

Δίκτυα Υπολογιστών
2ο Εργαστήριο: Δυναμική Δρομολόγηση
Εργασία: assign2

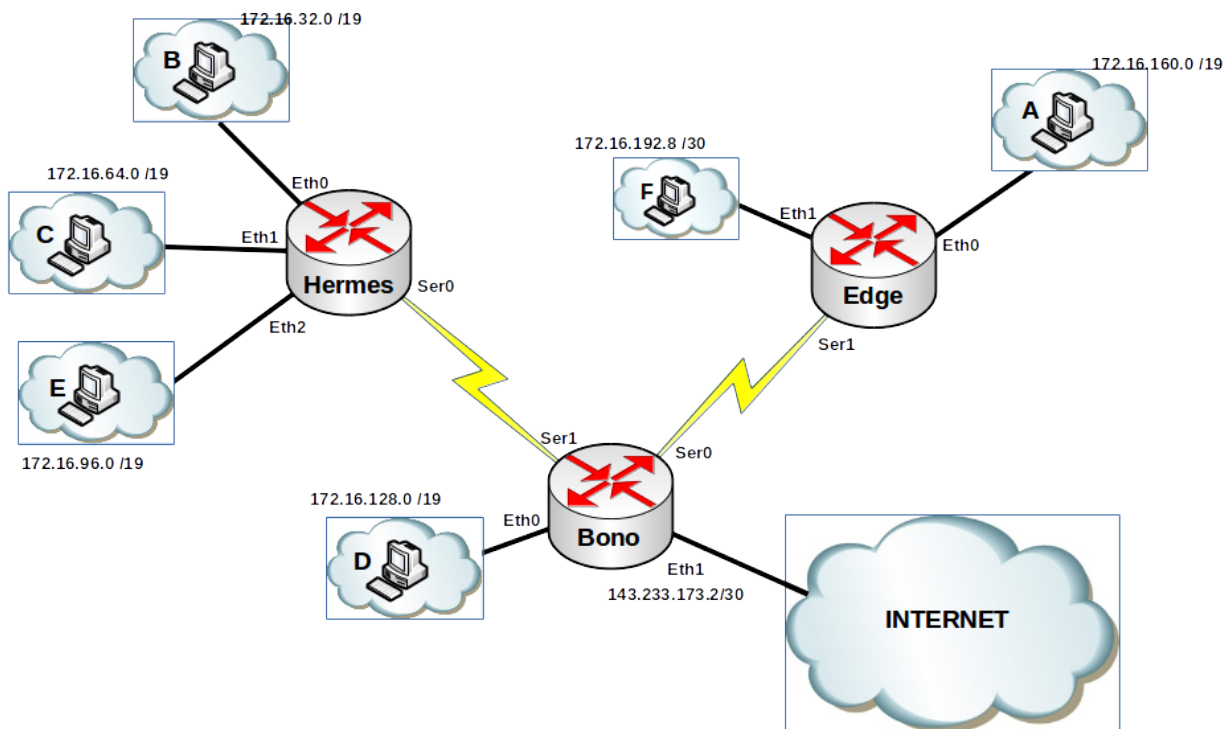
Αναγνωστόπουλος Βασίλης - Θάνος (ΜΠΠΛ 13002)
Βελισσαρίου Κυριάκος (ΜΠΠΛ 13005)

Αθήνα, 2015

Περιεχόμενα

1 Άσκηση 1η	1
2 Άσκηση 2η	3
3 Άσκηση 3η	5
4 Άσκηση 4η	7
5 Διευκρινήσεις	9

Δίνεται η παρακάτω τοπολογία:



Παραδοτέα:

1. Η έκθεσή σας:

- (α') Screenshot της τοπολογίας.
- (β') Screenshot που θα εμφανίζει τις επιτυχημένες προσπάθειες πρόσβασης 2 σταθμών στην υπηρεσία HTTP.
- (γ') Screenshot που θα αποδεικνύει το ζητούμενο 3, όπως διατυπώνεται παραπάνω.
- (δ') Screenshot με το αποτέλεσμα εκτέλεσης της εντολής `#show ip ospf`
- (ε') Screenshot με το αποτέλεσμα εκτέλεσης της εντολής `#show ip ospf database`

2. Τα αρχεία (.pkt) με την τοπολογία σας.

Ζητούμενα:

1 Άσκηση 1η

Εκφώνηση

Screenshot της τοπολογίας.

