

Εργαστήριο Δικτύων Υπολογιστών

Εργαστηριακή Άσκηση 7

Δημήτριος Κόγιος

03119220

Όνομα PC: lekog-HP-Laptop-15s-fq1xxx

Άσκηση 1:

1.1) vtysh

```
configure terminal
interface em0
ip address 192.168.1.2/24
ip route 0.0.0.0/0 192.168.1.1
```

1.2) vtysh

```
configure terminal
interface em0
ip address 192.168.2.2/24
ip route 0.0.0.0/0 192.168.2.1
```

1.3) cli

```
configure terminal
hostname R1
interface em0
ip address 192.168.1.1/24
exit
interface em1
ip address 172.17.17.1/30
```

1.4) do show ip route

Δεν βλέπουμε καμία εγγραφή με S.

1.5) router ?

Βλέπουμε 7 διαθέσιμα πρωτόκολλα δρομολόγησης

1.6) router rip

1.7) 18 εντολές.

1.8) version 2

1.9) network 192.168.1.0/24

1.10) network 172.17.17.0/30

1.11) exit. Όχι δεν έχει αλλάξει τίποτα.

1.12) Ναι επικοινωνούν τα δύο PC.

1.13) do show ip route

1.14) 172.17.17.0/30

192.168.1.0/24

192.168.2.0/24

1.15) Μας λέει ότι το επόμενο hop είναι ο εαυτός του.

1.16) Για τα πρώτα δύο πηγή είναι self και metric = 1 ενώ για το 192.168.2.0/24 πηγή 172.17.17.2 και metric = 2. Το metric μας

λέει πόσα hops χρειάζονται για να φτάσουν τα πακέτα στο δίκτυο προορισμό.

1.17) 4 εγγραφές.

1.18) Από το R> μπροστά από την εγγραφή αλλά και από τη διαχειριστική απόσταση 120.

1.19) Από το > .

1.20) Από το * μετά το > .

1.21) Είναι 120 και εμφανίζεται υπό τη μορφή [`<διαχειριστική_απόσταση> / <metric>`].

1.22) `show ip rip status`

Στέλνονται ενημερώσεις κάθε 30 δευτερόλεπτα +- 50 %.

1.23) `emo, em1`

`172.17.17.0/30, 192.168.1.0/24`

1.24) Λαμβάνει από την 172.17.17.2 .

Το last update μας δείχνει πριν από πόσο χρόνο ήρθε το τελευταίο πακέτο από αυτήν την πηγή.

1.25) 3 min = Χρόνος ζωής + last update

1.26) `netstat -r`

Βλέπουμε ότι η εγγραφή έχει το flag 1 που είναι protocol specific routing flag συνεπώς είναι δυναμική αφού προκλήθηκε από κάποιο πρωτόκολλο.

Άσκηση 2:

2.1) tcpdump -i em0 -n -vv

2.2) Βλέπω RIP request και RIP responses.

2.3) Πηγή : 192.168.1.1

Προορισμός : 224.0.0.9

Η 224.0.0.9 είναι η διεύθυνση προορισμού των μηνυμάτων RIP v2 και είναι multicast.

2.4) Όχι.

2.5) ttl = 1.

2.6) UDP και η θύρα είναι 520.

2.7) Τα δίκτυα 172.17.17.0/30 και 192.168.2.0/24. Δεν υπάρχει διαφήμιση για το δίκτυο του LAN1.

2.8) Ο χρόνος δεν είναι ακριβώς 30 δευτερόλεπτα αλλά 30 +- 50 % δηλαδή μπορεί να κυμαίνεται από 15 μέχρι και 45 δευτερόλεπτα.

2.9) tcpdump -i em1 -n -vv

Ναι βλέπω μηνύματα RIP από το R1.

2.10) Διαφημίζει το 192.168.1.0/24. Συνεπώς λείπουν τα 172.17.17.0/30 και 192.168.2.0/24.

2.11) Ναι βλέπουμε μηνύματα RIP του R2 που διαφημίζει το 192.168.2.0/24.

2.12) Όταν διαφημίζουν 1 δίκτυο 24 bytes ενώ όταν διαφημίζουν δύο δίκτυα 44 bytes. Μέγεθος της κάθε διαδρομής RIP είναι 20 bytes.

2.13) `tcpdump -i em0 -vv '(port 520)'`

2.14) `no network 192.168.2.0/24`

Εμφανίζεται το μήνυμα 192.168.2.0/24 με metric 16.

Ουσιαστικά το R2 στέλνει route poisoning για το 192.168.2.0/24 και το R1 στέλνει poison reverse στο LAN1.

