

**ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ**  
**ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ**  
**ΠΜΣ «Πληροφορική»**

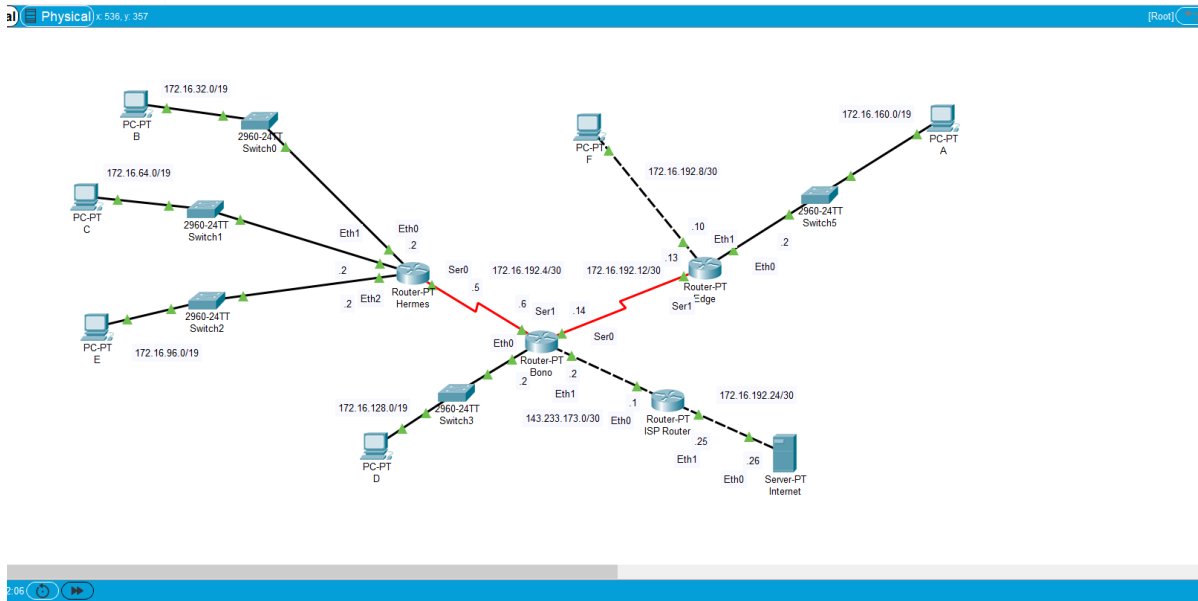


**Εργασία Μαθήματος**  
**«Δίκτυα Υπολογιστών»**

<b>2<sup>ο</sup> Εργαστήριο: Δυναμική Δρομολόγηση - Λίστες Ελέγχου - NAT</b>	
Όνομα φοιτητή – Αρ. Μητρώου	Μαρία Αμοργιανού
	ΜΠΠΛ2205
Ημερομηνία παράδοσης	21/2/2024

1)

Παρακάτω παρουσιάζεται η ζητούμενη τοπολογία. Για την υλοποίηση της χρησιμοποιήσα την έκδοση Packet Tracer 7.2.2.0418.



Εικόνα 1: Τοπολογία

Στο συγκεκριμένο δίκτυο υπάρχουν 4 δρομολογητές τους οποίους ονόμασα Hermes, Bono, Edge και ο ISP Router. Ο Hermes συνδέεται με 3 υποδίκτυα: 172.16.32.0/19, 172.16.64.0/19, 172.16.96.0/19, το κάθε υποδίκτυο έχει τους ακόλουθους υπολογιστές: B, C και E, στους οποίους έχουν ανατεθεί κάποιες διευθύνσεις IP. Αντίστοιχα, ο Edge συνδέεται με 2 υποδίκτυα: 172.16.192.8/30 και 172.16.160.0/19, το κάθε υποδίκτυο έχει τους ακόλουθους υπολογιστές: A και F και στους οποίους έχουν ανατεθεί κάποιες διευθύνσεις IP. Το ίδιο και για τον Bono δρομολογητή όπου έχει το ακόλουθο υποδίκτυο 172.16.128.0/19 που περιλαμβάνει τον D υπολογιστή και το υποδίκτυο 143.233.173.0/30 που ενώνεται με έναν ακόμα δρομολογητή τον ISP Router και ο οποίος περιλαμβάνει το δίκτυο 172.16.192.24/30 το οποίο ενώνεται με το Internet (έτσι γίνεται καλύτερα και η προσομοίωση του Internet). Επιπλέον πρόσθεσα κάποια υποδίκτυα για να ενώσω τους

δρομολογητές μεταξύ τους Hermes – Bono: 172.16.192.4/30 και Bono – Edge: 172.16.192.12/30 (η επιλογή έγινε κατά κάποιον τρόπο τυχαία με βάση τα μη χρησιμοποιημένα δίκτυα της τοπολογίας μου). Παρακάτω παραθέτω κάποια στοιχεία των υποδικτύων:

Για το δίκτυο 172.16.32.0/19 όπου περιλαμβάνει έναν υπολογιστή τον B: έχουμε τα ακόλουθα:

Mask: 255.255.224.0 αλλιώς 11111111.11111111.11100000.00000000

Prefix: 19

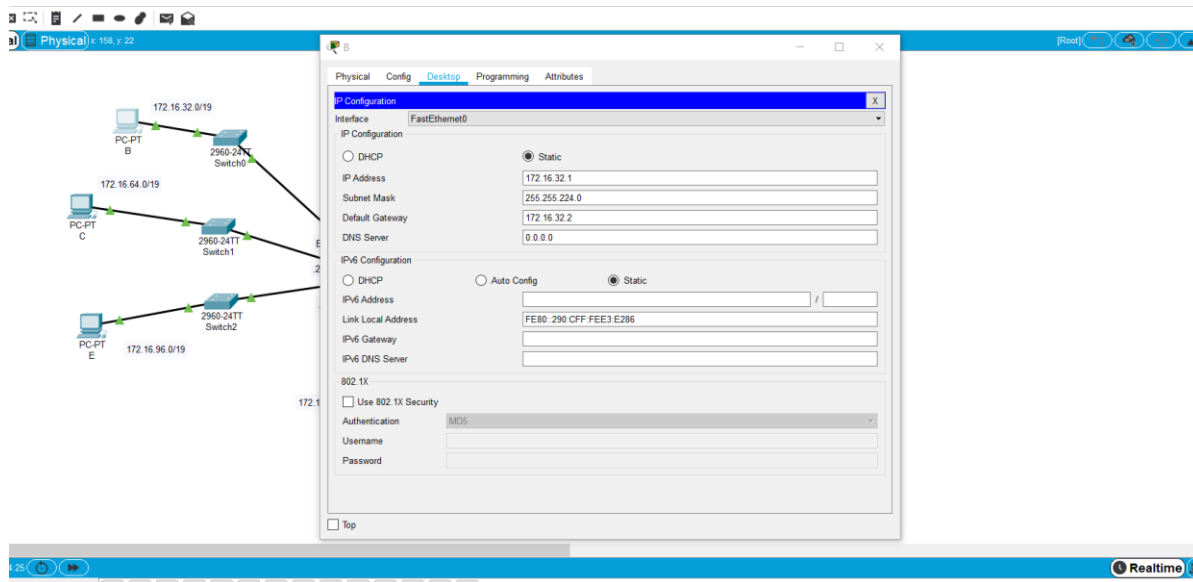
Πλήθος IP διευθύνσεων (Host IPs):  $2^{13} - 2 = 8192 - 2 = 8190$

IP δικτύου: 172.16.32.0

1<sup>η</sup> διαθέσιμη: 172.16.32.1

Τελευταία διαθέσιμη: 172.16.63.254

BC: 172.16.63.255



Εικόνα 2: PC - B

Για το δίκτυο 172.16.64.0/19 όπου περιλαμβάνει έναν υπολογιστή τον C: έχουμε τα ακόλουθα:

Mask: 255.255.224.0 αλλιώς 11111111.11111111.11100000.00000000

Prefix: 19

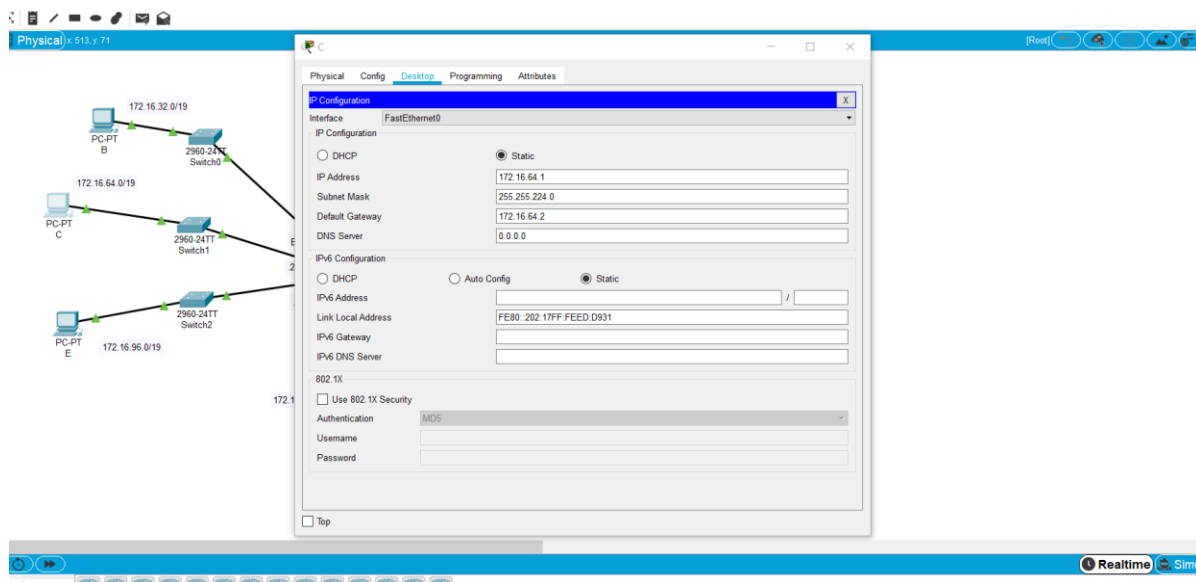
Πλήθος IP διευθύνσεων (Host IPs):  $2^{13} - 2 = 8192 - 2 = 8190$