Λύση

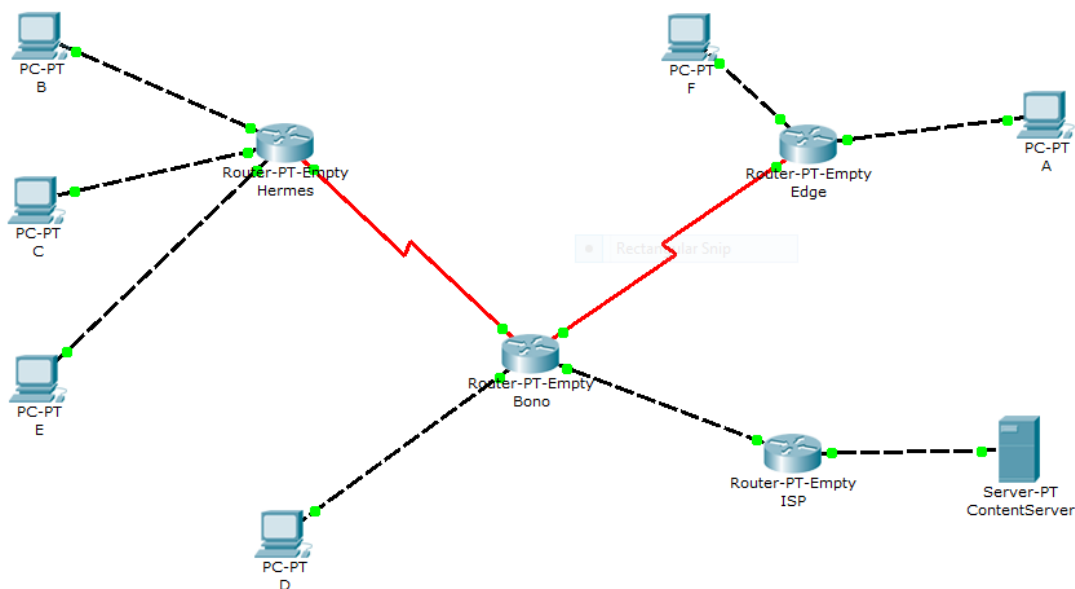
Η υλοποίηση στο Cisco Packet Tracer φαίνεται στο σχήμα 1.1.

Subnet	Subnet Address	Subnet Mask	Host Addresses	BroadCast Address
SubnetA	172.16.160.0	255.255.224.0	172.16.160.1 - 172.16.191.254	172.16.191.255
SubnetB	172.16.32.0	255.255.224.0	172.16.32.1 - 172.16.63.254	172.16.63.255
SubnetC	172.16.64.0	255.255.224.0	172.16.64.1 - 172.16.95.254	172.16.95.255
SubnetD	172.16.128.0	255.255.224.0	172.16.128.1 - 172.16.159.254	172.16.159.255
SubnetE	172.16.96.0	255.255.224.0	172.16.96.1 - 172.16.127.254	172.16.127.255
SubnetF	172.16.192.8	255.255.255.252	172.16.192.9 - 172.16.192.10	172.16.192.11
SubnetSer1	10.1.1.4	255.255.255.252	10.1.1.5 - 10.1.1.6	10.1.1.7
SubnetSer2	10.1.1.8	255.255.255.252	10.1.1.9 - 10.1.1.10	10.1.1.11
SubnetInt	143.233.173.0	255.255.255.252	143.233.173.1 - 143.233.173.2	143.233.173.3

Πίνακας 1.1: Ο πίνακας των υποδικτύων του δικτύου.

Device	Interface	IP Address	Subnet Mask	Default Gateway
Hermes	Fa8/0	172.16.32.1	255.255.224.0	-
	Fa7/0	172.16.64.1	255.255.224.0	-
	Fa6/0	172.16.96.1	255.255.224.0	-
	Ser5/0	10.1.1.5	255.255.255.252	-
Bono	Fa9/0	172.16.128.1	255.255.224.0	-
	Fa8/0	143.233.173.2	255.255.255.252	-
	Ser4/0	10.1.1.6	255.255.255.252	-
	Ser5/0	10.1.1.9	255.255.255.252	-
Edge	Fa7/0	172.16.160.1	255.255.224.0	-
	Fa8/0	172.16.192.9	255.255.255.252	-
	Ser6/0	10.1.1.10	255.255.255.252	-
PCA	Eth	172.16.160.2	255.255.224.0	172.16.191.1
PCB	Eth	172.16.32.2	255.255.224.0	172.16.32.1
PCC	Eth	172.16.64.2	255.255.224.0	172.16.64.1
PCD	Eth	172.16.128.2	255.255.224.0	172.16.128.1
PCE	Eth	172.16.96.2	255.255.224.0	172.16.96.1
PCF	Eth	172.16.192.10	255.255.255.252	172.16.192.9

Πίνακας 1.2: Ο πίνακας των ip διευθύνσεων του δικτύου.



