International Islamic University Chittagong

Department of Computer Science and Engineering

Course: Computer Networks Lab
Course Code: CSE3634
Section: 7BM Semester: Autumn Year: 2021

Implementation of OSPF routing on Campus Network of project-1

Project Report - 2

Authors: C183061 (Afnan), C183085 (Mahir)

Team Name: 0to255

Team Leader: Mahir Shadid(C183085)

Members:

1. Mahir (C183085)
2. Afnan (C183061)
3. Bashar (C183077)
4. Mahafuj (C183043)
5. Pritom (C193063)

Completion Date: 19.05.22

Course Instructor	**Course TA**
_____	_____
Abdullahil Kafi **Assistant Professor** **Department of CSE, IIUC**	**Mohammad Irfat Chowdhury** **Student** **Department of CSE, IIUC**

Abstract

The main goal of this project is to turn our project 2 from static routing to a dynamic routing using OSPF. Using this protocol has many benefits over VLSM protocol which we will discuss in details in this report. After the project is complete we will make sure that the PC and Routers can communicate with each other without any problem.

Acknowledgements

It has been a very challenging project for us due to its sequential procedure. Without the help of the team mates it'd be very hard for me to complete this project without any hassle. Thanks to Mushfiqus Salehin Afnan, Mahafujul Alam, Md. Abul Bashar and Pritom Saha, my fellow team mates to help me finish the project and to follow my lead – Mahir Shadid (Team Leader).

Table of Contents

Topic	Page
1. Introduction	3
2. Background	3
3. literature review	4
4. Problem Statement	5
5. Designs	6
6. Implementation	10
7. Experimental and Theoretical Results	10
8. Future Work	25
9. Conclusions	25
10. References	25

1. Introduction:

   In the project 1 we were instructed to create a campus network which includes various departments and make all the PCs communicate with each other without any faults. But in project 2 we will further improve the routing and make it dynamic which has many perks over VLSM. To do this we are basically using the same topology with minor tweaks which surprisingly makes the project a lot simpler. We also had to change the routing table a little and use totally different commands and procedure.

2. Background:

   The importance of our project pretty significant because by the perfect execution of our project we can make it very easy, simple and secure communication between the devices of different departments of our campus. Moreover we are using a more sufficient and easy protocol which is even better.

   The main tool that was used in building the project was a simulation software called GNS3. This mainly used by network developers to emulate their network structures in real time. This a pretty heavy software which requires high end PC if the network system is a major one containing huge amount of devices.

   The method to develop the campus network is called OSPF. These are further discussed down below.

3. Literature Review:

3.1. Campus Network:

We have to design a functional campus network where there are different departments that contains PCs and our job is to make the network in such ways so that the PCs can communicate with each other at ease. And we will do all these using the updated OSPF Protocol.

3.2. OSPF:

Open Shortest Path First (OSPF) is a link-state routing protocol that was developed for IP networks and is based on the Shortest Path First (SPF) algorithm. OSPF is an Interior Gateway Protocol (IGP).
In an OSPF network, routers or systems within the same area maintain an identical link-state database that describes the topology of the area. Each router or system in the area generates its link-state database from the link-state advertisements (LSAs) that it receives from all the other routers or systems in the same area and the LSAs that itself generates. An LSA is a packet that contains information about neighbors and path costs. Based on the link-state database, each router or system calculates a shortest-path spanning tree, with itself as the root, using the SPF algorithm.
OSPF has the following key advantages:

- Compared with distance-vector routing protocols such as the Routing Information Protocol (RIP), OSPF is more suitable for serving large, heterogeneous internetworks. OSPF can recalculate the routes in a short amount of time when the network topology changes.
- With OSPF, you can divide an Autonomous System (AS) into areas and keep area topologies separate to decrease the OSPF routing traffic and the size of the link-state database of each area.
- OSPF provides equal-cost multipath routing. You can add duplicate routes to the TCP stack using different next hops.

3.3. GNS3:

The software we used for our project is called GNS3. GNS3 is used by network engineers worldwide to emulate, configure, test and troubleshoot virtual and real networks. GNS3 allows us to run a small topology consisting of only a few devices on your laptop, to those that have many devices hosted on multiple servers or even hosted in the cloud.

3.4. Routing:

Network routing is the process of selecting a path across one or more networks. The principles of routing can apply to any type of network, from telephone networks to public

transportation. In packet-switching networks, such as the Internet, routing selects the paths for Internet Protocol (IP) packets to travel from their origin to their destination. These Internet routing decisions are made by specialized pieces of network hardware called routers.

3.5. Cisco images:

IOS image files contain the system code that your router uses to function, that is, the image contains the IOS itself, plus various feature sets (optional features or router-specific features). However, the features are not configured in any way. In our project, we are using the Cisco 7200 router ISO image as routers in our campus network system. This is downloaded from the official Cisco website / marketplace.

4. Problem Statement:

After doing the subnetting and topology in Project 1, the main works were done basically. Although Project 2 seems simple there was a challenging part. This was configuring the wildcards while doing the routings.

5. Designs:

   4.1. OSPF: *Open Shortest Path First* (OSPF) is a link-state routing protocol that was developed for IP networks and is based on the Shortest Path First (SPF) algorithm. OSPF is an Interior Gateway Protocol (IGP).

   In an OSPF network, routers or systems within the same area maintain an identical link-state database that describes the topology of the area. Each router or system in the area generates its link-state database from the link-state advertisements (LSAs) that it receives from all the other routers or systems in the same area and the LSAs that itself generates. An LSA is a packet that contains information about neighbors and path costs. Based on the link-state database, each router or system calculates a shortest-path spanning tree, with itself as the root, using the SPF algorithm.

   Subnet Mask: Every device on a network has an IP address. A subnet mask splits this IP address into the host and network addresses. This helps define which part of the IP address belongs to the network, and which part belongs to the device. The subnet mask is a 32-bit number, where all the host bits are set to 0, and the network bits are set to 1. So, the subnet mask consists of a sequence of 1s followed by a block of 0s, where the 1s represent the network prefix and the 0s mark the host identifier.

- Subnetting: In subnetting, a large network is logically or physically divided into multiple small networks or "subnets." The reason for subnetting a large network is to address network congestion and its negative impact on speed and productivity. Subnetting also improves efficiency due to the way an address space is utilized in a small network. Finally, the divisions between subnets allow organizations to enforce access control, which improves network security, and helps contain security incidents.

- Wildcards: A wildcard mask is similar to a subnet mask in that it uses the ANDing process to identify which bits in an IPv4 address to match. However, a wildcard mask and a subnet mask differ in the way they match binary 1s and 0s. Unlike with a subnet mask, in which binary 1 is equal to a match, and binary 0 is not a match, with a wildcard mask, the reverse is true.

  4.2. Calculations: The available IP address block is 169.110.224.0/21, and the requirement is to create subnets for six departments:

CSE: 225 hosts

EEE: 100 hosts

BBA: 70 hosts

Administrative: 50 hosts

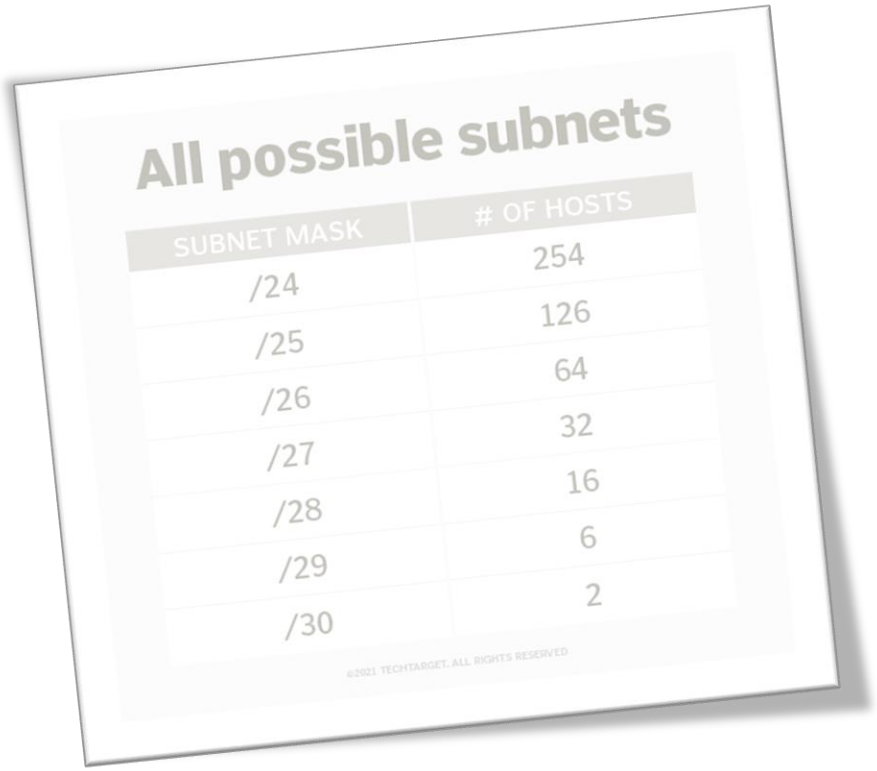
ELL: 40 hosts

Civil: 28 hosts

Here are the steps to allocate the IPs for departments using VLSM:

1. Select the block size for each segment. This must be greater than or at least equal to the sum of the host addresses, broadcast addresses and network addresses.

2. List all possible subnets:



All possible subnets

SUBNET MASK	# OF HOSTS
/24	254
/25	126
/26	64
/27	32
/28	16
/29	6
/30	2

Figure-1

3. Keeping the block size in mind, arrange all the segments in descending order, i.e. list the highest first, then the second highest, and so on, all the way down to the subnet with the lowest requirement. For this example, the order would be:

CSE: 225 hosts

EEE: 100 hosts

BBA: 70 hosts

Administrative: 50 hosts

ELL: 40 hosts

Civil: 28 hosts

4. Assign the appropriate subnet mask to each subnet. Identify the highest IP available and allocate it to the highest requirement. So, here, 169.110.224.0/24 has 256 valid IP addresses that can be assigned to the 225 hosts required by CSE.

5. For the next segment, an IP is required that can handle 100 hosts. The IP subnet mask /25 is the next highest in the list. It can accommodate 128 hosts, so it should be assigned to the 100-host requirement of EEE.