IP δικτύου: 172.16.64.0

1<sup>η</sup> διαθέσιμη: 172.16.64.1

Τελευταία διαθέσιμη: 172.16.95.254

BC: 172.16.95.255



Εικόνα 3: PC - C

Για το δίκτυο 172.16.96.0/19 όπου περιλαμβάνει έναν υπολογιστή τον E: έχουμε τα ακόλουθα:

Mask: 255.255.224.0 αλλιώς 11111111.11111111.11100000.00000000

Prefix: 19

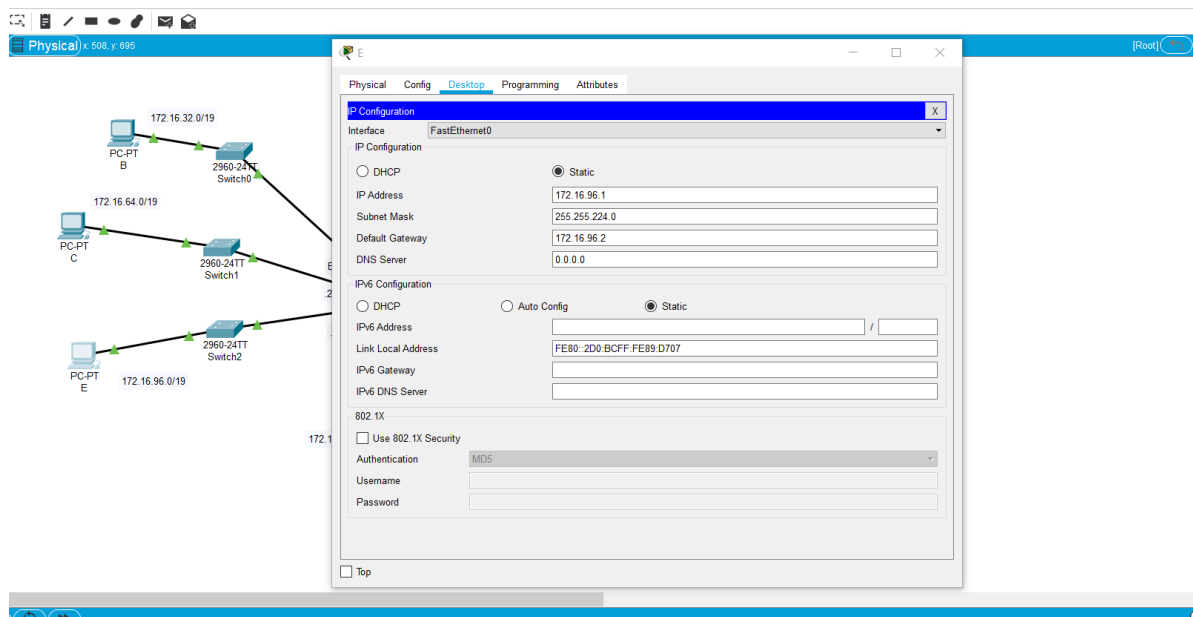
Πλήθος IP διευθύνσεων (Host IPs):  $2^{13} - 2 = 8192 - 2 = 8190$

IP δικτύου: 172.16.96.0

1<sup>η</sup> διαθέσιμη: 172.16.96.1

Τελευταία διαθέσιμη: 172.16.127.254

BC: 172.16.127.255



Εικόνα 4: PC - E

Για το δίκτυο 172.16.160.0/19 όπου περιλαμβάνει έναν υπολογιστή τον A: έχουμε τα ακόλουθα:

Mask: 255.255.224.0 αλλιώς 11111111.11111111.11100000.00000000

Prefix: 19

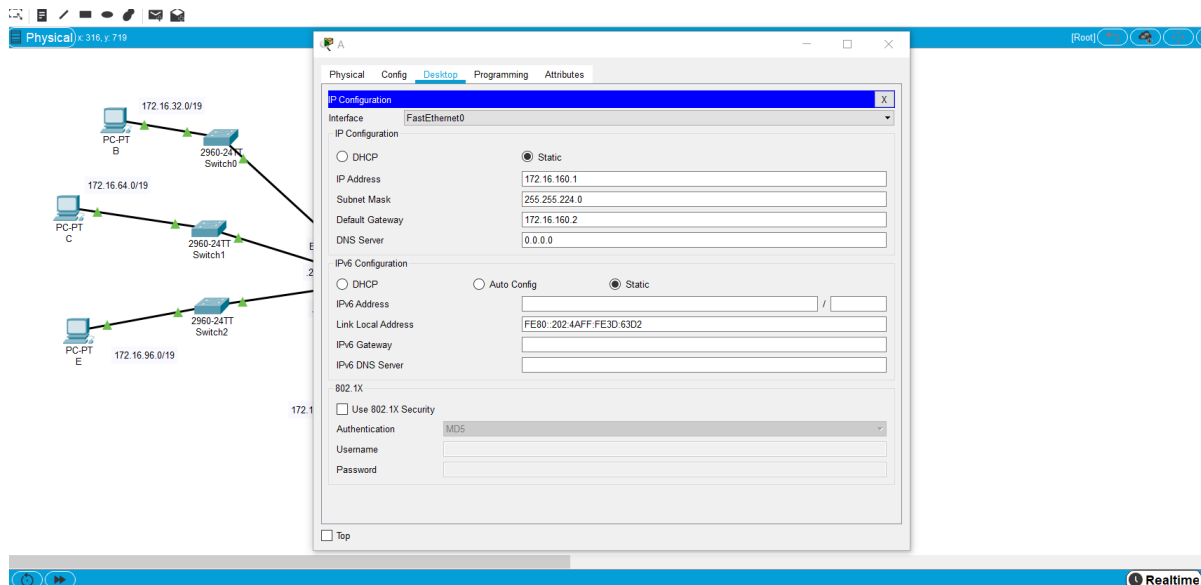
Πλήθος IP διευθύνσεων (Host IPs):  $2^{13} - 2 = 8192 - 2 = 8190$

IP δικτύου: 172.16.160.0

1<sup>η</sup> διαθέσιμη: 172.16.160.1

Τελευταία διαθέσιμη: 172.16.191.254

BC: 172.16.191.255



Εικόνα 5: PC - A

Για το δίκτυο 172.16.192.8/30 όπου περιλαμβάνει έναν υπολογιστή τον F: έχουμε τα ακόλουθα:

Mask: 255.255.255.252 αλλιώς 11111111.11111111.11111111.11111100

Prefix: 30

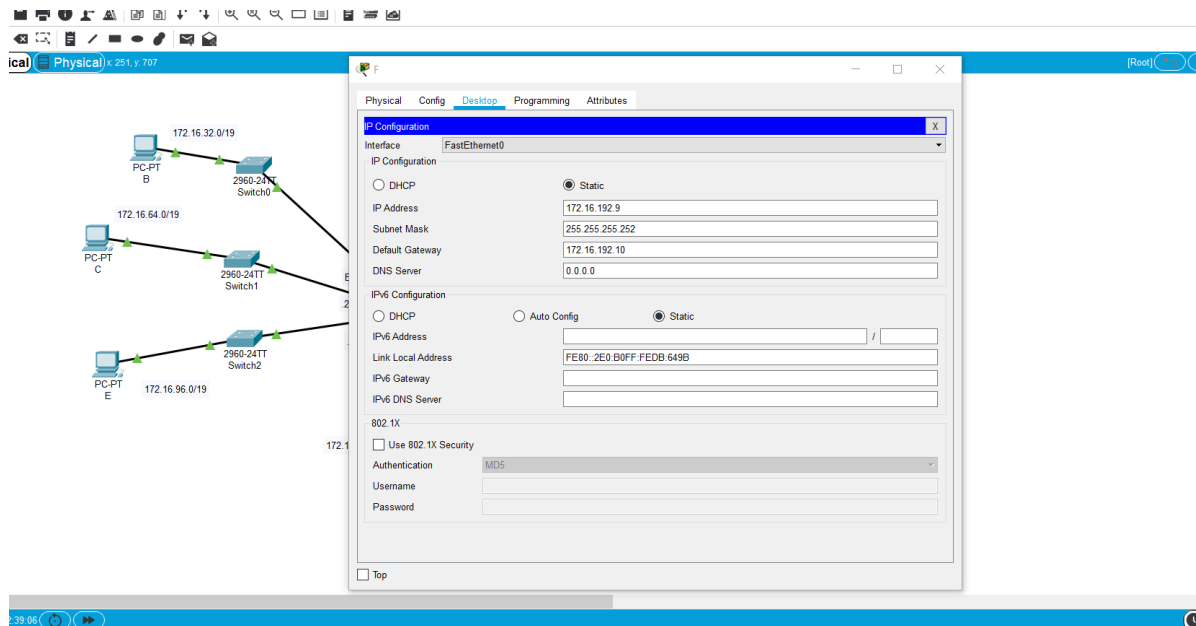
Πλήθος IP διευθύνσεων (Host IPs):  $2^2 - 2 = 4 - 2 = 2$

