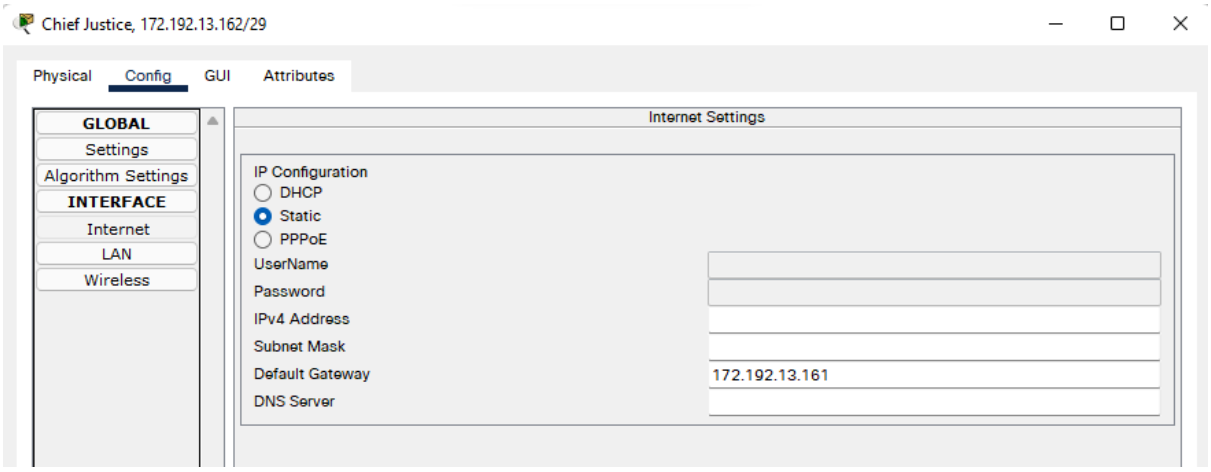


Figure 14: Assigning Default Gateway to Chief Justice wireless router

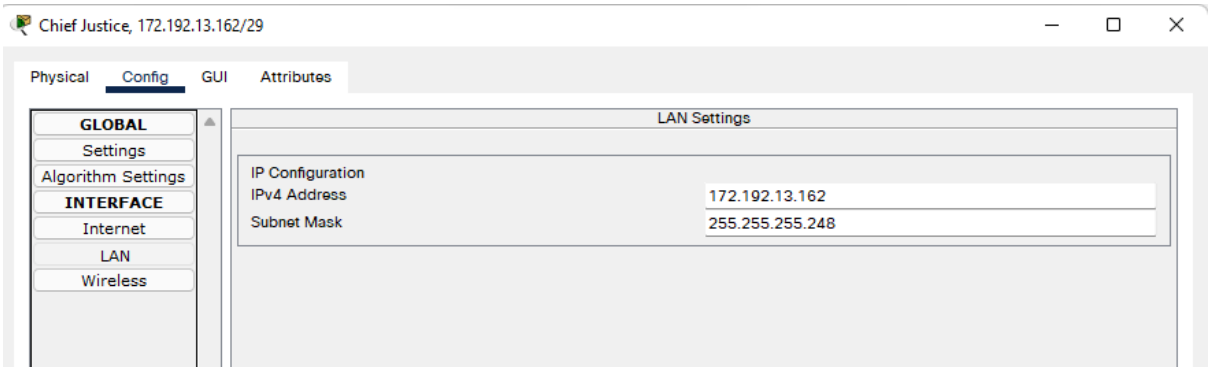


Figure 15: Assigning IPV4 Address and Subnet Mask to Chief Justice wireless router

3. Also, we have assigned a SSID "**Noman"** and WEP authentication password **"0123456789"** in Wireless.
4. Then, we have taken 4 wireless hosts which are 1 PC, 1 smartphone, 1 server and 1 printer. We do not need to configure the smartphone but the PC, server and printer need to be configured before using as wireless hosts. So we have turned off these 3 hosts mentioned above and added WPC300N to the PC and WMP300N to both the server and printer and then turned on again.

