Computer Ανάλυση – Σημειώσεις και Θέματα Εργαστηρίου Δικτύων

Περιεχόμενα

1. Α μέρος Διευθύνσεις IP

Μια διεύθυνση IP είναι ένας μοναδικός προσδιοριστής για ένα κόμβο (node ή host) σε ένα δίκτυο. Μια IP διεύθυνση είναι ένας 32 bit δυαδικός αριθμός που αποτελείται από 4 πεδία, το καθένα εκτός των οποίων περιλαμβάνει 8 bit, ενώ σε δεκαδική τιμή το κάθε πεδίο έχει τιμή στο εύρος από 0 - 255. Τα πεδία διαχωρίζονται μεταξύ τους με τελείες.

Παράδειγμα διεύθυνσης IP		
140.179.**220**.200	ή	**10001100**.10110011.**11011100**.11001000

Κάθε διεύθυνση IP αποτελείται από δύο τμήματα: **ένα που αναγνωρίζει το δίκτυο και ένα που αναγνωρίζει τον Η/Υ (host) στο δίκτυο**. Η κλάση της διεύθυνσης και η μάσκα υποδικτύου (subnet mask) που περιγράφονται στη συνέχεια καθορίζουν ποιο τμήμα της διεύθυνσης IP ανήκει στη διεύθυνση δικτύου και ποιο τμήμα ανήκει στη διεύθυνση κόμβου.

1.1 Κλάσεις Διευθύνσεων

Υπάρχουν 5 διαφορετικές κλάσεις-κατηγορίες διευθύνσεων. Μπορούμε να βρούμε την κλάση στην οποία ανήκει μια διεύθυνση IP εξετάζοντας τα 4 πρώτα bit της διεύθυνσης IP (σε δυαδική μορφή) ή τον ακέραιο αριθμό του 1^{ου} τμήματος (σε ακέραια μορφή)

- ✓ **Οι διευθύνσεις της Class A** αρχίζουν με **0xxx** ή σε δεκαδικό συμβολισμό από **1 έως 126**
- ✓ **Οι διευθύνσεις της Class B** αρχίζουν με **10xx** ή σε δεκαδικό συμβολισμό από **128 έως 191**
- ✓ **Οι διευθύνσεις της Class C** αρχίζουν με **110x** ή σε δεκαδικό συμβολισμό από **192 έως 223**
- ✓ **Οι διευθύνσεις της Class D** αρχίζουν με **1110** ή σε δεκαδικό συμβολισμό από **224 έως 239**
- ✓ **Οι διευθύνσεις της Class E** αρχίζουνε με **1111** ή σε δεκαδικό συμβολισμό από **240 έως 254**

Σημείωση

Οι διευθύνσεις που αρχίζουν με **01111111** ή **127** έχουν δεσμευτεί για εσωτερικό έλεγχο σε ένα Η/Υ. Οι διευθύνσεις της κλάσης D έχουν δεσμευτεί για multicasting ενώ αυτές της κλάσης Ε έχουν δεσμευτεί για μελλοντική χρήση και δεν θα χρησιμοποιούνται ως διευθύνσεις για host

1.2 Τμήμα Δικτύου και Τμήμα Host

Στο ακόλουθο σχήμα εξηγείται ποιο τμήμα μιας διεύθυνσης IP αφορά το Δίκτυο-Network (Συμβολισμός με **n**) και ποιο τμήμα αφορά τον Η/Υ ή host (Συμβολισμός με h).

- ✓ **Class A** -- **nnnnnnnn**.hhhhhhhh.hhhhhhhh.hhhhhhhh
- ✓ **Class B** -- **nnnnnnnn.nnnnnnnn**.hhhhhhhh.hhhhhhhh
- ✓ **Class C** -- **nnnnnnnn.nnnnnnnn.nnnnnnnn**.hhhhhhhh

Για παράδειγμα η διεύθυνση IP 140.179.220.200 ανήκει στην κλάση Β, άρα το Τμήμα Δικτύου (Network Part) της διεύθυνσης (το οποίο ονομάζεται και Διεύθυνση Δικτύου) προσδιορίζεται από τα δύο πρώτα τμήματα της διεύθυνσης IP (140.179.x.x), ενώ το τμήμα που αφορά τον Η/Υ ή Host (το οποίο ονομάζεται και Διεύθυνση Κόμβου) προσδιορίζεται από τα δύο τελευταία τμήματα της διεύθυνσης IP (x.x.220.200).

Για να προσδιορίσουμε τη Διεύθυνση Δικτύου για μια δοθείσα διεύθυνση IP, **όλα τα host bit τίθενται στο 0, ενώ για να προσδιορίσουμε τη διεύθυνση εκπομπής του δικτύου τα host bit τίθενται στο 1**. Στο παράδειγμα μας η διεύθυνση 140.179.0.0 προσδιορίζει τη Διεύθυνση Δικτύου για την IP Διεύθυνση 140.179.220.200, ενώ η διεύθυνση 140.179.255.255 προσδιορίζει τη Διεύθυνση Εκπομπής για την IP Διεύθυνση 140.179.220.200.

1.3 Υποδικτύωση (Subnetting)

Υπάρχουν πολλοί λόγοι για να κάνουμε Υποδικτύωση σε ένα δίκτυο IP, δηλαδή να το χωρίσουμε σε υποδίκτυα, με βασικότερο αυτό του ελέγχου της κυκλοφορίας στο δίκτυο.

1.3.1 Εξορισμού Μάσκες Υποδικτύων (Default subnet masks)

- ✓ **Class A** - **255**.0.0.0 - **11111111**.00000000.00000000.00000000
- ✓ **Class B** - **255.255**.0.0 - **11111111.11111111**.00000000.00000000
- ✓ **Class C** - **255.255.255**.0 - **11111111.11111111.11111111**.00000000

Άσκηση 1

Υποθέστε ότι είστε ένας διαχειριστής δικτύου και σας εκχωρείται το εύρος IP διευθύνσεων **200.35.1.0/24**
Απαντήστε στις παρακάτω ερωτήσεις:

a) Ποια είναι η κλάση του δικτύου;

Απάντηση

Για να προσδιορίσουμε την κλάση του δικτύου εξετάζουμε το πρώτο byte. Το πρώτο byte έχει την τιμή 200 (στο δεκαδικό) που βρίσκεται στην περιοχή 192-223, συνεπώς είναι κλάσης C.

b) Στην περίπτωση που δεν κάνουμε subnetting:
i) Ποια είναι η μάσκα του δικτύου; Πόσα είναι τα bits της μάσκας;

Απάντηση

Το εν λόγω δίκτυο είναι ένα δίκτυο κλάσης C, συνεπώς αφού δεν κάνουμε subnetting, η μάσκα είναι η **255.255.255.0** ή σε δυαδική μορφή η **11111111.11111111.11111111.00000000**, συνεπώς τα bits της μάσκας είναι συνολικά **24**

ii) Ποια είναι η διεύθυνση εκπομπής του δικτύου;

Απάντηση

Η διεύθυνση εκπομπής προκύπτει εάν δώσουμε την τιμή 1 σε όλα τα host bits δηλαδή είναι η **200.35.1.*11111111*** ή σε δεκαδική μορφή η **200.35.1.255**

iii) Πόσες και ποιες είναι οι διαθέσιμες διευθύνσεις Η/Υ;

Απάντηση

Έχουμε 8 host bits για host, άρα οι διαθέσιμες δ/νσεις Η/Υ είναι 2^8-2=254 και είναι οι ακόλουθες:

200.35.1.*00000001*	**200.35.1.*1***
200.35.1.*00000010*	**200.35.1.*2***
200.35.1.*00000011*	**200.35.1.*3***
……..	
200.35.1.*11111110*	**200.35.1.*254***

c) Στην περίπτωση που κάνουμε subnetting και θέλουμε να δημιουργηθούν 8 τουλάχιστον υποδίκτυα:
i) Προσδιορίστε τα Subnet Bits που απαιτούνται καθώς και τη Subnet Mask που προκύπτει.

Απάντηση

Αφού θέλουμε να δημιουργηθούν 8 υποδίκτυα, απαιτούνται τουλάχιστον 3 subnet bits, τα οποία μας δίνουν 2^3=8 υποδίκτυα.
Η subnet mask **πριν** το subnetting ήταν η **11111111.11111111.11111111.00000000**. Αφού θέλουμε 3 subnet bits, αυτό σημαίνει ότι η νέα μάσκα **μετά** το subnetting είναι η **1111111.11111111.11111111.<u>111</u>00000** ή σε δεκαδική μορφή η **255.255.255.<u>224</u>**

ii) Προσδιορίστε τα 8 υποδίκτυα που προκύπτουν.

Απάντηση

Η αρχική διεύθυνση του κάθε υποδικτύου είναι:

Υποδίκτυο #0: 200.35.1.**<u>000</u>**00000	200.35.1.**<u>0</u>**
Υποδίκτυο #1: 200.35.1.**<u>001</u>**00000	200.35.1.**<u>32</u>**
Υποδίκτυο #2: 200.35.1.**<u>010</u>**00000	200.35.1.**<u>64</u>**
Υποδίκτυο #3: 200.35.1.**<u>011</u>**00000	200.35.1.**<u>96</u>**
Υποδίκτυο #4: 200.35.1.**<u>100</u>**00000	200.35.1.**<u>128</u>**
Υποδίκτυο #5: 200.35.1.**<u>101</u>**00000	200.35.1.**<u>160</u>**
Υποδίκτυο #6: 200.35.1.**<u>110</u>**00000	200.35.1.**<u>192</u>**
Υποδίκτυο #7: 200.35.1.**<u>111</u>**00000	200.35.1.**<u>224</u>**

iii) Προσδιορίστε τις διευθύνσεις εκπομπής του κάθε υποδικτύου.

Απάντηση

Η δ/νση εκπομπής για κάθε ένα από τα υποδίκτυα είναι:

Υποδίκτυο #0: 200.35.1.**<u>000</u>***11111*	200.35.1.*31*
Υποδίκτυο #1: 200.35.1.**<u>001</u>***11111*	200.35.1.*63*
Υποδίκτυο #2: 200.35.1.**<u>010</u>***11111*	200.35.1.*95*
Υποδίκτυο #3: 200.35.1.**<u>011</u>***11111*	200.35.1.*127*
Υποδίκτυο #4: 200.35.1.**<u>100</u>***11111*	200.35.1.*159*
Υποδίκτυο #5: 200.35.1.**<u>101</u>***11111*	200.35.1.*191*
Υποδίκτυο #6: 200.35.1.**<u>110</u>***11111*	200.35.1.*223*

Υποδίκτυο #7: 200.35.1.**111***11111* 200.35.1.*255*

iv) Προσδιορίστε το πλήθος και τις διαθέσιμες διευθύνσεις Η/Υ για κάθε υποδίκτυο ξεχωριστά.

Απάντηση

Αφού έχουμε 5 host bits, το πλήθος των διαθέσιμων δ/νσεων Η/Υ **σε κάθε υποδίκτυο είναι 2^5-2=30**. Οι διαθέσιμες δ/νσεις Η/Υ (host) για κάθε υποδίκτυο αναλυτικά είναι:

Υποδίκτυο #0: Από 200.35.1.1 έως 200.35.1.30 (δηλαδή από **000** 00001 έως **000** 11110)

Υποδίκτυο #1: Από 200.35.1.33 έως 200.35.1.62

Υποδίκτυο #2: Από 200.35.1.65 έως 200.35.1.94

Υποδίκτυο #3: Από 200.35.1.97 έως 200.35.1.126

Υποδίκτυο #4: Από 200.35.1.129 έως 200.35.1.158

Υποδίκτυο #5: Από 200.35.1.161 έως 200.35.1.190

Υποδίκτυο #6: Από 200.35.1.193 έως 200.35.1.222

Υποδίκτυο #7: Από 200.35.1.225 έως 200.35.1.254

Άσκηση 2

Σας δίνονται οι παρακάτω IP διευθύνσεις:
i) 192.168.1.63/29
ii) 192.168.37.192/25
iii) 172.17.16.255/23
iv) 10.0.8.0/22

Τι είδους διευθύνσεις είναι αυτές: **network, directed broadcast ή host**;

Απάντηση

i) 192.168.1.63/29

Όταν μια IP δίνεται στη γενική μορφή A.B.C.D./E ο αριθμός Ε μετά το / υποδηλώνει πάντα τα networks bits και σε αυτή την περίπτωση ΔΕΝ δουλεύουμε με κλάσεις. Για παράδειγμα στη δοθείσα IP 192.168.1.63/29 έχουμε 29 networks bits, δεν μας ενδιαφέρει η κλάση στην οποία ανήκει η IP και ισχύουν τα εξής:

IP	192	168	1	63
Network bits	**nnnnnnnn**	**nnnnnnnn**	**nnnnnnnn**	**nnnnn***hhh*
	8 network bits	**8 network bits**	**8 network bits**	**5 network bits *και 3 host bits***

Τα host bits είναι στο τελευταίο τμήμα της IP, γιαυτό γράφουμε το 63 σε δυαδική μορφή ως εξής:

Θέση	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**
bit	**0**	**0**	**1**	**1**	**1**	***1***	***1***	***1***

Παρατηρούμε ότι ΟΛΑ ΤΑ HOST BIT είναι 1 συνεπώς η δοθείσα IP είναι DIRECTED BROADCAST διεύθυνση.

ii) 192.168.37.192/25

Στη δοθείσα IP 192.168.37.192/25 έχουμε 25 networks bits και ισχύουν τα εξής:

IP	192	168	37	192
Network bits	**nnnnnnnn**	**nnnnnnnn**	**nnnnnnnn**	**n***hhhhhhh*
	8 network bits	**8 network bits**	**8 network bits**	**1 network bit και** *7 host bits*

Τα host bits είναι στο τελευταίο τμήμα της IP, γιαυτό γράφουμε το 192 σε δυαδική μορφή ως εξής:

Θέση	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**
bit	1	***1***	***0***	***0***	***0***	***0***	***0***	***0***

Παρατηρούμε ότι τα HOST BIT ΔΕΝ ΕΙΝΑΙ ΟΥΤΕ ΟΛΑ 0 ΟΥΤΕ ΟΛΑ 1, συνεπώς η δοθείσα IP είναι διεύθυνση HOST.

iii) 172.17.16.255/23

Στη δοθείσα IP 172.17.16.255/23 έχουμε 23 networks bits και ισχύουν τα εξής:

IP	172	17	16	255
Network bits	**nnnnnnnn**	**nnnnnnnn**	**nnnnnnn***h*	*hhhhhhhh*
	8 network bits	**8 network bits**	**7 network bits** *και 1 host bit*	*8 host bits*

Τα host bits είναι στα 2 τελευταία τμήματα της IP, γιαυτό γράφουμε το 16 και το 255 σε δυαδική μορφή ως εξής:

Θέση	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**		**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**
bit	0	0	0	1	0	0	0	***0***		***1***	***1***	***1***	***1***	***1***	***1***	***1***	***1***

Παρατηρούμε ότι τα HOST BIT ΔΕΝ ΕΙΝΑΙ ΟΥΤΕ ΟΛΑ 1 ΟΥΤΕ ΟΛΑ 0, συνεπώς η δοθείσα IP είναι διεύθυνση HOST.

iv) 10.0.8.0/22

Στη δοθείσα IP 10.0.8.0/22 έχουμε 22 networks bits και ισχύουν τα εξής:

IP	10	0	8	0
Network bits	**nnnnnnnn**	**nnnnnnnn**	**nnnnnn***hh*	*hhhhhhhh*
	8 network bits	**8 network bits**	**6 network bits** *και 2 host bit*	*8 host bits*

Τα host bits είναι στα 2 τελευταία τμήματα της IP, γιαυτό γράφουμε το 8 και το 0 σε δυαδική μορφή ως εξής:

Θέση	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**		**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**
bit	0	0	0	0	1	0	***0***	***0***		***0***	***0***	***0***	***0***	***0***	***0***	***0***	***0***

Παρατηρούμε ότι τα HOST BIT ΕΙΝΑΙ ΟΛΑ 0, συνεπώς η δοθείσα IP είναι διεύθυνση NETWORK.

Άσκηση 3

Υποθέστε ότι είστε ένας διαχειριστής δικτύου και σας εκχωρείται το εύρος IP διευθύνσεων 170.5.0.0/16.

a) Ποια είναι η κλάση του δικτύου;

Απάντηση

Για να προσδιορίσουμε την κλάση του δικτύου, ελέγχουμε το πρώτο byte. Το πρώτο byte έχει την τιμή 170 (στο δεκαδικό) που βρίσκεται στην περιοχή 128-191, συνεπώς είναι κλάσης B.

b) Στην περίπτωση που δεν κάνουμε subnetting:

i) Ποια είναι η μάσκα του δικτύου; Πόσα είναι τα bits της μάσκας;

Απάντηση

Το εν λόγω δίκτυο είναι ένα δίκτυο κλάσης B, συνεπώς αφού δεν κάνουμε subnetting, η μάσκα είναι η **255.255**.0.0 ή σε δυαδική μορφή **11111111.11111111**.00000000.00000000 συνεπώς τα bits της μάσκας είναι 16

ii) Ποια είναι η διεύθυνση εκπομπής του δικτύου;

Απάντηση

Η δ/νση εκπομπής προκύπτει εάν δώσουμε την τιμή 1 σε όλα τα host bits δηλ. είναι η **170.5.11111111.11111111** ή σε δεκαδική μορφή η **170.5.255.255**

iii) Πόσες και ποιες είναι οι διαθέσιμες διευθύνσεις Η/Υ;

Απάντηση

Έχουμε 16 host bits κατάληξη δηλ. 16 bits διαθέσιμα για διευθύνσεις Η/Υ, συνεπώς οι διαθέσιμες δ/νσεις για Η/Υ είναι σε πλήθος 2^{16}-2=65534. Αναλυτικά είναι οι παρακάτω:

170.5.00000000.00000001 170.5.0.1
170.5.00000000.00000010 170.5.0.2
170.5.000000000.00000011 170.5.0.3
…..
170.5.00000000.11111111 170.5.0.255

170.5.00000001.00000001 170.5.1.0
170.5.00000001.00000010 170.5.1.1
170.5.00000001.00000010 170.5.1.2
…..
170.5.00000001.11111111 170.5.1.255
…..
170.5.11111111.11111110 170.5.255.0
170.5.11111111.11111110 170.5.255.1

170.5.11111111.11111110 170.5.255.2

…..