Σχήμα 1.1: Η υλοποίηση του δικτύου στο Cisco Packet Tracer

2 Άσκηση 2η

Εκφώνηση

Screenshot που θα εμφανίζει τις επιτυχημένες προσπάθειες πρόσβασης 2 σταθμών στην υπηρεσία HTTP.

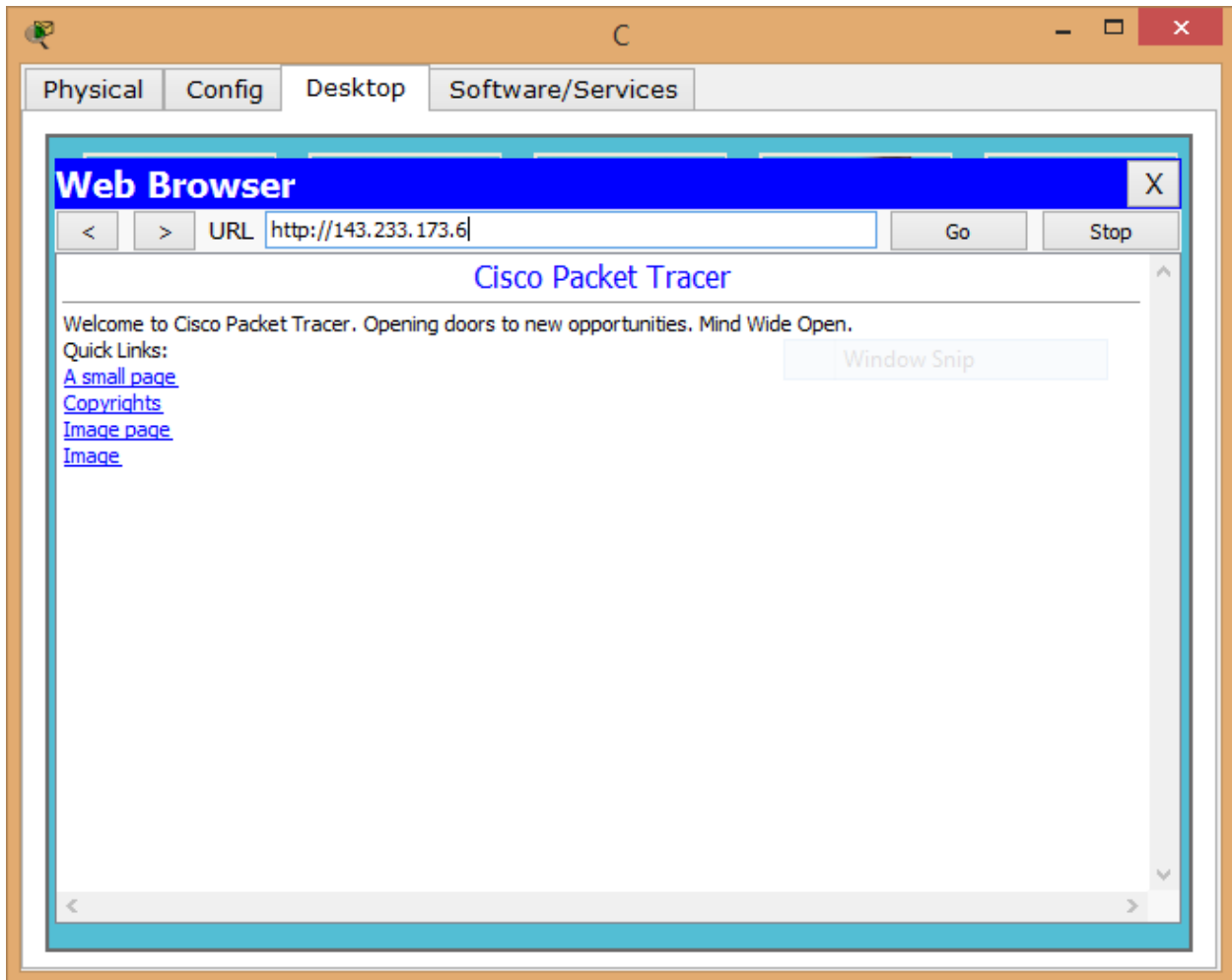
Λύση

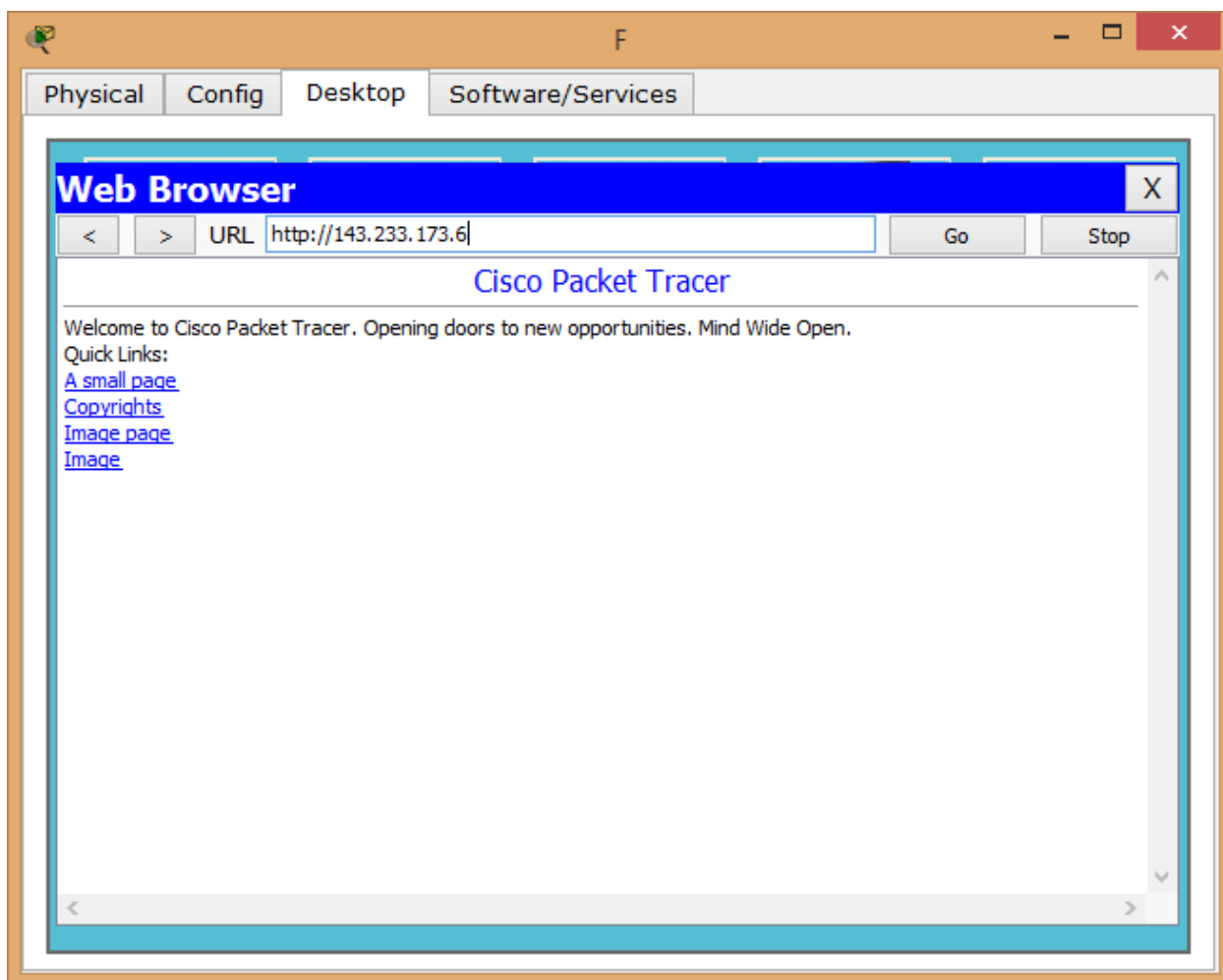
Για να είναι δυνατή η πρόσβαση των σταθμών στον στην υπηρεσία http και μόνο σε αυτή, εφαρμόστηκε στο interface Fa8/0 του Bono η εξής ACL:

Listing 1: ACL για το β'

```
1 permit tcp any any eq www
```

Ακολουθούν screenshot από επιτυχημένες προσπάθειες δύο σταθμών στην υπηρεσία http.





3 Άσκηση 3η

Εκφώνηση

Τα δίκτυα που βρίσκονται στον δρομολογητή Hermes είναι προσβάσιμα σε όλους τους άλλους μόνο σε περίπτωση χρήσης των εργαλείων ping και traceroute.