IP δικτύου: 172.16.192.8

1<sup>η</sup> διαθέσιμη: 172.16.192.9

Τελευταία διαθέσιμη: 172.16.192.10

BC: 172.16.192.11



Εικόνα 6: PC - F

Για το δίκτυο 172.16.128.0/19 όπου περιλαμβάνει έναν υπολογιστή τον D: έχουμε τα ακόλουθα:

Mask: 255.255.224.0 αλλιώς 11111111.11111111.11100000.00000000

Prefix: 19

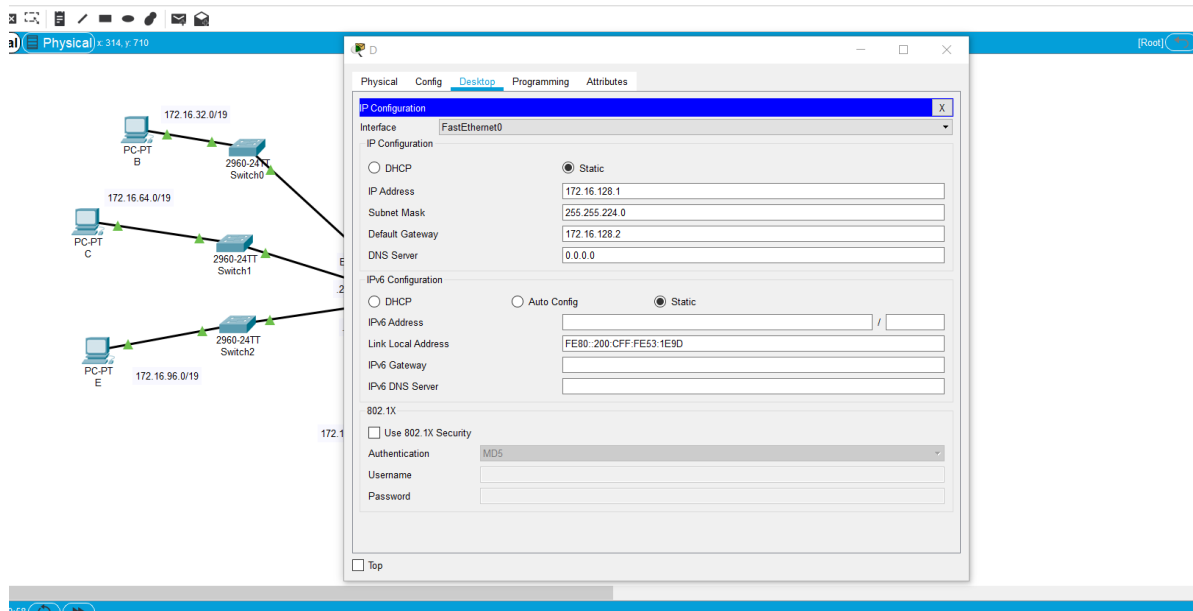
Πλήθος IP διευθύνσεων (Host IPs):  $2^{13} - 2 = 8192 - 2 = 8190$

IP δικτύου: 172.16.128.0

1<sup>η</sup> διαθέσιμη: 172.16.128.1

Τελευταία διαθέσιμη: 172.16.159.254

BC: 172.16.159.255



Εικόνα 7: PC - D

Για το δίκτυο 143.233.173.0/30 όπου συνδέει τον Βοηό με τον ISP Router έχουμε τα ακόλουθα:

	DEC	BIN
<b>Μάσκα</b>	255.255.255.252	11111111.11111111.11111111.11111100
<b>Διεύθυνση IP</b>	143.233.173.2	10001111.11101001.10101101.00000010
<b>IP δικτύου</b>	143.233.173.0	10001111.11101001.10101101.00000000

Mask: 255.255.255.252 αλλιώς 11111111.11111111.11111111.11111100

Prefix: 30

Πλήθος IP διευθύνσεων (Host IPs):  $2^2 - 2 = 4 - 2 = 2$

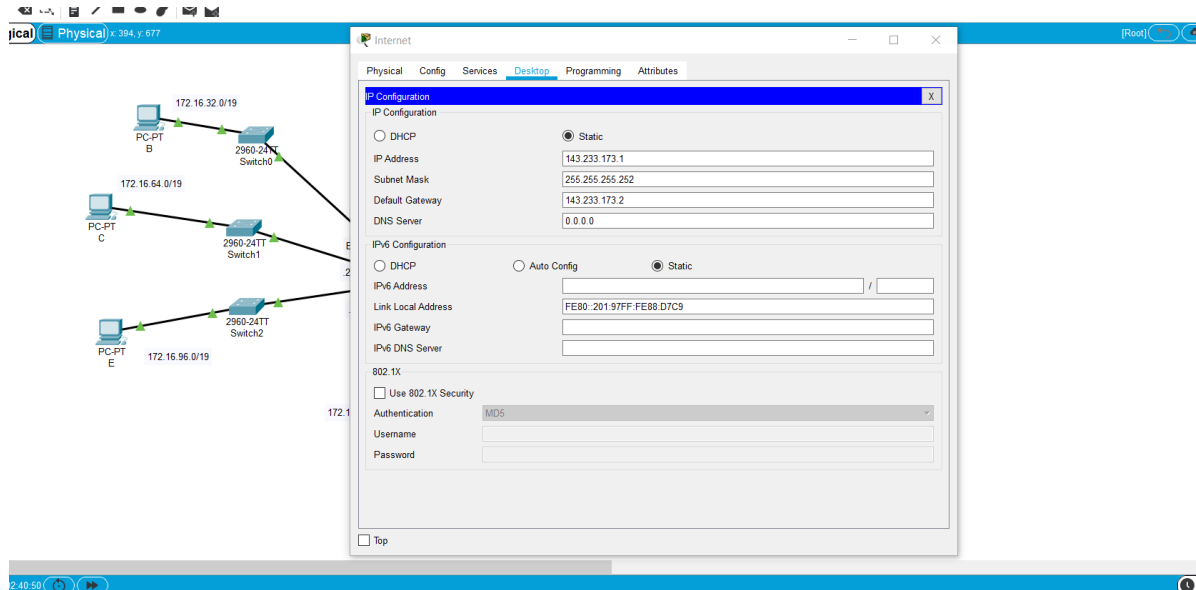
IP δικτύου: 143.233.173.0

1<sup>η</sup> διαθέσιμη: 143.233.173.1

Τελευταία διαθέσιμη: 143.233.173.2



BC: 143.233.173.3



Εικόνα 8: Σύνδεση Bono με ISP Router

Για το δίκτυο 172.16.192.24/30 που συνδέει το ISP Router με το Internet έχουμε τα ακόλουθα:

Mask: 255.255.255.252 αλλιώς 11111111.11111111.11111111.11111100

Prefix: 30

Πλήθος IP διευθύνσεων (Host IPs):  $2^2 - 2 = 4 - 2 = 2$

IP δικτύου: 172.16.192.24

1<sup>η</sup> διαθέσιμη: 172.16.192.25

Τελευταία διαθέσιμη: 172.16.192.26

BC: 172.16.192.27

Για το δίκτυο 172.16.192.4/30 που συνδέει το Hermes με τον Βοηό έχουμε τα ακόλουθα:

Mask: 255.255.255.252 αλλιώς 11111111.11111111.11111111.11111100

Prefix: 30

Πλήθος IP διευθύνσεων (Host IPs):  $2^2 - 2 = 4 - 2 = 2$

IP δικτύου: 172.16.192.4

1<sup>η</sup> διαθέσιμη: 172.16.192.5

Τελευταία διαθέσιμη: 172.16.192.6

BC: 172.16.192.7

Για το δίκτυο 172.16.192.12/30 που συνδέει το Βοηό με τον Edge έχουμε τα ακόλουθα:

Mask: 255.255.255.252 αλλιώς 11111111.11111111.11111111.11111100

Prefix: 30

Πλήθος IP διευθύνσεων (Host IPs):  $2^2 - 2 = 4 - 2 = 2$

IP δικτύου: 172.16.192.12

1<sup>η</sup> διαθέσιμη: 172.16.192.13

Τελευταία διαθέσιμη: 172.16.192.14

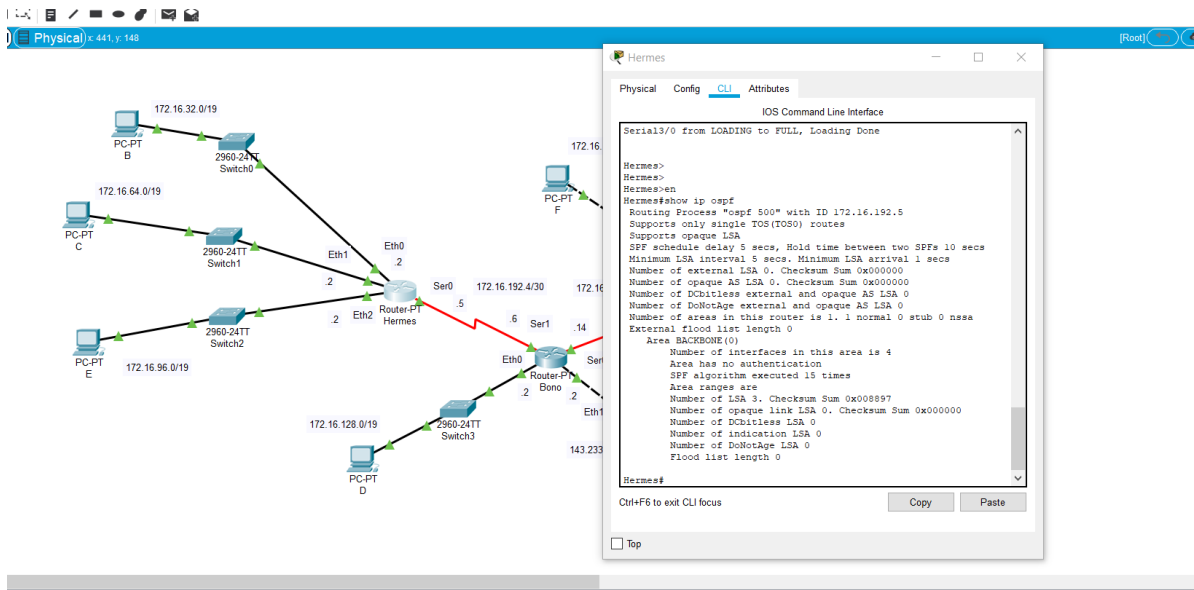
BC: 172.16.192.15

2)

Παρακάτω παρουσιάζονται στιγμιότυπα οθόνης με τα αποτελέσματα εκτέλεσης των εντολών **show ip ospf** και **show ip ospf neighbor**. Σε γενικές γραμμές το αποτέλεσμα της εντολής **show ip ospf** παρέχει πληροφορίες για την κατάσταση του OSPF (Open Shortest Path First) στον δρομολογητή ενώ η έξοδος της εντολής **show ip ospf neighbor** παρέχει πληροφορίες σχετικά με τους γείτονες OSPF που έχει ο εκάστοτε δρομολογητής.

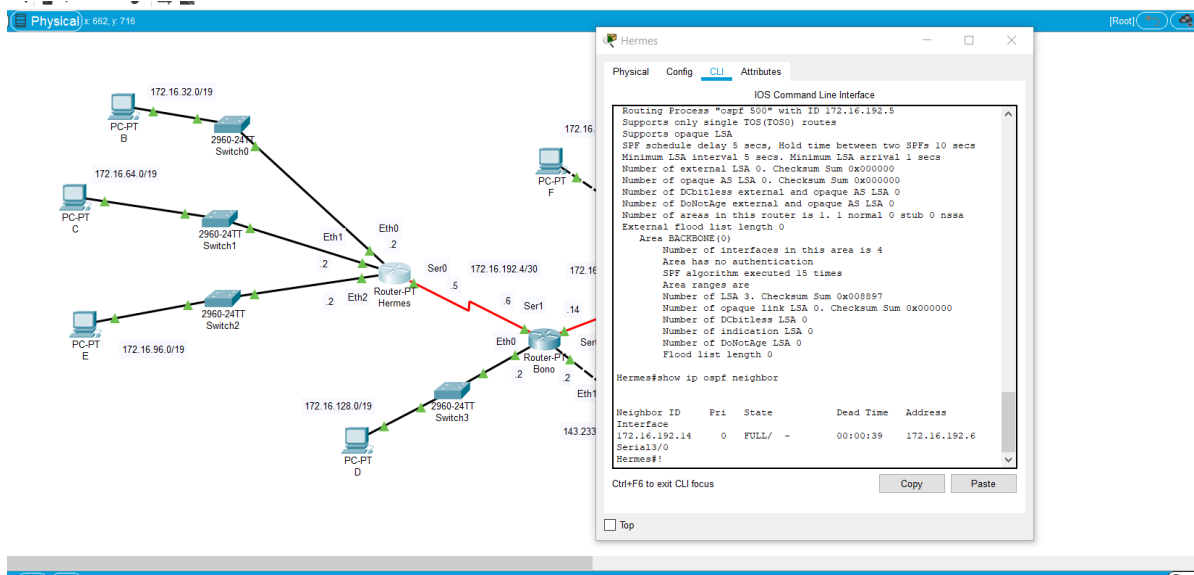
Για τον Hermes δρομολογητή εκτελώντας τις παραπάνω εντολές έχουμε τα ακόλουθα:

Αρχικά εκτελώντας την εντολή **show ip ospf** βλέπουμε από τα αποτελέσματα ότι ο δρομολογητής χρησιμοποιεί το OSPF με διεργασία OSPF 500 και Router ID 172.16.192.5, δηλώνοντας ότι υποστηρίζει μόνο μονοεπίπεδη (single TOS) δρομολόγηση και υποστηρίζει opaque LSA. Το χρονικό διάστημα καθυστέρησης για την εκτέλεση του SPF (Shortest Path First) είναι 5 secs και το χρονικό διάστημα που περιμένει μεταξύ δύο SPF είναι 10 secs. Τα ελάχιστα χρονικά διαστήματα για τη μεταφορά είναι 5 secs και την άφιξη των Link State Advertisements (LSA) είναι 1 secs. Επιπλέον εμφανίζεται ο αριθμός των εξωτερικών LSA όπου είναι 0, με τους υπολογισμούς checksum που πραγματοποιήθηκαν και είναι και αυτό 0. Παρουσιάζετε ο αριθμός των περιοχών OSPF που υποστηρίζονται στο δρομολογητή, με μια κανονική περιοχή και χωρίς stub ή NSSA περιοχές και τέλος βλέπουμε και το μήκος της λίστας εξωτερικών LSA, το οποίο είναι 0, υποδεικνύοντας ότι δεν υπάρχουν εξωτερικά LSA.



Εικόνα 9: Εκτελώντας την εντολή `show ip ospf` σε Hermes

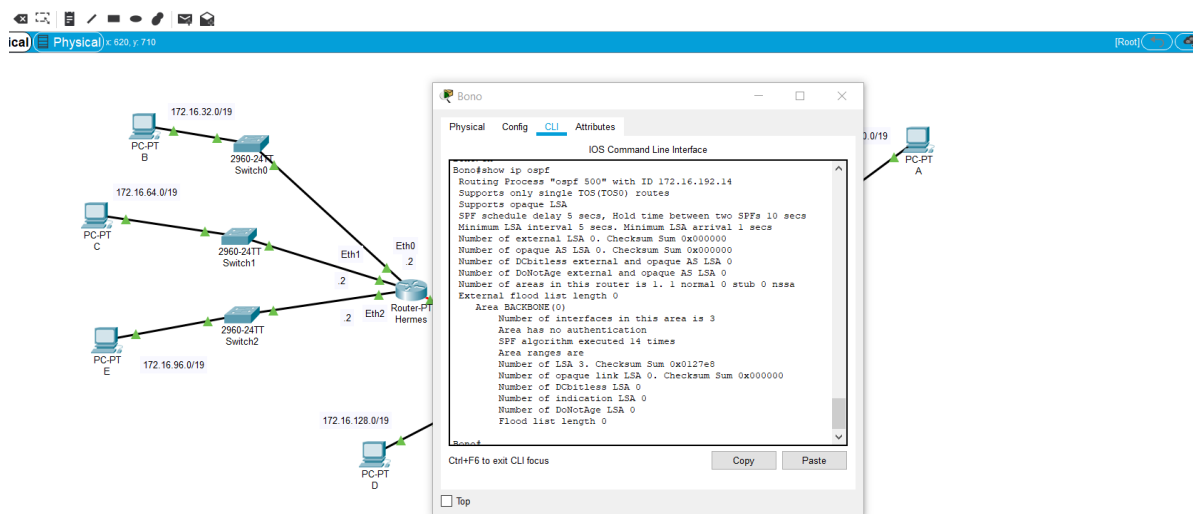
Εκτελώντας την εντολή **show ip ospf neighbor** παρατηρούμε ότι η διεύθυνση IP του γείτονα OSPF είναι η 172.16.192.14 και εμφανίζει και την προτεραιότητα του γείτονα OSPF όπου στην περίπτωση μας είναι 0. Σε αυτήν την περίπτωση, ο γείτονας είναι σε κατάσταση FULL, που σημαίνει ότι έχει επιτευχθεί πλήρης συμφωνία με το γείτονα. Ο χρόνος που απομένει μέχρι η σύνδεση με το γείτονα να θεωρηθεί "νεκρή" αν δεν ληφθούν ενημερώσεις OSPF από αυτόν είναι 00:00:29. Επιπλέον εμφανίζεται η διεύθυνση IP του γείτονα OSPF 172.16.192.6 και η διεπαφή μέσω της οποίας επικοινωνεί όπου είναι το Serial3/0.