170.5.11111111.11111110 170.5.255.254

c) Στην περίπτωση που κάνουμε subnetting και θέλουμε να δημιουργηθούν 70 τουλάχιστον υποδίκτυα:
i) Προσδιορίστε τα Subnet Bits που απαιτούνται καθώς και τη Subnet Mask που προκύπτει.
Απάντηση:
Αφού θέλουμε να δημιουργηθούν 70 υποδίκτυα, απαιτούνται τουλάχιστον 7 subnet bits, τα οποία μας δίνουν 2^7=128 υποδίκτυα. Η subnet mask πριν το subnetting ήταν η **11111111.11111111.00000000.00000000**. Αφού έχουμε 7 subnet bits, σημαίνει ότι η νέα μάσκα είναι η **1111111.11111111.11111110.00000000** δηλ. τελικά η **255.255.254.0**. Τα bits για subnetting τα παίρνουμε πάντα από τα network bits

ii) Προσδιορίστε τα 70 υποδίκτυα που προκύπτουν.
Απάντηση:
Τα 70 υποδίκτυα που προκύπτουν είναι:
Υποδίκτυο #0: 170.5.**0000000**0.00000000 ή 170.5.0.0
Υποδίκτυο #1: 170.5.**0000001**0.00000000 ή 170.5.2.0
Υποδίκτυο #2: 170.5.**0000010**0.00000000 ή 170.5.4.0
Υποδίκτυο #3: 170.5.**0000011**0.00000000 ή 170.5.6.0
…….
Υποδίκτυο #69: 170.5.**1000101**0.00000000 ή 170.5.138.0

iii) Προσδιορίστε τις διευθύνσεις εκπομπής του κάθε υποδικτύου.
Απάντηση
Η δ/νση εκπομπής για κάθε ένα από τα υποδίκτυα είναι:
Υποδίκτυο #0: 170.5.**0000000**1.11111111 ή 170.5.1.255
Υποδίκτυο #1: 170.5.**0000001**1.11111111 ή 170.5.3.255
Υποδίκτυο #2: 170.5.**0000010**1.11111111 ή 170.5.5.255
Υποδίκτυο #3: 170.5.**0000011**1.11111111 ή 170.5.7.255
…….
Υποδίκτυο #69: 170.5.**1000101**1.11111111 ή 170.5.139.255

iv) Προσδιορίστε το πλήθος και τις διαθέσιμες διευθύνσεις Η/Υ για κάθε υποδίκτυο αναλυτικά.
Απάντηση
Αφού έχουμε 16-7=9 host bits, το πλήθος των διαθέσιμων δ/νσεων Η/Υ ανά υποδίκτυο είναι 2^9-2=510. Άρα το κάθε υποδίκτυο θα έχει 510 Η/Υ.
Οι διαθέσιμες δ/νσεις για κάθε υποδίκτυο αναλυτικά είναι:
Υποδίκτυο #0: 170.5.**00000000.00000001** έως 170.5.**00000001.11111110** ή 170.5.0.1 έως 170.5.1.254
Υποδίκτυο #1: 170.5.**00000010.00000001** έως 170.5.**00000011.11111110** ή 170.5.2.1 έως 170.5.3.254
Υποδίκτυο #2: 170.5.**00000100.00000001** έως 170.5.**00000101.11111110** ή 170.5.4.1 έως 170.5.5.254
Υποδίκτυο #3: 170.5.**00000100.00000001** έως 170.5.**00000111.11111110** ή 170.5.6.1 έως 170.5.7.254
…….
Υποδίκτυο #69: 170.5. **10001010.00000001** έως 170.5.**10001011.11111110** ή 170.5.138.1 έως 170.5.139.254

Άσκηση 4
Τι είδους διευθύνσεις είναι οι **172.16.4.255/22**, **192.168.37.255/25**, **172.17.16.255/23** και **10.0.5.0/22; network, directed broadcast ή host**;
Απάντηση
i) **172.16.4.255/22**

IP	172	16	4	255
Network bits	**nnnnnnnn**	**nnnnnnnn**	**nnnnnn***hh*	*hhhhhhhh*
	8 network bits	**8 network bits**	**6 network bits** *και 2 host bits*	*8 host bits*

Τα host bits είναι στα 2 τελευταία τμήματα της IP, γιαυτό γράφουμε το 4 και το 255 σε δυαδική μορφή ως εξής:

Θέση	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**		**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**
bit	**0**	**0**	**0**	**0**	**0**	**1**	***0***	***0***		***1***	***1***	***1***	***1***	***1***	***1***	***1***	***1***

Παρατηρούμε ότι ΤΑ HOST BIT είναι ΔΕΝ ΕΙΝΑΙ ΟΥΤΕ ΟΛΑ 0 ΟΥΤΕ ΟΛΑ 1 συνεπώς η δοθείσα IP είναι HOST διεύθυνση.

ii) **192.168.37.255/25**

IP	192	168	37	255

Network bits	**nnnnnnnn**	**nnnnnnnn**	**nnnnnnnn**	**n***hhhhhhh*
	8 network bits	**8 network bits**	**8 network bits**	**1 network bit** *και 7 host bits*

Τα host bits είναι στο τελευταίο τμήμα της IP, γιαυτό γράφουμε το 255 σε δυαδική μορφή ως εξής:

Θέση	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**
bit	*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*

Παρατηρούμε ότι τα HOST BIT ΕΙΝΑΙ ΟΛΑ 1, συνεπώς η δοθείσα IP είναι DIRECTED BROADCAST διεύθυνση.

iii) **172.17.16.255/23**

IP	172	17	16	255
Network bits	**nnnnnnnn**	**nnnnnnnn**	**nnnnnnn***h*	*hhhhhhhh*
	8 network bits	**8 network bits**	**7 network bits** *και 1 host bit*	*8 host bits*

Τα host bits είναι στα 2 τελευταία τμήματα της IP, γιαυτό γράφουμε το 16 και το 255 σε δυαδική μορφή ως εξής:

Θέση	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**		**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**
bit	**0**	**0**	**0**	**1**	**0**	**0**	**0**	*0*		*1*	*1*	*1*	*1*	*1*	*1*	*1*	*1*

Παρατηρούμε ότι τα HOST BIT ΔΕΝ ΕΙΝΑΙ ΟΥΤΕ ΟΛΑ 0 ΟΥΤΕ ΟΛΑ 1, συνεπώς η δοθείσα IP είναι HOST διεύθυνση.

iv) **10.0.5.0/22**

Στη δοθείσα IP 10.0.5.0/2 έχουμε 22 networks bits και ισχύουν τα εξής:

IP	10	0	5	255
Network bits	**nnnnnnnn**	**nnnnnnnn**	**nnnnnn***hh*	*hhhhhhhh*
	8 network bits	**8 network bits**	**6 network bits** *και 2 host bit*	*8 host bits*

Τα host bits είναι στα 2 τελευταία τμήματα της IP, γιαυτό γράφουμε το 5 και το 0 σε δυαδική μορφή ως εξής:

Θέση	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**		**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**
bit	**0**	**0**	**0**	**0**	**0**	**1**	*0*	*1*		*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*

Παρατηρούμε ότι τα HOST BIT ΔΕΝ ΕΙΝΑΙ ΟΥΤΕ ΟΛΑ 0 ΟΥΤΕ ΟΛΑ 1, συνεπώς η δοθείσα IP είναι HOST διεύθυνση.

Άσκηση 5

Στις αρχές της δεκαετίας του ’90 η IP διευθυνσιοδότηση που βασιζόταν σε κλάσεις αντικαταστάθηκε από τη λύση της υποδικτύωσης με το Classless Interdomain Routing (CIDR). Υποθέστε ότι είστε ένας διαχειριστής δικτύου και σας εκχωρείται το εύρος IP διευθύνσεων 150.150.17.0/24. Απαντήστε στις παρακάτω ερωτήσεις:

a) Θεωρώντας ότι δεν χωρίζουμε το εύρος σε μικρότερα υποδίκτυα:
   i) Ποια είναι η μάσκα του δικτύου;
   ii) Ποια είναι η διεύθυνση εκπομπής του δικτύου;
   iii) Πόσες και ποιες είναι οι διαθέσιμες διευθύνσεις Η/Υ;

Αναζητήστε τις έννοιες των all ones και all zeros subnets στα RFC 950 και 1878 και καταγράψτε τι προτείνουν ως προς τη χρησιμοποίησή τους.

b) Θεωρώντας ότι θέλουμε να διαχωρίσουμε το παραπάνω εύρος διευθύνσεων σε 4 όσο γίνεται μεγαλύτερα υποδίκτυα ακολουθώντας το RFC 1878.
   i) Προσδιορίστε τα Subnet Bits που απαιτούνται καθώς και τη Subnet Mask που προκύπτει.
   ii) Προσδιορίστε τα 4 υποδίκτυα που προκύπτουν.
   iii) Προσδιορίστε τις διευθύνσεις εκπομπής του κάθε υποδικτύου.
   iv) Προσδιορίστε το πλήθος και τις διαθέσιμες διευθύνσεις Η/Υ για κάθε υποδίκτυο αναλυτικά.

c) Θεωρώντας ότι θέλουμε να διαχωρίσουμε το παραπάνω εύρος διευθύνσεων σε 4 όσο γίνεται μεγαλύτερα υποδίκτυα ακολουθώντας το RFC 950.
   i) Προσδιορίστε τα Subnet Bits που απαιτούνται καθώς και τη Subnet Mask που προκύπτει.
   ii) Προσδιορίστε τα 4 υποδίκτυα που προκύπτουν.
   iii) Προσδιορίστε τις διευθύνσεις εκπομπής του κάθε υποδικτύου.
   iv) Προσδιορίστε το πλήθος και τις διαθέσιμες διευθύνσεις Η/Υ για κάθε υποδίκτυο αναλυτικά.

Απάντηση

a)

i) Αφού η IP διεύθυνση είναι η 150.150.17.0/24, συμπεραίνουμε ότι για την ανάθεση διεύθυνσης στο υποδίκτυο αυτό απομένουν 8 bits, αφού τα 24 αποτελούν το αναγνωριστικό του υποδικτύου. Έτσι θα υπάρχουν 2^8 = 256 διαθέσιμες διευθύνσεις, πλην όμως του 0 (διεύθυνση υποδικτύου) και του 255 (διεύθυνση εκπομπής), άρα 254. Η μάσκα του υποδικτύου θα είναι η **255.255.255.0**

ii) Όπως και σε κάθε δίκτυο, η διεύθυνση εκπομπής θα είναι η τελευταία διαθέσιμη, η 150.150.17.255

iii) Έχουμε 256 διαθέσιμες διευθύνσεις από τις οποίες οι 254 (2^8-2) είναι διαθέσιμες για διευθύνσεις Η/Υ, μιας και οι διευθύνσεις 150.150.17.0 και 150.150.17.255 είναι δεσμευμένες ως διεύθυνση του υποδικτύου και διεύθυνση εκπομπής αντίστοιχα. Συνεπώς, οι διαθέσιμες διευθύνσεις είναι της μορφής 150.150.17.X, όπου X: οποιοσδήποτε αριθμός από 1 έως 254.

b) Για να γίνει διαχωρισμός ενός δικτύου σε υποδίκτυα, θα πρέπει η IP διεύθυνση να διαμορφωθεί με τρόπο που να περιγράφει όχι μόνο τον υπολογιστή, αλλά και το υποδίκτυο. Έτσι για τον καθορισμό των υποδικτύων χρησιμοποιούνται τα πιο σημαντικά και ελεύθερα bits της IP διεύθυνσης. Έτσι, στην περίπτωση της IP 150.150.17.0/24, τα 24 bits είναι δεσμευμένα και άρα 2 από τα 8 που απομένουν θα χρησιμοποιηθούν για τον καθορισμό των υποδικτύων. Οι έννοιες των all zeros και all ones subnets αναφέρονται στους συνδυασμούς των bits που χρησιμοποιούνται για τον καθορισμό του υποδικτύου οι οποίοι είναι «όλο μηδέν» ή «όλο ένα», δηλαδή στην προκειμένη περίπτωση τους 00 και 11. Αναλόγως το πρωτόκολλο, αυτοί οι συνδυασμοί είτε επιτρέπονται είτε όχι.

Το πρωτόκολλο RFC 1878 επιτρέπει τη χρήση των all zeros και all ones υποδικτύων αυτό σημαίνει ότι στα subnet bits μπορούν να τεθούν όλοι οι πιθανοί συνδυασμοί

Για να κωδικοποιηθούν 4 υποδίκτυα, θα χρειαστούν 2 subnet bits, αφού οι συνδυασμοί 00 και 11 επιτρέπονται. Έτσι, τα host bit θα είναι 6 με 2^6-2=62 host σε κάθε υποδίκτυο, ενώ με τα 2 subnet θα δημιουργηθούν 4 υποδίκτυα. Έτσι το εύρος του υποδικτύου θα είναι **150.150.17.0/26** και η μάσκα **255.255.255.192**

Στον ακόλουθο πίνακα φαίνονται τα 4 υποδίκτυα όπως καθορίζονται από τα 2 subnet bits, οι διευθύνσεις εκπομπής του καθενός, οι διαθέσιμες διευθύνσεις και το πλήθος τους.

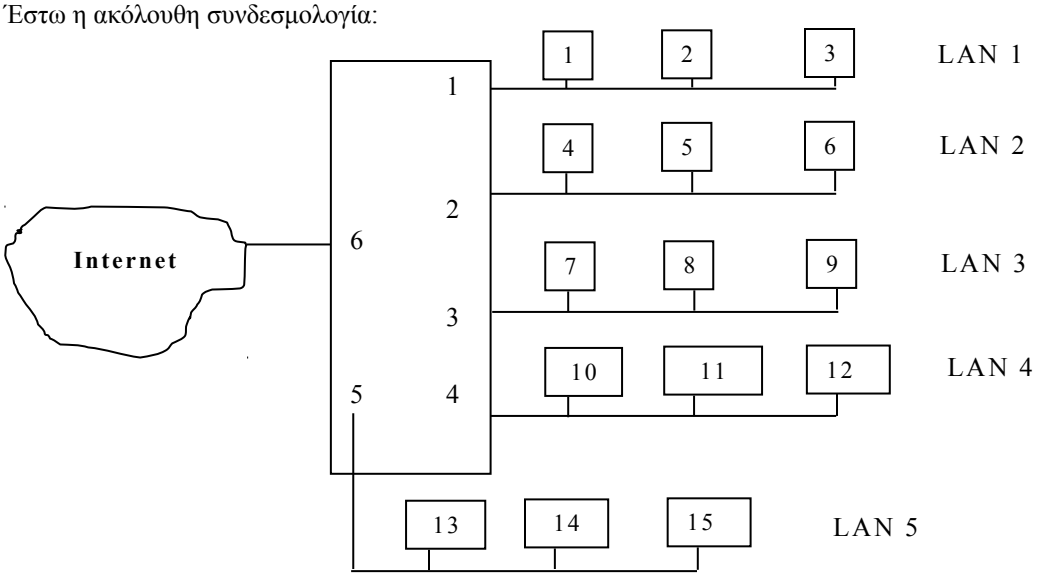
Subnet Bits	Διεύθυνση Υποδικτύου	Διεύθυνση Εκπομπής	Διαθέσιμες Διευθύνσεις	Πλήθος Η/Υ
00	150.150.17.0	150.150.17.63	150.150.17.1 - 150.150.17.62	62
01	150.150.17.64	150.150.17.127	150.150.17.65 - 150.150.17.126	62
10	150.150.17.128	150.150.17.193	150.150.17.129 - 150.150.17.190	62
11	150.150.17.192	150.150.17.255	150.150.17.193 - 150.150.17.254	62

c)**Το πρωτόκολλο RFC 950 ΔΕΝ επιτρέπει τη χρήση των all zeros και all ones υποδικτύων.**
Για να κωδικοποιηθούν 4 υποδίκτυα, θα χρειαστούν 3subnet bits, αφού οι συνδυασμοί 00 (all zeros) και 11 (all ones) δεν επιτρέπονται. Άρα θα χρειαστεί ένα ακόμη bit ώστε να υπάρξουν 4 αποδεκτοί συνδυασμοί. Έτσι τα host bit θα είναι 5 με 2^5-2=30 host σε κάθε υποδίκτυο και τα subnet bits 3. Έτσι το εύρος του υποδικτύου θα είναι **150.150.17.0/27** και η μάσκα **255.255.255.224**

Subnet Bits	Διεύθυνση Υποδικτύου	Διεύθυνση Εκπομπής	Διαθέσιμες Διευθύνσεις	Πλήθος Η/Υ
001	150.150.17.32	150.150.17.63	150.150.17.33 - 150.150.17.62	30
010	150.150.17.64	150.150.17.95	150.150.17.65 - 150.150.17.94	30
011	150.150.17.96	150.150.17.127	150.150.17.97 - 150.150.17.126	30
100	150.150.17.128	150.150.17.159	150.150.17.129 - 150.150.17.158	30

Ας σημειωθεί ότι υπάρχουν δυο συνδυασμοί (000, 111) που δεν επιτρέπονται, και ακόμη δυο (101, 110) των οποίων τα υποδίκτυα αγνοούνται, μιας και εδώ μας αρκούν 4.

Άτυπη 2009 – Θέμα 1
Έστω η ακόλουθη συνδεσμολογία:



Δίνεται η διεύθυνση 192.168.12.0 και θέλουμε να δημιουργήσουμε 5 υποδίκτυα (LANS). Να προσδιορίσετε τα ακόλουθα για το κάθε υποδίκτυο:
α)Διεύθυνση Υποδικτύου
β)Διεύθυνση Εκπομπής υποδικτύου
γ)Εύρος Διευθύνσεων host σε κάθε υποδίκτυο
δ)Πλήθος host σε κάθε υποδίκτυο
ε)Μάσκα Υποδικτύου
Απάντηση

IP Address 192.168.12.0 | Subnet Mask 255.255.255.224 | Generate Subnets

Mask Bits 27 | Number of Subnets 8

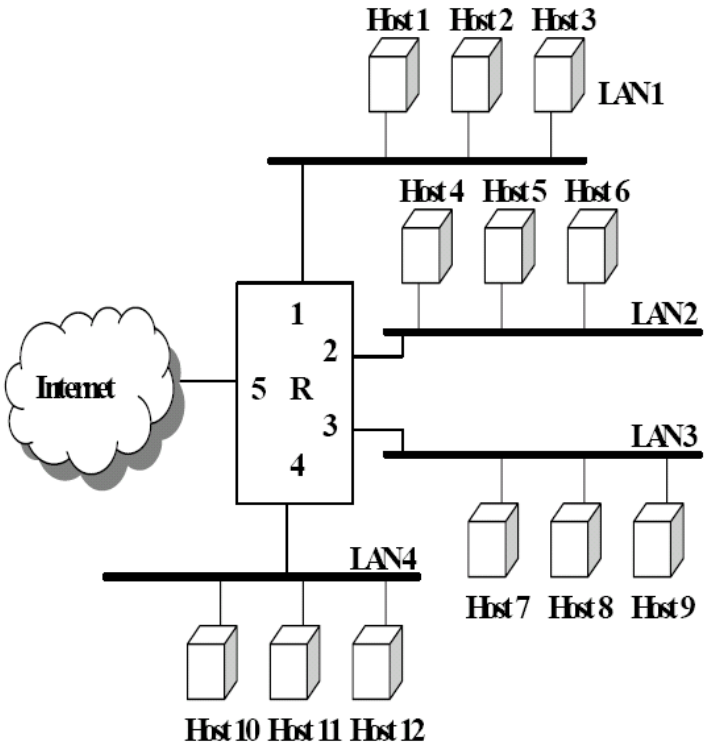
Host Bits 5 | Hosts per Subnet 30

Subnet Bit Mask 110nnnnn.nnnnnnnn.nnnnnnnn.sssHHHHH

Subnet	Mask	Inverse Mask	Subnet Size	Host Range	Broadcast
192.168.12.0	255.255.255.224	0.0.0.31	30	192.168.12.1 to 192.168.12.30	192.168.12.31
192.168.12.32	255.255.255.224	0.0.0.31	30	192.168.12.33 to 192.168.12.62	192.168.12.63
192.168.12.64	255.255.255.224	0.0.0.31	30	192.168.12.65 to 192.168.12.94	192.168.12.95
192.168.12.96	255.255.255.224	0.0.0.31	30	192.168.12.97 to 192.168.12.126	192.168.12.127
192.168.12.128	255.255.255.224	0.0.0.31	30	192.168.12.129 to 192.168.12.158	192.168.12.159
192.168.12.160	255.255.255.224	0.0.0.31	30	192.168.12.161 to 192.168.12.190	192.168.12.191
192.168.12.192	255.255.255.224	0.0.0.31	30	192.168.12.193 to 192.168.12.222	192.168.12.223
192.168.12.224	255.255.255.224	0.0.0.31	30	192.168.12.225 to 192.168.12.254	192.168.12.255

Άσκηση 6

(12)Σας δίνετε το δίκτυο 195.100.100.0, το οποίο πρέπει να χωρίσετε στα τέσσερα υποδίκτυα (LAN1 εώς LAN4) του ακόλουθου σχήματος. Τα εν λόγω υποδίκτυα βγαίνουν στο διαδίκτυο μέσω του δρομολογητή R. Συμπληρώστε τον πίνακα που ακολουθεί. Σημειώνεται ότι με RX (όπου X=1..5) συμβολίζεται η X διεπαφή του δρομολογητή R.