Λύση

Σχετικά με το ζητούμενο 3, θέλουμε τα δίκτυα πίσω από τον Hermes να είναι προσβάσιμα από τους άλλους μόνο για τις υπηρεσίες ping και traceroute. Συνεπώς, εφαρμόζουμε στα interface Fa6/0, Fa7/0 και Fa8/0 την ACL:

Listing 2: ACL για το γ'

```
1 permit icmp any any
```

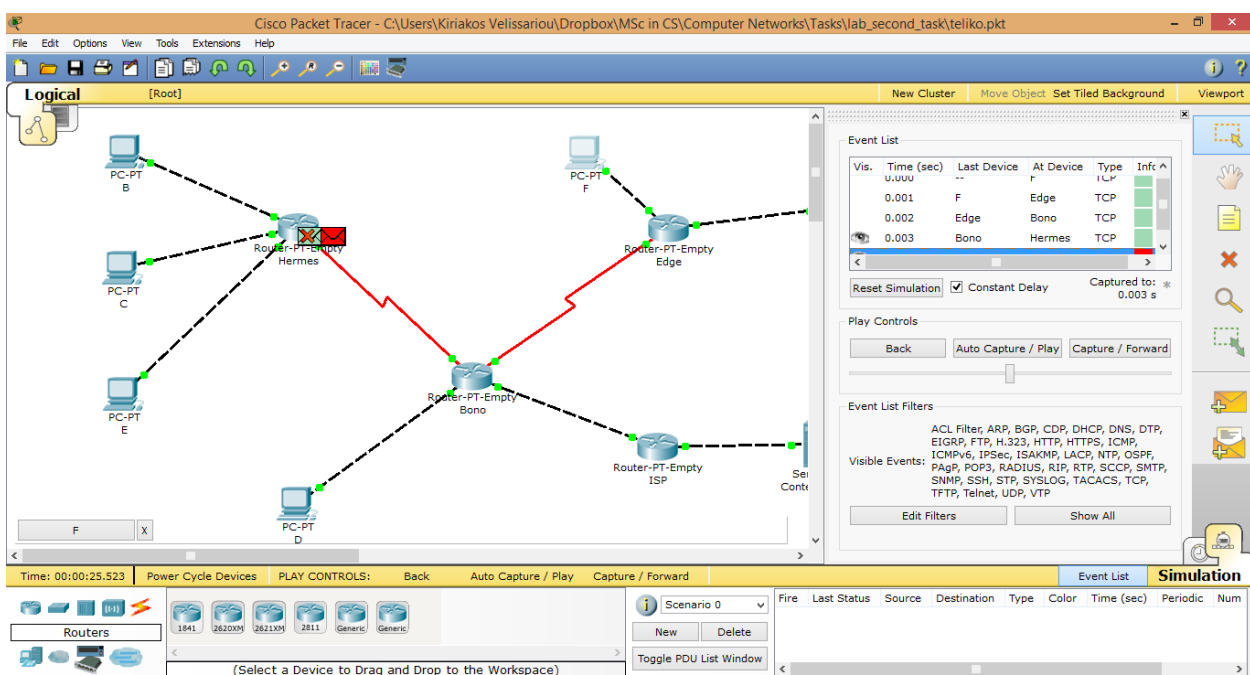
Όμως, εάν η ACL έμενε όπως παραπάνω θα υπήρχε το εξής πρόβλημα: Εάν κάποιο από τα τερματικά πίσω από τον Hermes ήθελε να έχει πρόσβαση στις υπηρεσίες HTTP του διαδικτύου ναι μεν η αίτηση του θα έφτανε στον