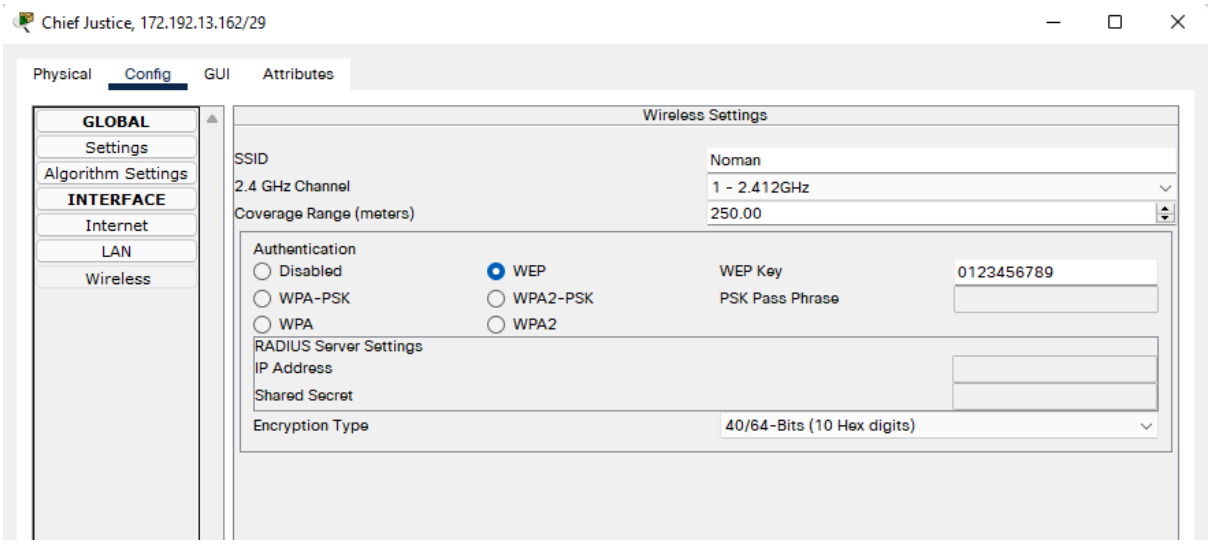


Figure 16: Assigning SSID and WEP authentication password to Chief Justice wireless router