2.15) Ναι εμφανίσθηκε μήνυμα RIP στο LAN1 που διαφημίζει το 192.168.2.0/24 με metric 2.

2.16) `tcpdump -i em0 -vv '(port 520 and src 172.17.17.1)'`

2.17) Ναι.

2.18) Όχι γιατί το LAN1 είναι συνδεδεμένο με το R1 μέσω της διεπαφής em0.

2.19) Ναι σβήστηκε από τον πίνακα δρομολόγησης.

2.20) Δεν έχει σβηστεί αλλά έχει metric = 16.

Όταν λήξει το time σβήνεται γιατί δεν έχει γίνει update.

2.21) `network 192.168.1.0/24`

`network 192.168.2.0/24`

2.22) R1 : passive-interface em0
R2 : passive-interface em1

2.23) Στις καταγραφές των LAN δεν βλέπουμε νέα RIP μηνύματα.

Άσκηση 3:

3.1) interface em2
ip address 172.17.17.5/30
exit
router rip
network 172.17.17.5/30

3.2) interface em2
ip address 172.17.17.9/30
exit
router rip
network 172.17.17.9/30

3.3) interface em0
ip address 172.17.17.6/30
exit
interface em1
ip address 172.17.17.10/30
exit
router rip

3.4) do show ip rip
Τα δίκτυα 172.17.17.8/30 (WAN3) και 192.168.2.0/24 (LAN2) .

3.5) do show ip rip
Τα δίκτυα 172.17.17.4/30 (WAN2) και 192.168.1.0/24 (LAN1) .

3.6) do show ip rip

Τα δίκτυα 172.17.17.0/30 (WAN1) και 192.168.1.0/24 (LAN1) και 192.168.2.0/24 (LAN2) .

3.7) Ναι επικοινωνούν.

3.8) interface em2

ip address 192.168.3.1/24

3.9) Όχι δεν έχουν αλλάξει.

3.10) router rip

network 192.168.3.0/24

3.11) Ναι προστέθηκε το δίκτυο 192.168.3.0/24.

3.12) Ναι στάλθηκε RIP μήνυμα αμέσως μετά την προσθήκη.

3.13) Είναι ο εαυτός του.

3.14) em0, em1, em2 , lo0

0.0.0.0/0

3.15) Όχι δεν έχει υπάρξει κάποια αλλαγή.

3.16) Διαφημίζει τα 172.17.17.8/30, 192.168.2.0/24 και

192.168.3.0/24.

3.17) Όχι γιατί δεν στέλνει μήνυμα RIP από την ίδια διαπαφή που το έλαβε (split horizon).

3.18) Βάζει αυτόματα στα μηνύματα RIP όλα τα δίκτυα στα οποία ανήκουν οι διεπαφές του.

3.19) Ο R3 διαφημίζει metric για το WAN3 ίσο με 1. Το ίδιο και ο R2. Ο R1 έχει επιλέξει τη διαδρομή μέσω R2.

3.20) Στο WAN2. Δεν θα μπορούσε στο WAN1 αφού η διαδρομή που έχει επιλέξει περνάει από το WAN1.

Άσκηση 4:

4.1) vtysh

configure terminal

interface em0

ip address 192.168.3.2/24

exit

ip route 0.0.0.0/0 192.168.3.1

4.2) Ναι.

4.3) Ναι.

4.4) Ναι.

4.5) do show ip route

R1 :

```
C>* 127.0.0.0/8 is directly connected, lo0
C>* 172.17.17.0/30 is directly connected, em1
C>* 172.17.17.4/30 is directly connected, em2
R>* 172.17.17.8/30 [120/2] via 172.17.17.2, em1, 00:40:39
C>* 192.168.1.0/24 is directly connected, em0
R>* 192.168.2.0/24 [120/2] via 172.17.17.2, em1, 00:55:33
R>* 192.168.3.0/24 [120/2] via 172.17.17.6, em2, 00:25:53
R1(config)#
```


R2 :

```
C>* 127.0.0.0/8 is directly connected, lo0
C>* 172.17.17.0/30 is directly connected, em0
R>* 172.17.17.4/30 [120/2] via 172.17.17.1, em0, 00:45:21
C>* 172.17.17.8/30 is directly connected, em2
R>* 192.168.1.0/24 [120/2] via 172.17.17.1, em0, 01:00:44
C>* 192.168.2.0/24 is directly connected, em1
R>* 192.168.3.0/24 [120/2] via 172.17.17.10, em2, 00:29:10
R2(config)#
```

R3 :

```
C>* 127.0.0.0/8 is directly connected, lo0
R>* 172.17.17.0/30 [120/2] via 172.17.17.5, em0, 00:30:30
C>* 172.17.17.4/30 is directly connected, em0
C>* 172.17.17.8/30 is directly connected, em1
R>* 192.168.1.0/24 [120/2] via 172.17.17.5, em0, 00:30:30
R>* 192.168.2.0/24 [120/2] via 172.17.17.9, em1, 00:30:30
C>* 192.168.3.0/24 is directly connected, em2
R3(config)#
```

4.6) Στο R1 τα em1, em2.

