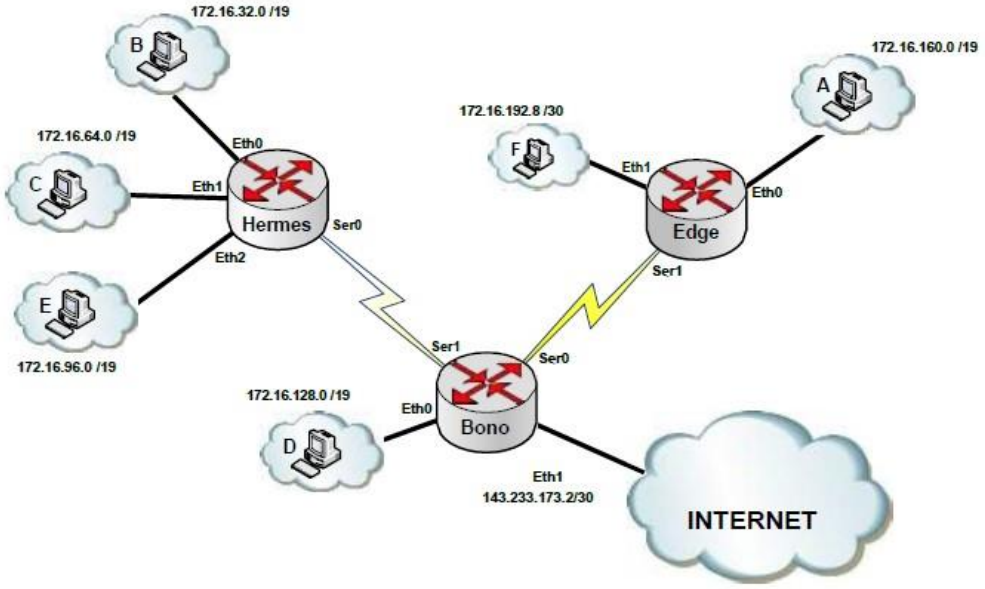
UNIVERSITY OF PIRAEUS - DEPARTMENT OF COMPUTER SCIENCE
MSc "Informatics"

Coursework
"Computer Networks"

2ο Laboratory: Dynamic Routing - Checklists - NAT	
Name of student - No. Registration Number	Evangelos Kormazos
	ΜΠλλ21036
Work	2η
Delivery date	21/1/2023

Requests

Δίνεται η παρακάτω τοπολογία:



Ζητούμενα:

1) Υλοποιήστε την τοπολογία με το λογισμικό που σας δόθηκε. Σε περιπτώσεις όπου δεν δίνονται IP διευθύνσεις, θα πρέπει να υπολογισθούν από εσάς και να αποδοθούν στα αντίστοιχα interface των δρομολογητών. Σημειώστε ότι οι δοθείσες IP διευθύνσεις ανταποκρίνονται στις IP των δικτύων της τοπολογίας – εξαιρείται η διεύθυνση IP του `eth1` του δρομολογητή `Bono`.
2) Οι δρομολογητές θα αξιοποιούν τον αλγόριθμο OSPF. Προς το Διαδίκτυο να χρησιμοποιήσετε στατική δρομολόγηση.
3) Όλοι οι σταθμοί της τοπολογίας πρέπει να έχουν πρόσβαση στην υπηρεσία `HTTP` που εξυπηρετείται από κάποιον διακομιστή στο Διαδίκτυο. Δεν έχουν πρόσβαση σε κάποια άλλη υπηρεσία του διαδικτύου.
4) Τα δίκτυα που βρίσκονται στον δρομολογητή `Hermes` είναι προσβάσιμα σε όλους τους άλλους σταθμούς της τοπολογίας μόνο σε περίπτωση χρήσης των εργαλείων `ping` και `traceroute`.
5) Στον `Bono` είναι απαραίτητο να υλοποιηθεί η τεχνική overloaded NAT (PAT) με overloaded δημόσια IP την 143.233.173.2/30.

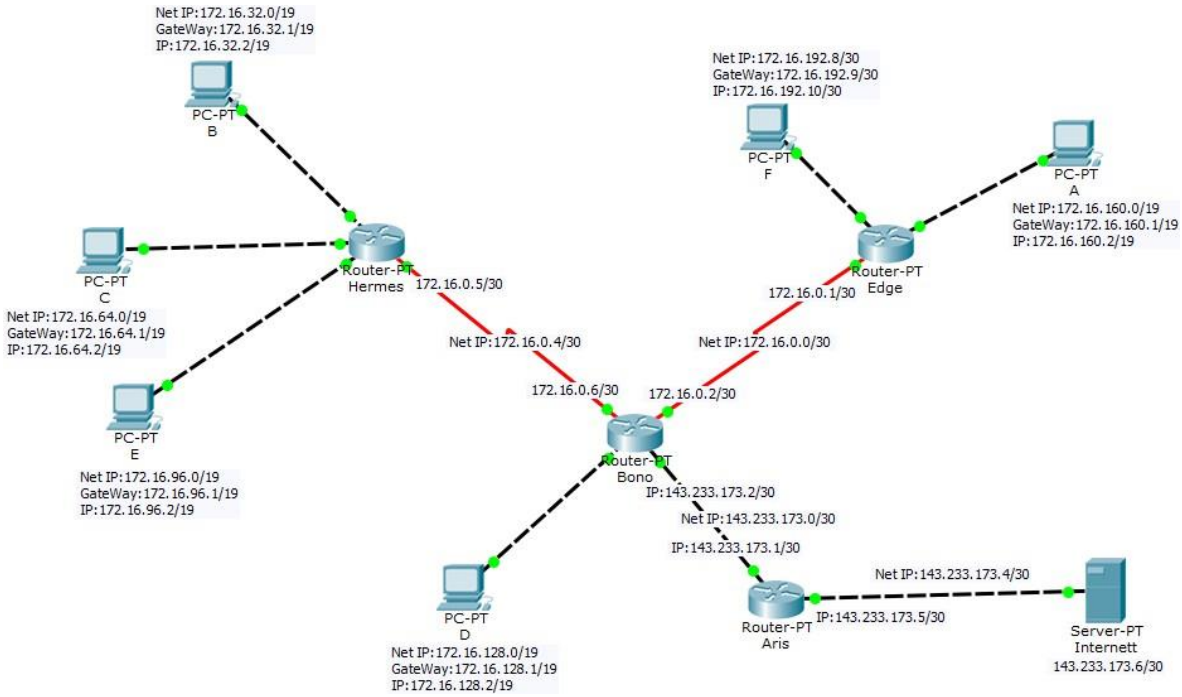
Question 1º

Implement the topology with the software provided. In cases where IP addresses are not given, they will have to be calculated by you and assigned to the respective router interfaces. Note that the IP addresses given correspond to the IPs of the networks in the topology - the IP address of the eth1 router Bono is excluded.