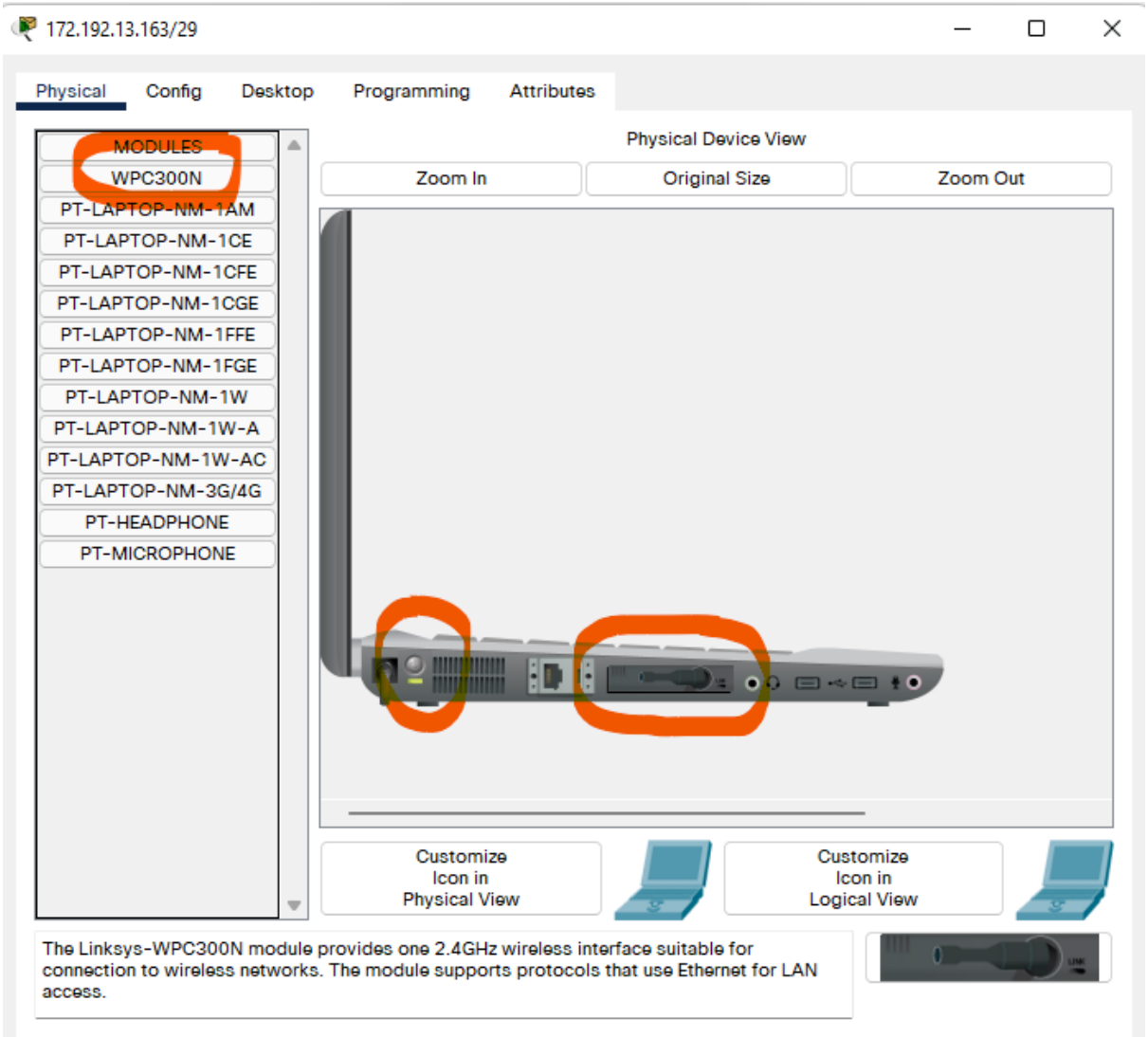


Figure 17: Adding WPC300N to PC in Chief Justice Wireless Network

5. To connect the PC, smartphone, server and printer with the wireless router, we have assigned 172.192.13.163, 172.192.13.164, 172.192.13.165 and 172.192.13.166 respectively as IPV4 address and 255.255.255.248 as subnet mask in wireless0. Also we have assigned SSID **"Noman"** and WEP authentication password **"0123456789"** and turned on the port status.