Για να φτιάξουμε 4 υποδίκτυα + Internet θα κλέψουμε 3 bit από τα host bit και η μάσκα υποδικτύου που προκύπτει είναι 255.255.255.11100000 ή 255.255.255.224

	IP Address	**Subnet Mask**
R1	**195.100.100.000<u></u>00000 ή 195.100.100.0**	**255.255.255.224**
Host 1	195.100.100.000<u></u>00001 ή 195.100.100.1	255.255.255.224
Host 2	195.100.100.000<u></u>00010 ή 195.100.100.2	255.255.255.224
Host 3	195.100.100.000<u></u>00011 ή 195.100.100.3	255.255.255.224
R2	**195.100.100.001<u></u>00000 ή 195.100.100.64**	**255.255.255.224**
Host 1	195.100.100.001<u></u>00001 ή 195.100.100.65	255.255.255.224
Host 2	195.100.100.001<u></u>00010 ή 195.100.100.66	255.255.255.224
Host 3	195.100.100.001<u></u>00011 ή 195.100.100.67	255.255.255.224
R3	**195.100.100.011<u></u>00000 ή 195.100.100.96**	**255.255.255.224**
Host 1	195.100.100.011<u></u>00001 ή 195.100.100.97	255.255.255.224
Host 2	195.100.100.011<u></u>00010 ή 195.100.100.98	255.255.255.224
Host 3	195.100.100.011<u></u>00011 ή 195.100.100.99	255.255.255.224

R4	**195.100.100.10000000 ή 195.100.100.128**	**255.255.255.224**
Host 1	195.100.100.10000001 ή 195.100.100.129	255.255.255.224
Host 2	195.100.100.10000010 ή 195.100.100.130	255.255.255.224
Host 3	195.100.100.10000011 ή 195.100.100.131	255.255.255.224
R5	**195.100.100.10100000 ή 195.100.100.162**	**255.255.255.224**

Άσκηση 7

Υποθέστε ότι είστε ένας διαχειριστής δικτύου και σας εκχωρείται το εύρος IP διευθύνσεων 132.90.0.0. Απαντήστε στις παρακάτω ερωτήσεις:

a) Στην περίπτωση που δεν κάνουμε subnetting
   i) Ποια είναι η κλάση του δικτύου;
   ii) Ποια είναι η μάσκα του δικτύου; Πόσα είναι τα bits της μάσκας;
   iii) Ποια είναι η διεύθυνση εκπομπής του δικτύου;
   iv) Πόσες και ποιες είναι οι διαθέσιμες διευθύνσεις Η/Υ;

b) Στην περίπτωση που κάνω subnetting, και θέλω να δημιουργηθούν 8 τουλάχιστον υποδίκτυα:
   i) Προσδιορίστε τα Subnet Bits που απαιτούνται καθώς και τη Subnet Mask που προκύπτει.
   ii) Προσδιορίστε τα 8 υποδίκτυα που προκύπτουν.
   iii) Προσδιορίστε τις διευθύνσεις εκπομπής του κάθε υποδικτύου.
   iv) Προσδιορίστε το πλήθος και τις διαθέσιμες διευθύνσεις Η/Υ για κάθε υποδίκτυο αναλυτικά.

c) Στη συνέχεια, το δεύτερο υποδίκτυο του ερωτήματος (b) θέλουμε να το χωρίσουμε σε 4 ίσα υποδίκτυα
   i) Προσδιορίστε τα Subnet Bits που απαιτούνται καθώς και τη Subnet Mask που προκύπτει.
   ii) Προσδιορίστε τα 4 υποδίκτυα που προκύπτουν.
   iii) Προσδιορίστε τις διευθύνσεις εκπομπής του κάθε υποδικτύου.
   iv) Προσδιορίστε το πλήθος και τις διαθέσιμες διευθύνσεις Η/Υ για κάθε υποδίκτυο αναλυτικά.

Απάντηση

a) Στην περίπτωση που δεν κάνουμε subnetting

i) Το εύρος διευθύνσεων που μας εκχωρείται είναι κλάσης Β, εφόσον η πρώτη οκτάδα ανήκει στην περιοχή 128-191 στην οποία αντιστοιχεί η κλάση Β.

ii) Εφόσον δεν δίνεται μάσκα δικτύου ρητά, χρησιμοποιούμε την default μάσκα δικτύου για την κλάση Β, η οποία είναι η 255.255.0.0. Η συγκεκριμένη μάσκα χρησιμοποιεί 16 bits.

iii) Η διεύθυνση εκπομπής του δικτύου είναι η διεύθυνση που προκύπτει αν σε όλα τα bits της διεύθυνσης που αντιστοιχούν σε bit της μάσκας που είναι 0, βάλουμε 1. Η διεύθυνση εκπομπής επομένως είναι η 132.90.255.255.

iv) Η μάσκα χρησιμοποιεί 16 bits, επομένως υπολείπονται 16 bits για τη διευθυνσιοδότηση των hosts. Θεωρώντας ως μη διαθέσιμες την διεύθυνση δικτύου και την διεύθυνση εκπομπής, ο αριθμός των hosts που μπορούν να διευθυνσιοδοτηθούν είναι: 2^(32-16)-2=65534.

b) Στην περίπτωση που κάνω subnetting και θέλω τουλάχιστον 8 υποδίκτυα

Σύμφωνα με το RFC950 το all zeros και το all ones subnets δεν είναι διαθέσιμα, καθώς έχουν ειδική σημασία. Αν κάνουμε την υποδικτύωση με το RFC1878 η ειδική σημασία δεν ισχύει, οπότε μπορούμε να τα χρησιμοποιήσουμε. Κάνουμε την παραδοχή ότι η υποδικτύωση γίνεται σύμφωνα με το RFC1878, οπότε μπορούμε να τα χρησιμοποιήσουμε.

i) Για να έχουμε 8 υποδίκτυα, πρέπει να δεσμεύσουμε 3 bits από τη subnet mask για να τα δημιουργήσουμε. Επομένως η νέα subnet mask είναι των 19 bits και συγκεκριμένα η 255.255.224.0.

ii)iii)iv) Τα νέα υποδίκτυα που προκύπτουν και τα χαρακτηριστικά τους είναι:

Υποδίκτυο	**Διεύθυνση εκπομπής**	**Διαθέσιμοι host**
132.90.0.0/19	132.90.31.255	132.90.0.1-132.90.31.254
132.90.32.0/19	132.90.63.255	132.90.32.1-132.90.63.254
132.90.64.0/19	132.90.95.255	132.90.64.1-132.90.95.254
132.90.96.0/19	132.90.127.255	132.90.96.1-132.90.127.254
132.90.128.0/19	132.90.159.255	132.90.128.1-132.90.159.254
132.90.160.0/19	132.90.191.255	132.90.160.1-132.90.191.254
132.90.192.0/19	132.90.223.255	132.90.192.1-132.90.223.254
132.90.224.0/19	132.90.255.255	132.90.224.1-132.90.255.254

- Σε κάθε υποδίκτυο ο αριθμός των διαθέσιμων hosts είναι: 2^(32-19)-2=8190

c) Το δεύτερο υποδίκτυο είναι το 132.90.32.0/19.

i) Θέλουμε να το χωρίσουμε σε 4 υποδίκτυα, επομένως χρειαζόμαστε 2 επιπλέον bits από το subnet mask. Η subnet mask θα έχει δηλαδή 21 bits και θα είναι η 255.255.248.0.

ii)iii)iv) Τα νέα υποδίκτυα που προκύπτουν και τα χαρακτηριστικά τους είναι:

Υποδίκτυο	**Διεύθυνση εκπομπής**	**Διαθέσιμοι host**
132.90.32.0/21	132.90.39.255	132.90.32.1-132.90.39.254
132.90.40.0/21	132.90.47.255	132.90.40.1-132.90.47.254
132.90.48.0/21	132.90.55.255	132.90.48.1-132.90.55.254
132.90.56.0/21	132.90.63.255	132.90.56.1-132.90.63.254

- Σε κάθε υποδίκτυο ο αριθμός των διαθέσιμων hosts είναι: 2^(32-21)-2=2046

Άσκηση 8

a) Σας δίνονται οι παρακάτω IPv4 διευθύνσεις:
   i) 172.16.1.255/23
   ii) 172.16.2.2/23
   iii) 192.168.1.128/26
   iv) 192.168.1.95/27
   Τι είδους διευθύνσεις είναι αυτές: δικτύου (network), εκπομπής (directed broadcast), Η/Υ (host);

b) Σας δίνονται οι εξής δύο IPv4 διευθύνσεις: 172.16.17.30/20 και 172.16.28.15/20. Ανήκουν στο ίδιο υποδίκτυο ή όχι.

c) Δίνονται οι παρακάτω IPv6 διευθύνσεις και εύρη διευθύνσεων:
   i. 2002:968c:8db5::
   ii. ::/128
   iii. fffe::1111:2222:3333

Απάντηση

a)Για τις διευθύνσεις που δίνονται:

i) 172.16.1.255/23 -> Directed broadcast διότι:

Το υποδίκτυο στο οποίο ανήκει η συγκεκριμένη διεύθυνση είναι το 172.16.0.0/23. Η 172.16.1.255 είναι η διεύθυνση εκπομπής του υποδικτύου.

ii) 172.16.2.2/23 -> Host διότι:

Η συγκεκριμένη διεύθυνση ανήκει στο υποδίκτυο 172.16.2.0/23. Διεύθυνση εκπομπής του είναι η 172.16.3.255 και οι διαθέσιμοι host είναι 172.16.2.1-172.16.3.254.Η διεύθυνση 172.16.2.2 ανήκει στο εύρος των διαθέσιμων hosts.

iii) 192.168.1.128/26 -> Network διότι:

Η διεύθυνση ανήκει στο υποδίκτυο 192.168.1.128/26, με διεύθυνση εκπομπής 192.168.1.191. Η 192.128.1.128 είναι η διεύθυνση που είναι η ταυτότητα του υποδικτύου.

iv) 192.168.1.95/27 -> Broadcast διότι:

Η διεύθυνση ανήκει στο υποδίκτυο 192.168.1.64/27, με διεύθυνση εκπομπής την 192.168.1.95.

b) Οι διευθύνσεις 172.16.17.30/20 και 172.16.28.15/20 ανήκουν στο ίδιο υποδίκτυο, το οποίο είναι το 172.16.16.0/20 με διεύθυνση εκπομπής την 172.16.31.255. Οι διευθύνσεις των διαθέσιμων hosts του υποδικτύου είναι 172.16.16.1-172.16.31.254 και οι δύο διευθύνσεις που δίνονται ανήκουν σε αυτό το εύρος.

c)

i. Η 2002:968c:8db5:: είναι IPv4 mapped στην 150.140.141.181
ii. Η ::/128 είναι μια διεύθυνση η οποία περιέχει μόνο μηδενικά. Οποιαδήποτε διεύθυνση περιέχει μόνο μηδενικά θεωρείται "un-specified address".
iii. Η fffe::1111:2222:3333 είναι μια multicast διεύθυνση

Φεβρουάριος 2009 - Θέμα 2

Συμπληρώστε τον παρακάτω πίνακα

Network	**Subnet Mask**	**Εύρος**
192.168.12.0		192.168.12.0-192.168.12.127
192.168.12.0	255.255.255.192	
		192.168.12.0-192.168.12.255
192.168.12.128	255.255.255.224	

Λύση

α)

Network	Subnet Mask	Εύρος
192.168.12.0	**255.255.255.128**	192.168.12.0-192.168.12.127

διότι η διεύθυνση που δίνεται ανήκει στην κλάση C και αφού το εύρος είναι μόνο 128 διευθύνσεις και όχι 255 (όπως είναι κανονικά το εύρος της κλάσης C με 8 host bit) αυτό σημαίνει ότι χρησιμοποιούνται μόνο 7 από τα 8 host bit, άρα 1 bit από τα host bit χρησιμοποιείται για υποδικτύωση οπότε με τα 7 host bit διευθυνσιοδοτούμε 2^7-2=126 host. Συνεπώς η διεύθυνση δικτύου είναι 192.168.12.0 (192.168.12.00000000), η διεύθυνση εκπομπής είναι 192.168.12.127 (192.168.12.100000000) και οι διευθύνσεις host θα είναι 192.168.12.1- 192.168.12.126. Γνωρίζουμε ότι η μάσκα δικτύου θέτει 0 στα host bit και 1 στα network bit οπότε η μάσκα πρέπει να είναι η 255.255.255.100000000 δηλαδή η 255.255.255.128

β)

Network	Subnet Mask	Εύρος
192.168.12.0	255.255.255.192	**192.168.12.0-192.168.12.63**

Αφού η μάσκα υποδικτύου είναι η 255.255.255.192 δηλαδή η 255.255.255.11000000 άρα έχουμε 6 host bit και μπορούμε να διευθυνσιοδοτήσουμε 2^6-2=62 host, οπότε όλες οι διευθύνσεις είναι:

Network	192.168.12.0
Broadcast	192.168.12.63
Hosts	192.168.12.1-192.168.12.62

γ)

Network	Subnet Mask	Εύρος
192.168.12.0	**255.255.255.0**	192.168.12.0-192.168.12.255

Αφού το εύρος διευθύνσεων περιλαμβάνει 256 διευθύνσεις (1 διεύθυνση υποδικτύου, 1 διεύθυνση εκπομπής και 254 διευθύνσεις host) και είμαστε στην κλάση C αυτό σημαίνει ότι χρησιμοποιούνται όλα τα host bit της κλάσης, οπότε με 8 host bit έχουμε 2^8-2=254 host. Άρα δεν γίνεται subnetting οπότε η διεύθυνση δικτύου είναι η 192.168.12.0 (αρχική), η διεύθυνση εκπομπής είναι 192.168.12.255 και η μάσκα υποδικτύου είναι 255.255.255.0

δ)

Network	Subnet Mask	Εύρος
192.168.12.128	255.255.255.224	**192.168.12.128-192.168.12.159**

Αφού η μάσκα υποδικτύου είναι η 255.255.255.224 και σε δυαδική μορφή η 255.255.255.**111**00000 αυτό σημαίνει ότι από τα 8 host bit που αντιστοιχούν κανονικά στην κλάση C που ανήκει η διεύθυνση 192.168.12.128, τα τρία έχουν δεσμευτεί ως subnet bit και τα 5 χρησιμοποιούνται ως host bit δίνοντας 2^5-2=30 host στο κάθε υποδίκτυο. Το συγκεκριμένο υποδίκτυο αφού αρχίζει από τη διεύθυνση 192.168.12.128 (192.168.12.**100**00000) θα έχει το 1ο host του να αρχίζει από την 192.168.12.129 (192.168.12.**100**00001) και το τελευταίο host του να έχει τη διεύθυνση 192.168.12.158 (192.168.12.**100**11110) ενώ η διεύθυνση εκπομπής του είναι η 192.168.12.159 (192.168.12.**100**11111)

Άσκηση 9 – Θέμα 2 Φεβρουάριος 2011

α) Υποθέστε ότι είστε ένας διαχειριστής δικτύου και σας εκχωρείται το εύρος IP διευθύνσεων 98.16.1.0/2. Θέλουμε να δημιουργήσουμε 4 υποδίκτυα.

i) Προσδιορίστε τα Subnet Bits που απαιτούνται καθώς και τη Subnet Mask που προκύπτει.
ii) Προσδιορίστε τα 4 υποδίκτυα που προκύπτουν.
iii) Προσδιορίστε τις διευθύνσεις εκπομπής του κάθε υποδικτύου.
iv) Προσδιορίστε το πλήθος και τις διαθέσιμες διευθύνσεις Η/Υ για κάθε υποδίκτυο αναλυτικά.

β1) Σας δίνονται οι παρακάτω IPv4 διευθύνσεις:

i) 192.168.1.63/29
ii) 172.17.16.255/23

Τι είδους διευθύνσεις είναι αυτές: δικτύου (network), εκπομπής (directed broadcast), Η/Υ (host);

β2) Σας δίνονται οι εξής δύο IPv4 διευθύνσεις: 142.18.37.12/22 και 142.18.41.15/22. Ανήκουν στο ίδιο υποδίκτυο ή όχι.

Λύση

α)

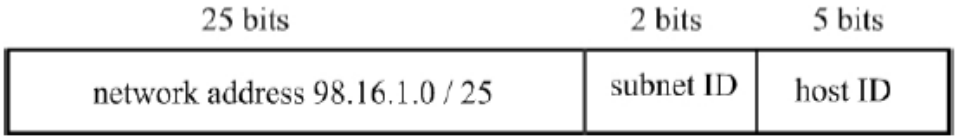
i)

Εφόσον το πρωτόκολλο είναι IPv4, έχουμε IP διευθύνσεις των 32 bits.

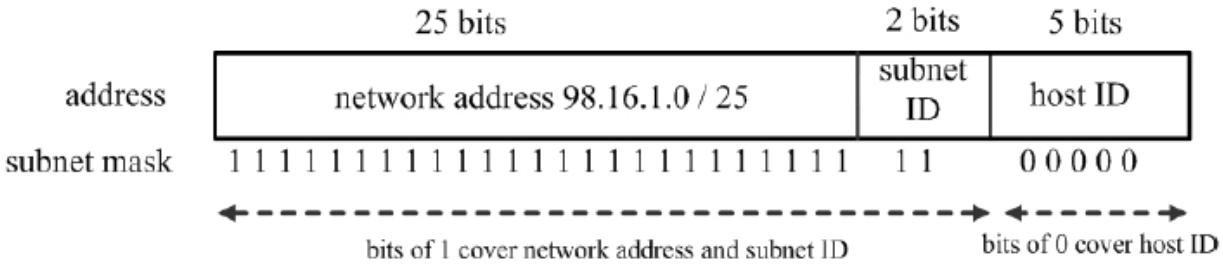
Η διεύθυνση δικτύου (network address) 98.16.1.0 / 25 απαιτεί 25 bits.

Εφόσον θέλουμε να δημιουργήσουμε 4 υποδίκτυα (subnets), θα χρειαστούμε 2 Subnet Bits.

Τα 5 bits που απομένουν θα χρησιμοποιηθούν για το host.



Για τον προσδιορισμό της μάσκας υποδικτύου (Subnet Mask) κάνουμε το εξής. Στα bits δικτύου και υποδικτύου βάζουμε 1, ενώ στα bits του host βάζουμε 0.



Επομένως, η Subnet Mask είναι 11111111 . 11111111 . 11111111 . 11100000

Στην δεκαδική αναπαράσταση η Subnet Mask γίνεται 255.255.255.224 ή / 27

ii)

Η διεύθυνση δικτύου είναι 98.16.1.0 / 25. Αυτή στην δυαδική αναπαράσταση γίνεται 11100010.00010000.00000001.0

Τα υπόλοιπα 7 bits, όπως έχει αναφερθεί προηγουμένως, θα χρησιμοποιηθούν για το subnet ID και το host ID.

Τα δύο Subnet Bits θα χρησιμοποιηθούν ως εξής:

00 για το υποδίκτυο #0
01 για το υποδίκτυο #1
10 για το υποδίκτυο #2
11 για το υποδίκτυο #3

Όπως έχει αναφερθεί, τα 5 τελευταία bits κάθε IP διεύθυνσης αναφέρονται σε host ID. Συνολικά υπάρχουν $2^5 = 32$ πεντάδες. Όμως από αυτές, η πρώτη και η τελευταία πεντάδα (δηλαδή 00000 και 11111) δεν εκχωρούνται ποτέ σε hosts. Η πεντάδα 00000 χρησιμοποιείται για την IP διεύθυνση κάθε υποδικτύου, ενώ η πεντάδα 11111 χρησιμοποιείται για την IP διεύθυνση εκπομπής (broadcast) κάθε υποδικτύου.