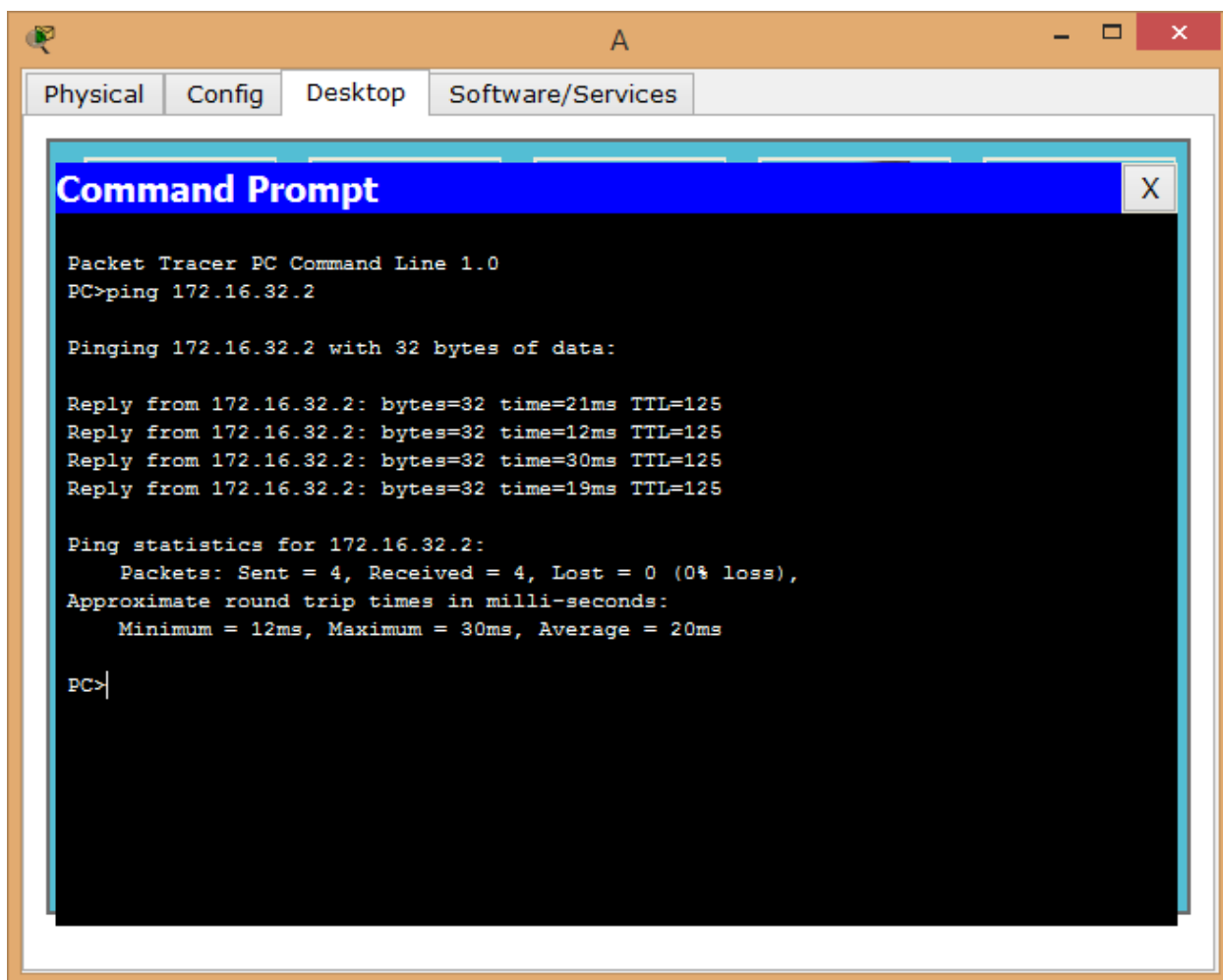
ContentServer, αλλά η απάντηση του Server θα αποριπτόταν από τον δρομολογητή Hermes καθώς επιτρέπει μόνο εισερχόμενη κυκλοφορία ICMP. Για να λυθεί αυτό το πρόβλημα, και παράλληλα να ισχύει το ζητούμενο 3, στα παραπάνω interface προστέθηκε και το παρακάτω φίλτρο στην ACL:

Listing 3: ACL για το γ' (2)

```
1 permit tcp any any established
```

Με το παραπάνω επιτρέπονται τα tcp πακέτα προς τα τερματικά πίσω από τον Hermes, αλλά μόνο από επικοινωνία που έχουν ξεκινήσει αυτά τα τερματικά. Σε ότι αφορά την απόδειξη, στα screenshot της προηγούμενης φαίνεται επιτυχημένο http request από τερματικό του Hermes. Τέλος, στα δύο screenshot που ακολουθούν φαίνεται επιτυχημένο ping request προς τερματικό του Hermes, καθώς και μπλοκαρισμένο πακέτο tcp από επικοινωνία που έχει ξεκινήσει από τερματικό εκτός του δικτύου Hermes. Το τελευταίο επιτεύχθηκε με την λειτουργία simulation του Packet Tracer.





4 Άσκηση 4η

Εκφώνηση

Οι δρομολογητές αξιοποιούν τον αλγόριθμο OSPF για τη διαδικασία της δρομολόγησης. Προς το Διαδίκτυο χρησιμοποιείται στατική δρομολόγηση. Εμφάνιση screenshots με τις εντολές `show ip ospf` και `show ip ospf database`.