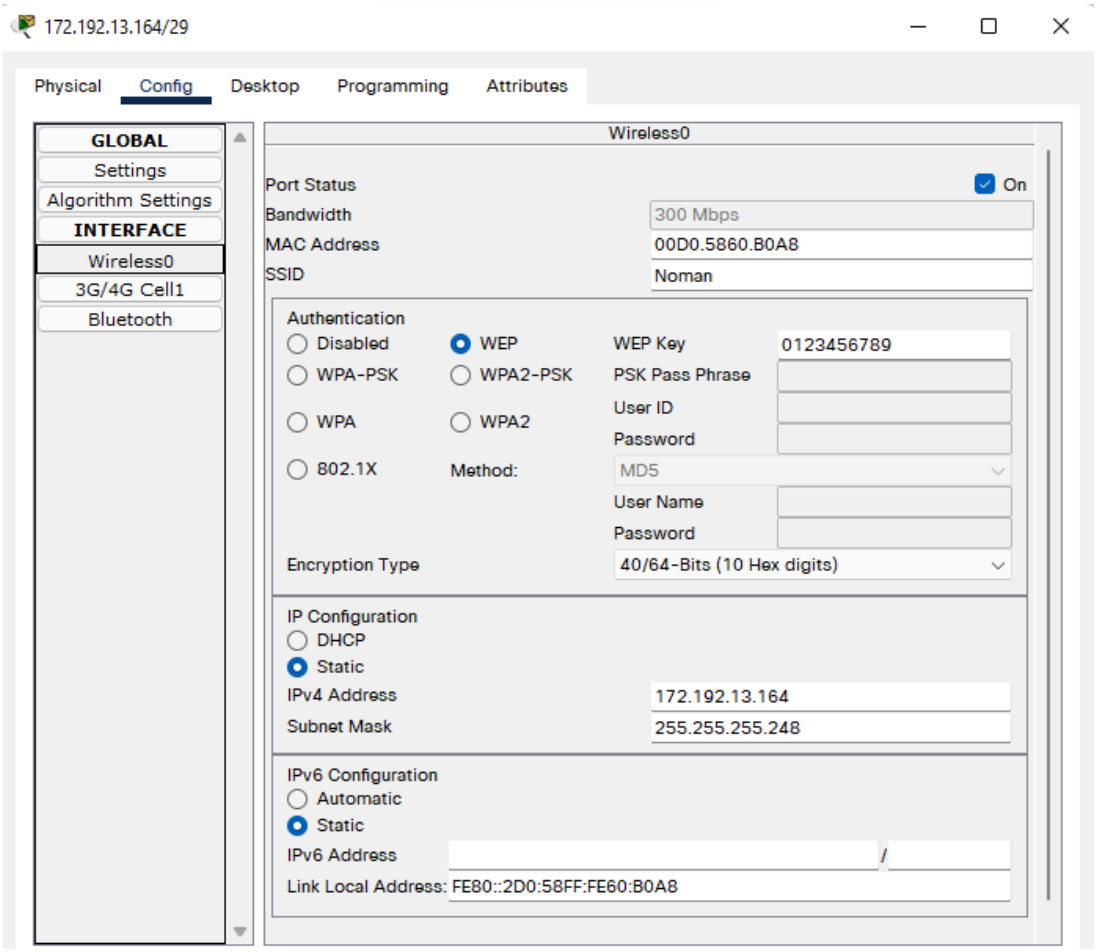


Figure 17: Assigning IPV4 Address, subnet mask, SSID and WEP authentication password to Smartphone in Chief Justice Wireless Network

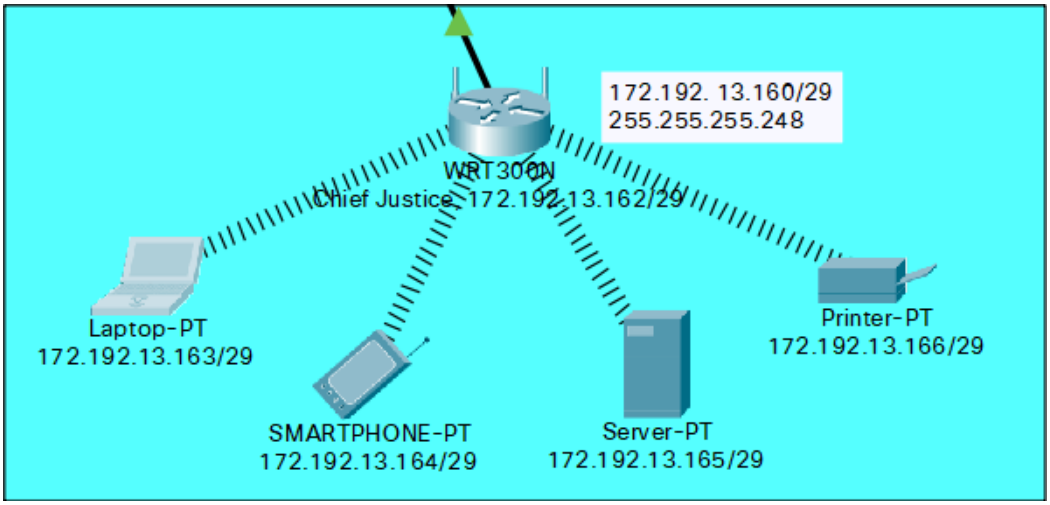


Figure 18: Chief Justice Network

6. Finally we have connected the wireless router with the Appellate Division router using copper straight-through and assigned 172.192.13.161 as IPV4 address and 255.255.255.248 as subnet mask in FastEthernet0/1 of Appellate Division router and turned on the port status.