For network functionality we will need to assign new network addresses as listed in the table below:

Network	Network address	Address Broadcast	Available from IP addresses
PC A - Edge	172.16.160.0/19	172.16.167.255/19	172.16.160.1-172.16. 167.254
PC B - Hermes	172.16.32.0/19	172.16.47.255/19	172.16.32.1-172.16.47.254
PC C - Hermes	172.16.64.0/19	172.16.79.255/19	172.16.64.1-172.16.79.254
PC E - Hermes	172.16.96.0/19	172.16.111.255/19	172.16.96.1-172.16.111.254
PC D - Bono	172.16.128.0/19	172.16.143.255/19	172.16.128.1-172.16.143.254
PC F - Edge	172.16.192.8/30	172.16.192.11/30	172.16.192.9-172.16.192.10
Hermes -Bono	172.16.0.4/30	172.16.0.7/30	172.16.0.5-172.16.0.6
Bono -Edge	172.16.0.0/30	172.16.0.3/30	172.16.0.1-172.16.0.2
Bono - Aris	143.233.173.0/30	143.233.173.0/30	143.233.173.2-143.233.173.2
Aris Internet	143.233.173.4/30	143.233.173.7/30	143.233.173.5-143.233.173.6

Our network will thus take the following form:

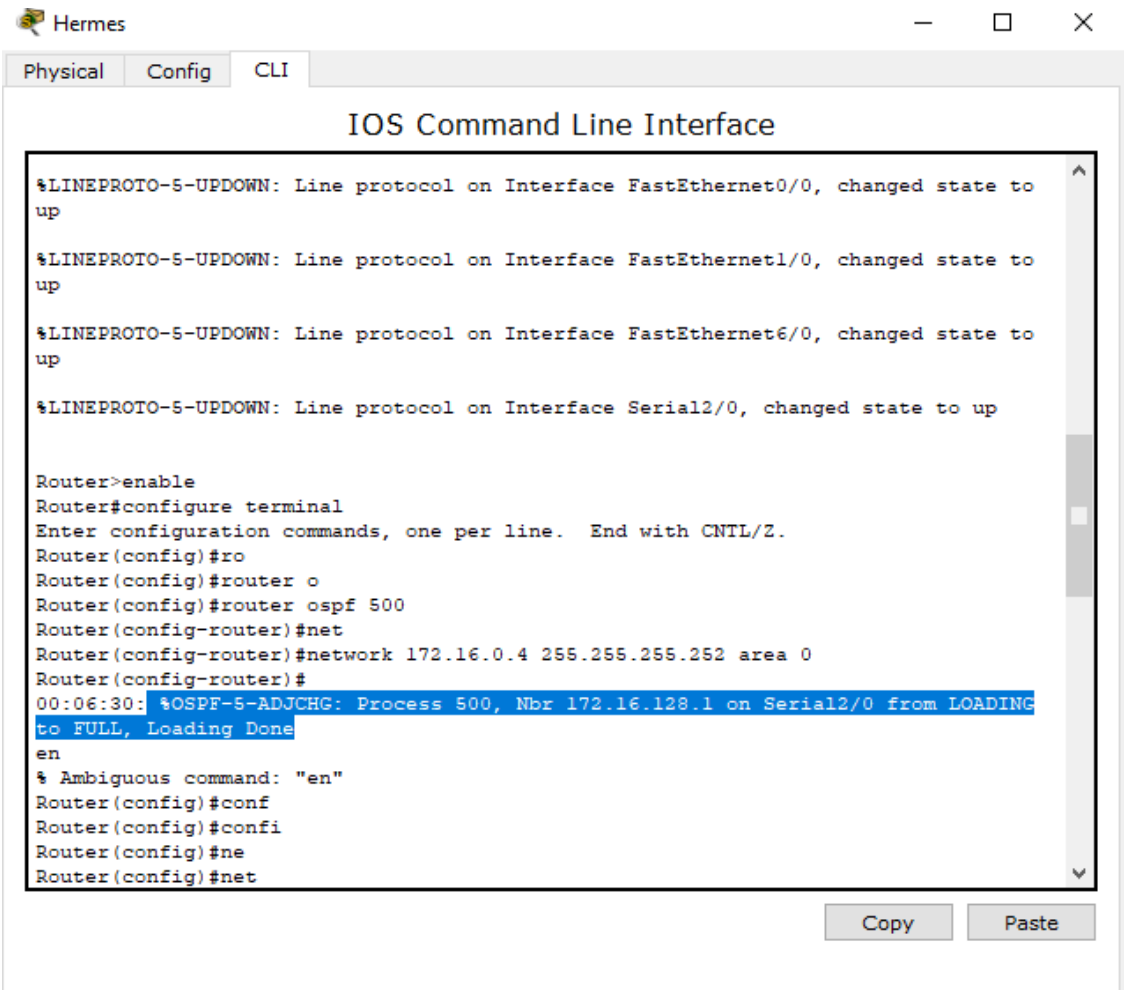


Question 2º

Routers will utilize the OSPF algorithm. To the Internet use static routing.

OSPF (Open Shortest Path First) is a routing algorithm used in IP networks. The OSPF algorithm is a dynamic routing protocol that allows the distribution of routing information across a network. In OSPF, networks are divided into zones and each zone has an area border router (ABR) that connects the zone to other zones or to the backbone. OSPF is mainly used in large networks, as it is designed to handle large amounts of data and to provide high performance in these networks. It is also reliable, as it has error handling and load balancing mechanisms.

By using the #router ospf 500 command on each router we can make use of it.



Edge □ X

Physical Config

IOS Command Line Interface

```
up
%LINEPROTO-5-UPDOWN: Line prot. col on Inte:r:fac.e Serial2/0, changed sta.te to up

Router>,en
Router#con
Router#conf
Router:Jconfigure
Gonfiguri.ng from termi.nal, memory, or network [terminal]?
Enter c1onfigura.ti1on commands, ,one pe:c: line.  Endwith CNTL/Z _
Router(config)#:r:o
Router (config} ttr.outer o
Router(config)#route:r:ospf 500
Router(config-router)lnetwor
Router ( config-route:r:) #network 172:.1€ .1€0. 0 255. 255. 224. 0 a :r:,ea. 0
Router(config-route:r:)#network 172.16.192.8 255.255.255.252 area 0
Router (config-router) #nett.ark 172. lE _O. 8 255. 2SS. 255 _252        a.r,ea O
Router(config-route:r:)#do w:r:
Buildi.ng c.onfiguration. _[OR]

Router(config-route:r:) #no network 172 .1€ .0 .8 255.25!5.2:SS .2!52 a.z:ea 0
Router (c-onfig-router) #network 172 .16. 0. 0 255. 255. 255 _252 a.re a 0
Router(config-routez:)#
00: lf.: 00: %0S PF-5-ADJCHG: Process 500, Nbr 172. lf.: 128.1 on Seria.12/0 from LOADING to
FULL, Loa.ding Done
```

'---G_o---'p---'y_ _ _L._, l_P_a_st_e_, .