Επομένως, οι ζητούμενες IP διευθύνσεις των 4 υποδικτύων είναι

υποδίκτυο #0 11100010.00010000.00000001.0 00 00000
υποδίκτυο #1 11100010.00010000.00000001.0 01 00000
υποδίκτυο #2 11100010.00010000.00000001.0 10 00000
υποδίκτυο #3 11100010.00010000.00000001.0 11 00000

Σε δεκαδική αναπαράσταση οι παραπάνω διευθύνσεις είναι

υποδίκτυο #0 98.16.1.0

υποδίκτυο #1 98.16.1.32

υποδίκτυο #2 98.16.1.64

υποδίκτυο #3 98.16.1.96

iii) Όπως έχει αναφερθεί στο προηγούμενο ερώτημα, στις διευθύνσεις εκπομπής κάθε υποδικτύου τα τελευταία 5 bits θα είναι άσσοι.

Επομένως, οι ζητούμενες IP διευθύνσεις εκπομπής των 4 υποδικτύων είναι

υποδίκτυο #0 11100010.00010000.00000001.0 00 11111

υποδίκτυο #1 11100010.00010000.00000001.0 01 11111

υποδίκτυο #2 11100010.00010000.00000001.0 10 11111

υποδίκτυο #3 11100010.00010000.00000001.0 11 11111

Σε δεκαδική αναπαράσταση οι παραπάνω διευθύνσεις είναι

υποδίκτυο #0 98.16.1.31

υποδίκτυο #1 98.16.1.63

υποδίκτυο #2 98.16.1.95

υποδίκτυο #3 98.16.1.127

iv)

Όπως έχει αναφερθεί στα προηγούμενα ερωτήματα, σε κάθε υποδίκτυο τα 5 τελευταία bits της διεύθυνσης υποδικτύου αντιστοιχούν στο host ID. Από τις 32 δυνατές πεντάδες, η πρώτη χρησιμοποιείται για την IP διεύθυνση υποδικτύου, ενώ η τελευταία για την IP διεύθυνση εκπομπής του υποδικτύου. Οι 30 πεντάδες που απομένουν, μπορούν να χρησιμοποιηθούν για τα host (δηλ. Η/Υ). Επομένως, το πλήθος των διαθέσιμων διευθύνσεων Η/Υ σε κάθε υποδίκτυο είναι 30.

Αναλυτικά, οι διευθύνσεις αυτές είναι:

υποδίκτυο #0 98.16.1.1 έως 98.16.1.30

υποδίκτυο #1 98.16.1.33 έως 98.16.1.62

υποδίκτυο #2 98.16.1.65 έως 98.16.1.94

υποδίκτυο #3 98.16.1.97 έως 98.16.1.126

β1)

i) Δίνεται η IP διεύθυνση 192.168.1.63/29

Βλέπουμε ότι τα πρώτα 29 bits αντιστοιχούν στη διεύθυνση δικτύου (μαζί με τα πιθανά υποδίκτυα) και τα υπόλοιπα 3 bits αντιστοιχούν σε host ID.

Ο αριθμός 63 σε δυαδική μορφή είναι 00111111. Επομένως τα 3 τελευταία bits της διεύθυνσης είναι 111. Άρα έχουμε τη διεύθυνση εκπομπής.

ii) Έχουμε την IP διεύθυνση 172.17.16.255/23

Εδώ τα πρώτα 23 bits αντιστοιχούν στη διεύθυνση δικτύου (μαζί με τα πιθανά υποδίκτυα) και τα υπόλοιπα 9 bits αντιστοιχούν σε host ID.

Ο αριθμός 16 σε δυαδική μορφή είναι 00010000, ενώ ο αριθμός 255 είναι 11111111. Επομένως τα 9 τελευταία bits της διεύθυνσης είναι 01111111. Άρα έχουμε τη διεύθυνση Η/Υ (host).

β2)

Δίνονται οι IP διευθύνσεις 142.18.37.12/22 και 142.18.41.15/22.

Για να ανήκουν στο ίδιο υποδίκτυο θα πρέπει να έχουν ίδια διεύθυνση υποδικτύου. Δηλαδή θα πρέπει τα 22 πρώτα bits των δύο παραπάνω IP διευθύνσεων να είναι ίσα.

Τα 16 πρώτα bits είναι ίσα, αφού και οι δύο διευθύνσεις ξεκινούν με 142.18

Ας δούμε την τρίτη οκτάδα κάθε διεύθυνσης.

Ο αριθμός 37 σε δυαδική μορφή είναι 00100101, ενώ ο αριθμός 41 είναι 00101001

Βλέπουμε ότι τα 6 πρώτα bits των δύο αριθμών δεν είναι ίσα.

Άρα οι δοσμένες IP διευθύνσεις δεν ανήκουν στο ίδιο υποδίκτυο.

Φετινή 1η Άσκηση

Άσκηση 1 (2.5 μονάδες)

Μας δίνονται για ένα μηχάνημα οι παρακάτω πληροφορίες:

MAC Address: 00:06:25:D8:14:60

Automatic Configuration - DHCP

IP Address:	68.174.242.175
Subnet Mask:	255.255.248.0
Default Gateway:	68.174.240.1
DNS:	24.29.99.21 24.29.103.10 24.29.103.11
DHCP Remaining Time:	14:35:10

α) Τι σημαίνουν τα παραπάνω;
β) Ποιο είναι το εύρος διευθυνσεων, η διεύθυνση δικτύου και η διεύθυνση εκπομπής του παραπάνω υποδικτύου;
γ) Είναι η προεπιλεγμένη πύλη στο ίδιο δίκτυο με το παραπάνω μηχάνημα;

Απάντηση

α) **Mac address είναι μια 48 bit διεύθυνση που χαρακτηρίζει μία συσκευή μοναδικά στο τοπικό δίκτυο**. Συγκεκριμένα εδώ, είναι η 00:06:25:D8:14:60 (Η διεύθυνση συνήθως δίνεται σε δεκαεξαδική μορφή).

Στη συνέχεια δίνονται οι πληροφορίες που έχει αποκτήσει το μηχάνημα χρησιμοποιώντας το DHCP πρωτόκολλο (Dynamic Host Configuration Protocol). Οι πληροφορίες αυτές χρησιμοποιούνται από το μηχάνημα για να επικοινωνήσει χρησιμοποιώντας το πρωτόκολλο IP. Οι πληροφορίες αυτές μπορούν να εισαχθούν και χειροκίνητα από τον χρήστη, αλλά η χρήση του πρωτοκόλλου DHCP μας επιτρέπει να έχουμε μία δυναμική ανάθεση των διευθύνσεων σε μηχανήματα, δίνοντάς μας τη δυνατότητα να αναθέσουμε την ίδια διεύθυνση IP (εξηγείται στη συνέχεια) σε δύο διαφορετικά μηχανήματα – σε αντίθεση με τη Mac address. Οι πληροφορίες αυτές είναι:

- **IP address:** μία 32bit διεύθυνση που χαρακτηρίζει μοναδικά το μηχάνημα στο διαδίκτυο και στην συγκεκριμένη περίπτωση είναι η 68.174.242.175 (Για την αναπαράσταση της διεύθυνσης χωρίζουμε τα ψηφία της σε ομάδες των 8 bit, Για κάθε ομάδα γράφουμε τη δεκαδική τιμή της και χωρίζουμε τις τέσσερις ομάδες χρησιμοποιώντας το σύμβολο '.')
- **Subnet mask**: είναι η μάσκα του δικτύου. Η μάσκα μας γνωστοποιεί το μέγεθος και το είδος του υποδικτύου στο οποίο εντάσσεται το μηχάνημα. Τα '1' στη μάσκα υποδηλώνουν τα bit της IP που δηλώνουν το id του υποδικτύου και τα '0' τα bit που δηλώνουν το id του μηχανήματος μέσα στο υποδίκτυο. (Η αναπαράσταση της είναι ίδια με την IP address) Η συγκεκριμένη Subnet mask μας δίνει την πληροφορία, ότι χρησιμοποιούνται τα πρώτα 21 bits της IP address για το network identification και τα υπόλοιπα 11 για hosts.
- **Default Gateway**: **είναι η διεύθυνση του μηχανήματος το οποίο αναλαμβάνει την κίνηση πληροφορίας των συσκευών που εντάσσονται στο υποδίκτυο από και προς συσκευές σε άλλα δίκτυα**. Στην συγκεκριμένη περίπτωση η IP address της συσκευής αυτής είναι η 68.174.240.1.
- **DNS**: είναι η διεύθυνση της συσκευής η οποία λειτουργεί ως DNS (Domain Name System) Server. Το Domain Name System έχει servers που είναι υπεύθυνοι για την αντιστοίχηση IP διευθύνσεων σε ονόματα (domain names). Στην συγκεκριμένη περίπτωση δίνονται 3 διευθύνσεις για DNS servers και είναι οι 24.29.99.21 , 24.29.103.10 και η 24.29.103.11 .
- **DHCP Remaining Time: ένας DHCP server αναθέτει μια IP address σε μία δικτυακή συσκευή για ένα συγκεκριμένο χρονικό διάστημα. Οι DHCP clients είναι υπεύθυνοι να ανανεώσουν την IP διεύθυνση πριν αυτό το διάστημα λήξει. Στην συγκεκριμένη περίπτωση, ο χρόνος που απομένει για την λήξη της IP διεύθυνσης είναι 14 ώρες, 35 λεπτά και 10 δεύτερα.**

β) Για να υπολογίσουμε το εύρος διευθύνσεων του 68.174.242.175/21, εργαζόμαστε ως εξής:
Εφόσον χρησιμοποιούμε 11 bits για διευθυνσιοδότηση των hosts του συγκεκριμένου υποδικτύου, έχουμε 211-2 = 2042 ελεύθερες διευθύνσεις για hosts. Κανονικά είναι 211, αλλά η πρώτη διεύθυνση είναι η διεύθυνση του δικτύου και η τελευταία είναι η broadcast.
Έτσι, έχουμε ότι η διεύθυνση δικτύου είναι η 68.174.240.0

ομάδες bit	32-25	24-17	16-9	8-1
δυαδικό	01000100	10101110	11110000	00000000
δεκαδικό	68	174	240	0

Άρα η πρώτη διαθέσιμη διεύθυνση για έναν host είναι η 68.174.240.1. Επομένως το εύρος διευθύνσεων είναι από 68.174.240.1 έως 68.174.247.254

Η διεύθυνση εκπομπής του υποδικτύου (broadcast) είναι η τελευταία διεύθυνση του δικτύου (αν τις ταξινομήσουμε κατά αύξουσα σειρά) και είναι η 68. 174. 247. 255

ομάδες bit	32-25	24-17	16-9	8-1
δυαδικό	01000100	10101110	11110111	11111111
δεκαδικό	68	174	247	255

γ) Για να ελέγξουμε αν το συγκεκριμένο μηχάνημα είναι στο ίδιο δίκτυο με την προεπιλεγμένη πύλη παίρνουμε τη διεύθυνση δικτύου με τη βοήθεια της μάσκας από τις IP και Gateway και εξετάζουμε αν είναι ίδιες.

Μηχάνημα: 01000100.10101110.11110010.1010111
Gateway: 01000100.10101110.11110000.0000001
Mask: 11111111.11111111.11111000.00000000

Τα bits που καθορίζουν το δίκτυο είναι ίδια, άρα το μηχάνημα και το default gateway ανήκουν στο ίδιο δίκτυο.

Άσκηση 2

Κάνοντας υποδικτύωση στο 210.106.140.0 με subnet mask/26. Πόσα υποδίκτυα και υπολογιστές ανά υποδίκτυο έχουμε;

Απάντηση

Η IP 210.106.14.0 ανήκει στην Class C. Η default subnet mask για την κλάση C είναι η 255.255.255.0, που σημαίνει ότι χρησιμοποιούνται 24 bits για το identification του δικτύου και τα υπόλοιπα 8 bit για ανάθεση διευθύνσεων σε hosts. Στη δική μας περίπτωση η υποδικτύωση γίνεται χρησιμοποιώντας 26 bits, πράγμα που σημαίνει ότι παίρνουμε 2 bit από την τελευταία 8-άδα για να φτιάξουμε τα υποδίκτυα.
Χρησιμοποιώντας τα δύο επιπλέον bit μπορούμε να ταυτοποιήσουμε 4 διαφορετικά υποδίκτυα:
210.106.14.0, 210.106.14.64, 210.106.14.128, 210.106.14.192

Με αυτό τον τρόπο περισσεύουν 6 bits για την διευθυνσιοδότηση των host.
Άρα σε κάθε υποδίκτυο μπορούμε να έχουμε 2^6-2 = 64-2=62 υπολογιστές

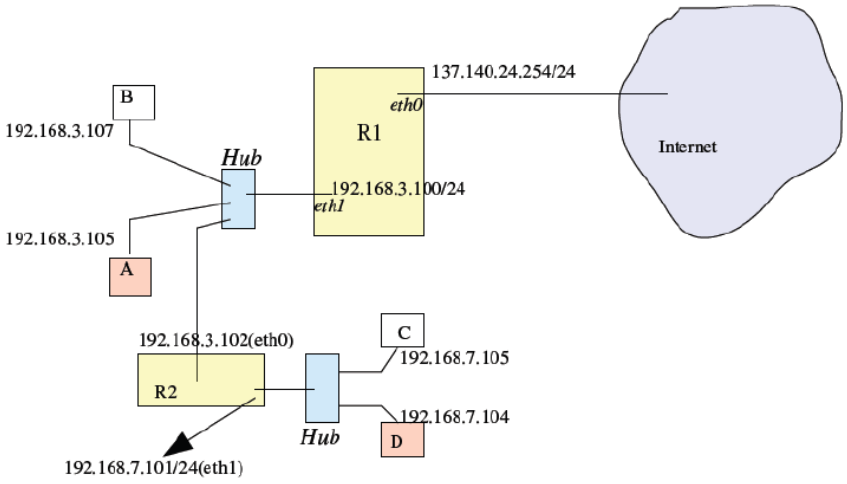
Άσκηση 3 (4 μοναδες)

Δίνεται η παρακάτω δικτυακή τοπολογία. Στην τοπολογία αυτή έχουμε έναν αριθμό δικτυακών συσκευών (2 δρομολογητές - R1, R2, 2 Hub) και 4 απλούς υπολογιστές (A,B,C,D) οι οποίοι και συνδέονται μέσω των δικτυακών συσκευών στο διαδίκτυο.

Ζητείται να συμπληρώσετε τους πίνακες δρομολόγησης των R1, R2, B,C.

π.χ. για τον υπολογιστή A

Destination Network IP	Destination Network Subnet Mask	Gateway	Interface
192.168.3.0	255.255.255.0	0.0.0.0 (or "on-link")	eth0
192.168.7.0	255.255.255.0	192.168.3.102	eth0
0.0.0.0	0.0.0.0	192.168.3.100	eth0



Σημείωση: στο παραπάνω σχήμα όταν δεν αναγράφεται το όνομα μιας δικτυακής διεπαφής τότε αυτή είναι η eth0

Απάντηση

Παραθέτουμε τα routing tables για τις ζητούμενες συσκευές:
Για το δρομολογητή R1

Destination Network IP	Destination Network subnet Mask	Gateway	Interface
192.168.3.0	255.255.255.0	0.0.0.0 (on-link)	eth1
192.168.7.0	255.255.255.0	192.168.3.102	eth1
0.0.0.0	0.0.0.0	137.140.24.254	eth0

Για το δρομολογητή R2

Destination Network IP	Destination Network Subnet Mask	Gateway	Interface
192.168.3.0	255.255.255.0	0.0.0.0 (on-link)	eth0
192.168.7.0	255.255.255.0	0.0.0.0 (on-link)	eth1
0.0.0.0	0.0.0.0	192.168.3.100	eth0

Για τον υπολογιστή B

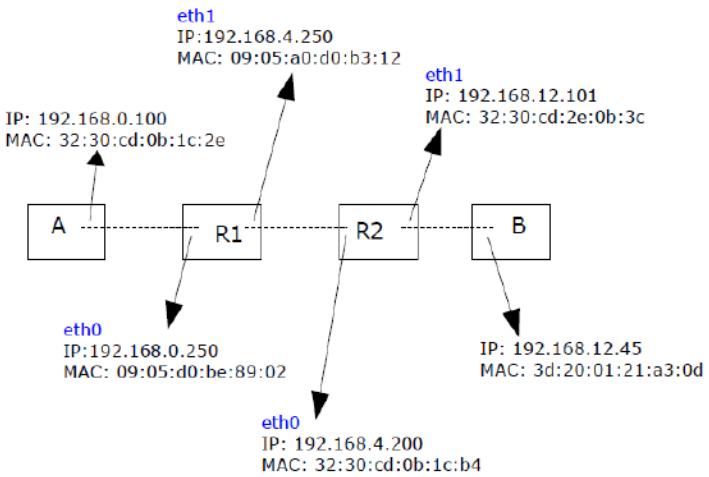
Destination Network IP	Destination Network Subnet Mask	Gateway	Interface
192.168.3.0	255.255.255.0	0.0.0.0 (on-link)	eth0
192.168.7.0	255.255.255.0	192.168.3.102	eth0
0.0.0.0	0.0.0.0	192.168.3.100	eth0

Για τον υπολογιστή C

Destination Network IP	Destination Network Subnet Mask	Gateway	Interface
192.168.3.0	255.255.255.0	192.168.7.101	eth0
192.168.7.0	255.255.255.0	0.0.0.0 (on-link)	eth0
0.0.0.0	0.0.0.0	192.168.7.101	eth0

Άσκηση 4 (2.5 μοναδες)

Στο παρακάτω δίκτυο ο υπολογιστής A στέλνει ένα πακέτο στον B.



α) Ποια είναι η MAC διεύθυνση προορισμού του πακέτου που φεύγει από τον υπολογιστή A;
β) Για ποια IP διεύθυνση, ο A θα κάνει μία ARP αίτηση;
γ) Ποια είναι η MAC και IP διεύθυνση προορισμού του πακέτου που φεύγει από τον R1 προς τον R2;

Απάντηση

α) Ο A στέλνει το πακέτο στον R1 **με MAC διεύθυνση προορισμού αυτήν του R1**. Αυτό συμβαίνει γιατί ο B δεν ανήκει στο ίδιο υποδίκτυο με τον A, οπότε ο A πρέπει να δρομολογήσει το μήνυμα για τον B μέσω του R1. Πιο συγκεκριμένα η διεύθυνση αυτή είναι η 09:05:d0:be:89:02.