Στο R2 τα em0, em2.

Στο R3 τα em0, em1.

4.7) Στο R1 σβήστηκε το δίκτυο 172.17.17.0/30 και το metric για το 192.168.2.0/24 αυξήθηκε σε 3.

Στο R2 σβήστηκε το δίκτυο 172.17.17.0/30 και το metric για το 192.168.1.0/24 αυξήθηκε σε 3.

Στο R3 σβήστηκε το δίκτυο 172.17.17.0/30.

4.8) Ναι επικοινωνούν.

4.9) Στο R1 σβήστηκε το 172.17.17.4/30, το 192.168.3.0/24 έχει πλέον metric ίσο με 3 και το 192.168.2.0/24 ίσο με 2.

Στο R2 σβήστηκε το 172.17.17.4/30 και το 192.168.1.0/24 έχει metric ίσο με 2.

Στο R3 σβήστηκε το 172.17.17.4/30 και το 192.168.1.0/24 έχει metric ίσο με 3.

4.10) Ναι επικοινωνούν.

4.11) Έγιναν αντίστοιχες αλλαγές με τα προηγούμενα ερωτήματα. Πλέον όλη η κίνηση θα περνάει από το R1. Χαρακτηριστικά στο R2 αυξήθηκε το metric του 192.168.3.0/24 σε 3 και το ίδιο έγινε στο R3 για το 192.168.2.0/24.

4.12) Ναι επικοινωνούν.

4.13) Περίπου 17 δευτερόλεπτα.

4.14) Το ttl γίνεται 62 από 61 που ήταν όσο είχαμε αποσυνδεδεμένο το καλώδιο που σημαίνει ότι παρεμβάλλονται δύο δρομολογητές αντί για τρεις.

4.15) do show ip rip
172.17.17.0/30 έχει metric 1
192.168.2.0/24 έχει metric 2

4.16) Είναι ο χρόνος που μένει για να σβηστούν από τον πίνακα διαδρομών άμα δεν λάβουμε “υπενθύμιση” για αυτές τις διαδρομές.

4.17) Έχουν metric = 16 και χρόνο ζωής περίπου 2 λεπτά.

4.18) Παίρνει metric = 3 και ο χρόνος ζωής ξαναπηγαίνει στα 3 λεπτά.

4.19) Σβήνεται εντελώς από τον πίνακα διαδρομών αφού δεν έχουμε λάβει κάποιο RIP μήνυμα για διαδρομή προς αυτό το δίκτυο.

4.20) Είναι το garbage.

4.21) Στο WAN1 γιατί έχει επιλεγμένη διαδρομή για το 172.17.17.8/30 μέσω του WAN2.

Άσκηση 5:

5.1) router rip
network 0.0.0.0/0

5.2) do show ip route rip -> 7 δυναμικές εγγραφές

5.3) do show ip route rip -> 7 δυναμικές εγγραφές

5.4) do show ip route rip -> 7 δυναμικές εγγραφές

5.5) do show ip route rip -> 7 δυναμικές εγγραφές

5.6) 0.0.0.0/0

5.7)

```
RIP02, Response, length: 204, routes: 10
AFI IPv4, 10.0.0.0/30, tag 0x0000, metric: 2, next-hop: self
AFI IPv4, 10.0.1.0/30, tag 0x0000, metric: 1, next-hop: self
AFI IPv4, 10.0.1.4/30, tag 0x0000, metric: 1, next-hop: self
AFI IPv4, 10.0.2.0/30, tag 0x0000, metric: 2, next-hop: self
AFI IPv4, 10.0.2.4/30, tag 0x0000, metric: 2, next-hop: self
AFI IPv4, 172.22.1.1/32, tag 0x0000, metric: 1, next-hop: self
AFI IPv4, 172.22.1.2/32, tag 0x0000, metric: 2, next-hop: self
AFI IPv4, 172.22.2.1/32, tag 0x0000, metric: 3, next-hop: self
AFI IPv4, 172.22.2.2/32, tag 0x0000, metric: 2, next-hop: self
AFI IPv4, 192.168.2.0/24, tag 0x0000, metric: 3, next-hop: self
```

5.8) Όχι.