Bono □ X

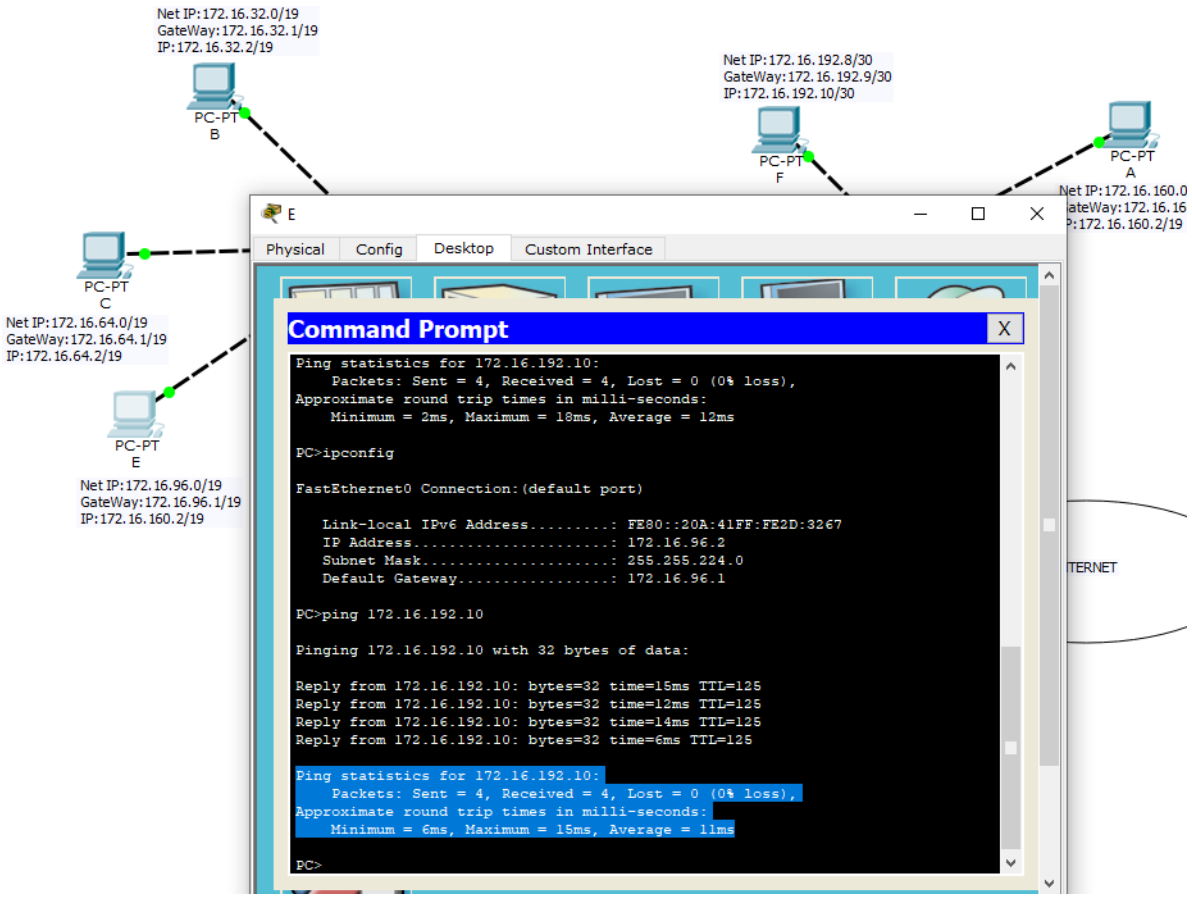
Physical Config

IOS Command IUne Interface

```
router oonfig-router)#net
R,out.e:i:::(c-,onfig-router)#netwo:i:::k 172.16..0.4 255.255.255.252 area 0 Router
loonfi,g-r,outer) #
R,out.erl
%SYS-5-CONFIG_I: Configured fz:.am oonsole by oonsole en
Router#c1onf
R,out.er#oonfigure
Gonfi.guring from termi.na.l, memory, or network [terminal]? Entez:
configuration commands, one per li.ne _End                with CNTL/Z _
Route:i:::(:c.onfi.g) I
00: 0e:30: OSPF-5-ADJCHG: Process 500, Nbr l 1- .1€. 9€. l on Seria.12/0 from LOADING
t.o FULL, Loadi.ng Done

R,out.er (c.onfig) #en
% Ambiguous command: ""en"'
R,out.er ( c.onfig) lro Routerc.onfi.g)
#z:.outer o R.out.e:i::(:c.onfig) lrout.er
ospf 500
Rauterloanfi,g-r.auter)#172.1c.0.0 255.255.255.252 area 0

% Invalid input detected a.t ' .,,,._' ma :c:ke:c:.

Route:i:::(c.onfi,g-r.outer)lne 172.lE.0.0 255.255.255.252 a:i::::ea 0
R,out.erfoonfig-router)#network 172.16..0.0 255.255.2!5!5.252 area 0
Router (c.onfi.g-r.outer) tt
00:1e:00: JI.j]u]rfiMAA-'44i♦■■■■l■MhMiMIWI-WA-I,4MiiM-F¥imlMiHS
In.,11+M _ · _!--
```

_c o P Y_l l

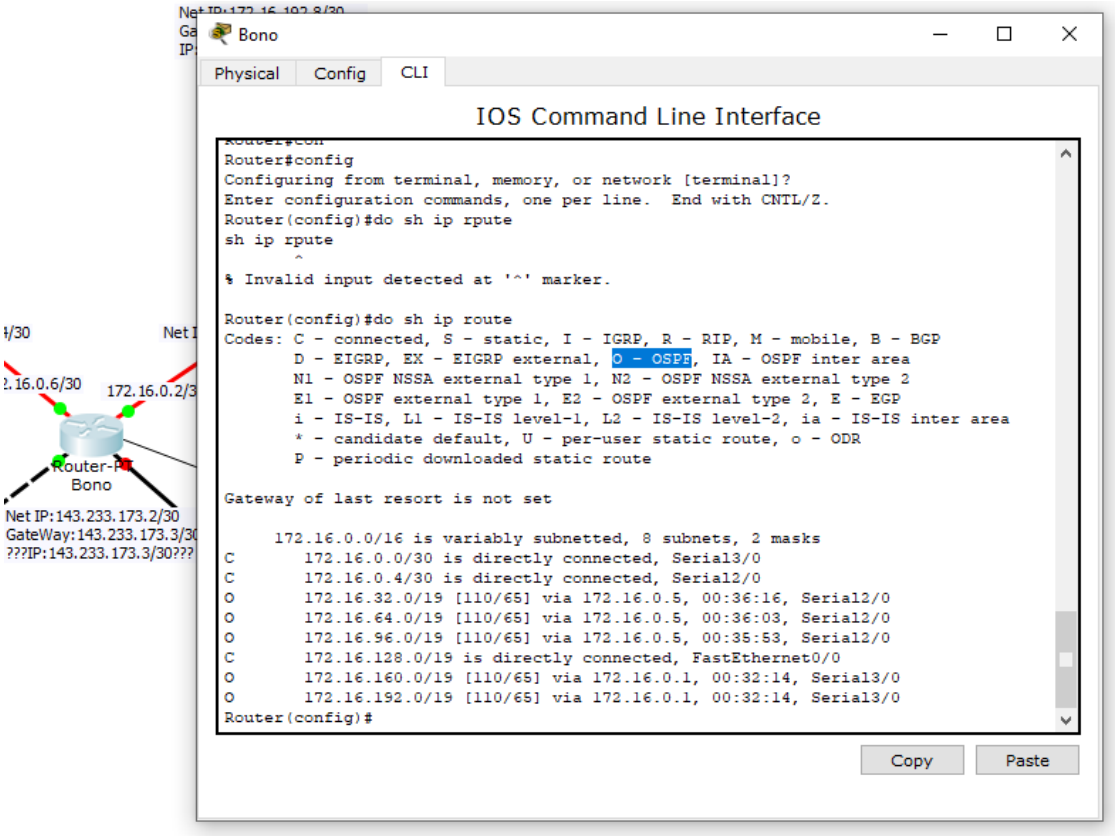
Control between PC-E with PC-F using #ping:



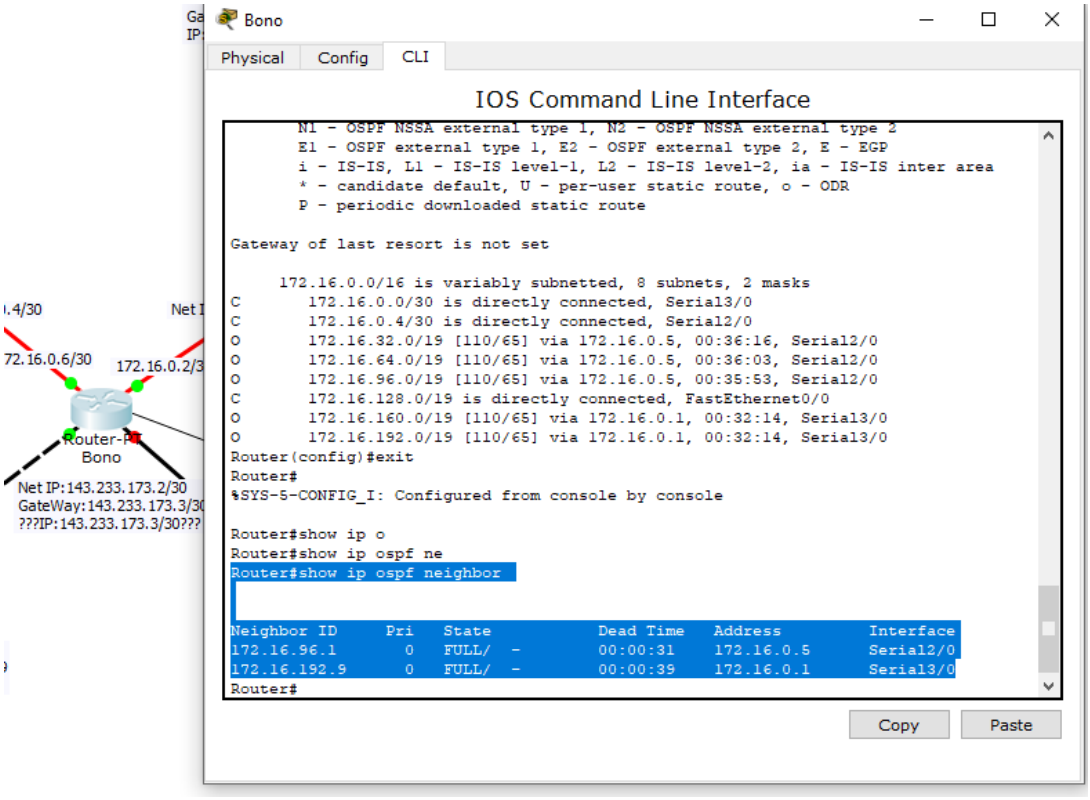
The #show ip route command is a Cisco IOS command that displays the table routing of the router. Displays the routes learned by the router either from directly connected interfaces or through a routing protocol such as OSPF, BGP, or EIGRP. It also displays the distance, metric,
next jump address and outgoing interface for each route.

This command can be useful for troubleshooting problems
network connectivity, as it allows you to see the route that traffic will take through the network.

Using #do sh ip route in Bono we will also be able to tell which IP addresses were routed through the algorithm:



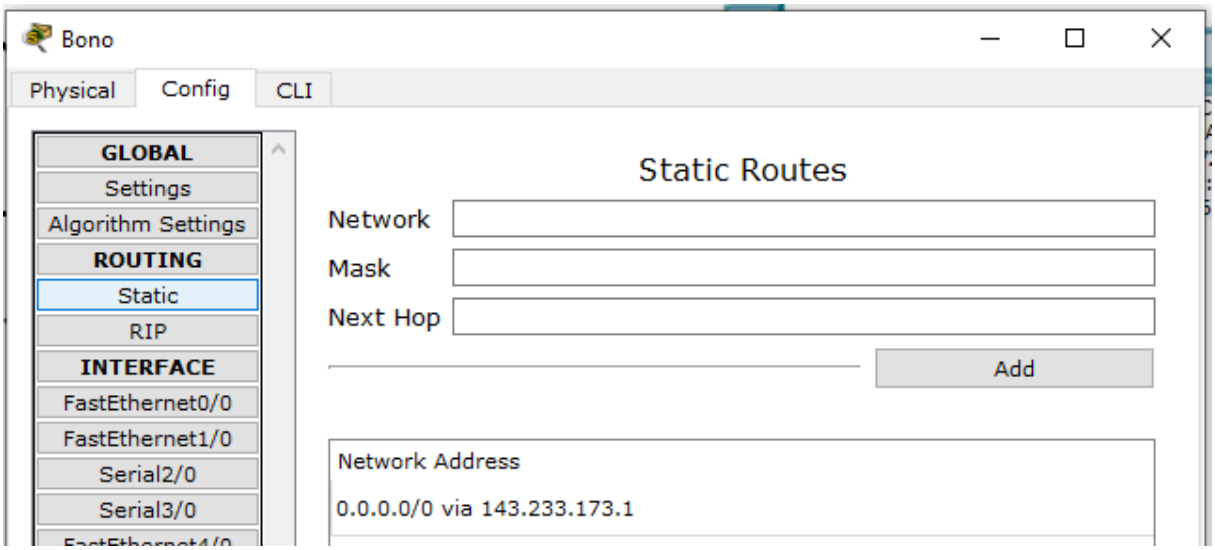
Bono's neighbors can be found with the #show ip neighbor command:



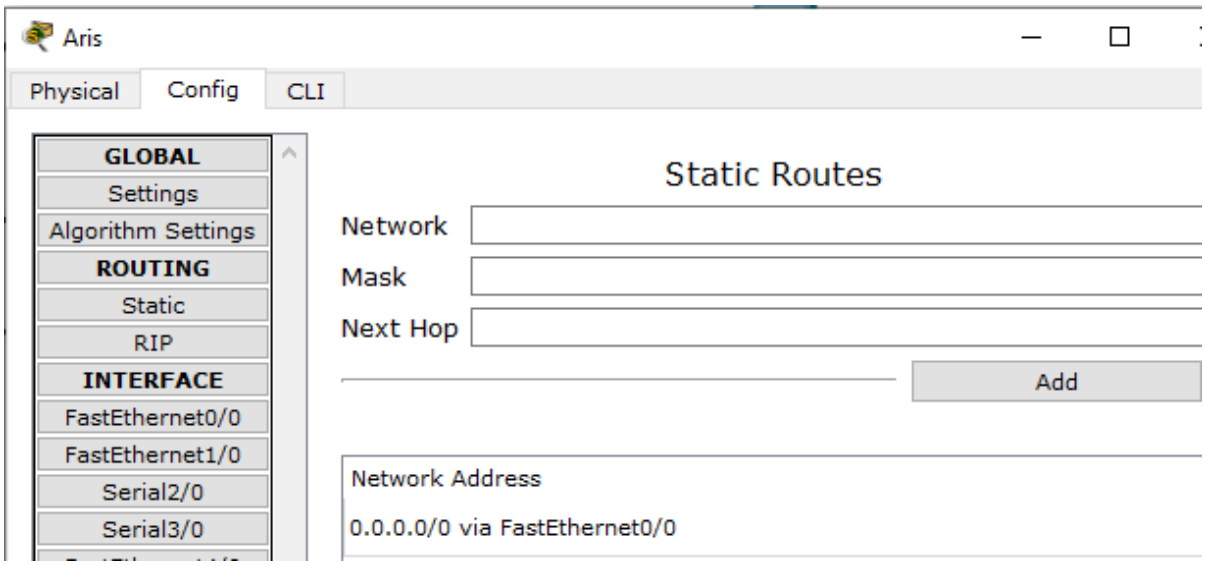
The #show ip ospf command in Bono:

```
Router#show ip ospf
 Routing Process "ospf 500" with ID 172.16.128.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 1. Checksum Sum 0x00fc95
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 3
        Area has no authentication
        SPF algorithm executed 4 times
        Area ranges are
        Number of LSA 3. Checksum Sum 0x024dbd
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Static routing to the web is achieved by using the command #ip route as follows:

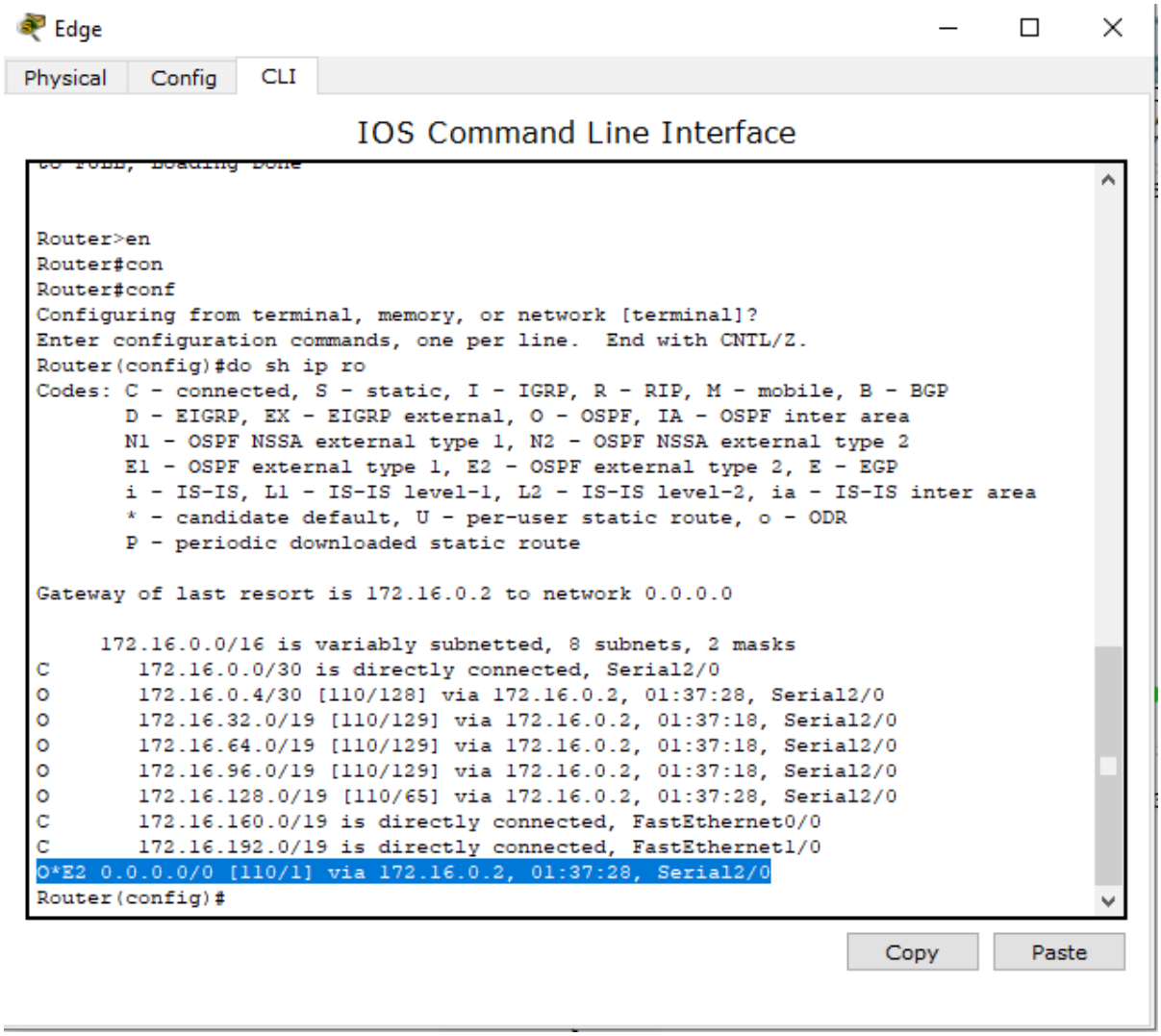


This way I define a (default-path) path that accepts any Subnet with any mask that if not in the routing table is forwarded to the gateway with IP 143.233.173.1



While the reverse procedure is followed with the Aris router.

Finally, if we give some time to run our OSPF network we will notice that the default router address will have been added to each of my routers.



Extra tests:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	A	Edge	ICMP		0.000	N	1	(edit)	
	Successful	C	A	ICMP		0.000	N	2	(edit)	
	Successful	F	D	ICMP		0.000	N	3	(edit)	
	Successful	Edge	E	ICMP		0.000	N	4	(edit)	

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	B	Internett	ICMP		0.000	N	0
	Successful	C	Internett	ICMP		0.000	N	1
	Successful	Internett	B	ICMP		0.000	N	2
	Successful	Internett	F	ICMP		0.000	N	3

Question 3º

All stations in the topology must have access to the HTTP service served by a server on the Internet. They do not have access to any other Internet service.

To achieve the result of query 3, we need to create an access list that only allows access to the HTTP service and denies all other network services.

An access list, also known as an ACL, is a set of rules or filters used to determine whether network traffic should be allowed or denied. Access lists are commonly used in computer networks to filter incoming and outgoing traffic based on various criteria, such as IP address, protocol type, and port number. They can be configured on routers, switches and firewalls to provide security and control the flow of network traffic. Access lists can also be used to prioritise traffic, limit bandwidth usage and prevent denial of service attacks.

TCP is widely used to transmit data over the Internet and other computer networks, such as email, web browsing, file transfer, and other applications that require reliable data transfer.

To achieve this result we enter the Bono CLI and type #access-list 121 deny tcp any any eq ?