β) **Ο Α ΘΑ ΚΆΝΕΙ ARP ΑΊΤΗΣΗ ΓΙΑ ΤΗΝ IP ΤΟΥ R1 192.168.0.250 ΔΙΌΤΙ ΑΝΤΙΛΑΜΒΆΝΕΤΑΙ ΌΤΙ Ο Β ΔΕΝ ΑΝΗΚΕΙ ΣΤΟ ΙΔΙΟ ΥΠΟΔΙΚΤΥΟ**

γ)**ΟΤΑΝ Ο Α ΣΤΕΛΝΕΙ ΠΑΚΕΤΟ ΜΕ ΠΡΟΟΡΙΣΜΟ ΤΟΝ Β Η ΔΙΕΥΘΥΝΣΗ MAC ΠΡΟΟΡΙΣΜΟΥ ΘΑ ΕΙΝΑΙ ΑΥΤΗ ΤΟΥ R1 ΑΛΛΑ Η IP ΠΑΡΑΛΗΠΤΗ ΘΑ ΕΙΝΑΙ ΤΟΥ Β. ΕΠΕΙΔΗ Ο R1 ΔΕΝ ΓΝΩΡΙΖΕΙ ΤΗ MAC ΔΙΕΥΘΥΝΣΗ ΤΟΥ ΥΠΟΛΟΓΙΣΤΗ Β (ΜΕ IP 192.168.12.45), ΓΙΑΥΤΟ ΤΟ ΛΟΓΟ ΣΤΕΛΝΕΙ ΕΝΑ ARP ΑΙΤΗΜΑ ΣΤΟΝ R2, Ο ΟΠΟΙΟΣ ΤΟ ΔΙΑΒΑΖΕΙ ΚΑΙ ΣΤΕΛΝΕΙ ΩΣ ΑΠΑΝΤΗΣΗ ΣΤΟΝ R1 ΤΗ ΔΙΕΥΘΥΝΣΗ ΥΛΙΚΟΥ ΤΟΥ (ΤΗ MAC ΤΟΥ). ΕΤΣΙ ΜΕΤΑ Ο R1 ΜΠΟΡΕΙ ΝΑ ΣΤΕΙΛΕΙ ΤΟ ΠΑΚΕΤΟ ΣΤΟΝ Β ΜΕ IP 192.168.12.45 ΚΑΙ MAC ΔΙΕΥΘΥΝΣΗ ΤΗ ΔΙΕΥΘΥΝΣΗ ΤΟΥ R2**

Σημείωση: Στην πραγματικότητα, υπάρχει ένα ξεχωριστό πρωτόκολλο για το σκοπό αυτό, που καλείται ARP (Adress resolution protocol). Υποθέστε ότι βρίσκεστε στο σύστημα 128.6.4.194 και θέλετε να συνδεθείτε στο σύστημα 128.6.4.7. Το σύστημά σας πρέπει πρώτα να επαληθεύσει ότι το 128.6.4.7 βρίσκεται στο ίδιο δίκτυο κι έτσι να μπορεί απευθείας να μιλήσει μέσω Ethernet. Κατόπιν, θα κοιτάξει στον ARP πίνακά του για να δει αν το 128.6.4.7 γνωρίζει ήδη την Ethernet διεύθυνση. Αν ναι, την προσαρτεί στην επικεφαλίδα Ethernet και στέλνει το πακέτο. Ας υποθέσουμε όμως ότι αυτό το σύστημα δεν βρίσκεται στον ARP πίνακά του. Δεν υπάρχει τρόπος να σταλεί το πακέτο επειδή είναι απαραίτητη η Ethernet διεύθυνση. Έτσι, χρησιμοποιείται το πρωτόκολλο ARP για να στείλει μια αίτηση. Στην ουσία μια ARP αίτηση λέει ζητώ την Ethernet διεύθυνση για το 128.6.4.7. Όλα τα συστήματα ακούνε τις αιτήσεις ARP. Όταν ένα σύστημα καταλάβει ότι η αίτηση ARP απευθύνεται σ αυτό πρέπει να απαντήσει. Έτσι, το 128.6.4.7 θα δει την αίτηση και θα στείλει μια ARP απάντηση που λέει: το 128.6.4.7 αντιστοιχεί στο 8:0:20:1:56:34

Θέμα 2 – Σεπτέμβριος 2012

a. Έχετε την ακόλουθη διεύθυνση: 192.16.5.133/29. Πόσα συνολικά bits χρησιμοποιούνται για να προσδιορίζουν το δίκτυο, τα subnet και πόσα τους host;

b. Ποια είναι η πλήρης μάσκα υποδικτύου για τη διεύθυνση 172.16.5.10/28

c. Έχετε το δίκτυο 192.168.1.0 με μάσκα 255.255.255.240. Αναφέρετε τα εξής: τον αριθμό των υπο-δικτύων, τον αριθμό των host ανά υποδίκτυο, το πλήρες εύρος διευθύνσεων των 3 πρώτων δικτύων και το χρησιμοποιήσιμο (από hosts) εύρος διευθύνσεων από αυτά τα τρία δίκτυα;

d. Ομοίως για το δίκτυο 200.138.1.0 με μάσκα υποδικτύου 255.255.255.252. Επιπλέον ποια είναι η broadcast διεύθυνση για τα δίκτυα αυτά

Απάντηση

α)Τα bits δικτύου είναι 29, τα subnet bits είναι 5 και τα host bit είναι 3

β)Η μάσκα υποδικτύου είναι 255.255.255.240

γ)Το δίκτυο 192.168.1.0. έχει

16 υποδίκτυα (4 subnet bits)

14 hosts σε κάθε υποδίκτυο

1ο υποδίκτυο

Αρχική διεύθυνση υποδικτύου:	192.168.1.0
1ος host 1ου υποδικτύου:	192.168.1.1
Τελευταίος host 1ου υποδικτύου:	192.168.1.14
Διεύθυνση εκπομπής 1ου υποδικτύου:	192.168.1.15

2ο υποδίκτυο

Αρχική διεύθυνση υποδικτύου:	192.168.1.16
1ος host 2ου υποδικτύου:	192.168.1.17
Τελευταίος host 2ου υποδικτύου:	192.168.1.30
Διεύθυνση εκπομπής 2ου υποδικτύου:	192.168.1.31

3ο υποδίκτυο

Αρχική διεύθυνση υποδικτύου: 192.168.1.32

1ος host 3ου υποδικτύου: 192.168.1.33

Τελευταίος host 3ου υποδικτύου: 192.168.1.46

Διεύθυνση εκπομπής 3ου υποδικτύου: 192.168.1.47

Συνολικά χρησιμοποιούνται 42 διευθύνσεις host στα 3 δίκτυα

δ)

Το δίκτυο 200.138.1.0. έχει

64 υποδίκτυα (6 subnet bits)

2 hosts σε κάθε υποδίκτυο

1ο υποδίκτυο

Αρχική διεύθυνση υποδικτύου: 200.138.1.0

1ος host 1ου υποδικτύου: 200.138.1.1

Τελευταίος host 1ου υποδικτύου: 200.138.1.2

Διεύθυνση εκπομπής 1ου υποδικτύου: 200.138.1.3

2ο υποδίκτυο

Αρχική διεύθυνση υποδικτύου: 200.138.1.4

1ος host 2ου υποδικτύου: 200.138.1.5

Τελευταίος host 2ου υποδικτύου: 200.138.1.6

Διεύθυνση εκπομπής 2ου υποδικτύου: 200.138.1.7

3ο υποδίκτυο

Αρχική διεύθυνση υποδικτύου: 192.168.1.8

1ος host 3ου υποδικτύου: 192.168.1.9

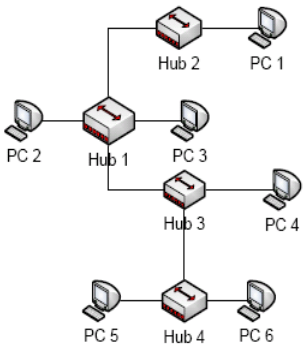
Τελευταίος host 3ου υποδικτύου: 192.168.1.10

Διεύθυνση εκπομπής 3ου υποδικτύου: 192.168.1.11

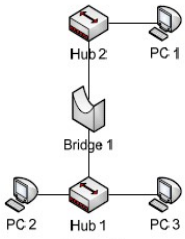
2. Β μέρος Broadcast και Collisions Domains

Άσκηση 1

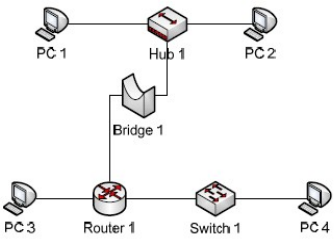
1. Ποια η διαφορά ενός collision domain από ένα broadcast domain;
2. Σε κάθε ένα από τα παρακάτω σχήματα, εξηγήστε πόσα collision domains, πόσα broadcast domains υπάρχουν και γιατί. Μπορείτε να οριοθετήσετε κάθε broadcast και collision domain στην αναφορά σας καταγράφοντας μεταξύ ποιων συσκευών βρίσκεται.



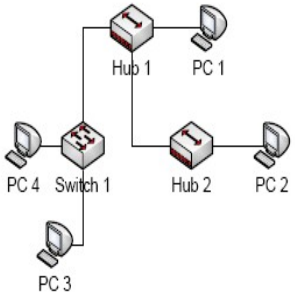
Εικόνα 1



Εικόνα 2



Εικόνα 3 (Στο switch 1 δεν έχουν οριστεί VLANs)



Εικόνα 4 (Στο switch 1 έχει οριστεί ένα VLAN στις συνδέσεις με τα PC3, PC4, και ένα άλλο στη σύνδεση με το Hub1)

Απάντηση

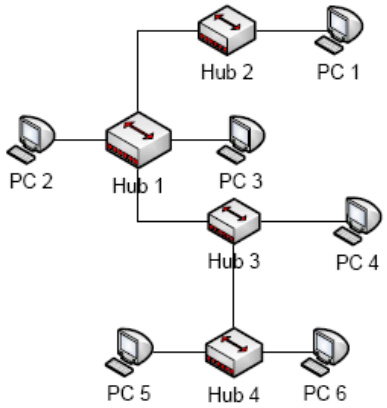
Ένα **collision domain** είναι ένα λογικό τμήμα δικτύου όπου τα πακέτα δεδομένων μπορούν να συγκρουστούν το ένα με το άλλο όταν στέλνονται ταυτόχρονα σε ένα κοινό μέσο. Αυτό συνήθως συναντάται στο Ethernet Networking πρωτόκολλο. Μόνο μια συσκευή στο collision domain μπορεί να μεταδώσει σε κάθε στιγμή, ενώ οι άλλες συσκευές «αφουγκράζονται το δίκτυο προκειμένου να αποφευχθούν οι συγκρούσεις δεδομένων οι οποίες καθιστούν το δίκτυο μη αποδοτικό. **Ένα broadcast domain** είναι ένα λογικό τμήμα δικτύου στο οποίο οποιαδήποτε δικτυακή συσκευή μπορεί να μεταδώσει άμεσα τα δεδομένα της σε άλλη χωρίς να περάσει από μια συσκευή δρομολόγησης. Πιο συγκεκριμένα το broadcast domain είναι η περιοχή του δικτύου που αποτελείται από Η/Υ και άλλες συσκευές οι οποίες μπορούν να προσπελαστούν άμεσα στέλνοντας ένα απλό πλαίσιο δεδομένων στη διεύθυνση εκπομπής του επιπέδου ζεύξης δεδομένων

Η διαφορά ανάμεσα σε ένα collision domain και σε ένα broadcast domain είναι ότι σε ένα collision domain όλα τα δεδομένα (data frames) που στέλνει μία από της συσκευές του δικτύου μεταφέρεται σε όλες τις συσκευές που ανήκουν στο ίδιο δίκτυο και κάθε συσκευή είναι υπεύθυνη να ανακαλύψει μόνη της αν τα δεδομένα προορίζονται για αυτήν. Σε ένα broadcast domain όμως μόνο τα broadcast πακέτα μεταφέρονται σε όλες τις συσκευές που ανήκουν στο ίδιο δίκτυο. Για παράδειγμα ένα άθροισμα συσκευών που είναι συνδεδεμένα σε ένα hub αποτελούν ένα collision domain, καθώς κάθε πακέτο που στέλνει μια συσκευή του δικτύου αυτού μεταφέρεται σε όλες, ανεξάρτητα αν το πακέτο προορίζεται για αυτές ή όχι. Σε ένα (broadcast domain) δίκτυο όμως που οι συσκευές συνδέονται μέσω ενός switch μόνο τα broadcast πακέτα μεταφέρονται σε όλες τις συσκευές του δικτύου, καθώς το switch απομονώνει κάθε port και χρησιμοποιεί κανόνες που σχετίζονται με τον τελικό προορισμό του πακέτου.

Ports Συσκευών

- ✓ Κάθε **Hub** αποτελεί ένα **Collision Domain** ανεξάρτητα Από Τον Αριθμό Των Ports Του
- ✓ Κάθε **Port** ενός **Switch/Bridge** αποτελεί ένα **Collision Domain**
- ✓ Κάθε **Port** ενός **Router** λειτουργεί και σαν **ένα Collision Domain και σαν ένα Broadcast Domain**
- ✓ Κάθε **VLAN** αποτελεί ένα **Broadcast Domain**

2.i)



Εικόνα 1

Στην Εικόνα 1 ισχύουν τα ακόλουθα:

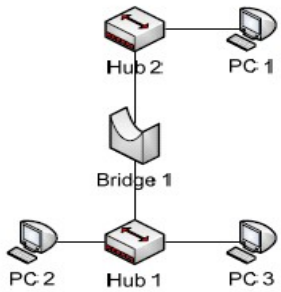
Collisions domains: 1

- PC1 Hub2 Hub1 PC2 PC3 Hub3 PC4 Hub4 PC5 PC6

Broadcast domains: 1

- PC1 Hub2 Hub1 PC2 PC3 Hub3 PC4 Hub4 PC5 PC6

ii)



Εικόνα 2

Στην Εικόνα 2 ισχύουν τα ακόλουθα:

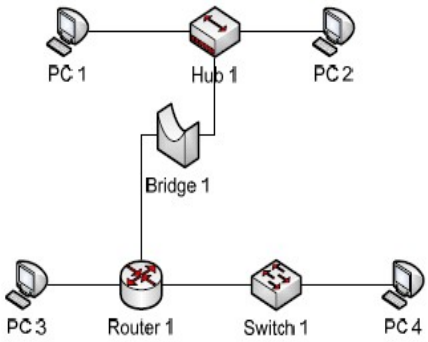
Collisions domains: 2

- PC1 Hub2 Bridge1
- Bridge1 Hub1 PC2 PC3

Broadcast domains: 1

- PC1 Hub2 Bridge1 Hub1 PC2 PC3

iii)



Εικόνα 3 (Στο switch 1 δεν έχουν οριστεί VLANs)

Στην Εικόνα 3 ισχύουν τα ακόλουθα:

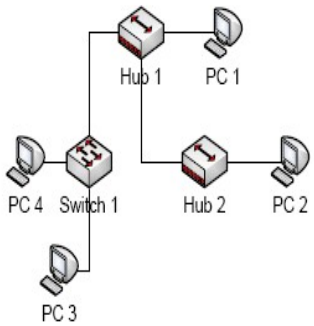
Collisions domains: 5

- PC1 Hub1 PC2 Bridge1
- Bridge1 Router1
- Router1 PC3
- Router1 Switch1
- Switch1 PC4

Broadcast domains: 3

- PC1 Hub1 PC2 Bridge1 Router1
- Router1 PC3
- Router1 Switch1 PC4

iv)



Εικόνα 4 (Στο switch 1 έχει οριστεί ένα VLAN στις συνδέσεις με τα PC3, PC4, και ένα άλλο στη σύνδεση με το Hub1)

Στην Εικόνα 4 ισχύουν τα ακόλουθα:

Collisions domains: 3

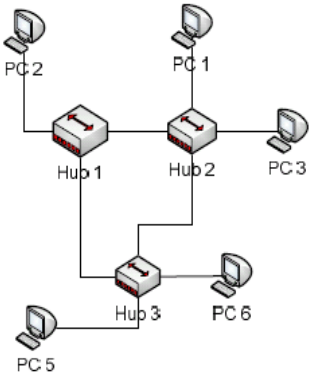
- PC4 Switch1
- PC3 Switch1
- Switch1 Hub1 PC1 Hub2 PC2

Broadcast domains: 2

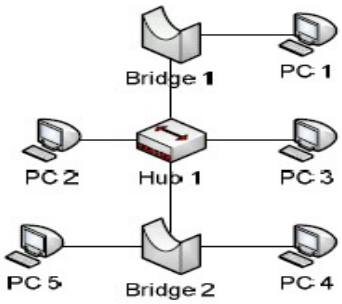
- PC4 Switch1 PC3 (1ο VLAN)
- Switch1 Hub1 PC1 Hub2 PC2 (2ο VLAN)

Άσκηση 2

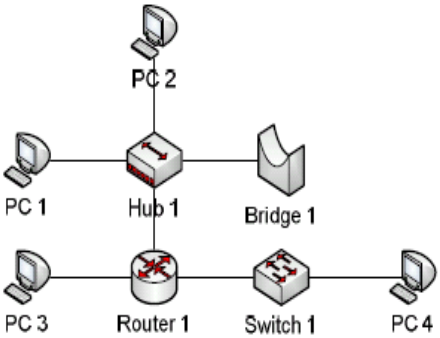
1. Σε κάθε ένα από τα παρακάτω σχήματα, εξηγήστε πόσα collision domains, πόσα broadcast domains υπάρχουν και γιατί. Μπορείτε να οριοθετήσετε κάθε broadcast και collision domain στην αναφορά σας καταγράφοντας μεταξύ ποιων συσκευών βρίσκεται.



Εικόνα 1

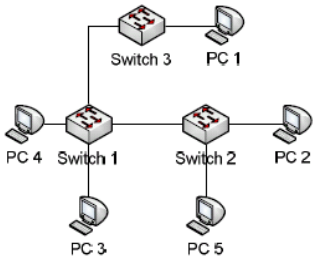


Εικόνα 2



Εικόνα 3 (Στο switch 1 δεν έχουν οριστεί VLANs)

2. Στο παρακάτω σχήμα, θεωρήστε ότι τα 3 switch έχουν διαμορφωθεί ως εξής: Στα switch 1, 2 και 3 έχουν οριστεί δύο VLAN με αριθμούς 100 και 200. Στο VLAN 100 ανήκουν οι συνδέσεις του switch 1 με τα PC3, PC4 και του switch 2 με το PC5, ενώ στο VLAN 200 ανήκουν οι συνδέσεις του switch3 με το PC1 και του switch 2 με το PC2. Εξηγήστε πόσα collision domains, πόσα broadcast domains υπάρχουν και γιατί. Επίσης καταγράψτε ποια ports των switch είναι trunk ports και ποια access ports.



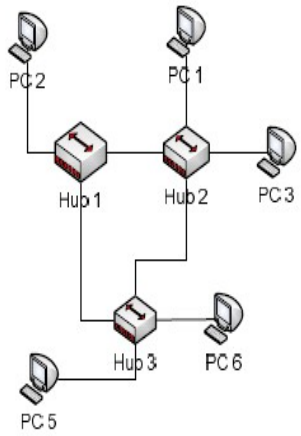
Εικόνα 4

Απάντηση

Ports Συσκευών

- ✓ Κάθε hub αποτελεί ένα collision domain ανεξάρτητα από τον αριθμό των ports του
- ✓ Κάθε port ενός switch/bridge αποτελεί ένα collision domain
- ✓ Κάθε port ενός Router λειτουργεί και σαν ένα collision domain και σαν ένα broadcast domain.
- ✓ Κάθε VLAN αποτελεί ένα broadcast domain

Στην Εικόνα 1 ισχύουν τα ακόλουθα:



Εικόνα 1

Collisions domains: 1

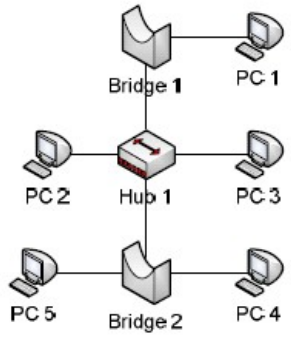
- PC2 PC5 Hub1 PC1 Hub2 Hub3 PC3 PC6

Broadcast domains: 1

- PC2 PC5 Hub1 PC1 Hub2 Hub3 PC3 PC6

Παρατηρούμε δηλαδή ότι όλα τα PC 1, …, PC 6 συνδέονται στα hubs 1, 2, 3. Οπότε όλες οι δικτυακές συσκευές ανήκουν σε 1 broadcast domain. Επιπλέον, όλα τα PC 1,…, PC 6 συνδέονται με hubs (layer 1 συσκευές) οπότε ορίζουν και 1 collision domain.