Εικόνα 10: Εκτελώντας την εντολή `show ip ospf neighbor` σε Hermes

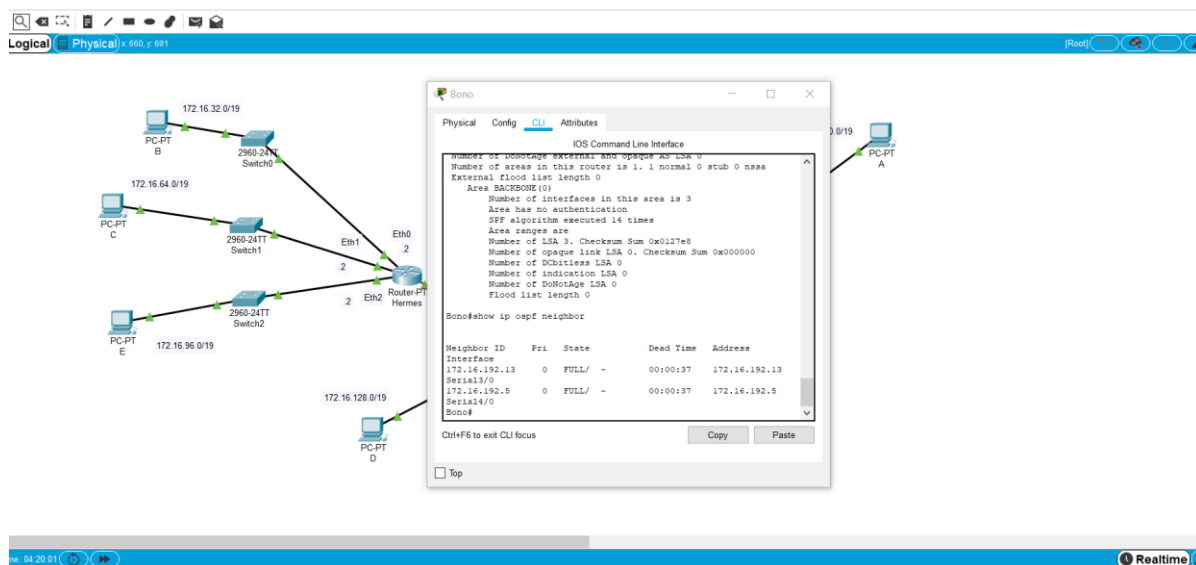
Για τον Βοπο δρομολογητή εκτελώντας τις παραπάνω εντολές έχουμε τα ακόλουθα:

Αρχικά εκτελώντας την εντολή **show ip ospf** βλέπουμε από τα αποτελέσματα ότι ο δρομολογητής χρησιμοποιεί το OSPF με διεργασία OSPF 500 και Router ID 172.16.192.14, δηλώνοντας ότι υποστηρίζει μόνο μονοεπίπεδη (single TOS) δρομολόγηση και υποστηρίζει opaque LSA. Το χρονικό διάστημα καθυστέρησης για την εκτέλεση του SPF (Shortest Path First) είναι 5 secs και το χρονικό διάστημα που περιμένει μεταξύ δύο SPF είναι 10 secs. Τα ελάχιστα χρονικά διαστήματα για τη μεταφορά είναι 5 secs και την άφιξη των Link State Advertisements (LSA) είναι 1 secs. Επιπλέον εμφανίζεται ο αριθμός των εξωτερικών LSA όπου είναι 0, με τους υπολογισμούς checksum που πραγματοποιήθηκαν και είναι και αυτό 0. Παρουσιάζετε ο αριθμός των περιοχών OSPF που υποστηρίζονται στο δρομολογητή, με μια κανονική περιοχή και χωρίς stub ή NSSA περιοχές και τέλος βλέπουμε και το μήκος της λίστας εξωτερικών LSA, το οποίο είναι 0, υποδεικνύοντας ότι δεν υπάρχουν εξωτερικά LSA.



Εικόνα 11: Εκτελώντας την εντολή `show ip ospf` σε Bono

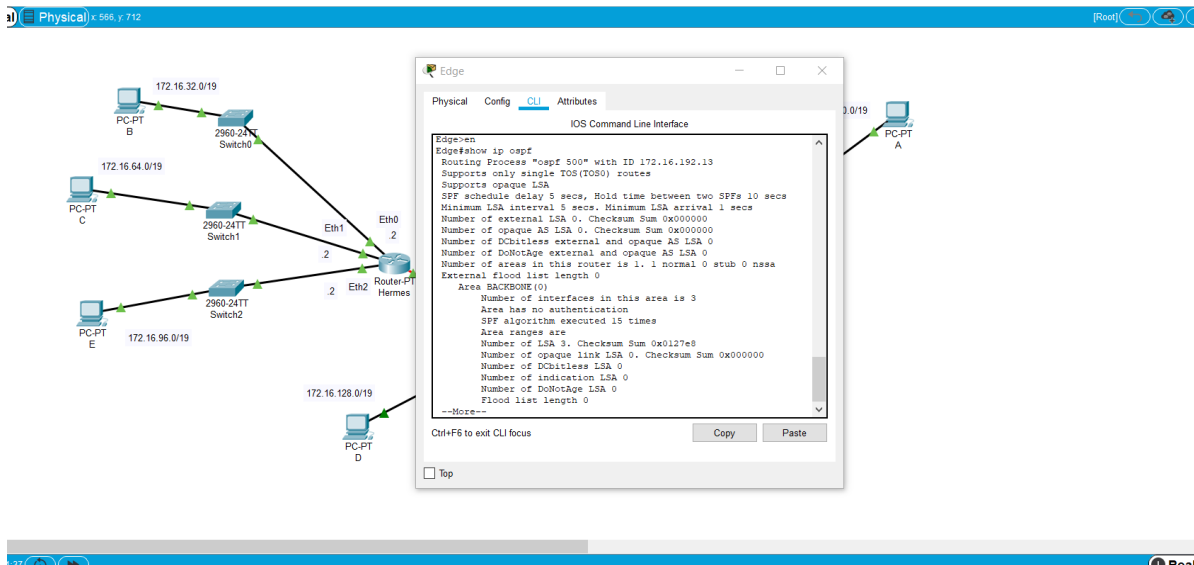
Εκτελώντας την εντολή **show ip ospf neighbor** παρατηρούμε ότι η διεύθυνση IP του γείτονα OSPF είναι η 172.16.192.13 και εμφανίζει και την προτεραιότητα του γείτονα OSPF όπου στην περίπτωση μας είναι 0. Σε αυτήν την περίπτωση, ο γείτονας είναι σε κατάσταση FULL, που σημαίνει ότι έχει επιτευχθεί πλήρης συμφωνία με το γείτονα. Ο χρόνος που απομένει μέχρι η σύνδεση με το γείτονα να θεωρηθεί "νεκρή" αν δεν ληφθούν ενημερώσεις OSPF από αυτόν είναι 00:00:39. Επιπλέον εμφανίζεται η διεύθυνση IP του γείτονα OSPF 172.16.192.13 και η διεπαφή μέσω της οποίας επικοινωνεί όπου είναι το Serial3/0. Επιπρόσθετα έχουμε ακόμα μια διεύθυνση IP του γείτονα OSPF την 172.16.192.5 με επίσης 0 προτεραιότητα. Σε αυτήν την περίπτωση, ο γείτονας είναι επίσης σε κατάσταση FULL, που σημαίνει ότι έχει επιτευχθεί πλήρης συμφωνία με το γείτονα. Ο χρόνος που απομένει μέχρι η σύνδεση με το γείτονα να θεωρηθεί "νεκρή" αν δεν ληφθούν ενημερώσεις OSPF από αυτόν είναι 00:00:38. Επιπλέον εμφανίζεται η διεύθυνση IP του γείτονα OSPF 172.16.192.5 και η διεπαφή μέσω της οποίας επικοινωνεί όπου είναι το Serial4/0.



Εικόνα 12: Εκτελώντας την εντολή `show ip ospf neighbor` σε Bono

Για τον Edge δρομολογητή εκτελώντας τις παραπάνω εντολές έχουμε τα ακόλουθα:

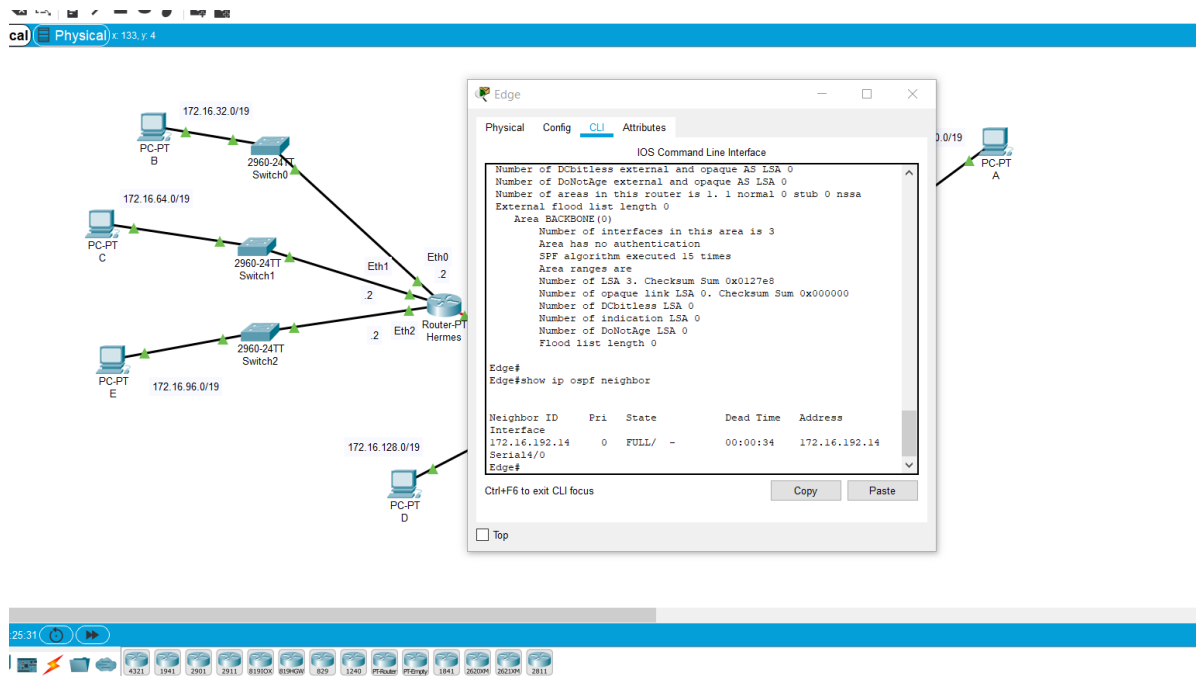
Αρχικά εκτελώντας την εντολή **show ip ospf** βλέπουμε από τα αποτελέσματα ότι ο δρομολογητής χρησιμοποιεί το OSPF με διεργασία OSPF 500 και Router ID 172.16.192.13, δηλώνοντας ότι υποστηρίζει μόνο μονοεπίπεδη (single TOS) δρομολόγηση και υποστηρίζει opaque LSA. Το χρονικό διάστημα καθυστέρησης για την εκτέλεση του SPF (Shortest Path First) είναι 5 secs και το χρονικό διάστημα που περιμένει μεταξύ δύο SPF είναι 10 secs. Τα ελάχιστα χρονικά διαστήματα για τη μεταφορά είναι 5 secs και την άφιξη των Link State Advertisements (LSA) είναι 1 secs. Επιπλέον εμφανίζεται ο αριθμός των εξωτερικών LSA όπου είναι 0, με τους υπολογισμούς checksum που πραγματοποιήθηκαν και είναι και αυτό 0. Παρουσιάζετε ο αριθμός των περιοχών OSPF που υποστηρίζονται στο δρομολογητή, με μια κανονική περιοχή και χωρίς stub ή NSSA περιοχές και τέλος βλέπουμε και το μήκος της λίστας εξωτερικών LSA, το οποίο είναι 0, υποδεικνύοντας ότι δεν υπάρχουν εξωτερικά LSA.



Εικόνα 13: Εκτελώντας την εντολή show ip ospf σε Edge

Εκτελώντας την εντολή show ip ospf neighbor παρατηρούμε ότι η διεύθυνση IP του γείτονα OSPF είναι η 172.16.192.14 και εμφανίζει και την προτεραιότητα του γείτονα OSPF όπου στην περίπτωση μας είναι 0. Σε αυτήν την περίπτωση, ο γείτονας είναι σε κατάσταση FULL, που σημαίνει ότι έχει επιτευχθεί πλήρης συμφωνία με το γείτονα. Ο χρόνος που απομένει μέχρι η σύνδεση με το γείτονα να θεωρηθεί "νεκρή" αν δεν ληφθούν ενημερώσεις OSPF από αυτόν είναι 00:00:35. Επιπλέον εμφανίζεται η διεύθυνση IP του γείτονα OSPF 172.16.192.14 και η διεπαφή μέσω της οποίας επικοινωνεί όπου είναι το Serial4/0.

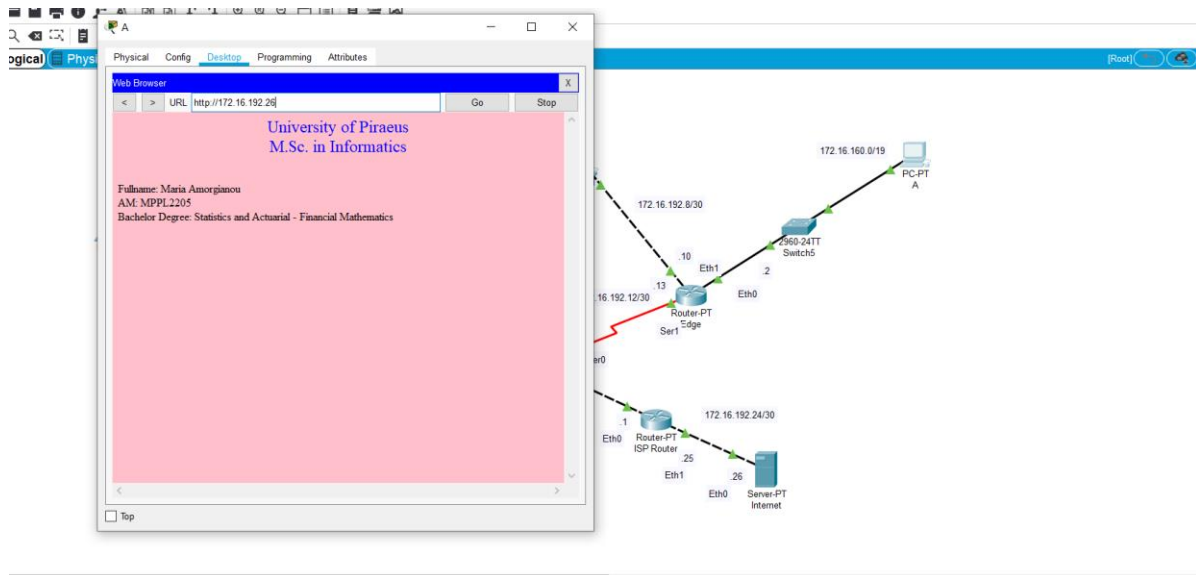




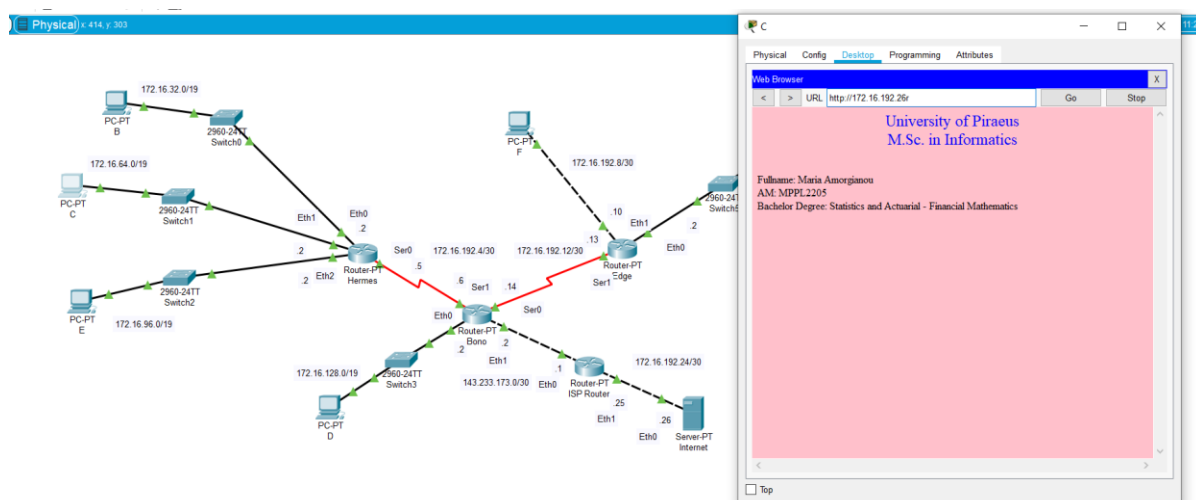
Εικόνα 14: Εκτελώντας την εντολή `show ip ospf neighbor` σε Edge

3)

Εδώ θέλουμε όλοι οι σταθμοί της τοπολογίας να έχουν πρόσβαση στην υπηρεσία HTTP που εξυπηρετείται από κάποιον διακομιστή στο διαδίκτυο και να μην έχουν πρόσβαση σε κάποια άλλη υπηρεσία του διαδικτύου. Παρακάτω εμφανίζονται δύο στιγμιότυπα οθόνης που εμφανίζει τις επιτυχημένες προσπάθειες πρόσβασης των δύο σταθμών στην διαδικτυακή υπηρεσία HTTP.