```
Router(config)#access-list 121 deny tcp any any eq ?
  <0-65535>  Port number
  ftp        File Transfer Protocol (21)
  pop3       Post Office Protocol v3 (110)
  smtp       Simple Mail Transport Protocol (25)
  telnet     Telnet (23)
  www        World Wide Web (HTTP, 80)
```

After reading what options we can register we will deny the ftp,pop3,smtp,telnet and permit www.

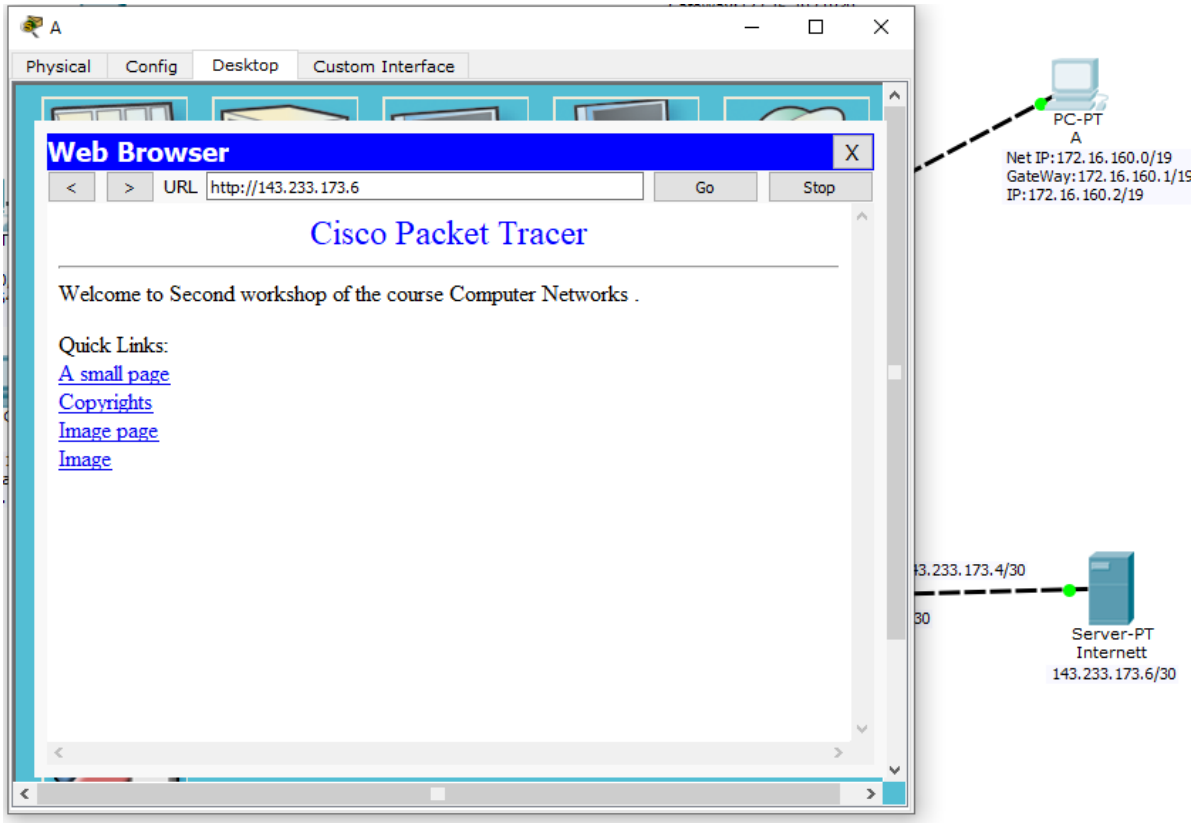
Using the command #sh access-lists 121 we can view our list.

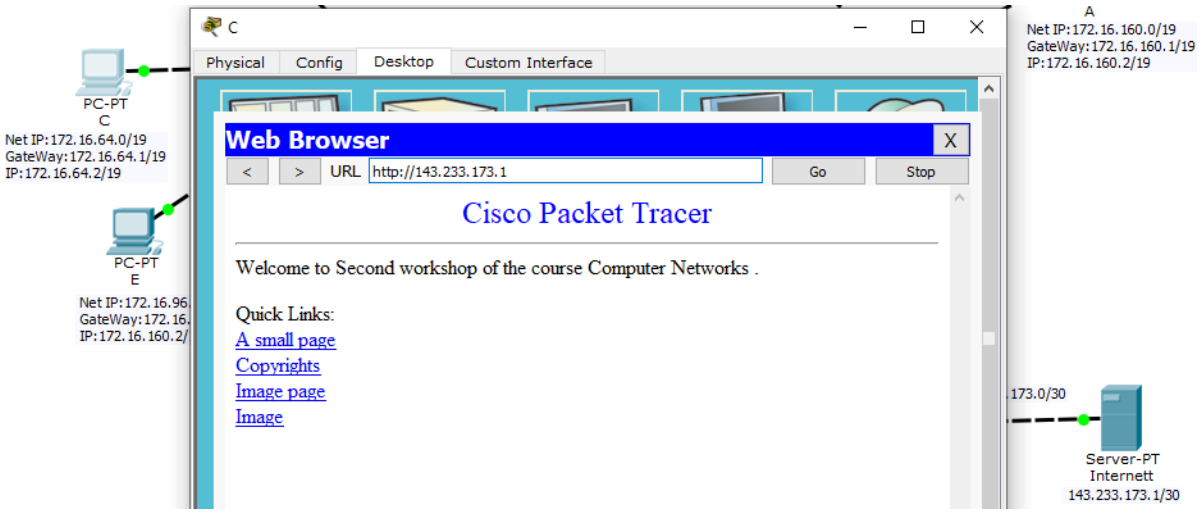
```
Router#sh access-lists 121
Extended IP access list 121
    deny tcp any any eq ftp
    deny tcp any any eq smtp
    deny tcp any any eq telnet
    deny tcp any any eq pop3
    permit tcp any any eq www (5 match(es))
    permit ip any any (4 match(es))
```

To apply the list we will type the following:

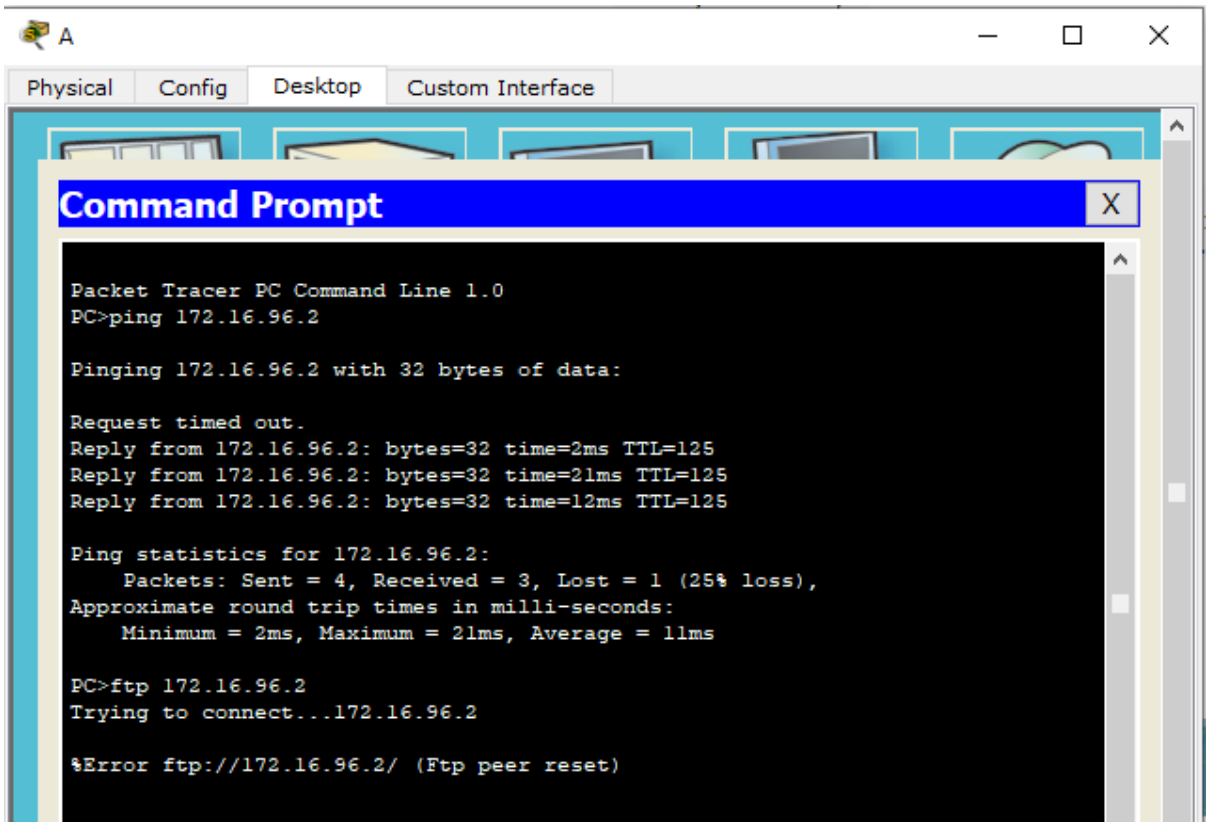
```
Router(config)#interface fastEthernet 1/0
Router(config-if)#ip
Router(config-if)#ip acc
Router(config-if)#ip access-group 121 out
```

Finally, we will test from the web browser of computers A and C.





Below we will run the #ping command from computer A to computer E.



Question 4ο

The networks on the Hermes router are accessible to all other stations in the topology only when using the ping and traceroute tools.

To implement the above query we will construct a second access list which we will apply to the serial2/0 interface connected to the Hermes router. We can apply the list to either the Bono or Hermes router.For security reasons and to prevent packets from circulating through the network
we'll apply it to Hermes.