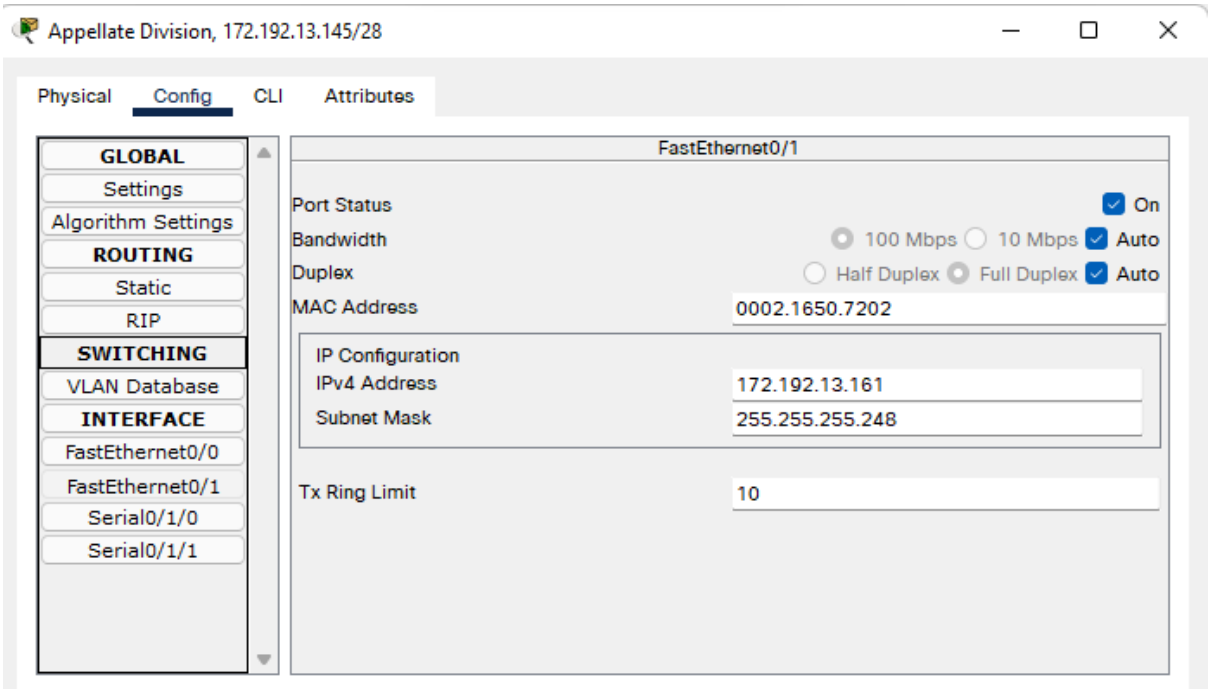


Figure 19: Assigning IPV4 address and subnet mask Appellate Division router to connect with Chief Justice Router

Routing Table

We have used static routing for faster data communication among all the networks except Chief Justice as it is wireless network. The routing tables for the 6 networks are given below:

Metropolitan Session Courts

Network	Mask	Next Hop
172.192.12.128	255.255.255.128	14.10.10.2
172.192.13.0	255.255.255.192	14.10.10.2
172.192.13.64	255.255.255.192	14.10.10.2
172.192.13.128	255.255.255.240	14.10.10.2
172.192.13.144	255.255.255.240	14.10.10.2

Metropolitan Magistrates Courts

Network	Mask	Next Hop
172.192.12.0	255.255.255.128	14.10.10.1
172.192.13.0	255.255.255.192	15.10.10.2
172.192.13.64	255.255.255.192	15.10.10.2
172.192.13.128	255.255.255.240	15.10.10.2
172.192.13.144	255.255.255.240	15.10.10.2

Civil Courts

Network	Mask	Next Hop
172.192.12.0	255.255.255.128	15.10.10.1
172.192.12.128	255.255.255.128	15.10.10.1
172.192.13.64	255.255.255.192	16.10.10.2
172.192.13.128	255.255.255.240	16.10.10.2
172.192.13.144	255.255.255.240	16.10.10.2

Criminal Courts

Network	Mask	Next Hop
172.192.12.0	255.255.255.128	16.10.10.1
172.192.12.128	255.255.255.128	16.10.10.1
172.192.13.0	255.255.255.192	16.10.10.1
172.192.13.128	255.255.255.240	17.10.10.1
172.192.13.144	255.255.255.240	17.10.10.1

High Court Division

Network	Mask	Next Hop
172.192.12.0	255.255.255.128	17.10.10.2
172.192.12.128	255.255.255.128	17.10.10.2
172.192.13.0	255.255.255.192	17.10.10.2
172.192.13.64	255.255.255.192	17.10.10.2
172.192.13.144	255.255.255.240	18.10.10.1

Appellate Division

Network	Mask	Next Hop
172.192.12.0	255.255.255.128	18.10.10.2
172.192.12.128	255.255.255.128	18.10.10.2
172.192.13.0	255.255.255.192	18.10.10.2
172.192.13.64	255.255.255.192	18.10.10.2
172.192.13.128	255.255.255.240	18.10.10.2

ICMP Packet Passing-Reply & Hop Count

We have checked our whole network whether it is working fine or not and found that the network is working completely fine. For example:

Appellate Division Laptop (IP: 172.192.13.148/28) wants to fetch data from the server (IP: 172.192.12.2/25) of Metropolitan Session Courts. So, if we go to the command prompt of Metropolitan Session Courts server and type a command **"ping 172.192.13.148",** we can see that replies are coming from the Appellate Division Laptop and there is 0% data loss in the communication system.