Εικόνα 15: Επιτυχημένη προσπάθεια πρόσβασης πρώτου σταθμού (PC-A) στην διαδικτυακή υπηρεσία

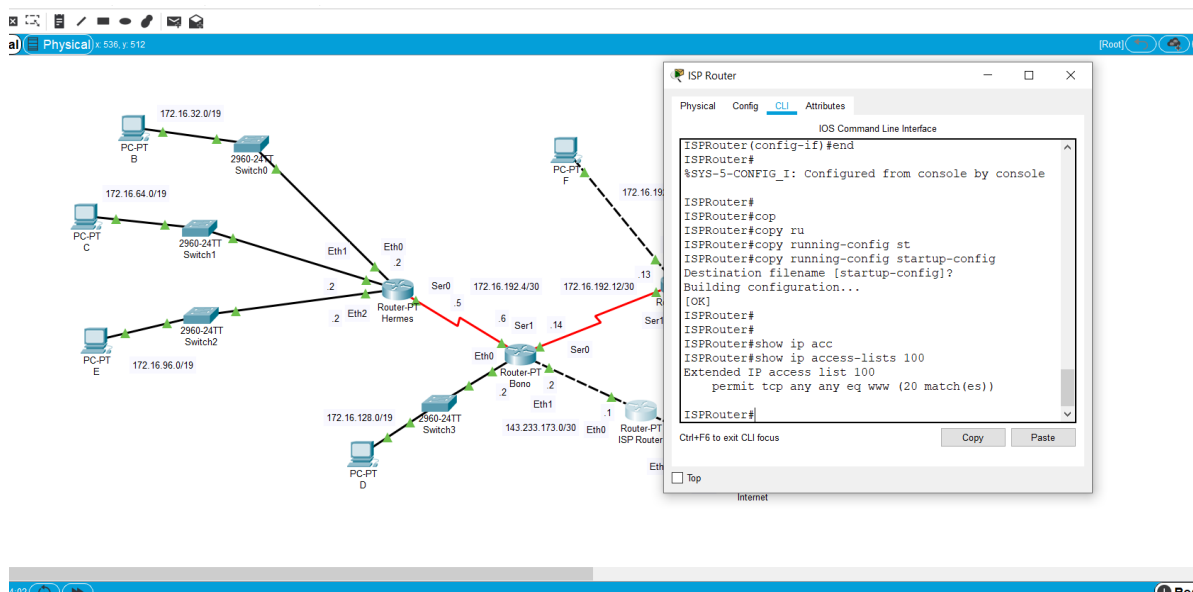


Εικόνα 16: Επιτυχημένη προσπάθεια πρόσβασης δεύτερου σταθμού (PC-C) στην διαδικτυακή υπηρεσία

Το ζητούμενο 3 επιτεύχθηκε τρέχοντας τις παρακάτω εντολές στον δρομολογητή ISP Router με την σειρά:

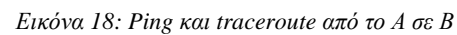
1. **access-list 100 permit tcp any any eq www** : αυτή η εντολή πρόσθεσε έναν κανόνα στην λίστα ελέγχου πρόσβασης (ACL) με αριθμό 100. Το **permit tcp** σημαίνει ότι επιτρέπονται μόνο πακέτα TCP. Το **any** σημαίνει ότι η πηγή και ο προορισμός μπορούν να είναι οποιαδήποτε διεύθυνση IP. Το **eq www** σημαίνει ότι η επικοινωνία επιτρέπεται μόνο για τη θύρα 80 (που χρησιμοποιείται για την υπηρεσία HTTP).
2. **int f1/0** : αυτή η εντολή μεταβαίνει στο FastEthernet1/0.
3. **ip access-group 100 out** : αυτή η εντολή εφαρμόζει την ACL με αριθμό 100 στην εξερχόμενη κίνηση της διεπαφής FastEthernet1/0. Αυτό σημαίνει ότι οι κανόνες της ACL 100 θα ελεγχθούν για όλα τα πακέτα που φεύγουν από τη διεπαφή FastEthernet1/0. Μόνο τα πακέτα TCP με προορισμό τη θύρα 80 (HTTP) θα επιτρέπονται να φύγουν, σύμφωνα με τον κανόνα που ορίζεται στην ACL 100. Οποιοδήποτε άλλο πακέτο TCP ή πακέτο από διαφορετικό πρωτόκολλο ή προς διαφορετική θύρα θα απορρίπτεται.

Όπως και από το ακόλουθο screenshot υπάρχει μια Extended IP access list 100



Εικόνα 17: Εμφάνιση της access list

Σε αυτό το ερώτημα θέλουμε τα δίκτυα που βρίσκονται στον δρομολογητή Hermes να είναι προσβάσιμα σε όλους τους άλλους σταθμούς της τοπολογίας μόνο σε περίπτωση χρήσης των εργαλείων **ping** και **traceroute**. Παρακάτω παρουσιάζουμε στιγμιότυπα οθόνης που αποδεικνύουν το ζητούμενο μας.



Οι εντολές που χρησιμοποιήσα είναι οι ακόλουθες:

1. **access-list 100 permit icmp any any echo:** επιτρέπει την προώθηση ICMP πακέτων τύπου «echo» από οποιαδήποτε πηγή προς οποιοδήποτε προορισμό. Τα ICMP πακέτα τύπου «echo» χρησιμοποιούνται κυρίως για ping εντολές, δηλαδή για τον έλεγχο της συνδεσιμότητας μεταξύ δύο συσκευών σε ένα δίκτυο. Με άλλα λόγια, αυτή η ACL επιτρέπει σε όλες τις συσκευές στο δίκτυο να απαντούν σε αιτήματα ping που προέρχονται από οποιαδήποτε πηγή.
2. **access-list 100 permit icmp any any echo-reply:** επιτρέπει τη διέλευση ICMP πακέτων τύπου «echo-reply» από οποιαδήποτε πηγή προς οποιοδήποτε προορισμό. Τα ICMP πακέτα τύπου «echo-reply» είναι η απάντηση σε ICMP «echo» αιτήματα, δηλαδή στα ping. Αυτό σημαίνει ότι με αυτήν την ACL επιτρέπεται στις συσκευές στο δίκτυο να απαντούν σε αιτήματα ping που έχουν σταλεί από άλλες συσκευές.
3. **access-list 100 permit udp any any eq 33434:** επιτρέπει τη διέλευση UDP πακέτων από οποιαδήποτε πηγή προς οποιοδήποτε προορισμό, με προορισμό θύρα 33434. Αυτό σημαίνει ότι η ACL επιτρέπει τη μετάδοση UDP πακέτων που στέλνονται ή προορίζονται στη θύρα 33434. Αυτό μπορεί να χρησιμοποιηθεί για την επιτροπή συγκεκριμένων εφαρμογών που λειτουργούν σε αυτήν τη θύρα.
4. **access-list 100 permit udp any any eq 33435:** επιτρέπει τη διέλευση UDP πακέτων από οποιαδήποτε πηγή προς οποιοδήποτε προορισμό, με προορισμό θύρα 33435. Αυτό σημαίνει ότι η ACL επιτρέπει τη μετάδοση UDP πακέτων που στέλνονται ή προορίζονται στη θύρα 33435. Αυτό μπορεί να χρησιμοποιηθεί για την επιτροπή συγκεκριμένων εφαρμογών που λειτουργούν σε αυτήν τη θύρα.
5. **access-list 100 permit tcp any any eq 80:** επιτρέπει τη διέλευση TCP πακέτων από οποιαδήποτε πηγή προς οποιοδήποτε προορισμό, με προορισμό τη θύρα 80. Η θύρα 80 είναι η προκαθορισμένη θύρα για το πρωτόκολλο HTTP, οπότε αυτός ο κανόνας επιτρέπει τη μετάδοση TCP πακέτων που αποστέλλονται ή προορίζονται στη θύρα 80, δηλαδή τη θύρα που χρησιμοποιείται για τις συνδέσεις HTTP.
6. **int s3/0:** αυτή η εντολή μεταβαίνει στη διεπαφή Serial3/0.

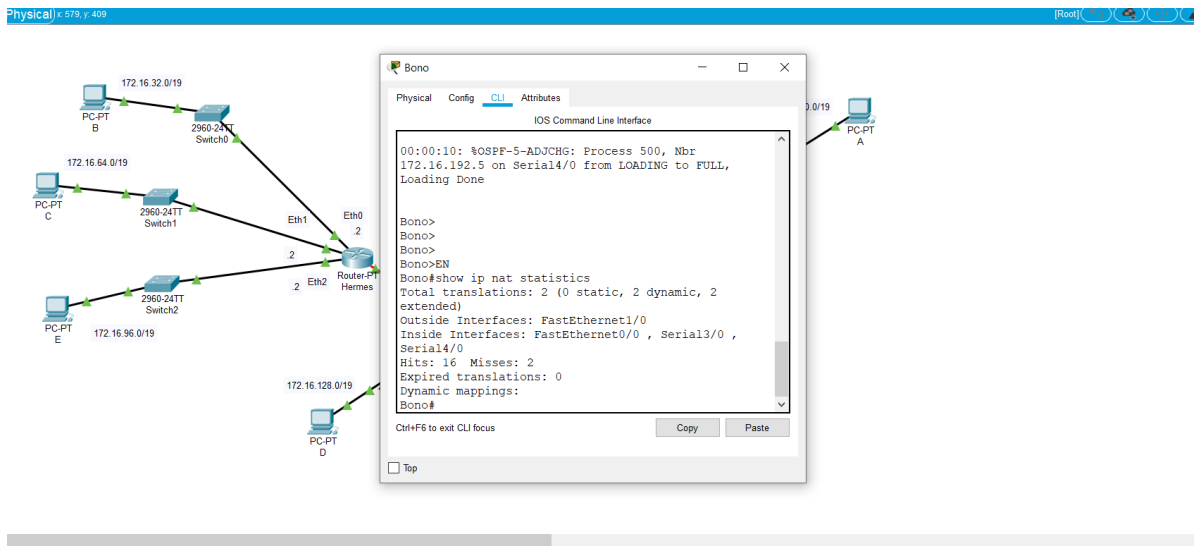
7. **ip access-group 100 out:** εφαρμόζει τη λίστα ελέγχου πρόσβασης με αριθμό 100 στην εξερχόμενη κίνηση της διεπαφής Serial3/0. Αυτό σημαίνει ότι οι κανόνες της ACL 100 θα ελεγχθούν για κάθε πακέτο που βγαίνει στη διεπαφή Serial3/0 και θα εφαρμοστούν οι αντίστοιχες ενέργειες που ορίζονται στη λίστα ελέγχου πρόσβασης. Εφαρμόζοντας μια ACL στην εξερχόμενη κίνηση, μπορείτε να ελέγξετε ποια πακέτα επιτρέπονται να φύγουν από τον δρομολογητή και προς ποιους προορισμούς. Αυτό είναι χρήσιμο για την επιβολή πολιτικών ασφαλείας και για τον έλεγχο της εξερχόμενης κίνησης από το δίκτυο.