```
Extended IP access list 121
    10 permit icmp any any
    20 deny ip any any
```

```
Router(config)#interface Serial2/0
Router(config-if)#ip acc
Router(config-if)#ip access-group 121 out
Router(config-if)#no ip access-group 122 out
Router(config-if)#do wr
Building configuration...
```

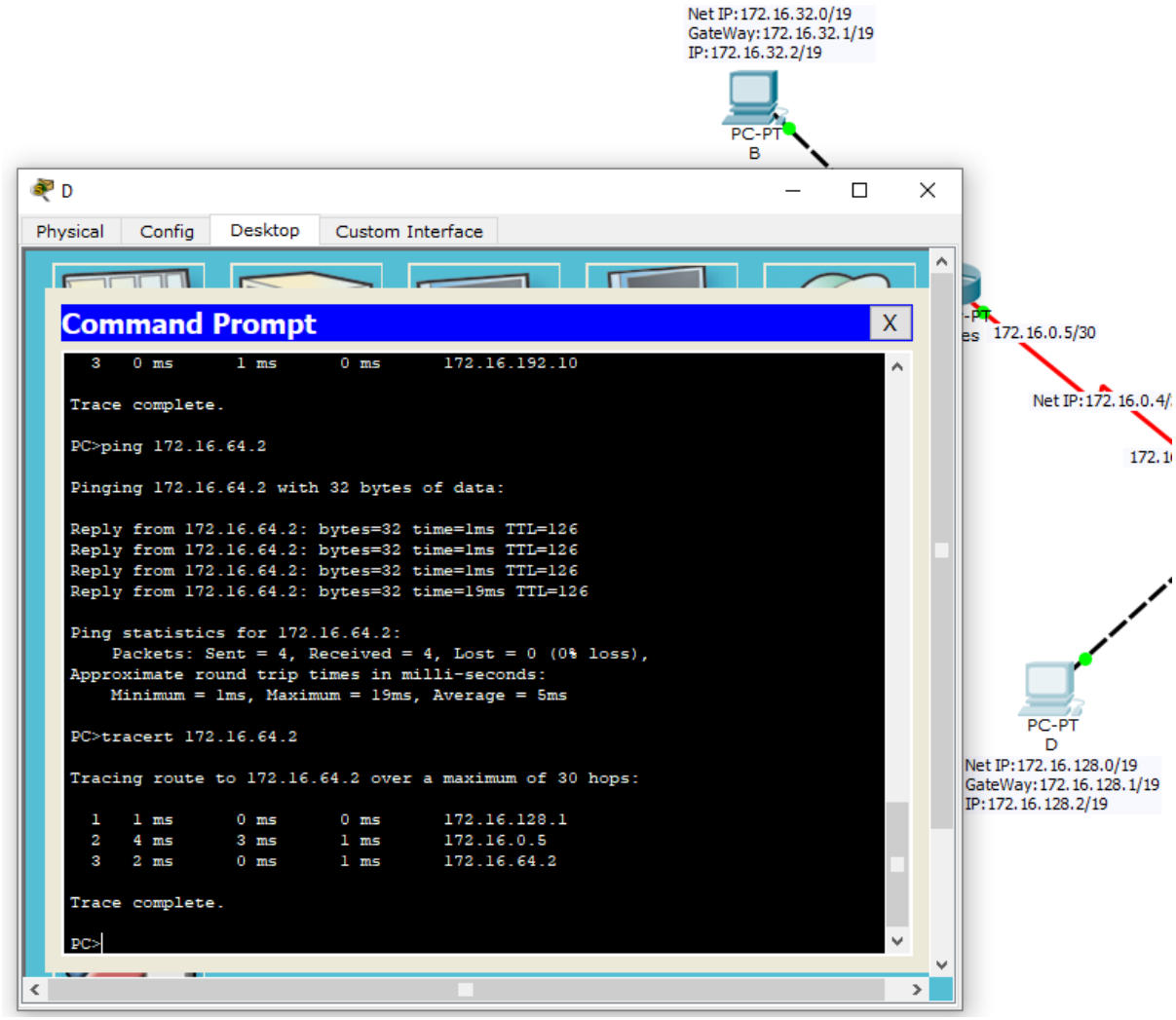
The access control entry #permit icmp any any allows Internet Control Message Protocol (ICMP) messages to be sent over the network from any source to any destination.

ICMP is a network protocol used to report errors and provide diagnostic information about IP network problems. Some common uses of ICMP include the "ping" command, which sends an ICMP echo request to check network connectivity, and the "traceroute" command, which uses ICMP packets to trace the path that packets take through the network.

The access control entry #deny ip any any denies all IP traffic from any source to any destination. This rule effectively prevents all IP traffic from passing through the network.

Denying all IP traffic in this way can be useful for testing or for implementing a security policy where all traffic is denied by default and only certain types of traffic are explicitly allowed. However, in practice, blocking all IP traffic can render the network unusable, as most network services and applications rely on IP for communication.

With the commands #ping & #tracert we can verify that the networks on the router are accessible to all other stations, as in the example below:



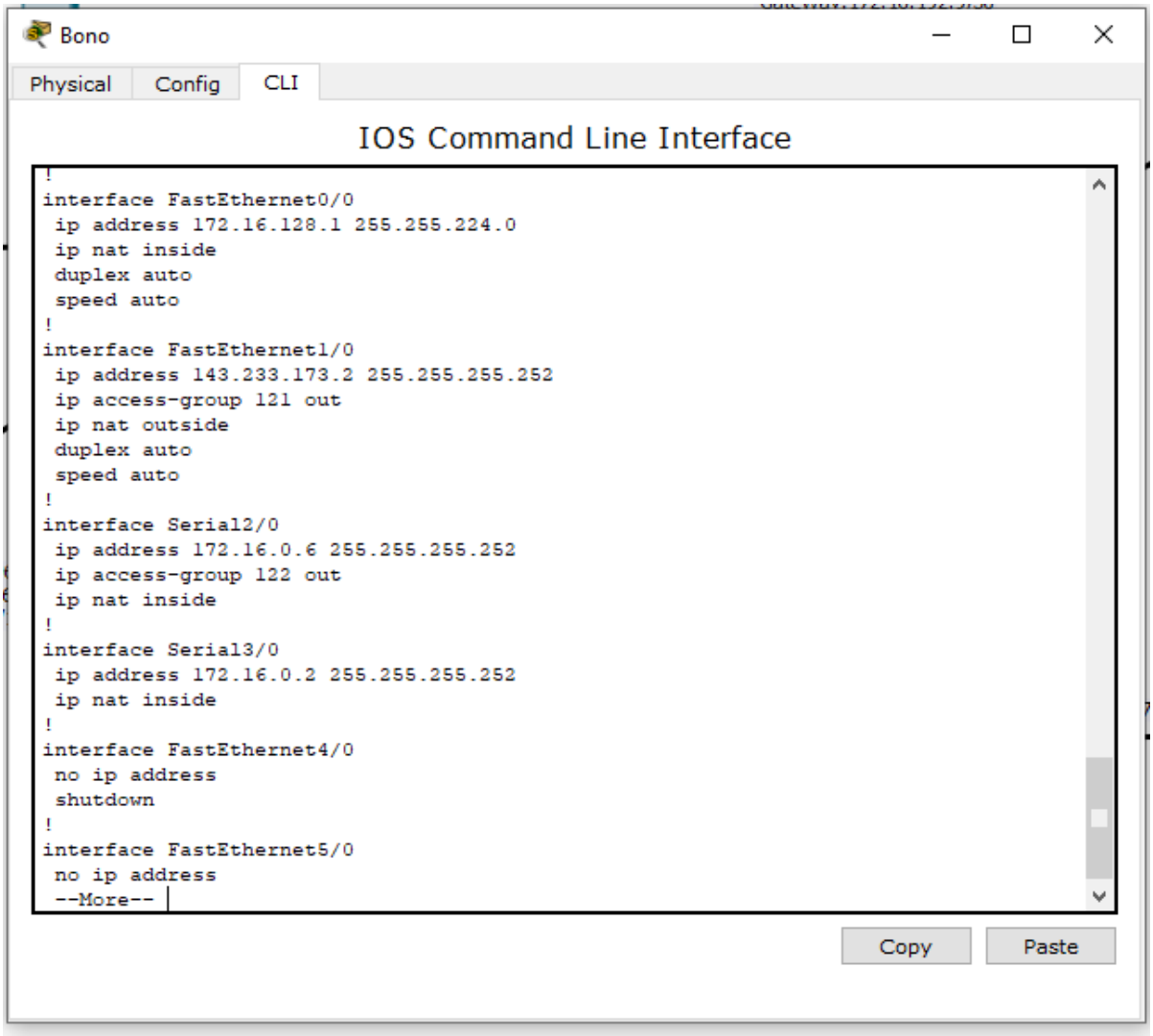
Question 5º

On Bono it is necessary to implement the overloaded NAT (PAT) technique with an overloaded public IP of 143.233.173.2/30.

First we will define which part of the subnet is internal and which is external. As you will see in the following picture, we will consider the networks that leave the Bono router as external networks.

Inside each Bono interface using the #ip nat outside or #ip nat inside command we will define the inner and outer part of my network. Command #do

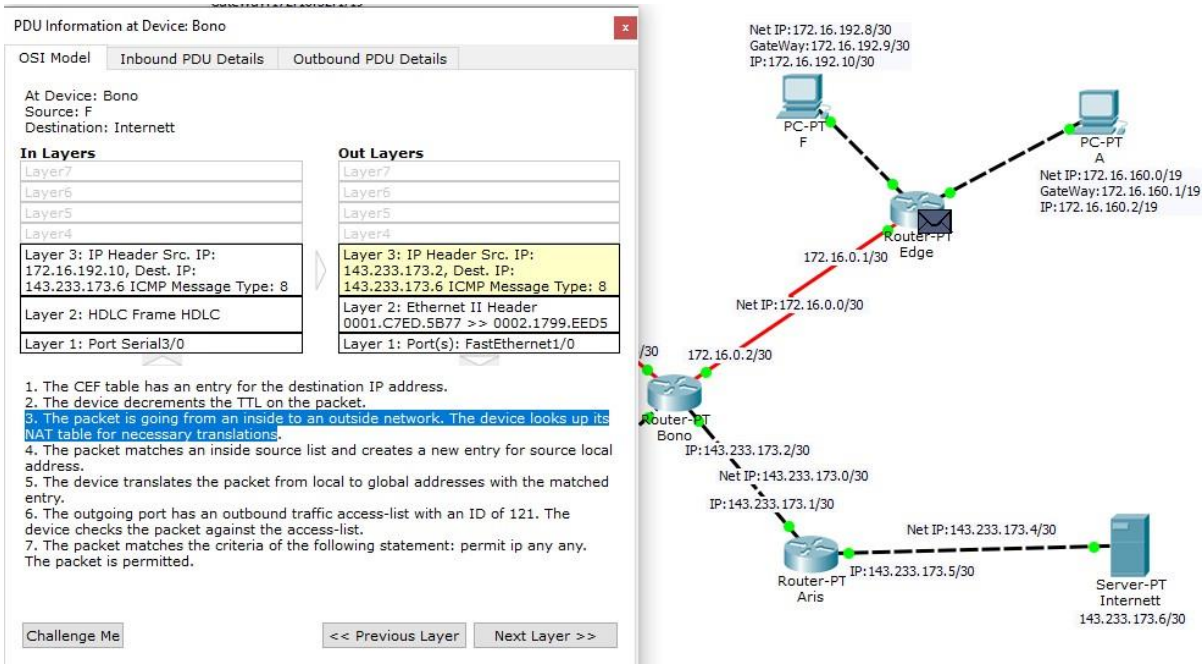
show run to Bono:



Then using a standard access list we will group the internal networks and give it the following command to achieve IP conversion.