Στην Εικόνα 2 ισχύουν τα ακόλουθα:



Εικόνα 2

Collisions domains: 4

- PC2 Hub1 PC3 Bridge1 Bridge2
- PC5 Bridge2
- PC4 Bridge2
- PC1 Bridge1

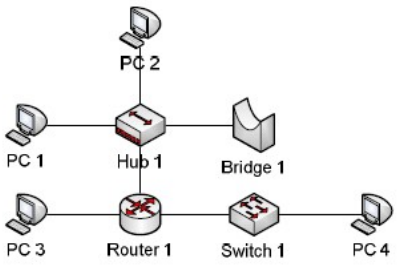
Broadcast domains: 1

- PC2 PC5 Bridge1 Hub1 Bridge2 PC1 PC3 PC4

Παρατηρούμε δηλαδή ότι όλα τα PC 1, ..., PC 5 συνδέονται μεταξύ τους μέσω του hub 1 και των bridge 1 και 2. Οπότε όλες οι δικτυακές συσκευές ανήκουν σε 1 broadcast domain. Επιπλέον, η ύπαρξη των bridge 1 και 2 ορίζει 4 collision domains :

- στο 1ο περιλαμβάνεται το τερματικό PC 1.
- στο 2ο περιλαμβάνονται τα PC 2 και PC 3 τα οποία συνδέονται μεταξύ τους με μια δικτυακή layer 1 συσκευή (hub 1).
- στο 3ο περιλαμβάνεται το τερματικό PC 4
- στο 4ο περιλαμβάνεται το τερματικό PC 5

Στην Εικόνα 3 ισχύουν τα ακόλουθα:



Εικόνα 3 (Στο switch 1 δεν έχουν οριστεί VLANs)

Collisions domains: 4

- PC1 Hub1 PC2 Bridge1 Router1
- PC3 Router1
- PC4 Switch1
- Router1 Switch1

Broadcast domains: 3

- PC1 Hub1 Bridge1 PC2 Router1
- PC3 Router1
- PC4 Switch1 Router1

Παρατηρούμε δηλαδή ότι όλα τα PC 1, ..., PC 4 συνδέονται μεταξύ τους μέσω των hub 1, bridge 1, switch 1 και ότι υπάρχει ο router 1 ο οποίος διαχωρίζει τα broadcast domains. Έτσι, υπάρχουν 3 broadcast domains :

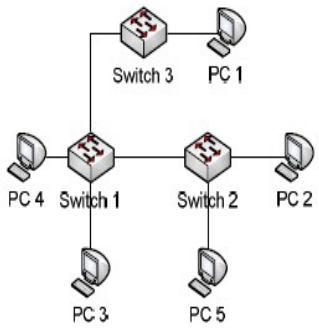
- στο 1ο περιλαμβάνονται οι δικτυακές συσκευές bridge 1, hub 1 και τα τερματικά PC 1, PC 2.
- στο 2ο περιλαμβάνεται το τερματικό PC 3.

- στο 3ο περιλαμβάνονται η δικτυακή συσκευή switch 1 και το τερματικό PC 4.

Επιπλέον, το switch 1 καθορίζει τα collision domains. Έτσι, υπάρχουν 3 collision domains:

- στο 1ο περιλαμβάνεται το PC 3.
- στο 2ο περιλαμβάνεται το PC 4.
- στο 3ο περιλαμβάνονται τα PC 1 και PC 2, τα οποία συνδέονται μεταξύ τους με μια δικτυακή layer 1 συσκευή (hub 1)

Στην Εικόνα 4 ισχύουν τα ακόλουθα:



Εικόνα 4

Collision domains: 7

- PC4 Switch1
- PC3 Switch1
- PC1 Switch3
- PC5 Switch2
- PC2 Switch2
- Switch1 Switch3
- Switch1 Switch2

Broadcast domains: 2

- PC4 Switch1 PC3 Switch2 PC5
- PC1 Switch3 Switch2 PC2

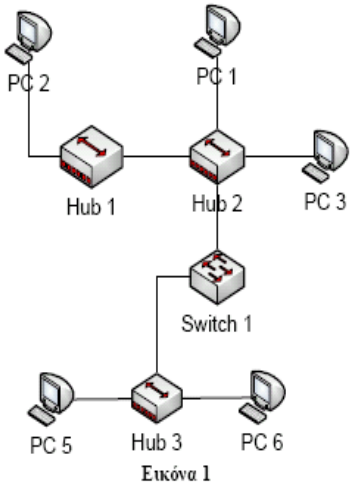
2.

Τύπος Port	Port
Access Port	Switch1-PC4
Access Port	Switch1-PC3
Access Port	Switch1-Switch2
Access Port	PC5-Switch2
Access Port	PC1-Switch3
Access Port	PC2-Switch2
Trunk Port	**Switch1-Switch3**
Trunk Port	**Switch1-Switch2**

Στα δίκτυα της Cisco (Cisco networks), το trunking είναι μια ειδική λειτουργία που μπορεί να καταχωρηθεί-αντιστοιχηθεί σε ένα port κάνοντας το ικανό να μεταφέρει κυκλοφορία (traffic) για οποιοδήποτε ή για όλα τα VLAN που είναι προσβάσιμα από ένα συγκεκριμένο switch. Ένα τέτοιο port ονομάζεται trunk σε αντίθεση με το access port το οποίο μεταφέρει κυκλοφορία μόνο στο συγκεκριμένο/από το συγκεκριμένο VLAN που του έχει καταχωρηθεί. Εδώ οι συνδέσεις Switch1-Switch3 και Switch1-Switch2 συνδέουν τα 2 τμήματα του VLAN 200 ενώ το Switch1-Switch2 συνδέει τα τμήματα του VLAN 100 μεταξύ τους. Με πιο απλά λόγια τα Access Port συνδέουν συσκευές του ίδιου VLAN, ενώ τα Trunk Port συνδέουν συσκευές διαφορετικών VLAN

Άσκηση 3

1. Σε κάθε ένα από τα παρακάτω σχήματα, εξηγήστε πόσα collision domains, πόσα broadcast domains υπάρχουν και γιατί. Μπορείτε να οριοθετήσετε κάθε broadcast και collision domain στην αναφορά σας καταγράφοντας μεταξύ ποιων συσκευών βρίσκεται. Θεωρήστε ότι σε κανένα switch δεν έχουν οριστεί VLANs.

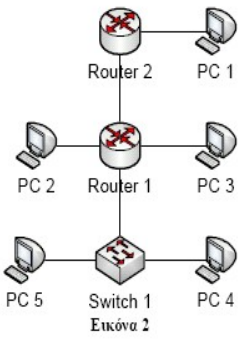


Εικόνα 1

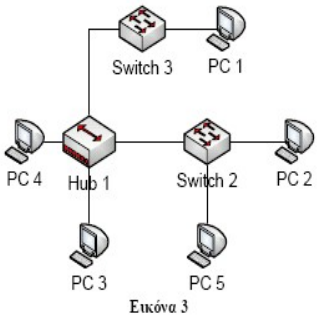
Τα collision domain έχουν όριο το switch 1 και είναι τα ακόλουθα:

1. Συνδέσεις PC2-Hub1, Hub1-Hub2, Hub2-Switch1, Hub2-PC3, Hub2-PC1
2. Συνδέσεις Switch1-Hub3, Hub3-PC5, Hub3-PC6

Το broadcast domain είναι ένα και περιλαμβάνει όλο το σχήμα, καθώς δεν υπάρχουν routers.



Εικόνα 2



Εικόνα 3

<u>Εικόνα 2</u>

Τα collision domains έχουν όριο τα Switch1, Router1 και Router2 και είναι τα ακόλουθα:

1. Σύνδεση PC1-Router2
2. Σύνδεση Router2-Router1
3. Σύνδεση Router1-PC2
4. Σύνδεση Router1-PC3
5. Σύνδεση Router1-Switch1
6. Σύνδεση PC5-Switch1
7. Σύνδεση Switch1-PC4

Τα broadcast domains έχουν όριο τα Router1 και Router2 και είναι τα ακόλουθα:

1. Συνδέσεις Router1-Switch1, PC5-Switch1, PC4-Switch1
2. Σύνδεση Router1-PC3
3. Σύνδεση Router1-PC2
4. Σύνδεση Router1-PC1
5. Σύνδεση Router1-Router2

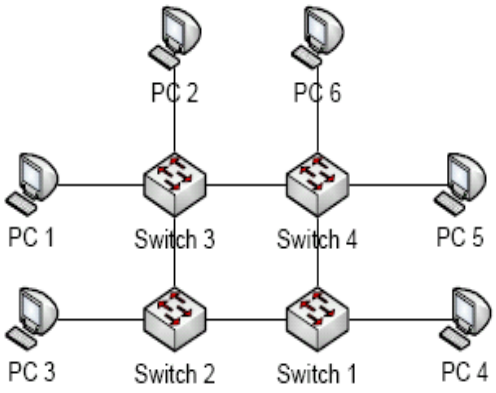
Εικόνα 3

Τα collision domains έχουν όρια τα Switch2 και Switch3 και είναι τα ακόλουθα:

1. Σύνδεση Switch2-PC2
2. Σύνδεση Switch2-PC5
3. Σύνδεση Switch2-PC1
4. Συνδέσεις Switch3-Hub1, Hub1-PC4, Hub1-PC3, Switch2-Hub1

Το broadcast domain είναι ένα και περιλαμβάνει όλο το σχήμα, καθώς δεν υπάρχουν routers.

2. Στο παρακάτω σχήμα, θεωρήστε ότι όλα τα switch διαχειρίζονται από VTP server (http://en.wikipedia.org/wiki/VLAN_Trunking_Protocol) που τα έχει διαμορφώσει ως εξής: Στα switch 1, 2 και 3 έχει οριστεί το VLAN 100 που περιλαμβάνει τα ports στα οποία συνδέονται τα PC4, PC3 και PC1 αντίστοιχα. Στο switch 3 και switch 4 έχει οριστεί το VLAN 200 που περιλαμβάνει την κίνηση από τα ports που συνδέονται τα PC2 και PC 5 αντίστοιχα. Τέλος στο switch 4 έχει οριστεί το VLAN 300 που περιλαμβάνει το port που συνδέεται το PC6.
Εξηγήστε πόσα collision domains, πόσα broadcast domains υπάρχουν και γιατί. Επίσης καταγράψτε ποια ports των switch είναι trunk ports και ποια access ports.



Εικόνα 4

2.

Τα collision domains έχουν όρια τα Switch1, Switch2, Switch3 και Switch4 και είναι τα ακόλουθα:

1. Σύνδεση Switch1-Switch2
2. Σύνδεση Switch1-PC4
3. Σύνδεση Switch1-Switch4
4. Σύνδεση Switch4-PC5
5. Σύνδεση Switch4-PC6
6. Σύνδεση Switch4-Switch3
7. Σύνδεση Switch3-PC2
8. Σύνδεση Switch3-PC1
9. Σύνδεση Switch3-Switch2
10. Σύνδεση Switch2-PC3

Το broadcast domain θα έπρεπε να είναι ένα και να περιλαμβάνει όλο το σχήμα, καθώς δεν υπάρχουν routers, όμως εφόσον ορίζονται VLANs, τότε ορίζονται broadcast domains σε αυτά τα VLAN:

1. VLAN100, συνδέσεις PC1-Switch3, PC3-Switch2, PC4-Switch1
2. VLAN200, συνδέσεις PC2-Switch3, PC5-Switch4
3. VLAN300, συνδέσεις PC6-Switch4

Για να υλοποιηθούν τα **trunk links** που χρειάζονται για τα VLAN που ορίζονται, χρειάζονται τα εξής trunk ports:

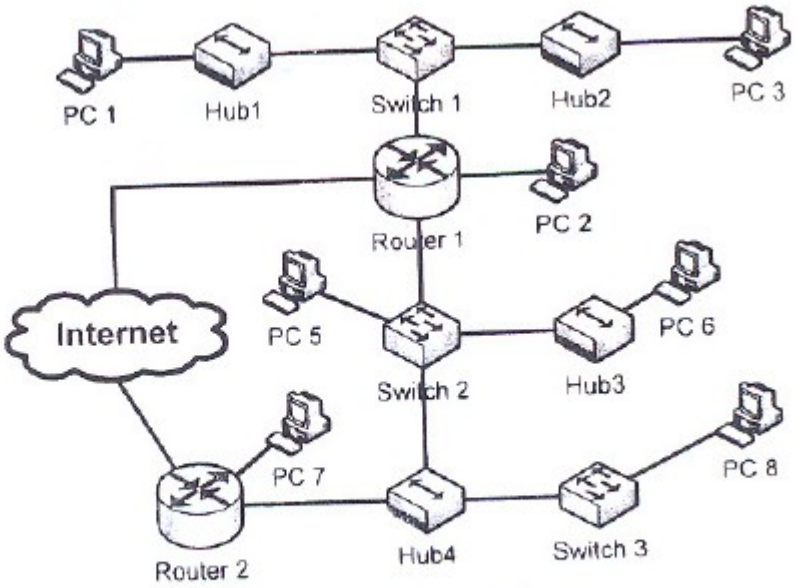
- Για το VLAN100 στα άκρα των συνδέσεων Switch1-Switch2, Switch2-Switch3, Switch1-Switch4

- Για το VLAN200 στα άκρα της σύνδεσης Switch3-Switch4
- Για το VLAN300, εφόσον δεν υπάρχει trunk link μεταξύ των switches, μπορεί να δηλωθεί ένα trunk port στο Switch4

Access ports είναι τα ports που υλοποιούν όλες τις υπόλοιπες συνδέσεις εσωτερικά στα VLAN:

- Switch1-PC4
- Switch4-PC5
- Switch4-PC6
- Switch3-PC2
- Switch3-PC1
- Switch2-PC3

Θέμα 3β -Φεβρουάριος 2011



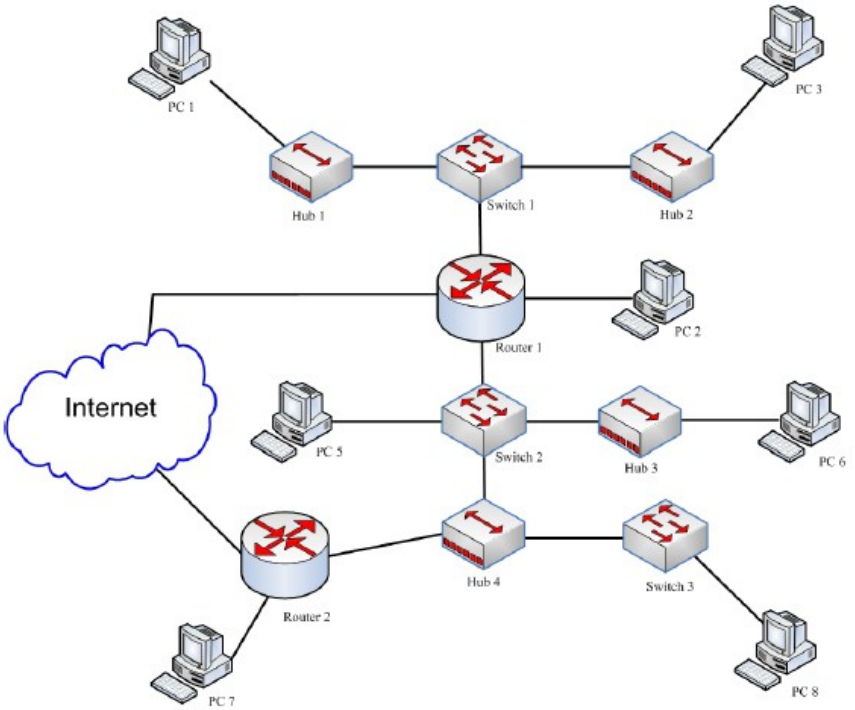
i) Ποια είναι τα collision domains στο παραπάνω σχήμα;
ii) Ποια είναι τα broadcast domains στο παραπάνω σχήμα;

Απάντηση

Είναι γνωστό ότι

- ο Επαναλήπτης (Hub) λειτουργεί στο 1° επίπεδο της στοίβας πρωτοκόλλων TCP/IP. Απλά προωθεί τα bits σε όλες τις εξόδους του.
- ο Μεταγωγέας (Switch) λειτουργεί στο 2° επίπεδο της στοίβας TCP/IP. Προωθεί την εισερχόμενη κίνηση μόνο στην κατάλληλη έξοδο.
- Ο Δρομολογητής (Router) λειτουργεί στο 3° επίπεδο. Συνδέει διαφορετικού τύπου δίκτυα. Προωθεί τα πακέτα στον επόμενο Δρομολογητή ανάλογα με τον προορισμό του πακέτου.

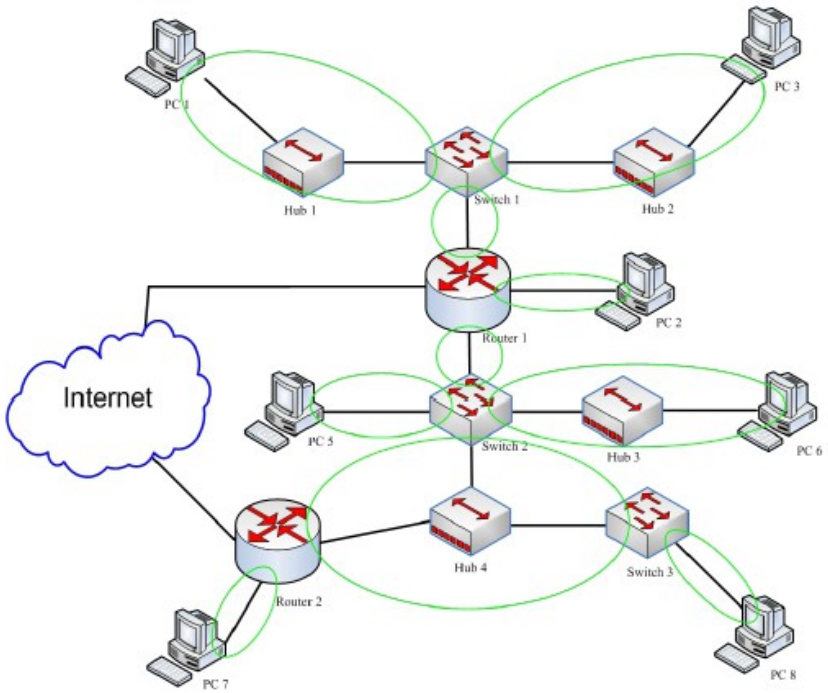
Δίνεται το παρακάτω δίκτυο.



i) Ένα collision domain αποτελεί ένα τμήμα του δικτύου, όπου τα πακέτα δεδομένων μπορούν να συγκρουστούν όταν αποστέλλονται μέσω ενός διαμοιραζόμενου μέσου μετάδοσης.