5)

Στον Bono υλοποιήθηκε η τεχνική overloaded NAT (PAT) με overloaded δημόσια IP την 143.233.173.2/30. Για την υλοποίηση της τεχνικής τρέξαμε τον παρακάτω κώδικα:

1. **router ospf 500:** η εντολή κάνει εισαγωγή στο ospf 500
2. **ip route 0.0.0.0 0.0.0.0 FastEthernet1/0:** ότι έρχεται από οπουδήποτε θα πηγαίνει σε fastEthernet 1/0
3. **default-information originate:** χρησιμοποιείται εντός της διαμόρφωσης OSPF για να δηλώσει στον δρομολογητή ότι πρέπει να αποστείλει μια προεπιλεγμένη διαδρομή στο OSPF domain. Αυτή η προεπιλεγμένη διαδρομή, γνωστή και ως default route, χρησιμοποιείται όταν ο δρομολογητής δεν έχει καμία καταχώρηση για ένα συγκεκριμένο προορισμό στον πίνακα δρομολόγησής του. Η χρήση μιας προεπιλεγμένης διαδρομής επιτρέπει στον δρομολογητή να αποφασίσει πού να κατευθύνει πακέτα που δεν ταιριάζουν με καμία άλλη καταχώρηση στον πίνακα δρομολόγησης.
4. **access-list 1 permit 172.16.0.0 0.0.255.255:** δημιουργείται μια επέκταση της λίστας ελέγχου πρόσβασης (ACL) με αριθμό 1 και επιτρέπει όλη την κίνηση από το δίκτυο 172.16.0.0/16. Αυτό συμπεριλαμβάνει όλες τις διευθύνσεις IP που ανήκουν στο εύρος από το 172.16.0.0 μέχρι το 172.16.255.255.
5. **ip nat inside source list 100 interface f1/0 overload:** αυτή η εντολή θέτει μια μετάφραση διευθύνσεων NAT στον δρομολογητή. Τα πακέτα που προέρχονται από εσωτερικές διευθύνσεις IP και που περιλαμβάνονται στη λίστα ελέγχου πρόσβασης 100 θα μεταφραστούν στην διεπαφή FastEthernet1/0 του δρομολογητή. Η μετάφραση θα γίνει με χρήση της τεχνικής Overloaded NAT (PAT), επιτρέποντας σε πολλές εσωτερικές διευθύνσεις IP να μοιράζονται μια μόνο δημόσια διεύθυνση IP, με τη χρήση διαφορετικών θυρών για να διακρίνονται.
6. **int f1/0:** πρόσβαση σε διεπαφή FastEthernet

7. **ip nat outside:** σημαίνει ότι αυτή η διεπαφή θεωρείται ως έξω προς το δίκτυο. Συνήθως αυτό σημαίνει ότι η διεπαφή συνδέεται με τον διακομιστή ή τον ISP και χρησιμοποιείται για την επικοινωνία με το εξωτερικό δίκτυο, όπως το Διαδίκτυο.



Εικόνα 20: Εκτέλεση εντολής `show ip nat statistics`

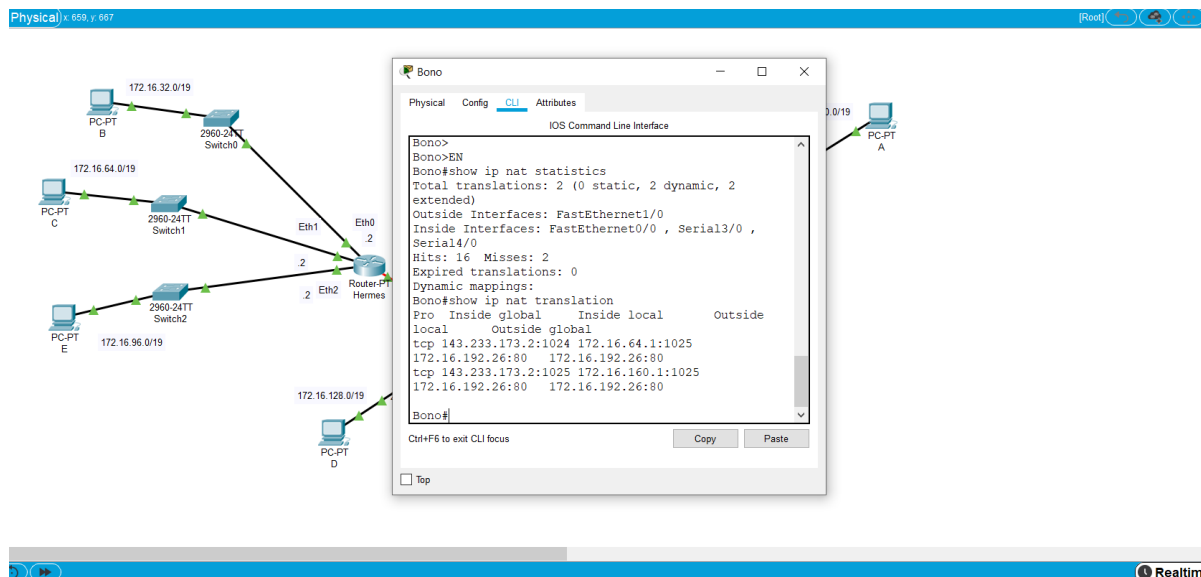
Τα στατιστικά που παρουσιάζονται με την εντολή **show ip nat statistics** παρέχουν πληροφορίες σχετικά με την λειτουργία της διεύθυνσης NAT (network address translations) στον δρομολογητή. Παρακάτω αναλύονται τα αποτελέσματα:

1. **Total translations:** αυτός ο αριθμός αναφέρει το συνολικό αριθμό των μεταφράσεων που έχουν πραγματοποιηθεί και χωρίζεται σε στατικές, δυναμικές και εκτεταμένες μεταφράσεις.
2. **Outside interfaces:** αυτές είναι οι διεπαφές που χρησιμοποιούνται για τις μεταφράσεις προς το εξωτερικό δίκτυο.
3. **Inside interfaces:** αυτές είναι οι εσωτερικές διεπαφές του δικτύου που έχουν συσχετιστεί με τις μεταφράσεις NAT.
4. **Hits:** αυτός είναι ο αριθμός των φορών που πακέτα είχαν μια επιτυχή αντιστοίχιση στον πίνακα μεταφράσεων NAT.



5. **Misses:** αυτός είναι ο αριθμός των φορών που πακέτα δεν είχαν επιτυχή αντιστοίχιση στον πίνακα μεταφράσεων NAT.
6. **Expired translations:** αυτός είναι ο αριθμός των μεταφράσεων που έχουν λήξει λόγω χρονικού ορίου.
7. **Dynamic mappings:** αυτός είναι ο αριθμός των δυναμικών μεταφράσεων που έχουν δημιουργηθεί αυτόματα από τον δρομολογητή, συνήθως βασισμένος στις ανάγκες του δικτύου.

Οι στατιστικές που παρουσιάζονται δείχνουν ότι έχει γίνει ένας αριθμός μεταφράσεων, με την πλειονότητα αυτών να είναι δυναμικές.



Εικόνα 21: Εκτέλεση εντολής `show ip nat translations`

Τα στατιστικά που παρουσιάζονται με την εντολή **show ip nat translations** παρουσιάζει τις ενεργές μεταφράσεις διευθύνσεων NAT (network address translations) στον δρομολογητή. Παρακάτω αναλύονται τα αποτελέσματα:

1. **Pro:** αυτός είναι ο τύπος του πρωτοκόλλου του πακέτου (σε αυτήν την περίπτωση tcp).

2. **Inside global:** αυτή είναι η δημόσια διεύθυνση IP και ο αριθμός θύρας που χρησιμοποιούνται στον εξωτερικό κόσμο για αναπαράσταση της εσωτερικής διεύθυνσης.
3. **Inside local:** αυτή είναι η εσωτερική διεύθυνση IP και ο αριθμός θύρας του εσωτερικού υπολογιστή ή συσκευής που ξεκίνησε το πακέτο
4. **Outside local:** αυτή είναι η διεύθυνση IP και ο αριθμός θύρας του προορισμού στο εξωτερικό δίκτυο (σε αυτήν την περίπτωση, η διεύθυνση IP και ο αριθμός θύρας του διακομιστή HTTP).
5. **Outside global:** αυτή είναι η δημόσια διεύθυνση IP και ο αριθμός θύρας του προορισμού στον εξωτερικό κόσμο.

Συνοπτικά, η συγκεκριμένη εγγραφή δείχνει ότι ένα πακέτο TCP που προέρχεται από την εσωτερική διεύθυνση 172.16.160.1 και έχει πηγαία θύρα 1025, έχει μεταφραστεί σε μια δημόσια διεύθυνση IP 143.233.173.2 με προορισμό τη διεύθυνση IP του διακομιστή HTTP 143.233.173.1, ενώ ο αριθμός θύρας παραμένει ο ίδιος (80).