5.9) network emο

5.10) 10 δυναμικές εγγραφές.

5.11) network emο

5.12) 2 διαδρομές.

Η PC1 <-> R1 <-> C2 <-> R2 <-> PC2

Και η PC1 <-> R1 <-> C1 <-> R2 <-> PC2

5.13) PC1 -> R1 -> C1 -> R2 -> PC2

5.14) PC2 -> R2 -> C1 -> R1 -> PC1

5.15) Ναι.

5.16) Ναι.

5.17) Ναι.

5.18) WAN1 : επικοινωνία παραμένει

WAN2: επικοινωνία παραμένει

WAN3: επικοινωνία παραμένει

WAN4: επικοινωνία παραμένει

CORE: επικοινωνία παραμένει

5.19) Ακόμα και αν αποσυνδέσουμε και τα τρία ταυτόχρονα η επικοινωνία δεν θα διακοπεί, απλά η κίνηση θα περνάει από το C2.

5.20) Η επικοινωνία των PC1 και PC2 θα διακοπεί αφού δεν θα υπάρχει διαδρομή μετά το C1.

5.21) Η επικοινωνία δεν θα διακοπεί αφού η κίνηση θα περνάει από το CORE.

5.22) Η επικοινωνία των PC1 και PC2 θα διακοπεί αφού δεν θα υπάρχει διαδρομή μετά το C2.

5.23) Ακόμα και αν αποσυνδέσουμε και τα τρία ταυτόχρονα η επικοινωνία δεν θα διακοπεί, απλά η κίνηση θα περνάει από το C1.

5.24) Η επικοινωνία δεν θα διακοπεί αφού τα πακέτα θα κάνουν κίνηση "X" δηλαδή $R1 \leftrightarrow C2 \leftrightarrow C1 \leftrightarrow R2$.

5.25) No route to host αφού πλέον έπεσε το WAN3 που χρησιμοποιούταν πριν.

5.26) Περίπου 15 δευτερόλεπτα.

Άσκηση 6:

6.1) ip route 4.0.0.0/8 172.22.1.2

6.2) Ναι το βλέπουμε από το S (=static).

6.3) Όχι.

6.4) Όχι δεν βλέπω κάποια αλλαγή.

6.5) Ναι προστέθηκε και είναι δυναμική εγγραφή του RIP (R).

6.6) ip route 0.0.0.0/0 172.22.2.2

6.7) Ναι προστέθηκε.

6.8) Όχι.

6.9) Όχι.

6.10) Προστέθηκε η default διαδρομή 0.0.0.0/0 .

6.11) C2 : no default-information originate

```
C1 : ip route 0.0.0.0/0 10.0.0.2  
      router rip  
      default-information originate
```

6.12) Πλέον έχει δύο εγγραφές για το 0.0.0.0/0 (=default), αυτήν που ορίσαμε στατικά στο ερώτημα 6 αλλά και αυτήν που διαφημίζει ο C1. Επιλεγμένη είναι η στατική.

6.13) no route 0.0.0.0/0 172.22.2.2

Σβήνεται η στατική εγγραφή και επιλέγεται αυτόματα η ενναλλακτική διαδρομή μέσω του C1.

6.14) 13 εγγραφές.

6.15) Γίνεται match η εγγραφή 4.0.0.0/8 του πίνακα δρομολόγησης του C1 και συνεπώς ο C1 προωθεί τα πακέτα στον 172.22.1.2 δηλαδή στον εαυτό του μέχρι να μηδενιστεί το ttl.

6.16) tcpdump -i em0 -vvv

Ο C1 έχει ως default τον C2 οπότε προωθεί το ICMP στον C2. Όμως στον πίνακα δρομολόγησης του C2 έχουμε διαδρομή default μέσω του C1 (γιατί ο C1 διαφημίζει τη διαδρομή 0.0.0.0/0 με metric 1) οπότε ο C2 προωθεί το πακέτο ξανά στον C1. Έχουμε λούπα μέχρι να μηδενιστεί το TTL.

6.17) access-list private permit 192.168.0.0/16

6.18) password ntua

exit

exit

6.19) telnet 172.22.1.1 ripd (χρησιμοποιούμε τη διεύθυνση της loopback)

6.20) enable

configure terminal

router rip

distribute-list private out em2

6.21) Μετά από τρία λεπτά λήγει το timeout και αυξάνεται σε 16 το metric όσων δικτύων δεν έχουν prefix 192.168 δηλαδή παύουν να ισχύουν οι εγγραφές.

6.22) Μετά από δύο λεπτά λήγει το garbage collect και σβήνονται εντελώς οι εγγραφές.