- Ένα Hub ορίζει ένα collision domain
- Κάθε θύρα ενός Switch ορίζει ένα collision domain

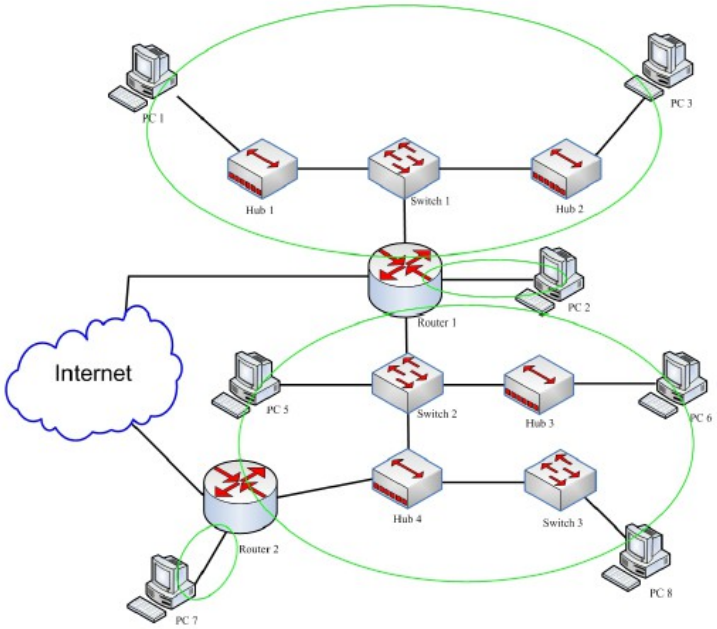
Στο ακόλουθο σχήμα δείχνουμε τα collision domains του δικτύου μας.



ii) Ένα broadcast domain αποτελεί ένα τμήμα ενός δικτύου, στο οποίο όλες οι συσκευές μπορούν να επικοινωνήσουν στο επίπεδο ζεύξης δεδομένων η μια με την άλλη μέσω broadcast μηνυμάτων.

- Οι Δρομολογητές διαχωρίζουν το δίκτυο σε broadcast domains

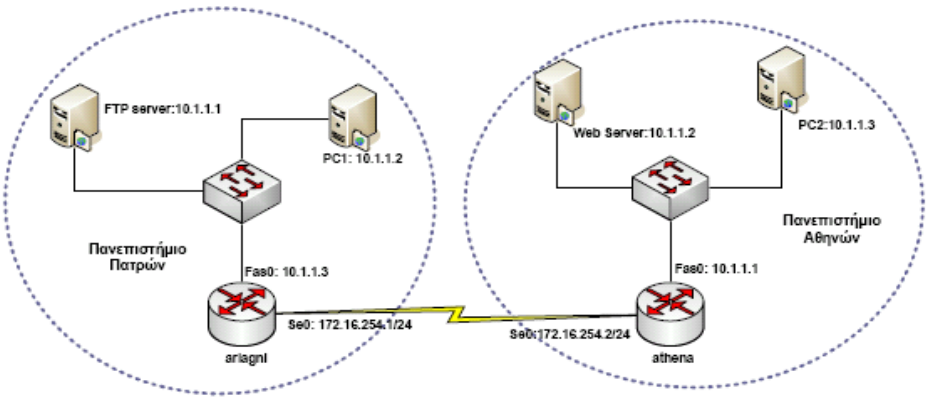
Στο ακόλουθο σχήμα δείχνουμε τα broadcast domains του δικτύου μας.



3. Γ Μέρος ACL Lists και Boson Routers

Άσκηση 1

Υποθέστε ότι εργάζεστε ως μηχανικός δικτύων στο Κέντρο Διαχείρισης Δικτύων του Πανεπιστημίου Πατρών και σας ζητείται η δικτυακή διασύνδεση του δικτύου του Πανεπιστημίου Πατρών με το δίκτυο του Πανεπιστημίου Αθηνών. Για την υλοποίηση του δικτυακού κορμού χρησιμοποιούνται δύο Cisco δρομολογητές. Κάθε δρομολογητής διαθέτει μία σειριακή διεπαφή για την διασύνδεσή του με τον άλλο δρομολογητή καθώς και μία FastEthernet διεπαφή για την διασύνδεσή του στο τοπικό δίκτυο. Για την διασύνδεση των 2 δικτύων σας έχει αποδοθεί το δημόσιο δίκτυο 172.16.254.0/24. Επιπλέον όπως φαίνεται και στο παρακάτω σχήμα σε κάθε μία συσκευή κάθε δικτύου έχει εκχωρηθεί μία ιδιωτική IP διεύθυνση.



Εικόνα 5

3. εφαρμόζοντας τις κατάλληλες Access Control Lists (ACLs) στον κατάλληλο κάθε φορά δρομολογητή να:

   a. μην επιτρέπεται η εξερχόμενη IP κίνηση από την Serial 0 διεπαφή του δρομολογητή Athena, η οποία προέρχεται από το PC2 και καταλήγει στο PC1.
   b. επιτρέπεται η εισερχόμενη ftp κίνηση από την Serial 0 διεπαφή του δρομολογητή Ariagni, η οποία προέρχεται από το PC2 και καταλήγει στον FTP server.
   c. επιτρέπεται η εισερχόμενη Web κίνηση από την Serial 0 διεπαφή του δρομολογητή Athena, η οποία προέρχεται από το PC1 και καταλήγει στον Web Server.
   d. επιτρέπεται η εισερχόμενη IP κίνηση από την Fast Ethernet 0 διεπαφή του δρομολογητή Athena, η οποία προέρχεται από το FTP server και καταλήγει στο PC2.

   Προσοχή: Αναλόγως με την διεπαφή στην οποία θέλετε να εφαρμόσετε την κάθε μία ACL, πρέπει να χρησιμοποιήσετε τις κατάλληλες ιδιωτικές ή δημόσιες IP διευθύνσεις, κατά την δήλωση της ACL.

Λύση

Για την αντιστοίχιση των ιδιωτικών σε δημόσιες IP διευθύνσεις χρησιμοποιήσαμε τις εξής IP

FTPServer: 10.1.1.1 → 172.16.254.3
PC1 : 10.1.1.2 → 172.16.254.4
WebServer : 10.1.1.2 → 172.16.254.5
PC2 : 10.1.1.3 → 172.16.254.6

Για την υλοποίηση της τεχνολογίας static NAT σε κάθε δρομολογητή χρησιμοποιούμε τις παρακάτω εντολές:

Ariagni

Στη διεπαφή Fas0 (FastEthernet0) του router Ariagni δίνουμε τις ακόλουθες εντολές:
ip nat inside source static 10.1.1.1 172.16.254.3
ip nat inside source static 10.1.1.2 172.16.254.4

Athena

Στη διεπαφή Fas0 (FastEthernet0) του router Athena δίνουμε τις ακόλουθες εντολές:
ip nat inside source static 10.1.1.2 172.16.254.5
ip nat inside source static 10.1.1.3 172.16.254.6

a)

Athena

Στη διεπαφή Se0 (Serial 0) του router Athena δίνουμε τις ακόλουθες εντολές:
access-list 100 deny ip host 10.1.1.3 host 172.16.254.4

access-list 100 permit ip any any

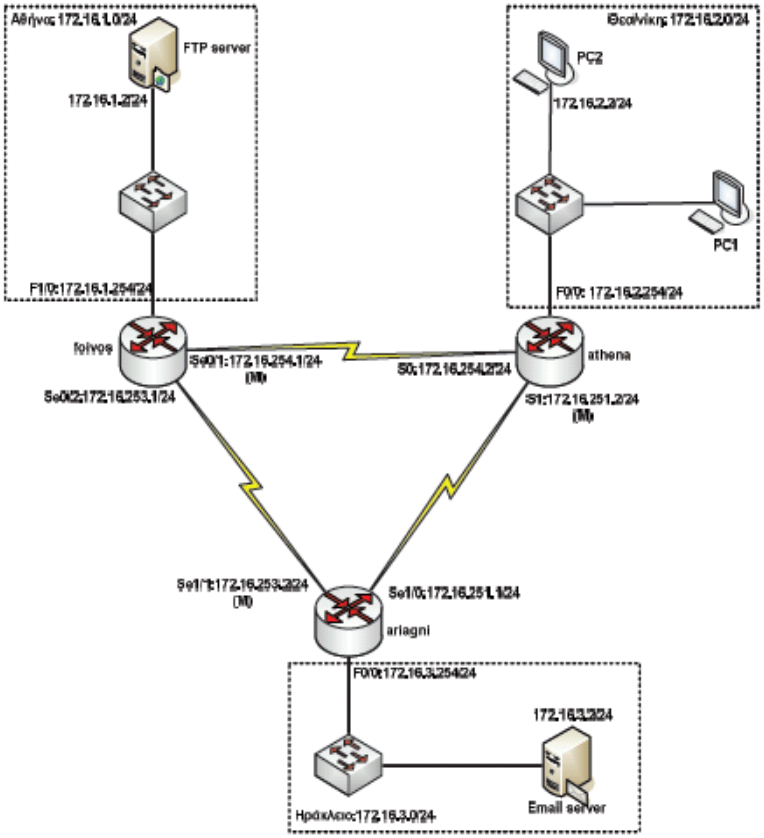
b)
Ariagni
Στη διεπαφή Se0 (Serial 0) του router Ariagni δίνουμε τις ακόλουθες εντολές:
access-list 110 permit tcp host 172.16.254.6 host 10.1.1.1 eq ftp

c)
Athena
Στη διεπαφή Se0 (Serial 0) του router Athena δίνουμε τις ακόλουθες εντολές:
access-list 120 permit tcp host 172.16.254.4 host 10.1.1.2 eq www

d) Οι κατάλληλες εντολές είναι οι παρακάτω:
Athena
Στη διεπαφή Fas0 (FastEthernet0) του router Athena δίνουμε τις ακόλουθες εντολές:
access-list 130 permit ip host 172.16.254.3 host 10.1.1.3

Άσκηση 2

Υποθέστε ότι εργάζεστε ως μηχανικός δικτύων σε μία εταιρία η οποία διαθέτει γραφεία σε Αθήνα, Θεσ/νίκη και Ηράκλειο και σας ζητείται η δικτυακή διασύνδεση των γραφείων της εταιρίας. Για την υλοποίηση του δικτυακού κορμού χρησιμοποιούνται τρεις Cisco δρομολογητές. Κάθε δρομολογητής διαθέτει δύο σειριακές διεπαφές για την διασύνδεσή του με τον άλλους δρομολογητές καθώς και μία FastEthernet διεπαφή για την διασύνδεσή του στο τοπικό δίκτυο. Για την υλοποίηση κάθε τοπικού δικτύου έχει εκχωρηθεί ένα συγκεκριμένο εύρος διευθύνσεων όπως φαίνεται στο παρακάτω σχήμα και χρησιμοποιούνται Cisco μεταγωγείς στους οποίους διασυνδέονται οι διάφοροι σταθμοί εργασίας και εξυπηρετητές της εταιρίας.



Αρχικά σχεδιάστε την τοπολογία του παραπάνω σχήματος κάνοντας χρήση του "Boson Network Designer", χρησιμοποιώντας τις κατάλληλες δικτυακές συσκευές, με κριτήριο τις εγκατεστημένες διεπαφές σε κάθε συσκευή, όπως φαίνεται στο παραπάνω σχήμα. Για την δημιουργία των σειριακών συνδέσεων μεταξύ των δρομολογητών του δικτύου της εταιρίας, το πρόγραμμα προσομοίωσης σας ζητά να ορίσετε ποια διεπαφή από τα δύο άκρα του σειριακού κυκλώματος θα δίνει το ρολόι. Σε μία πραγματική εγκατάσταση αυτό καθορίζεται από το καλώδιο που χρησιμοποιείται. Στον προσομοιωτή δηλώνουμε τον τύπο του καλωδίου σύνδεσης (DCE ή DTE). Τα Interfaces που είναι Master-DCE δηλώνονται στο σχήμα με το (M).

Εφόσον σχεδιάσετε την τοπολογία του παραπάνω σχήματος, φορτώσετε την στο "Boson Netsim" και πραγματοποιήστε τις κατάλληλες ρυθμίσεις στις δικτυακές συσκευές και τους υπολογιστές και εξυπηρετητές του δικτύου έτσι ώστε:

1. κάνοντας χρήση στατικής δρομολόγησης να αποκατασταθεί η δρομολόγηση μεταξύ των τριών δρομολογητών και να μπορούν όλοι οι υπολογιστές και εξυπηρετητές να κάνουν ping ο ένας στον άλλο.
2. δεδομένου ότι εξαρχής δεν επιτρέπεται καμία μορφή κίνησης μεταξύ των τερματικών και εξυπηρετητών του δικτύου της εταιρίας, εφαρμόστε τις κατάλληλες Access Control Lists στην κατάλληλη διεπαφή κάθε δρομολογητή, έτσι ώστε να:
   a. επιτρέπεται η FTP κίνηση από το PC1 και το PC2 προς τον FTP server της εταιρίας.
   b. επιτρέπεται η IP κίνηση από το PC1 προς τον e-mail server της εταιρίας.
   c. επιτρέπεται η ssh σύνδεση στον FTP server από το PC1.
   d. επιτρέπεται ο FTP server να κάνει telnet στο PC2.

Απάντηση

Το configuration των routers για την στατική δρομολόγηση έγινε ως εξής (εξηγούνται οι εντολές που χρησιμοποιούνται πρώτη φορά):

foivos

```
foivos(config)#interface fastethernet0/0 Επιλογή interface
foivos(config-if)#ip address 172.16.1.254 255.255.255.0 Δήλωση διεύθυνσης & μάσκας
foivos(config)#interface serial0
foivos(config-if)#ip address 172.16.254.1 255.255.255.0
foivos(config)#interface serial1
foivos(config-if)#ip address 172.16.253.1 255.255.255.0
foivos(config)#ip route 172.16.2.0 255.255.255.0 172.16.254.2
foivos(config)#ip route 172.16.3.0 255.255.255.0 172.16.253.2
```

athena

```
athena(config)#interface fastethernet0/0
athena(config-if)#ip address 172.16.2.254 255.255.255.0
athena(config)#interface serial0
athena(config-if)#ip address 172.16.254.2 255.255.255.0
athena(config)#interface serial1
athena(config-if)#ip address 172.16.251.2 255.255.255.0
athena(config)#ip route 172.16.1.0 255.255.255.0 172.16.254.1
athena(config)#ip route 172.16.3.0 255.255.255.0 172.16.251.1
```

ariagni

```
Router(config)#interface fastethernet0/0
Router(config-if)#ip address 172.16.3.254 255.255.255.0
Router(config)#interface serial0
Router(config-if)#ip address 172.16.251.1 255.255.255.0
Router(config)#interface serial1
Router (config-if)#ip address 172.16.253.2 255.255.255.0
Router(config)#ip route 172.16.1.0 255.255.255.0 172.16.253.1
Router(config)#ip route 172.16.2.0 255.255.255.0 172.16.251.2
```

2

a) Δήλωση των access lists για την FTP κίνηση από το PC1 και PC2 προς τον FTP server:

athena

```
athena(config)#access-list 100 permit tcp host 172.16.2.1 host 172.16.1.2 eq ftp
athena(config)#access-list 101 permit tcp host 172.16.2.2 host 172.16.1.2 eq ftp
athena(config)#interface serial0
athena(config-if)#ip access-group 100 out
athena(config-if)#ip access-group 101 out
```

foivos

```
foivos(config)#access-list 100 permit tcp host 172.16.2.1 host 172.16.1.2 eq ftp
foivos(config)#access-list 101 permit tcp host 172.16.2.2 host 172.16.1.2 eq ftp
foivos(config)#interface serial0
foivos(config-if)#ip access-group 100 in
foivos(config-if)#ip access-group 101 in
```

b) Δήλωση των access lists για την IP κίνηση από το PC1 προς τον email server:
athena

```
athena(config)#access-list 100 permit ip host 172.16.2.1 host 172.16.3.2
athena(config)#interface serial1
athena(config-if)#ip access-group 100 out
```

ariagni

```
ariagni(config)#access-list 100 permit ip host 172.16.2.1 host 172.16.3.2
ariagni(config)#interface serial0
ariagni(config-if)#ip access-group 100 in
```

c) Δήλωση των access lists για την ssh σύνδεση από το PC1 προς τον FTP server:
athena

```
athena(config)#access-list 100 permit tcp host 172.16.2.1 host 172.16.1.2 eq ssh
athena(config)#interface serial0
athena (config-if)#ip access-group 100 out
```

foivos

```
foivos (config)#access-list 100 permit tcp host 172.16.2.1 host 172.16.1.2 eq ssh
foivos(config)#interface serial0
foivos(config-if)#ip access-group 100 in
```

d) Δήλωση των access lists για την telnet σύνδεση από το PC2 προς τον FTP server:
foivos

```
foivos(config)#access-list 100 permit tcp host 172.16.1.2 host 172.16.2.2 eq telnet
foivos(config)#interface serial0
foivos(config-if)#ip access-group 100 out
```

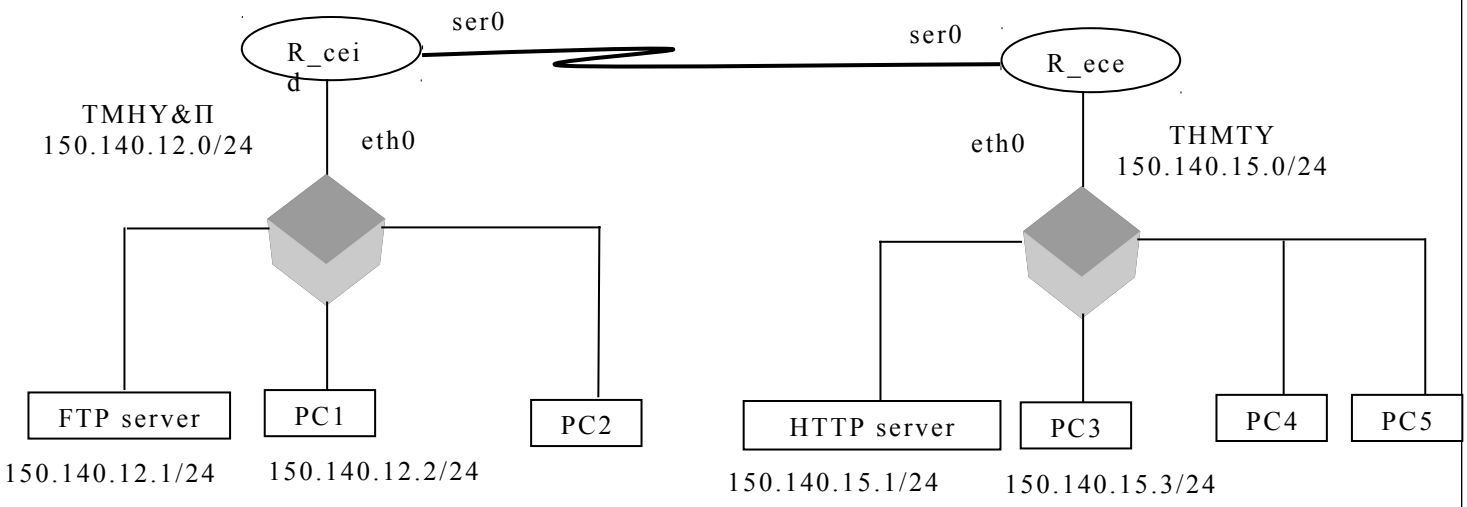
athena

```
athena(config)#access-list 100 permit tcp host 172.16.1.2 host 172.16.2.2 eq telnet
athena(config)#interface serial0
athena(config-if)#ip access-group 100 in
```

Φεβρουάριος 2009 - Θέμα 3

Θεωρείστε την δικτυακή τοπολογία του παρακάτω σχήματος που συνδέει το δίκτυο του τμήματος Μηχανικών Η/Υ και Πληροφορικής (ΤΜΗΥ&Π) με το δίκτυο του Τμήματος Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών (ΤΗΜΤΥ). Δεδομένου ότι αρχικά επιτρέπεται οποιαδήποτε μορφή κίνησης μεταξύ των δύο δικτύων, ορίστε τις κατάλληλες Access Control Lists (ACL) έτσι ώστε:

(i) Να μην επιτρέπονται οι FTP συνδέσεις από τις συσκευές του ΤΗΜΤΥ προς τον FTP server του ΤΜΗΥ&Π
(ii) Να μην επιτρέπεται το PC1 που βρίσκεται στο ΤΜΗΥ&Π να στέλνει HTTP requests στον HTTP server του ΤΗΜΤΥ
(iii) Να μην επιτρέπεται το PC3 του ΤΗΜΤΥ να κάνει telnet στο PC1 του ΤΜΗΥ&Π
(iv) Να μην επιτρέπονται οι συσκευές του ΤΜΗΥ&Π να κάνουν telnet στο PC3 του ΤΗΜΤΥ
(v) Να μην επιτρέπεται οι συσκευές του ΤΜΗΥ&Π να έχουν πρόσβαση στις συσκευές του ΤΗΜΤΥ
(vi) Να επιτρέπεται οι συσκευές του ΤΜΗΥ&Π να έχουν πρόσβαση στις συσκευές του ΤΗΜΤΥ
(vii) Να απαγορεύεται η πρόσβαση του PC1 του ΤΜΗΥ&Π στο PC3 του ΤΗΜΤΥ και να επιτρέπεται οποιαδήποτε άλλη κίνηση
(viii) Να απαγορεύεται η web κίνηση από το ΤΗΜΤΥ προς τον FTP server του ΤΜΗΥ&Π
(ix) Να μην επιτρέπεται η web κίνηση από το ΤΜΗΥ&Π στο PC3 του ΤΗΜΤΥ



Υπόδειξη: θα πρέπει να αναφέρετε σε ποια διεπαφή ποιου δρομολογητή θα εφαρμοστεί η ACL καθώς και σε ποια ροή κίνησης (εισερχόμενη ή εξερχόμενη κίνηση). Ο router του τμήματος ΤΜΗΥ&Π συμβολίζεται ως R_ceid ενώ ο router του τμήματος ΤΗΜΤΥ συμβολίζεται ως R_ece.