```
Standard IP access list 2
    10 permit 172.16.0.0 0.0.255.255
Router#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip nat inside source list 2 interface fastEthernet 1/0 overload
Router(config)#do wr
```

Running a test from a computer to the server. From the simulation of the program we are able to see in the following picture the IP conversion that is done.



Finally, using the #show ip nat statistics and #show ip nat transactions commands we will display the following information:

#show ip nat statistics :

```
Router#show ip nat statistics
Total translations: 5 (0 static, 5 dynamic, 5 extended)
Outside Interfaces: FastEthernet1/0
Inside Interfaces: FastEthernet0/0 , Serial2/0 , Serial3/0
Hits: 18  Misses: 70
Expired translations: 32
Dynamic mappings:
```

The #show ip nat transactions describes the translations it has made:

```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 143.233.173.2:1025 172.16.160.2:1025  143.233.173.6:80   143.233.173.6:80
```

Here describes that the server externally and internally is described by 143. 233.173.6 while the local internal network is described by 143.233.173.2.Finally, globally translates to 143.233.173.2 and gets the same port number 1025 as it has internally.

The #show ip nat statistics command displays statistics about the network address translation (NAT) process on a Cisco router. NAT is a process of modifying the IP addresses and/or port numbers in the IP header of a packet to allow traffic to flow between networks that use private IP address ranges and the public Internet that uses globally routable IP addresses. The output of this command includes various statistics related to the NAT process, such as the number of translated packets, the number of translation failures, the success rate for the NAT translation cache, and more. This information can be useful for troubleshooting NAT-related problems and for monitoring the performance of the NAT process on a router.

The #show ip nat transactions command is used to display the NAT translations that are currently active on a Cisco router. It provides information about the source IP address, destination IP address, protocol, and NAT translation type (static or dynamic).This command can be useful for troubleshooting NAT-related problems, as it shows which translations are currently in use and how traffic is being translated. It can also be used to monitor NAT usage and to determine if there are any potential performance or security issues that need to be addressed.

Extras:

Μάσκες

MASK, PREFIX		MASK, PREFIX		MASK, PREFIX		MASK, PREFIX	
128.0.0.0	/1	255.128.0.0	/9	255.255.128.0	/17	255.255.255.128	/25
192.0.0.0	/2	255.192.0.0	/10	255.255.192.0	/18	255.255.255.192	/26
224.0.0.0	/3	255.224.0.0	/11	255.255.224.0	/19	255.255.255.224	/27
240.0.0.0	/4	255.240.0.0	/12	255.255.240.0	/20	255.255.255.240	/28
248.0.0.0	/5	255.248.0.0	/13	255.255.248.0	/21	255.255.255.248	/29
252.0.0.0	/6	255.252.0.0	/14	255.255.252.0	/22	255.255.255.252	/30
254.0.0.0	/7	255.254.0.0	/15	255.255.254.0	/23	255.255.255.254	/31
255.0.0.0	/8	255.255.0.0	/16	255.255.255.0	/24	255.255.255.255	/32

DEC	BIN
128	10000000
192	11000000
224	11100000
240	11110000
248	11111000
252	11111100
254	11111110
255	11111111

Popular Tools

- ping will send a series of ICMP echo requests to the target device and report the results.
- Traceroute is similar to ping, but it shows the path that packets take to reach the target device.

Other popular tools:

1. Nslookup/dig - these tools allow you to lookup DNS information for a domain name or IP address.
2. Netstat - displays the active network connections and their status.
3. Telnet/ssh - used for remote access to a server or network device.
4. Ftp/sftp - used for transferring files over a network.
5. Tcpdump - logs and analyzes network traffic.
6. Wireshark - a network protocol analyzer that allows you to see detailed information about network traffic.
7. Nmap - a tool used for network discovery and security auditing.
8. Iperf - used for testing and measuring network performance.

Wildcard mask calculation

The wildcard mask for the 255.255.255.252 subnet mask is 0.0.0.3. The wildcard mask is the inverse of the subnet mask, where any digit set to 1 in the subnet mask is set to 0 in the wildcard mask and vice versa.

To understand why the wildcard mask for 255.255.255.252 is 0.0.0.3, you can convert the subnet mask and wildcard mask to binary:

Subnet mask: 11111111111111111111111111111100

Wildcard mask: 00000000 00000000 00000000 00000011

As you can see, bits that are set to 1 in the subnet mask are set to 0 in the wildcard mask and vice versa.