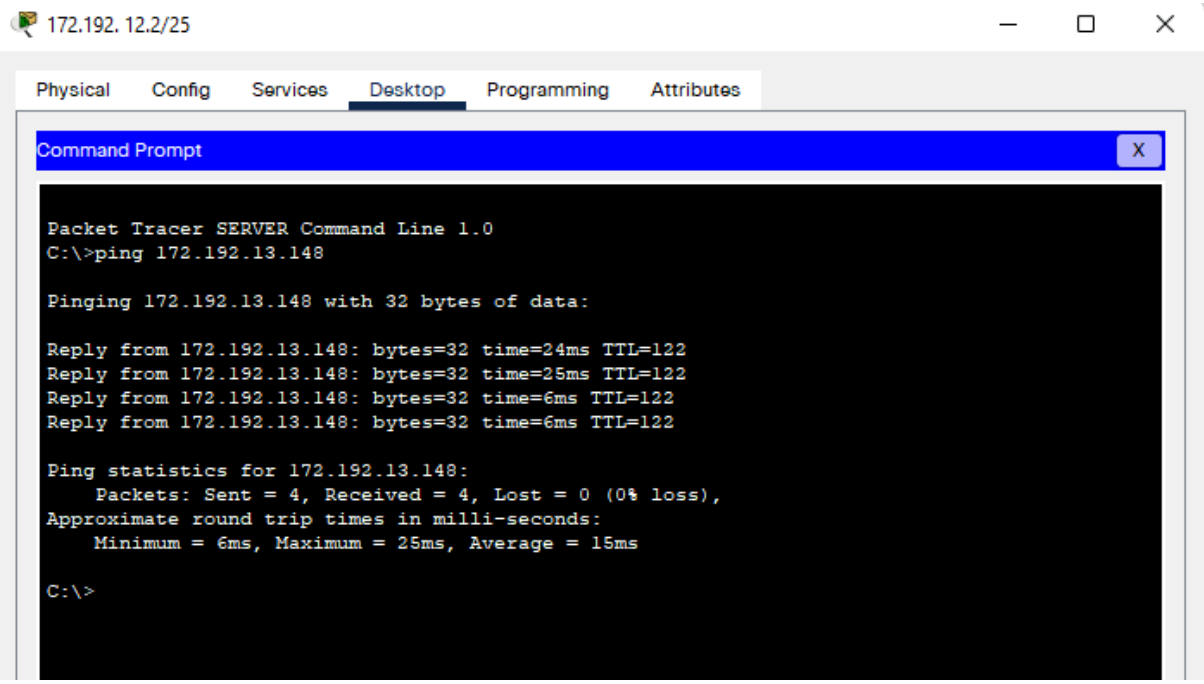


Figure 20: Checking reply massage using **"ping"** command

Besides, we can check the ICMP packet passing-reply status using simulation where the status will be successful if there is no error in the network.