6. Similarly, other departments requirements are also fulfilled withing 2^11=2048 hosts.
7. Area segment is made to use among routers to exchange packets.
8. Wildcard is calculated using (255 - Last Byte of Subnet mask).

4.3. **IP Table**:

Building	NET ID	FIRST ADD.	LAST ADD.	BROAD. ADD.	NET MASK
CSE	169.110.224.0	169.110.224.1	169.110.224.254	169.110.224.255	255.255.255.0
EEE	169.110.225.0	169.110.225.1	169.110.225.126	169.110.225.127	255.255.255.128
BBA	169.110.225.128	169.110.225.129	169.110.225.254	169.110.225.255	255.255.255.128
ADMINISTRATIVE	169.110.226.0	169.110.226.1	169.110.226.62	169.110.226.63	255.255.255.192
ELL	169.110.226.64	169.110.226.65	169.110.226.126	169.110.226.127	255.255.255.192
CIVIL	169.110.226.128	169.110.226.129	169.110.226.158	169.110.226.159	255.255.255.224
AREA-SEG	169.110.226.160	169.110.226.161	169.110.226.190	169.110.226.191	255.255.255.224

4.4. **Software and hardware**:

The software used is GNS3. GNS3 is used by hundreds of thousands of network engineers worldwide to emulate, configure, test and troubleshoot virtual and real networks. GNS3 allows you to run a small topology consisting of only a few devices on your laptop, to those that have many devices hosted on multiple servers or even hosted in the cloud. GNS3 is open source, free software that you can download from http://gns3.com. It is actively developed and supported and has a growing community of over 800,000 members. GNS3 has allowed network engineers to virtualize real hardware devices for over 10 years. Originally only emulating Cisco devices using software called Dynamips, GNS3 has now evolved and supports many devices from multiple network vendors including Cisco virtual switches, Cisco ASAs, Brocade vRouters, Cumulus Linux switches, Docker instances, HPE VSRs, multiple Linux appliances and many others.

The hardware used is above average Computer or Laptop that provides efficient emulation of the routers as the routers requires virtual RAM and they have high CPU usage. Shortly, More threads, more performance.

4.5. **Topology**:

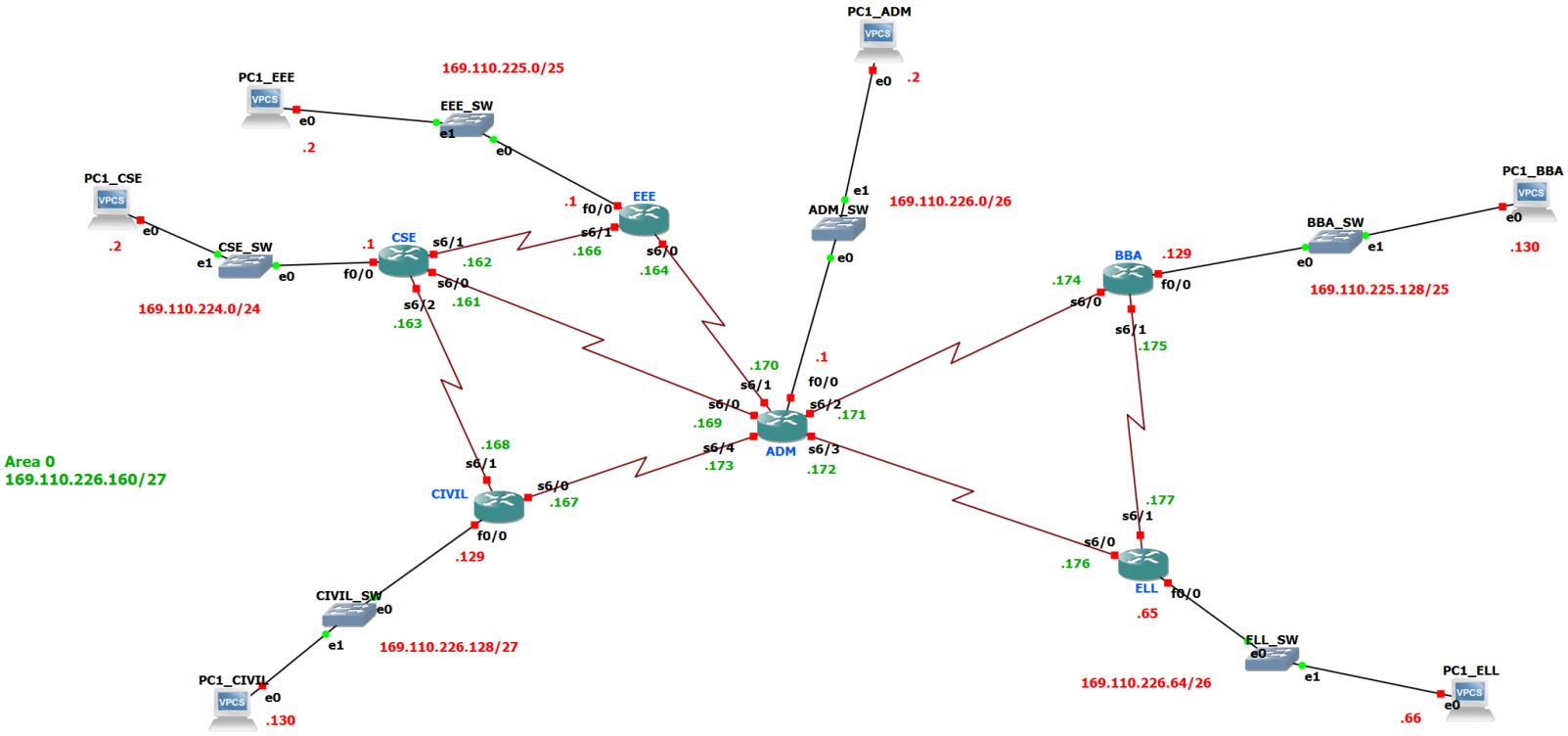

PC1_ADM
VPCS
e0
.2
169.110.225.0/25
PC1_EEE
VPCS
e0
.2
EEE_SW
e1
e0
PC1_CSE
VPCS
.2
e0
CSE_SW
e1
e0
.1
CSE
f0/0
s6/1
.162
s6/0
.161
s6/2
.163
169.110.224.0/24
.1
f0/0
s6/1
.166
s6/0
.164
EEE
e1
ADM_SW
e0
169.110.226.0/26
PC1_BBA
VPCS
e0
.130
BBA_SW
e0
e1
169.110.225.128/25
BBA
.129
.174
s6/0
f0/0
s6/1
.175
.1
f0/0
.170
s6/1
s6/0
.169
s6/2
.171
s6/4
.173
ADM
s6/3
.172
Area 0
169.110.226.160/27
.168
s6/1
CIVIL
s6/0
.167
f0/0
.129
CIVIL_SW
e0
e1
169.110.226.128/27
PC1_CIVIL
VPCS
e0
.130
.177
s6/1
s6/0
.176
ELL
f0/0
.65
ELL_SW
e0
e1
169.110.226.64/26
PC1_ELL
VPCS
e0
.66

Figure-2

6. Implementation:

5.1. Install GNS3: Download GNS3 from the official website. And then follow the instructions that are given in their website to successfully install GNS3 in windows operating system. The link is: https://docs.gns3.com/docs/getting-started/installation/windows/

5.2. Importing Routers: The router we used to build the campus network is Cisco 7200. To import the router in GNS3 we have to get the ISO file of this router from the official marketplace of Cisco. Then we have follow the instruction that are given in the following link: https://www.cybrary.it/blog/0p3n/installing-cisco-ios-router-gns3-vm/#:~:text=STEP%201%3A%20Open%20the%20GNS3,by%20clicking%20on%20%E2%80%9CBrowse%E2%80%9D.

5.3. Configuration:

- First thing was to create the topology
- Then assigning the IPs to the respected Hosts and Routers
- Routers then connected by OSPF method
- Testing was done using Debug method of OSPF

7. Experimental and Theoretical Results:
6.1. Tools:

Ping Tool: After designing the network we use the ping tool to configure the PC and routers. To do this we use various syntaxes. They are given below:

For routers:

```
R1#config t
R1(config)#int f1/0
R1(config-if)#ip add 169.110.226.161 255.255.255.252
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#
```

For PCs:

```
PC1> ping 169.110.225.1
```

OSPF tool: OSPF has many types of tools to use. Some of them that we used are,

```
R1#config t
R1(config)#int f0/0
R1(config-if)#ip add 169.110.226.161 255.255.255.252
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#router ospf 10
R1(router-config)#network 169.110.226.160 0.0.0.3 area 0
R1(router-config)#end
```

Here, 0.0.0.3 is called a Wildcard address.

6.2. IP OSPF Database:

Admin:

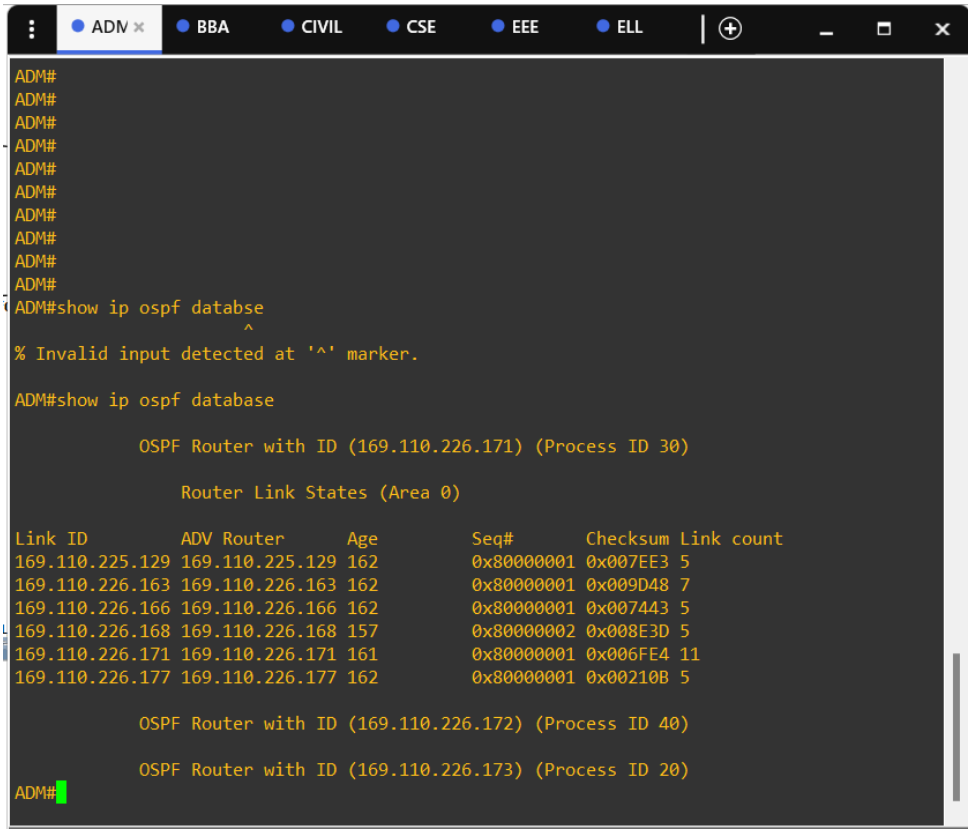


Figure-3

BBA:

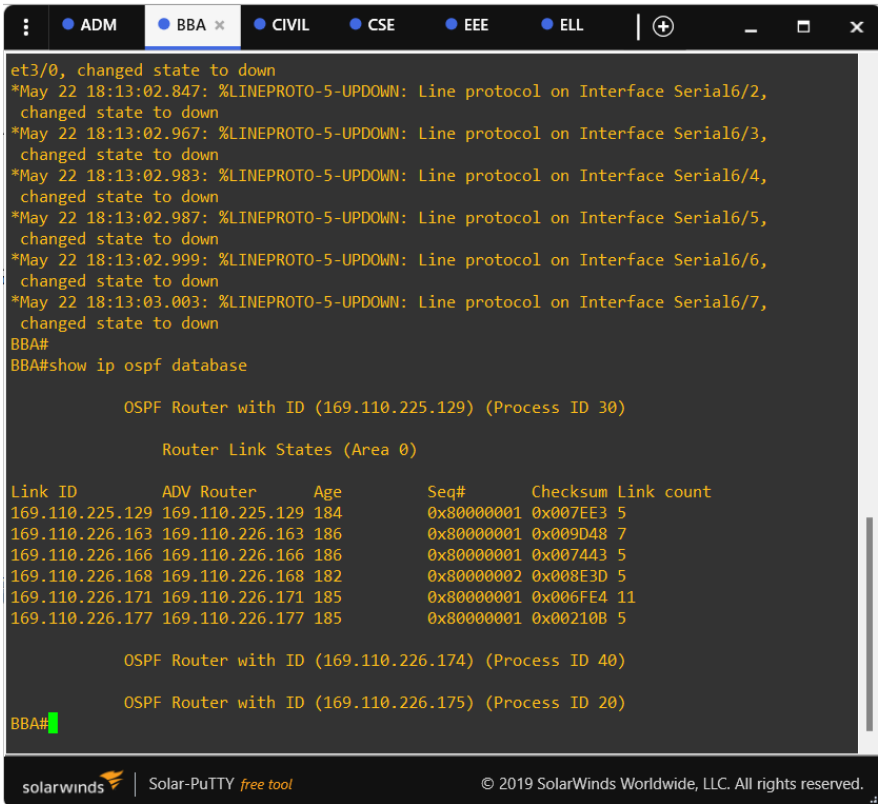


Figure-4

CIVIL:

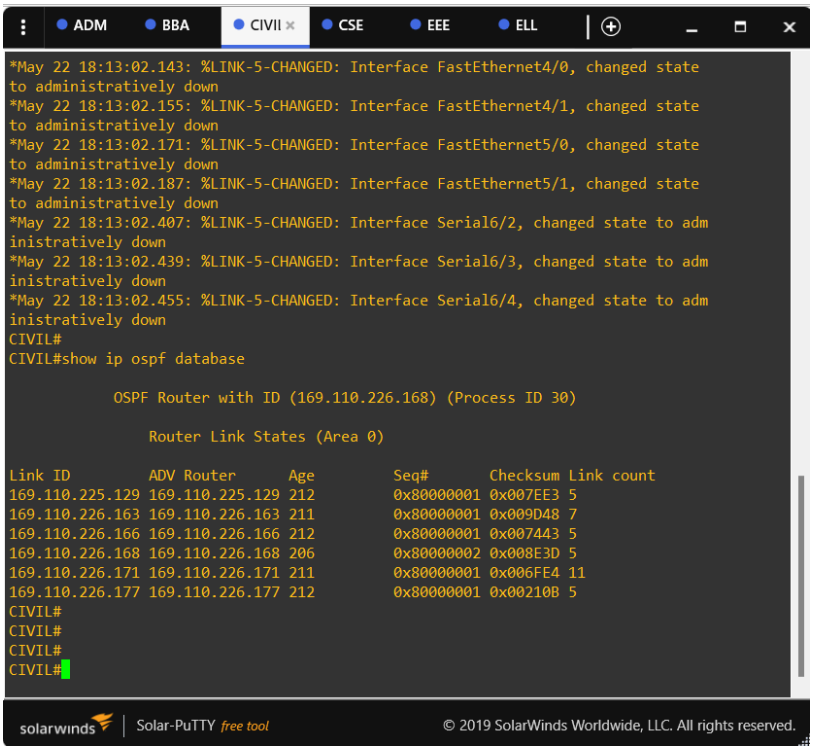


Figure-5

CSE:

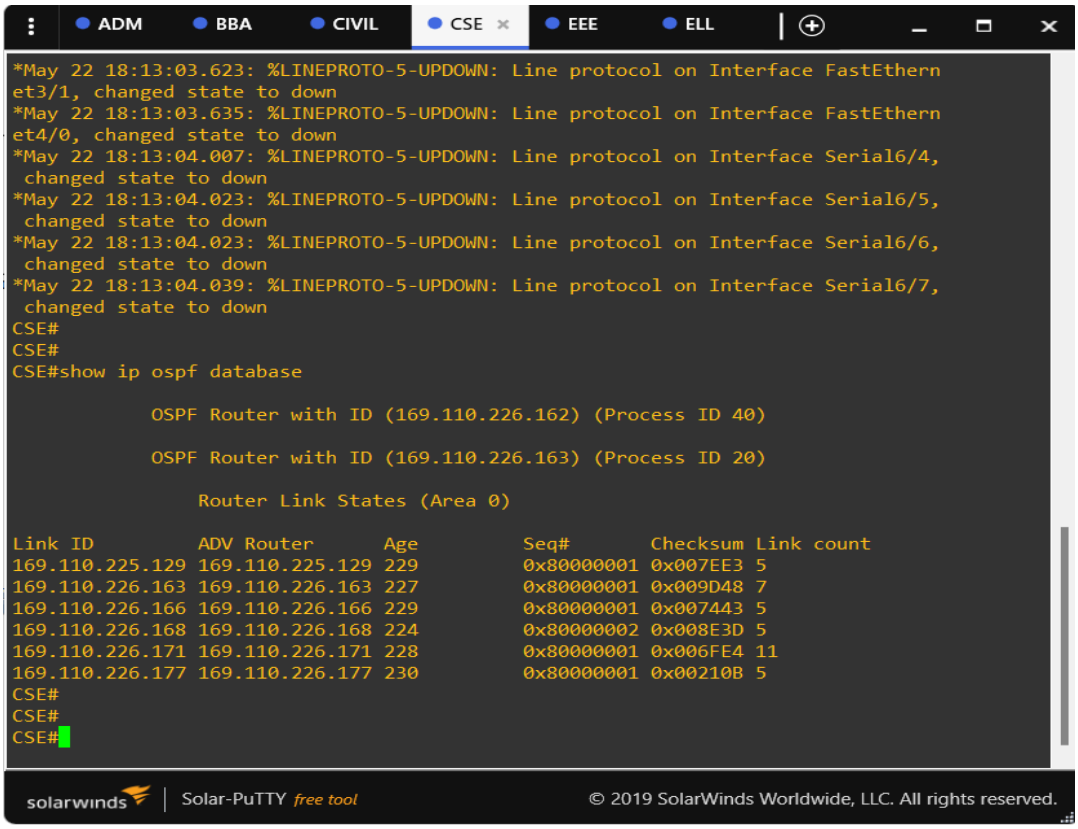


Figure-6

EEE:

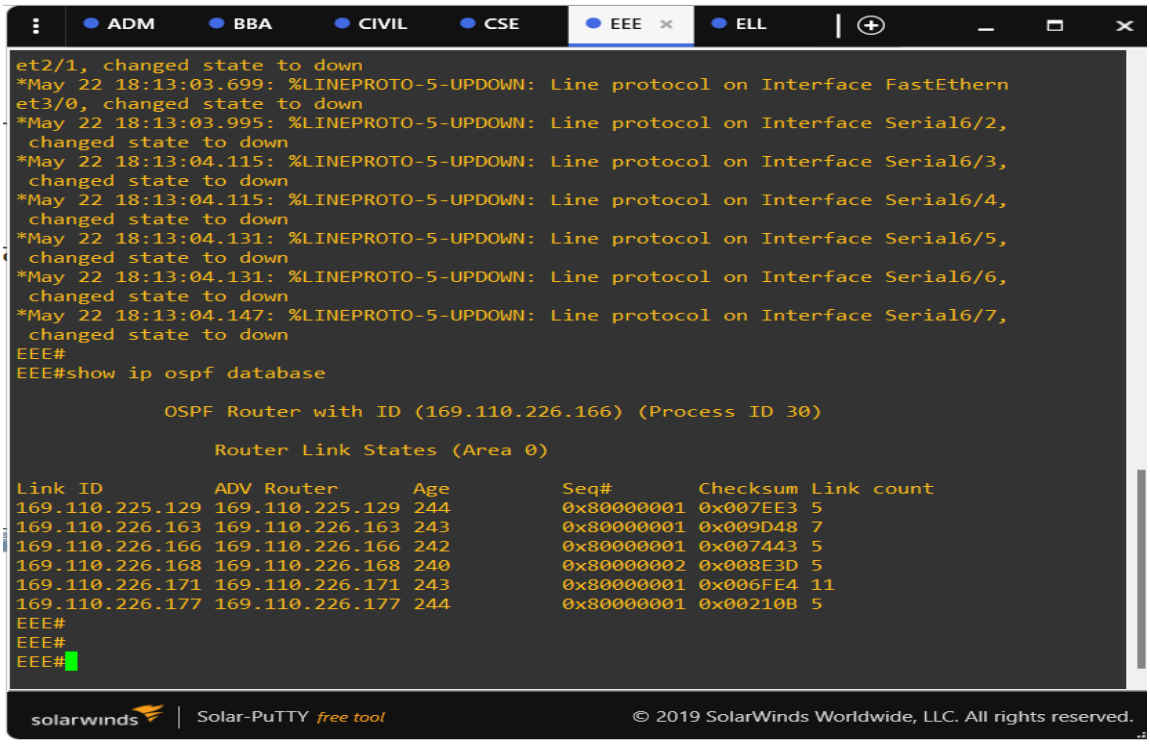


Figure-7

ELL:

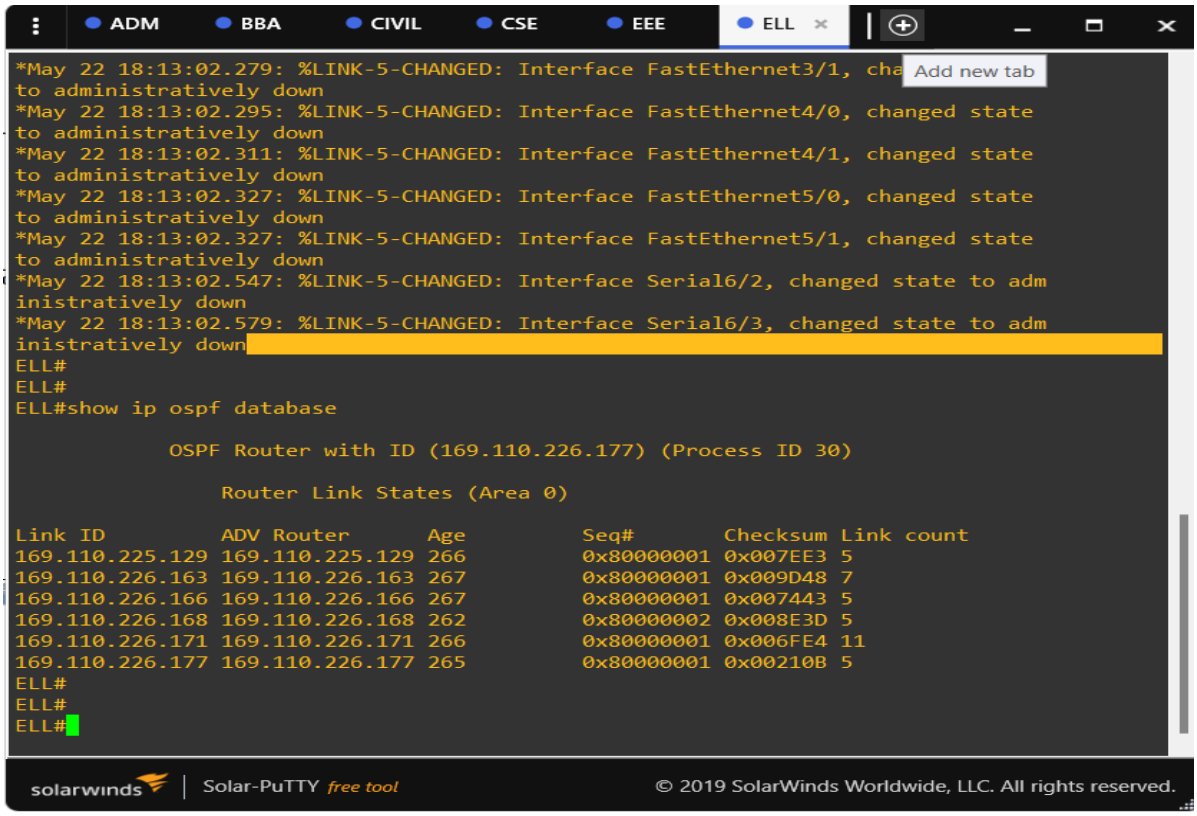


Figure-8

6.3. IP OSPF Neighbors:

Admin:

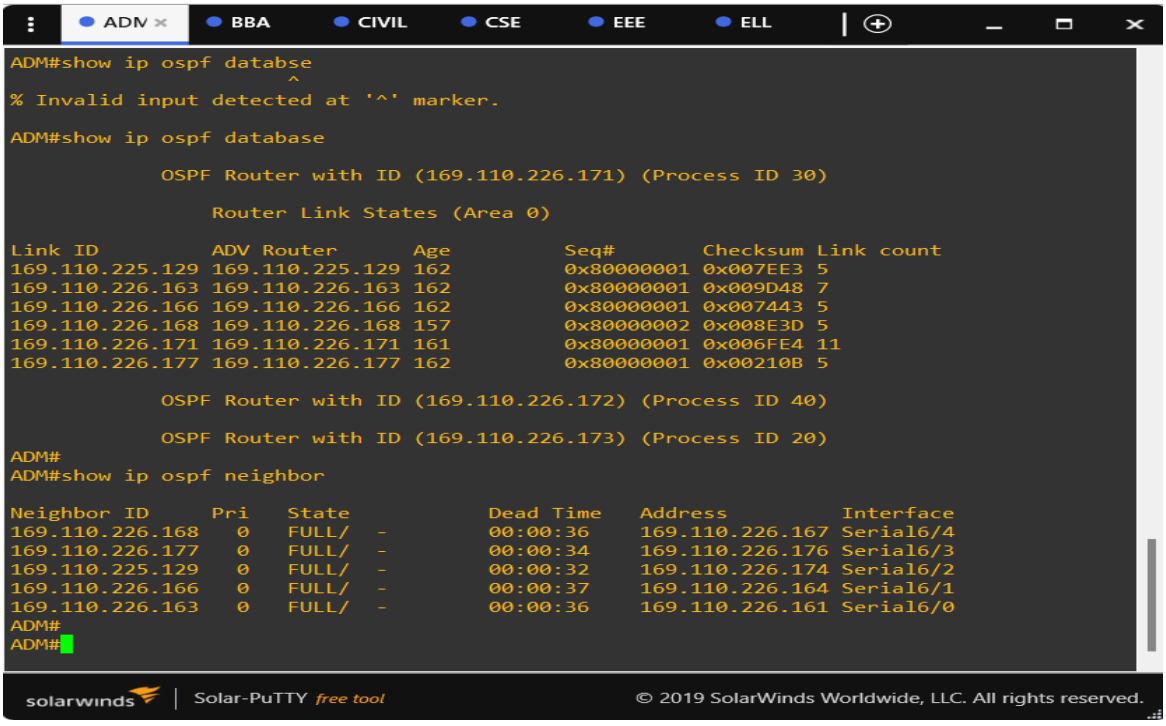


Figure-9

EEE:

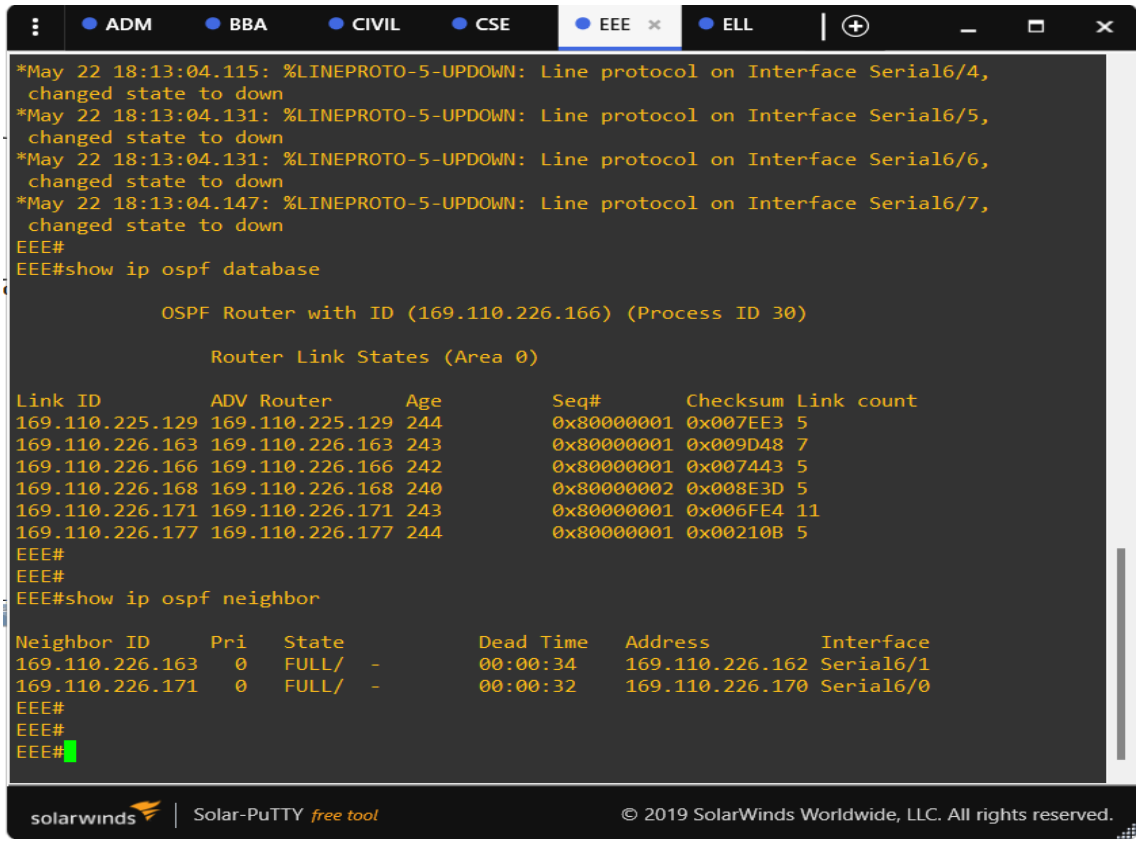


Figure-10

ELL:

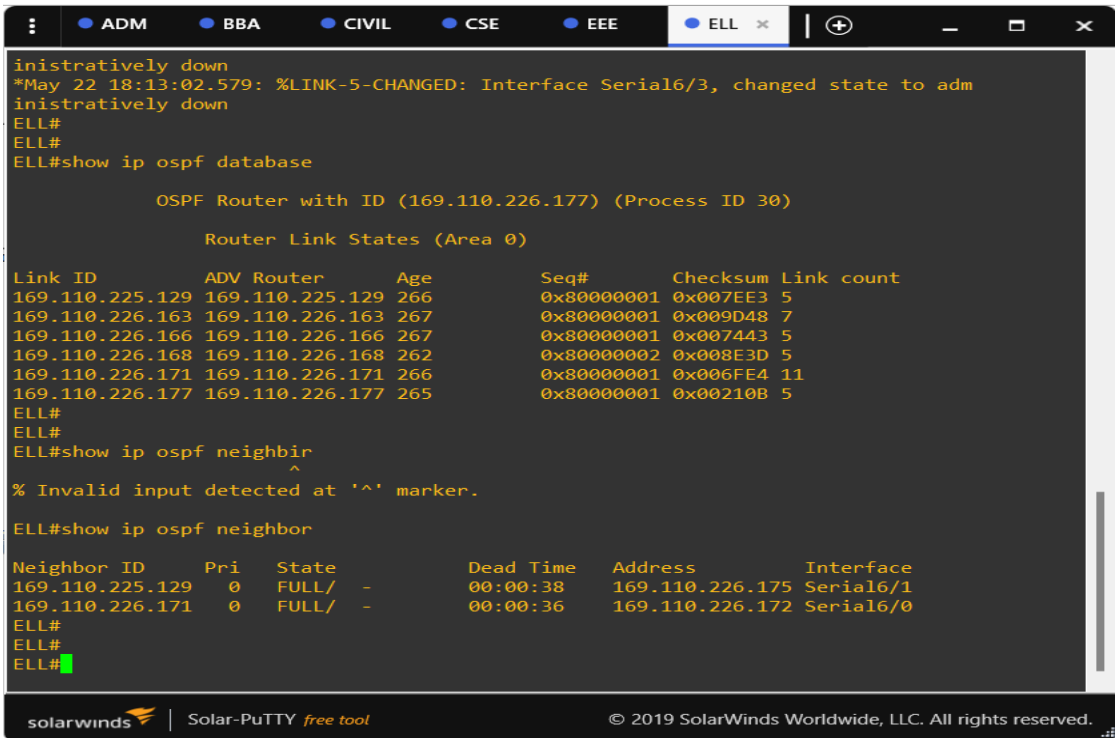


Figure-11

CSE:

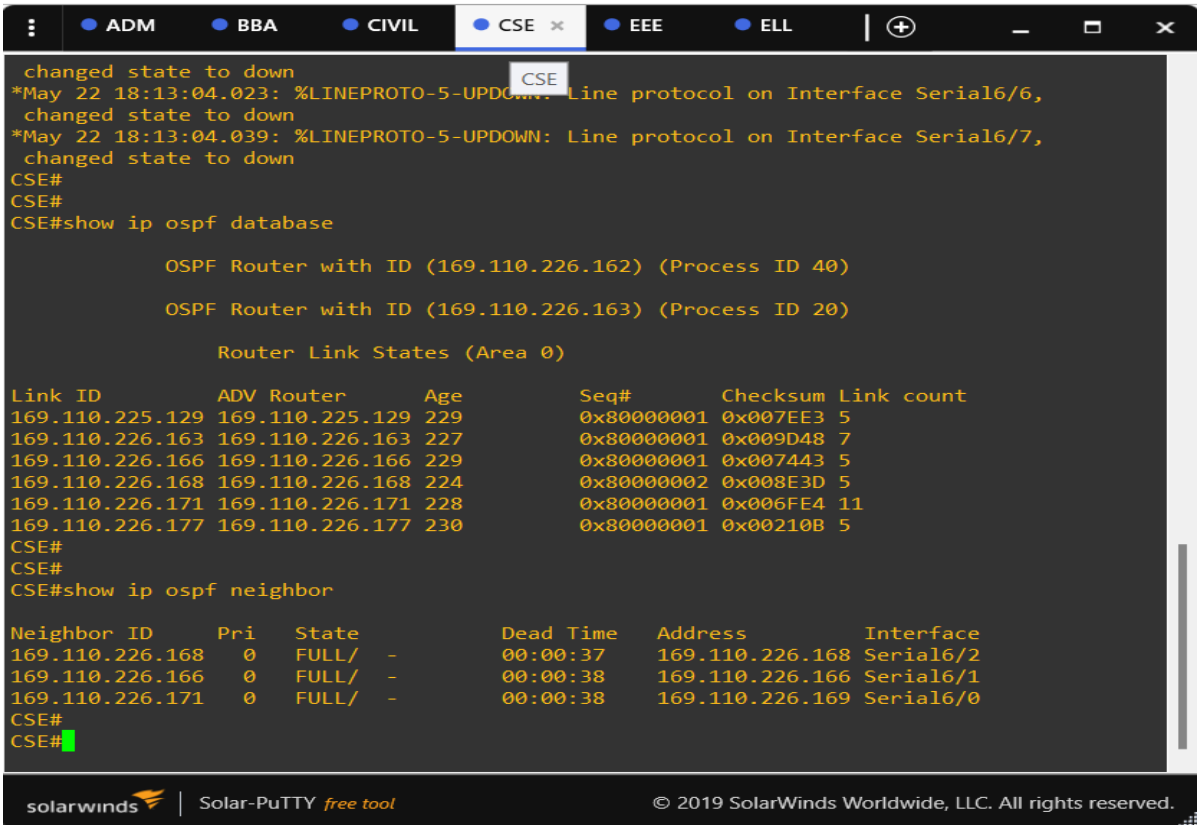


Figure-12

BBA:

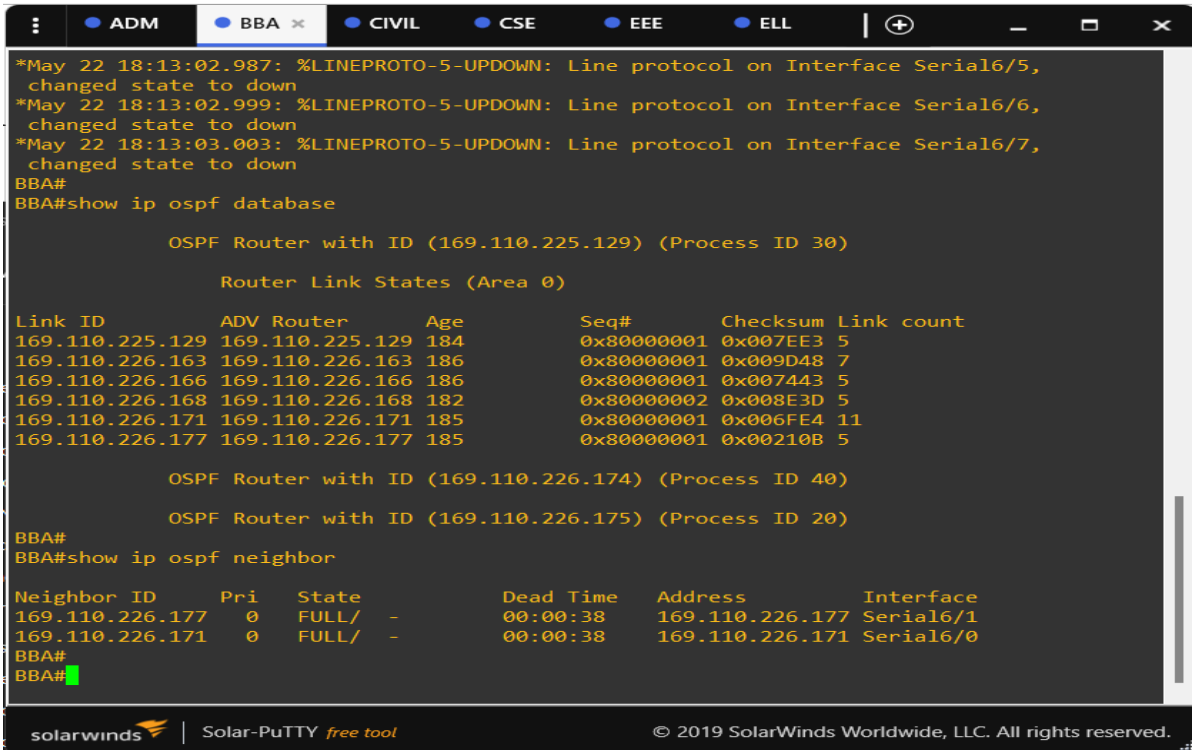


Figure-13

CIVIL:

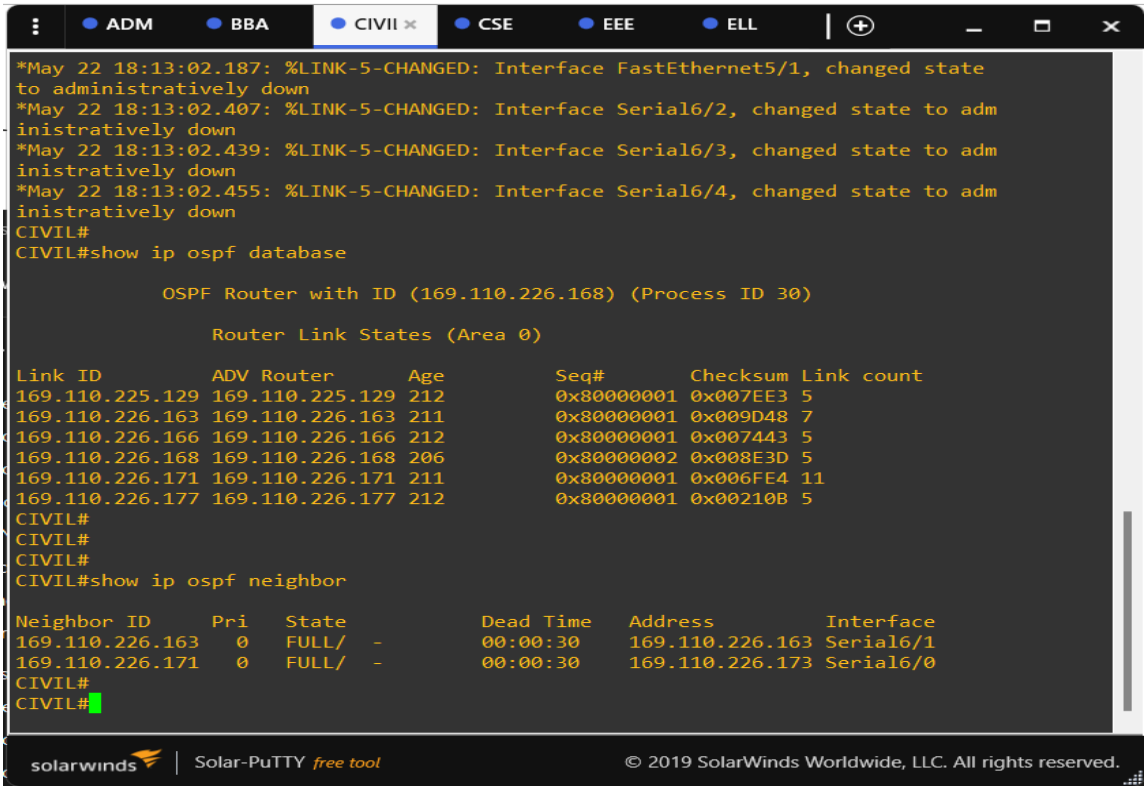


Figure-14

6.4. IP Routes:

Admin:

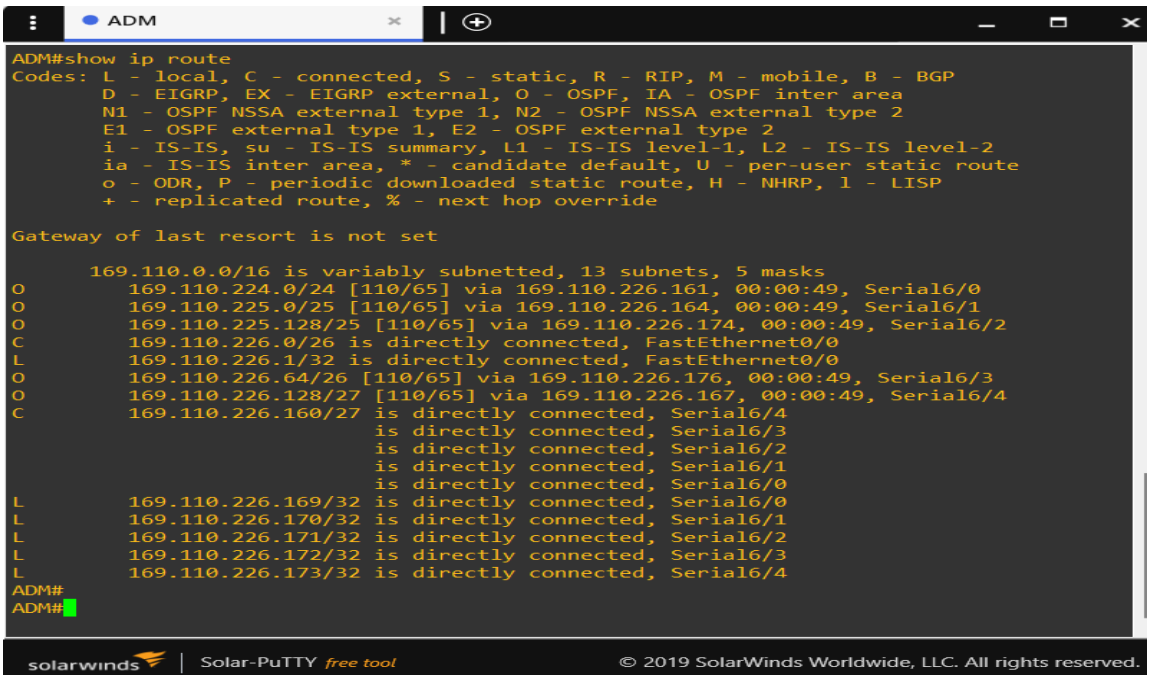


Figure-15

BBA:

Figure-16

CSE:

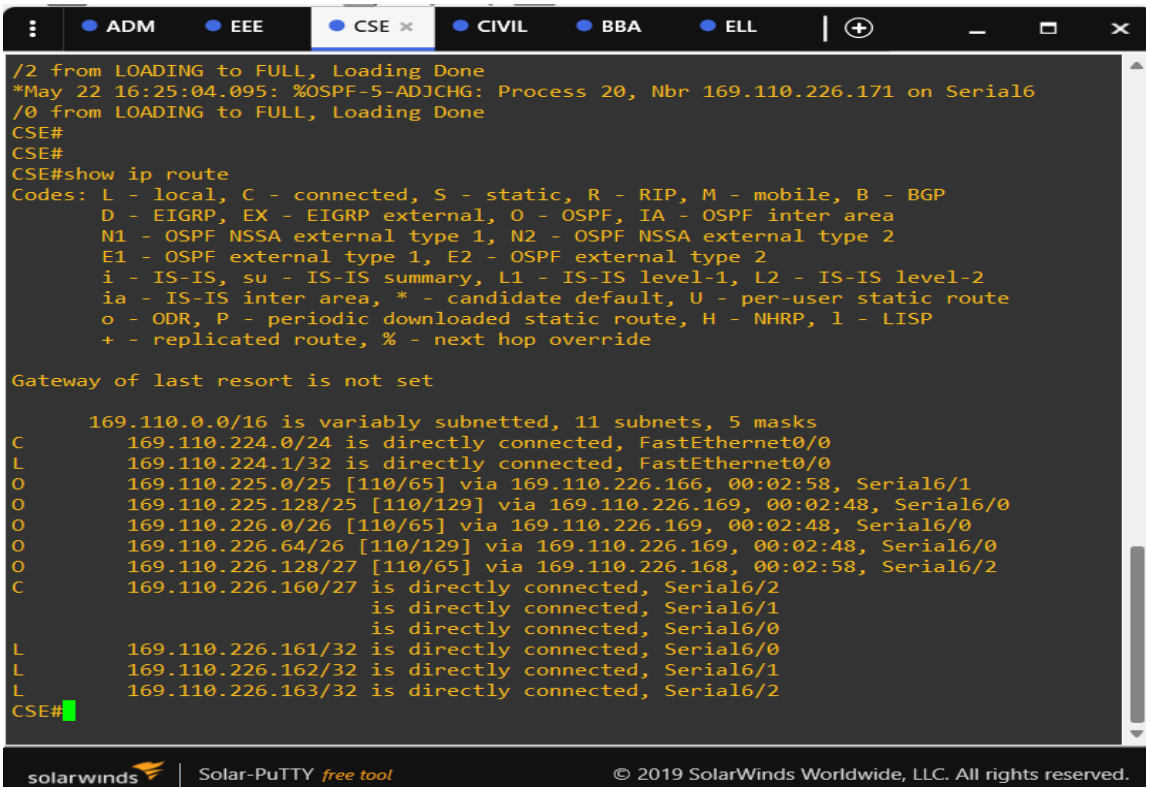


Figure-17

CIVIL:

Figure-18

EEE:

Figure-19

ELL:

Figure-20

6.5. Debug IP OSPF:

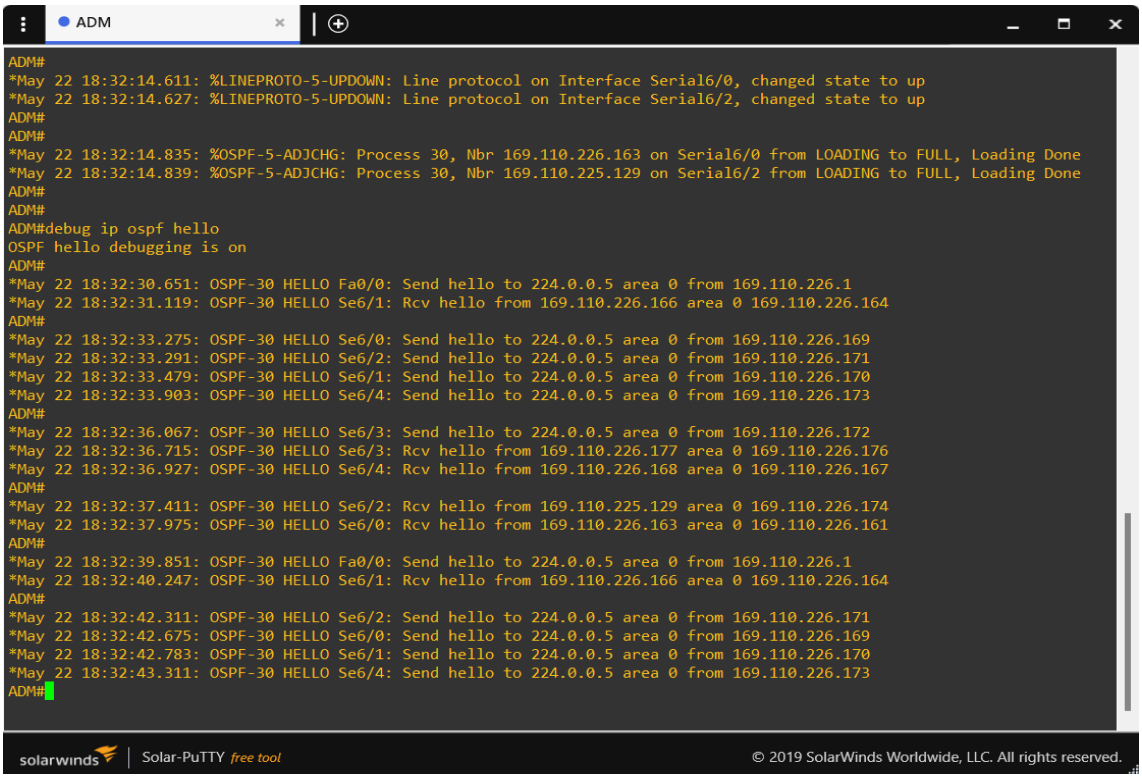


Figure-21

6.6. Pings:

BBA to CIVIL:

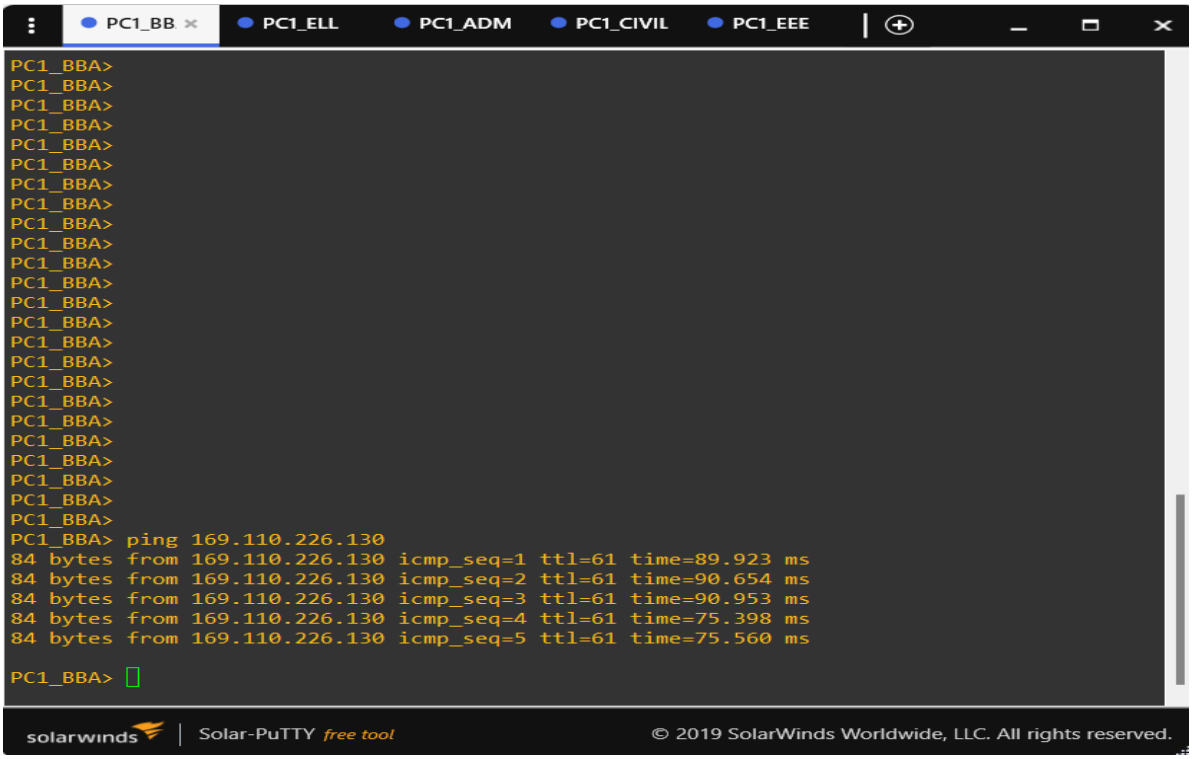


Figure-22

CIVIL to ELL:

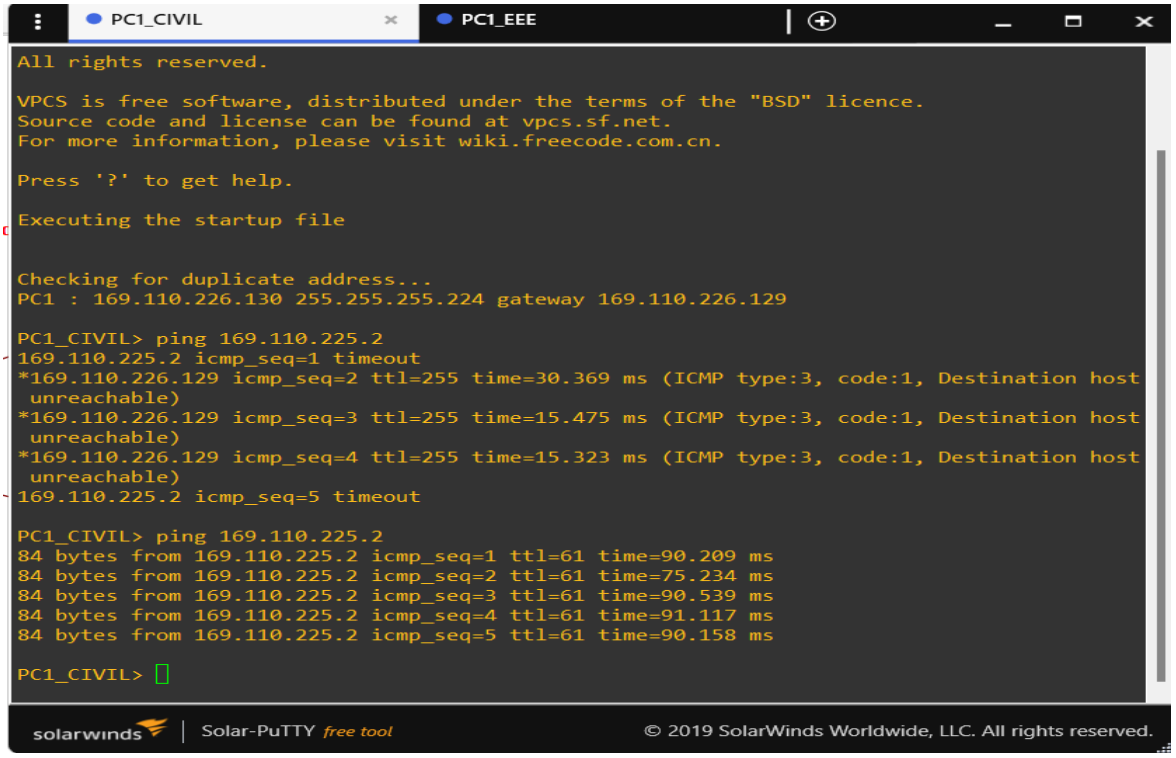


Figure-23

CSE to BBA:

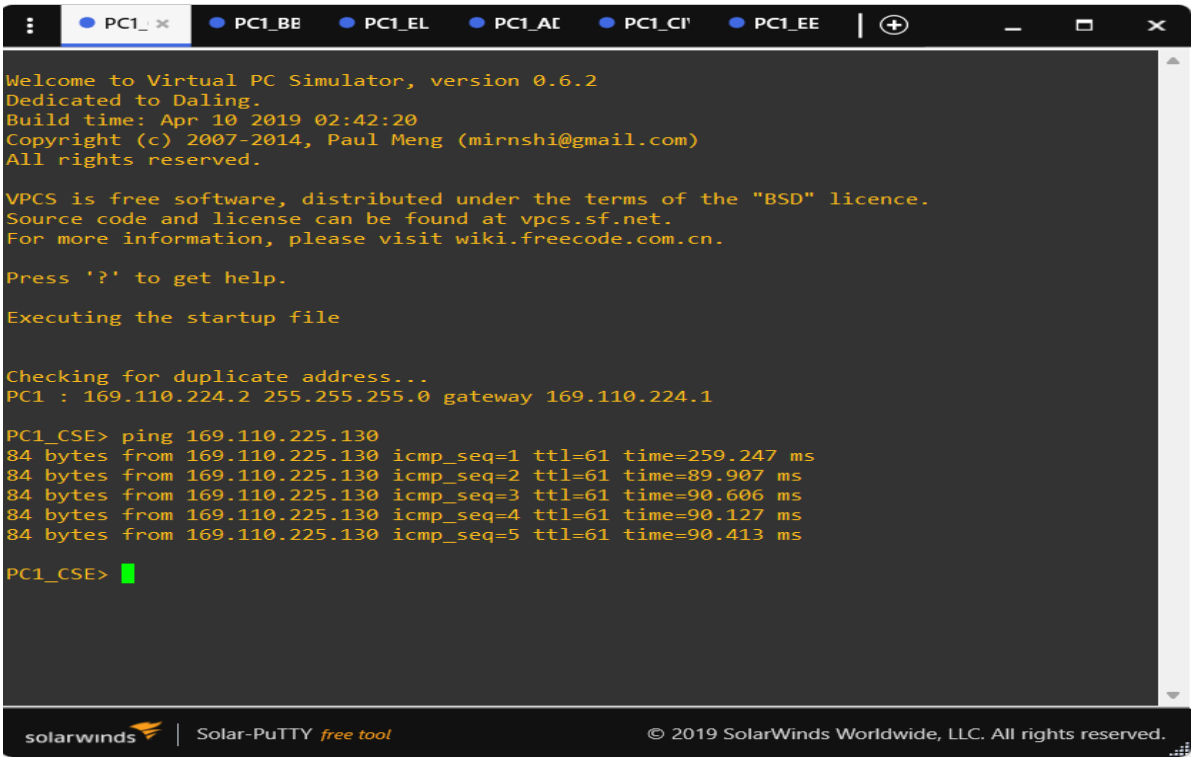


Figure-24

EEE to ADM:

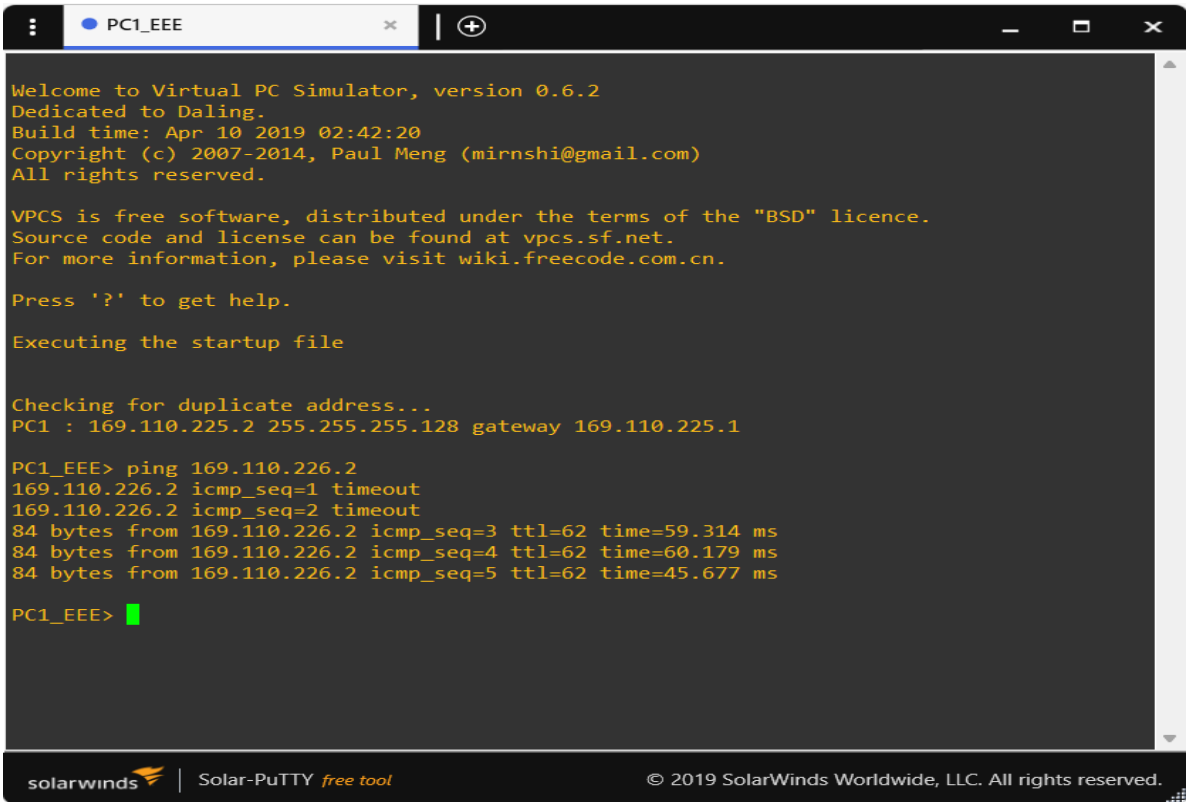


Figure-25

ELL to ADM:

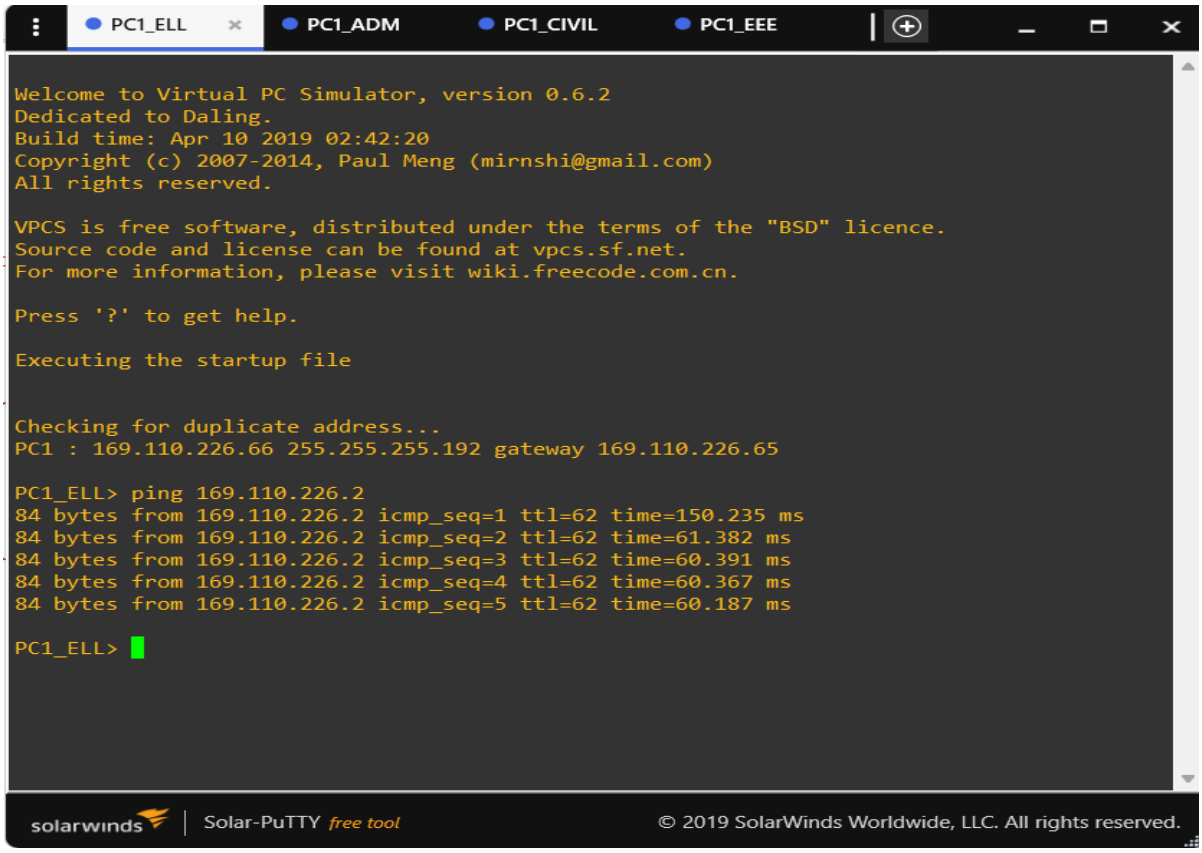
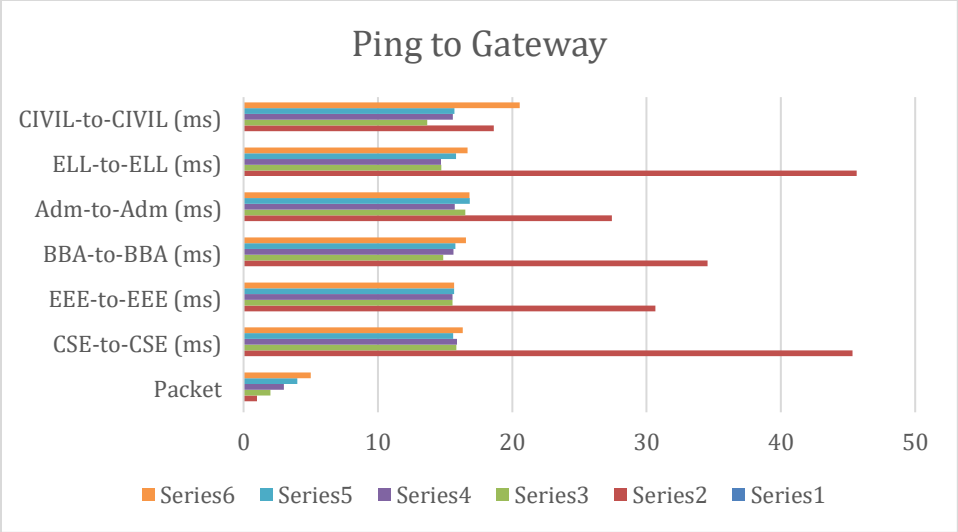


Figure-26

6.7. Table of ping results:

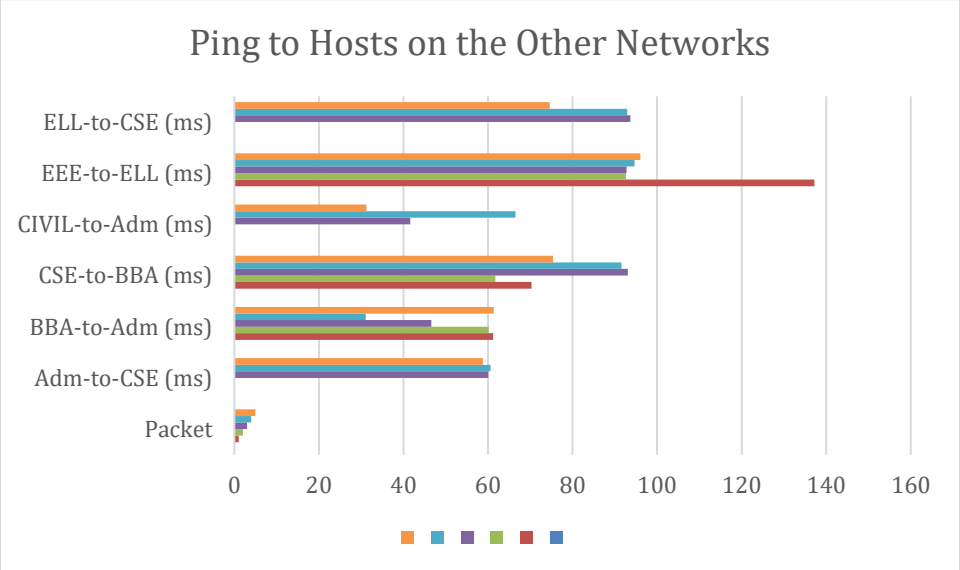
Ping to Gateway:

Packet No.	CSE-to-CSE (ms)	EEE-to-EEE (ms)	BBA-to-BBA (ms)	Adm-to-Adm (ms)	ELL-to-ELL (ms)	CIVIL-to-CIVIL (ms)
1	45.326	30.666	34.549	27.427	45.655	18.627
2	15.846	15.551	14.875	16.517	14.729	13.663
3	15.889	15.559	15.627	15.713	14.707	15.570
4	15.608	15.682	15.780	16.832	15.825	15.708
5	16.310	15.670	16.569	16.819	16.688	20.571



Ping to the Hosts to other networks:

Packet No.	Adm-to-CSE (ms)	BBA-to-Adm (ms)	CSE-to-BBA (ms)	CIVIL-to-Adm (ms)	EEE-to-ELL (ms)	ELL-to-CSE (ms)
1	timeout	61.235	70.329	timeout	137.180	timeout
2	timeout	60.184	61.732	timeout	92.653	timeout
3	60.063	46.594	93.088	41.584	92.776	93.665
4	60.613	31.067	91.534	66.545	94.694	92.953
5	58.821	61.357	75.340	31.265	96.022	74.606



6.8. Discussion on result: After doing all the routing and pinging we can see that all the test results came back positive which means in all the cases the other device pinged back and the debug hello is also working properly. So it is safe to say we did our project perfectly and without fault.

8. Future Work: In future we can further do more to improve project 2 network even more by adding something like cloud pinging, authentication etc.

9. Conclusions: After doing all the designing, subnetting, routing, ip assigning, result analysis we can say that our project is a success. Because by looking at the results we can see that all the devices and routers of all the departments can communicate with each other without any problem and that was our main goal when we started the project. Our OSPF works without any faults which means the routing, wildcard configurations and everything else were done perfectly.

10. References:

- GNS3 doc: https://docs.gns3.com/docs/
- Project Format: https://docs.google.com/document/d/1XYSfDQnW0E2sAnnB1_5auTSHXd9CAIhDbgRZt5EYgY0/edit
- Yaser Rahmati's Exercise on commands: https://yaserrahmati.gitbook.io/gns3/lab-3-configure-static-route-in-gns3
- Dr. AK session: https://www.youtube.com/watch?v=HkizT7oNLtE&feature=youtu.be
- Documentation of GNS3: https://gns3.com/community/discussions/gns3-documentation
- Section IO: https://www.section.io/engineering-education/understanding-static-dynamic-routing/
- Sysnet: https://www.sysnettechsolutions.com/en/configure-ospf-on-cisco-router-in-gns3/