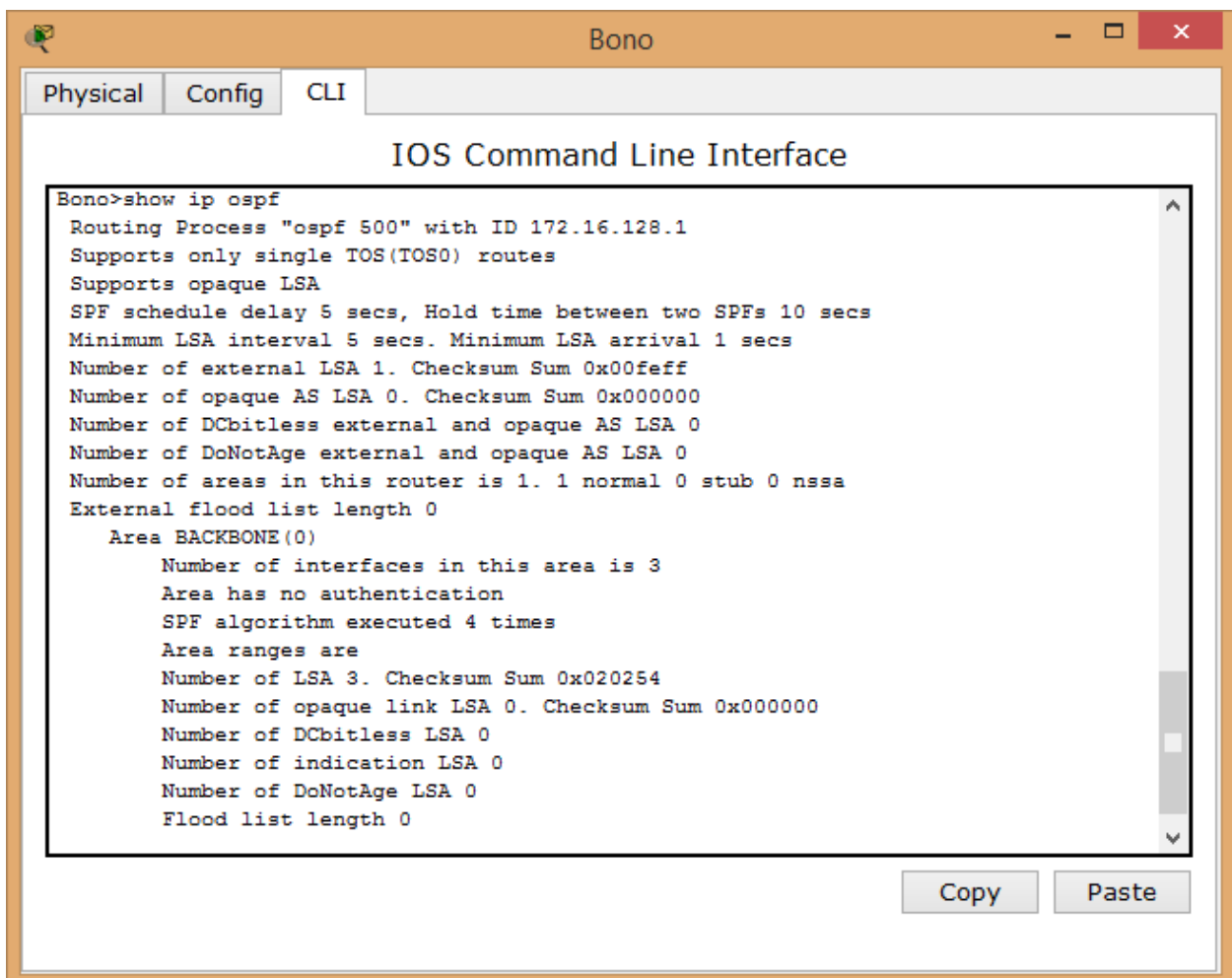
Λύση

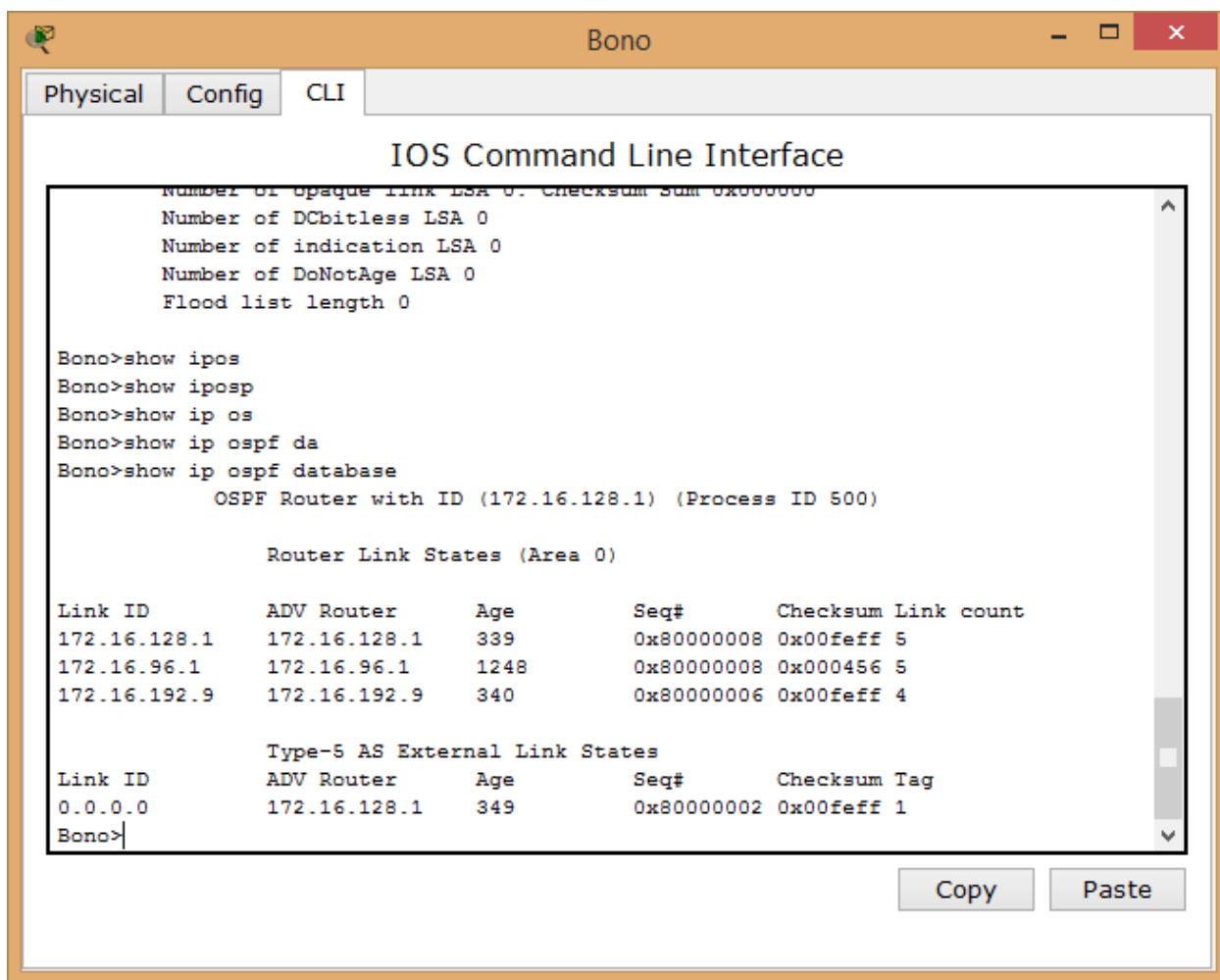
Σε ότι αφορά το τέταρτο μέρος του παραδοτέου, παρατίθενται screenshots από τα αποτελέσματα των ζητούμενων εντολών, καθώς και ο κώδικας για την δυναμική δρομολόγηση.

Listing 4: Οι εντολές για το OSPF στον Hermes

```
1 Hermes(config)# router ospf 500
2 Hermes(config-router)# network 172.16.32.0 0.0.31.255 area 0
3 Hermes(config-router)# network 172.16.64.0 0.0.31.255 area 0
4 Hermes(config-router)# network 172.16.96.0 0.0.31.255 area 0
```

```
5 Hermes(config-router)# network 10.1.1.4 0.0.0.3 area 0
6 Hermes(config-router)# ^Z
```





Listing 5: Οι εντολές για το OSPF στον Edge

```
1 Edge(config)# router ospf 500
2 Edge(config-router)# network 172.16.192.8 0.0.0.3 area 0
3 Edge(config-router)# network 172.16.160.0 0.0.31.255 area 0
4 Edge(config-router)# network 10.1.1.8 0.0.0.3 area 0
5 Edge(config-router)# ^Z
```

Listing 6: Οι εντολές για το OSPF στον Bono

```
1 Bono(config)# router ospf 500
2 Bono(config-router)# network 172.16.128.0 0.0.31.255 area 0
3 Bono(config-router)# network 10.1.1.8 0.0.0.3 area 0
4 Bono(config-router)# network 10.1.1.4 0.0.0.3 area 0
5 Edge(config-router)# ^Z
```

5 Διευκρινήσεις

Για την προσομοίωση του διαδικτύου χρησιμοποιήθηκε ένας isp δρομολογητής και ένας εξυπηρετητής. Επίσης, εφαρμόστηκε overloaded NAT έτσι ώστε

όλες οι ιδιωτικές διευθύνσεις να μεταφράζονται στην δημόσια διεύθυνση που αντιστοιχεί στο interface Fa8/0 του δρομολογητή Bono πριν βγουν προς το διαδίκτυο. Αυτό επετεύχθη με την χρήση της ip access list NAT. Τέλος, ορίστηκε σαν default διαδρομή το interface Fa8/0 του Bono.