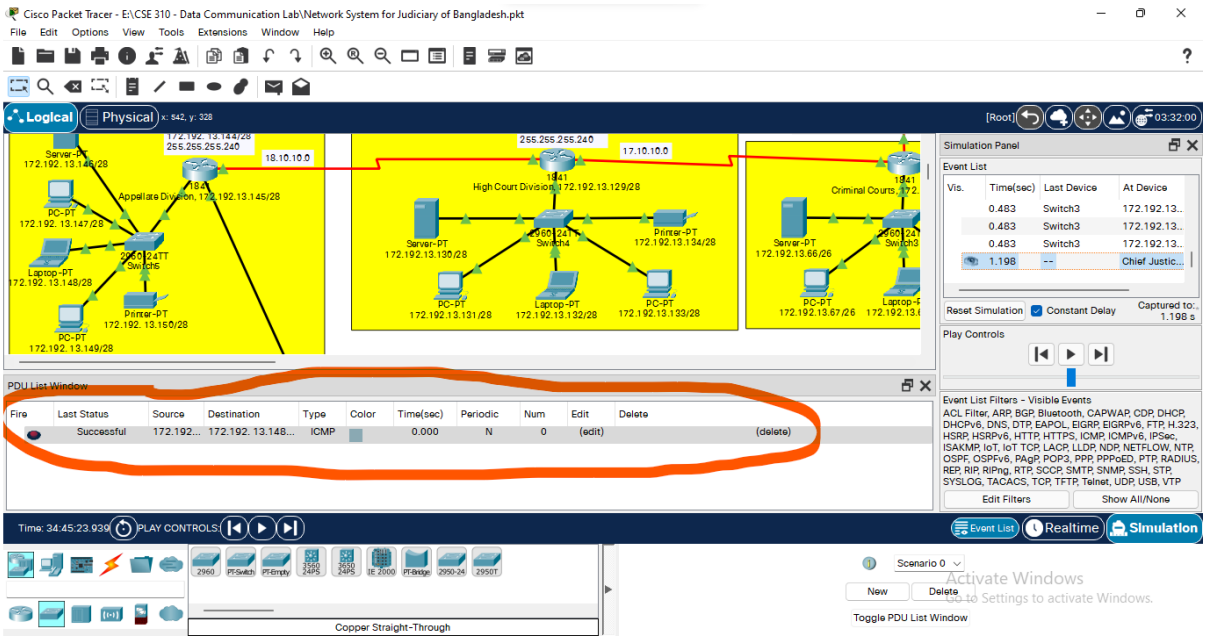


Figure 21: Checking ICMP packet passing-reply using Simulation

We can also count the hop between the Metropolitan Session Courts and Appellate Division by using **"tracert"** command. If we go to the command prompt of any host of Metropolitan Session Courts and type a command **"tracert 172.192.13.148"**, we can show the hop count between these two networks.

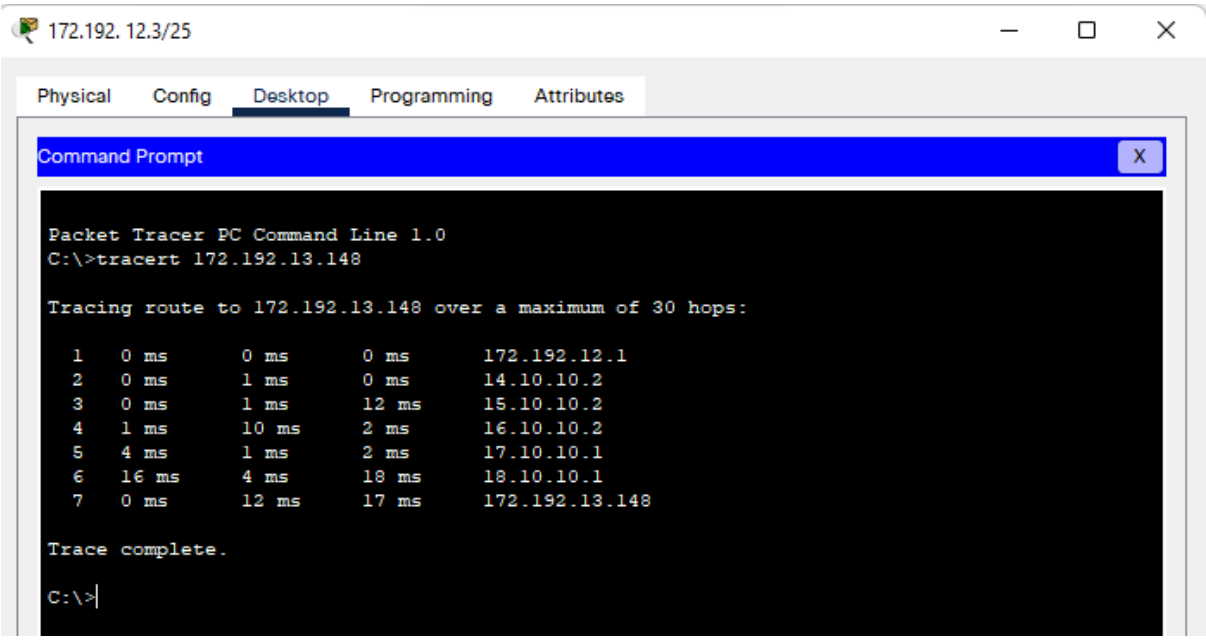


Figure 22: Hop count between Metropolitan Session Courts and Appellate Division

Conclusion

Though we have developed just a demo structure of a Judiciary network due to using simulator, we have future scope to develop this **"Judiciary System for Bangladesh"** using Python (Django) and also we will extend this network for every district of Bangladesh. Moreover, as this project is a very sensitive one, so it needs more research and security concern to make it more realistic and worthy. Thus, we can develop a complete network system for our Judiciary system which can be a sustainable solution for our country's Judiciary system that can be an inspiration to take another step forward in fulfilling the dream of Digital Bangladesh.