Απάντηση
Όλες οι ACL τοποθετούνται στην Ser0 διεπαφή του αντίστοιχου δρομολογητή

(i) Στην **εισερχόμενη κίνηση του router R_ceid** ή στην **εξερχόμενη κίνηση του router R_ece** γράφουμε την εντολή:
deny tcp 150.140.15.0 0.0.0.255 host 150.140.12.1 eq ftp

Γράφουμε την IP όλου του δικτύου και τη μάσκα του προκειμένου να προσδιορίσουμε όλο το δίκτυο ΤΗΜΤΥ. Επίσης γράφουμε την εντολή host διότι θέλουμε να προσδιορίσουμε συγκεκριμένο υπολογιστή. Κανονικά η μάσκα του υποδικτύου του ΤΜΗΥ&Π είναι 255.255.255.0. Επειδή όμως χρησιμοποιούνται 24 bit για το δίκτυο άρα η μάσκα γίνεται 255.255.255.0

(ii) Στην **εισερχόμενη κίνηση του router R_ece** ή στην **εξερχόμενη κίνηση του router R_ceid** γράφουμε την εντολή:
deny tcp host 150.140.12.2 host 150.140.15.1 eq www

(iii) Στην **εξερχόμενη κίνηση του router R_ece** ή στην **εισερχόμενη κίνηση του router R_ceid** γράφουμε την εντολή:
deny tcp host 150.140.15.3 host 150.140.12.2 eq telnet

(iv) Στην **εξερχόμενη κίνηση του router R_ceid** ή στην **εισερχόμενη κίνηση του router R_ece** γράφουμε την εντολή:
deny tcp 150.140.12.0 0.0.0.255 host 150.140.15.3 eq telnet

(v) Στην **εξερχόμενη κίνηση του router R_ceid** ή στην **εισερχόμενη κίνηση του router R_ceid** γράφουμε την εντολή:
deny ip 150.140.12.0 0.0.0.255 150.140.15.0 0.0.0.255

(vi) Στην **εξερχόμενη κίνηση του router R_ceid** ή στην **εισερχόμενη κίνηση του router R_ece** γράφουμε την εντολή:
permit ip 150.140.12.0 0.0.0.255 150.140.15.0 0.0.0.255

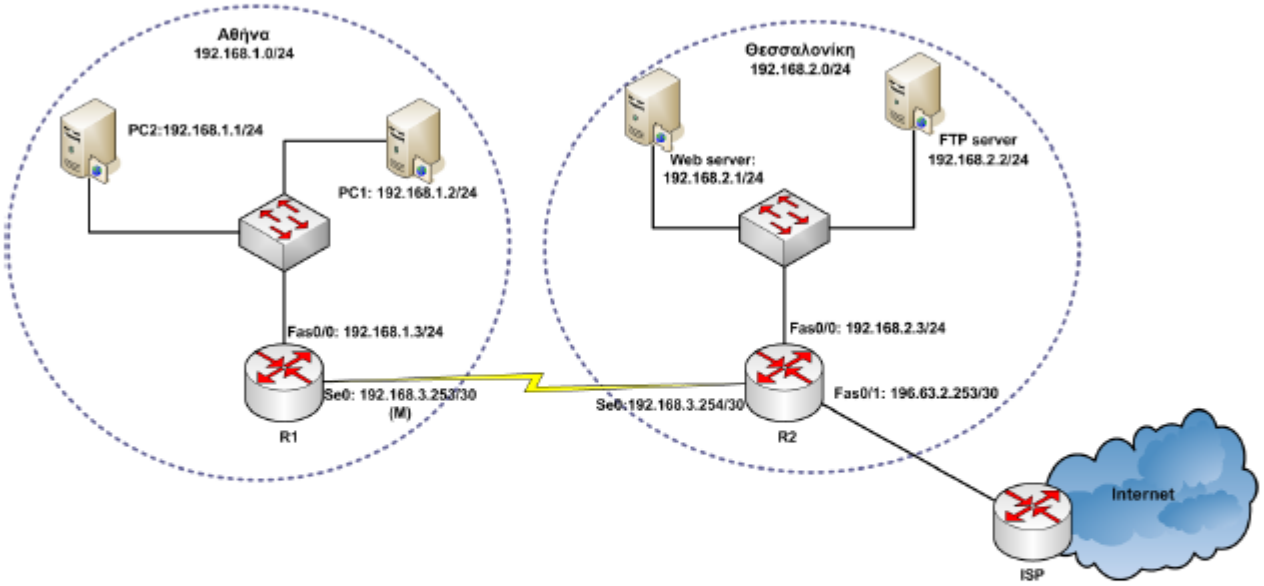
(vii) Στην **εισερχόμενη κίνηση του router R_ece** ή στην **εξερχόμενη κίνηση του router R_ceid** γράφουμε την εντολή:
deny ip host 150.140.12.2 host 150.140.15.3
permit any any

(viii) Στην **εξερχόμενη κίνηση του router R_ece** ή στην **εισερχόμενη κίνηση του router R_ceid** γράφουμε την εντολή:
deny tcp 150.140.15.0 0.0.0.255 host 150.140.12.1 eq www

(ix) Στην **εξερχόμενη κίνηση του router R_ece** ή στην **εισερχόμενη κίνηση του router R_ceid** γράφουμε την εντολή:
deny tcp 150.140.12.0 0.0.0.255 host 150.140.15.3 eq www

Άσκηση 2

Υποθέστε ότι μία εταιρία διαθέτει γραφεία σε Αθήνα και Θεσσαλονίκη τα οποία και επιθυμεί να διασυνδέσει στο Internet, όπως φαίνεται στο παρακάτω σχήμα. Στα γραφεία της Αθήνας η εταιρία διαθέτει ένα πλήθος από PCs (στο σχήμα φαίνονται μόνο 2 PCs), ενώ στα γραφεία της Θεσσαλονίκης έναν πλήθος από PCs, έναν Web server και έναν FTP server.



Για την υλοποίηση του δικτυακού κορμού της εταιρίας χρησιμοποιούνται δύο Cisco δρομολογητές ενώ για την υλοποίηση του τοπικού δικτύου στην Αθήνα και στην Θεσσαλονίκη χρησιμοποιείται από ένας Cisco μεταγωγέας. Ο δρομολογητής R1 διαθέτει μία σειριακή διεπαφή για την διασύνδεσή του με τον δρομολογητή της Θεσσαλονίκης, καθώς και μία Fast Ethernet διεπαφή για την διασύνδεσή του στο τοπικό δίκτυο της Αθήνας. Ο δρομολογητής R2 διαθέτει μία σειριακή διεπαφή για την διασύνδεσή του με τον δρομολογητή της Αθήνας, μία Fast Ethernet διεπαφή για την διασύνδεσή του στο τοπικό δίκτυο της Θεσσαλονίκης και άλλη μία Fast Ethernet διεπαφή για την πρόσβασή του στο Internet. Για λόγους οικονομίας και ασφάλειας, το δίκτυο της εταιρίας έχει υλοποιηθεί χρησιμοποιώντας ιδιωτικές IP διευθύνσεις, ενώ και για την διασύνδεση των δύο υποδικτύων της εταιρίας χρησιμοποιούνται επίσης ιδιωτικές IP διευθύνσεις, μία σε κάθε ένα άκρο του σειριακού κυκλώματος που συνδέει τα δύο υποδίκτυα. Συγκεκριμένα στο δίκτυο της Αθήνας έχει αποδοθεί το υποδίκτυο 192.168.1.0/24, ενώ στο δίκτυο της Θεσσαλονίκης το υποδίκτυο 192.168.2.0/24. Όλη η κίνηση της εταιρίας δρομολογείται στο Internet, μέσω του δρομολογητή R2 χρησιμοποιώντας ένα Ethernet κύκλωμα πρόσβασης που παρέχεται από έναν ISP (π.χ. Metro Ethernet). Επιπλέον, για να έχουν πρόσβαση όλα τα PC και οι servers της εταιρίας στο Internet, χρησιμοποιείται η τεχνολογία NAT-PAT **μόνο** στον δρομολογητή R2.

Εφόσον σχεδιάσετε την τοπολογία του παραπάνω σχήματος, φορτώσετε την στο "Boson Netsim" και πραγματοποιήστε τις κατάλληλες ρυθμίσεις στις δικτυακές συσκευές και τους υπολογιστές, εξυπηρετητές του δικτύου έτσι ώστε:

1. στους δρομολογητές R1 και R2, να οριστούν τα ονόματα τους, να ενεργοποιηθούν οι διεπαφές τους και να εκχωρηθούν οι κατάλληλες IP διευθύνσεις σε κάθε μία διεπαφή τους, όπως φαίνεται στο παραπάνω σχήμα (15 μονάδες).
2. να οριστούν οι στατικές διαδρομές δρομολόγησης μεταξύ των 2 υποδικτύων της εταιρίας, έτσι ώστε να είναι δυνατή η επικοινωνία μεταξύ των δύο υποδικτών της (π.χ να μπορεί το PC1 να κάνει ping στον Web server). (15 μονάδες).
3. να υλοποιηθεί η τεχνολογία NAT-PAT στον δρομολογητή R2, έτσι ώστε οι δύο server της εταιρίας να είναι προσβάσιμοι από το Internet (30 μονάδες).
4. δεδομένου ότι εξαρχής δεν επιτρέπεται καμία μορφή κίνησης μεταξύ των τερματικών και εξυπηρετητών του δικτύου της εταιρίας, εφαρμόστε τις κατάλληλες Access Control Lists στην κατάλληλη διεπαφή κάθε δρομολογητή, έτσι ώστε να:
    a. επιτρέπονται οι HTTP συνδέσεις από το PC1 προς τον Web server (10 μονάδες).
    b. επιτρέπονται οι HTTP συνδέσεις από το PC2 προς τον Web server (10 μονάδες).
    c. επιτρέπεται όλο το δίκτυο της Αθήνας να κάνει FTP στον FTP server (10 μονάδες).
    d. επιτρέπεται όλη η IP κίνηση από τον FTP server προς το δίκτυο της Αθήνας (10 μονάδες).

Λύση

2) Για να ορίσουμε τις στατικές δρομολογήσεις ανάμεσα στα δύο υποδίκτυα της εταιρίας αρκεί να δώσουμε από τους δρομολογητές R1 και R2 τις ακόλουθες εντολές

R1
#ip route 192.168.2.0 255.255.255.0 192.168.3.254

R2
#ip route 192.168.1.0 255.255.255.0 192.168.3.253

3) Για να είναι οι server της εταιρίας προσβάσιμοι από το internet θα πρέπει να αντιστοιχίσουμε την (εξωτερική) διεύθυνση του δικτύου της εταιρίας και τα port των υπηρεσιών HTTP(80) και FTP(21) στις αντίστοιχες (εσωτερικές) διευθύνσεις (και port) των server. Δηλαδή:

R2
#nat (inside) 1 192.168.2.0 255.255.255.0 0 0 #global (outside) 1 196.63.2.253 #static (inside, outside) tcp 196.63.2.253 80 192.168.2.1 80 netmask 255.255.255.255 #static (inside, outside) tcp 196.63.2.253 21 192.168.2.2 21 netmask 255.255.255.255

4) Η γενική διαδικασία που πρέπει να ακολουθήσουμε για να δημιουργήσουμε και να ενεργοποιήσουμε μία access-list είναι η ακόλουθη.

- Βήμα 1: Δημιουργούμε την access-list ενώ βρισκόμαστε σε configure mode
  πχ. access-list 101 permit tcp host 192.168.2.1 host 192.16.1.2 eq www
- Βήμα 2: Ενεργοποιούμε το configuration του interface που μας ενδιαφέρει πχ. interface serial 0
- Βήμα 3: Ενεργοποιούμε την access-list είτε για εισερχόμενη είτε για εξερχόμενη κίνηση πχ. ip access-group 101 in

a) Για να επιτρέψουμε την κίνηση από το PC1 προς τον Web Server εκτελούμε

R1
#access-list 101 permit tcp host 192.168.1.2 host 192.168.2.1 eq 80 #interface serial 0 #ip access-group 101 out

R2
#access-list 101 permit tcp host 192.168.1.2 host 192.168.2.1 eq 80 #interface serial 0 #ip access-group 101 in

b) Για να επιτρέψουμε την κίνηση από το PC2 προς τον Web Server εκτελούμε τις εντολές:

R1

```
#access-list 102 permit tcp host 192.168.1.1 host 192.168.2.1 eq 80
#interface serial 0
#ip access-group 102 out
```

R2
#access-list 102 permit tcp host 192.168.1.1 host 192.168.2.1 eq 80 #interface serial 0 #ip access-group 102 in

c) Για να κάνουμε ftp από το δίκτυο της Αθήνας προς τον FTP Server δίνουμε τις εντολές:

R1
#access-list 103 permit tcp 192.168.1.0 225.225.255.0 host 192.168.2.2 eq 21 #interface serial 0 #ip access-group 103 out

R2
#access-list 103 permit tcp 192.168.1.0 225.225.255.0 host 192.168.2.2 eq 21 #interface serial 0 #ip access-group 103 in

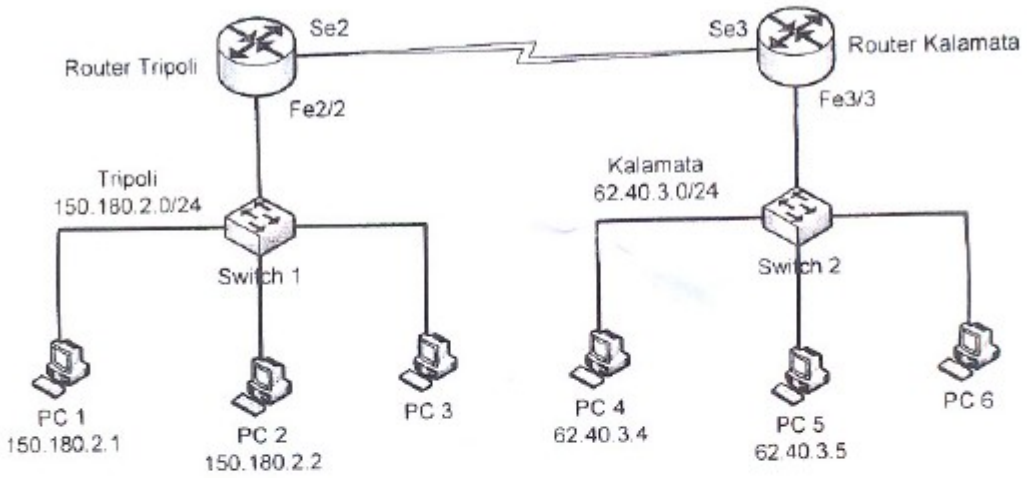
d) Για να επιτρέψουμε όλη την IP κίνηση από τον FTP server προς το δίκτυο της Αθήνας δίνουμε τις εντολές:

R1
#access-list 104 permit ip host 192.168.2.2 192.168.1.0 225.225.255.0 #interface serial 0 #ip access-group 104 in

R2
#access-list 104 permit ip host 192.168.2.2 192.168.1.0 225.225.255.0 #interface serial 0 #ip access-group 104 out

Θέμα 5 Φεβρουάριος 2011

Θεωρήστε την δικτυακή τοπολογία του παρακάτω σχήματος.



Ορίστε τις κατάλληλες Access Control Lists στον κατάλληλο κάθε φορά δρομολογητή και interface έτσι ώστε:

i) Να επιτρέπεται οι υπολογιστές που βρίσκονται στην Καλαμάτα να επικοινωνούν με ftp με το PC 1.
ii) Να μην επιτρέπονται τα ICMP πακέτα από όλα τα PC στο υποδίκτυο της Τρίπολης προς όλα τ PC στο υποδίκτυο της Καλαμάτας.
iii) Να μην επιτρέπεται οποιαδήποτε εξερχόμενη telnet κίνηση από το υποδίκτυο της Τρίπολης.
iv) Να μην επιτρέπονται οι UDP συνδέσεις από το PC5 προς το υποδίκτυο της Τρίπολης.

Θεωρήστε κάθε ένα από τα παραπάνω υπο-ερωτήματα ανεξάρτητο από τα υπόλοιπα.

Υποδείξεις/βοηθητικό υλικό

Η γενική μορφή σύνταξης των Access Control Lists στους Cisco δρομολογητές (ότι δίνεται με πλάγια γράμματα μέσα σε tags < > πρέπει να αντικατασταθεί από την κατάλληλη τιμή, ότι βρίσκεται μέσα σε αγκύλες { } πρέπει να επιλεγεί η κατάλληλη τιμή, ενώ ότι βρίσκεται σε άγκιστρα [ ] είναι προαιρετικό) είναι η παρακάτω:

Απάντηση

i) Στον Router Tripoli, interface Fe2/2

ip access-list extended 100 permit tcp 62.40.3.0 255.255.255.0 150.180.2.1 255.255.255.0 eq 21

Επεξήγηση της παραπάνω λίστας.
Επιτρέπονται (permit) τα πακέτα TCP που προέρχονται από Καλαμάτα (ip address 62.40.3.0, subnet mask 255.255.255.0) και προορίζονται για το PC 1 (ip address 150.180.2.1, subnet mask 255.255.255.0) σε port number ίσο (eq) με 21 (FTP).

ii) Στον Router Kalamata, interface Fe3/3

ip access-list extended 101 deny icmp 150.180.2.0 255.255.255.0 62.40.3.0 255.255.255.0

Επεξήγηση της παραπάνω λίστας.
Δεν επιτρέπονται (deny) τα πακέτα ICMP που προέρχονται από Τρίπολη (ip address 150.180.2.0, subnet mask 255.255.255.0 ή /24) και προορίζονται για Καλαμάτα (ip address 62.40.3.0, subnet mask 255.255.255.0 ή /24).

iii) Στον Router Tripoli, interface Se2

ip access-list extended 102 deny ip 150.180.2.0 255.255.255.0 any eq 23

Επεξήγηση της παραπάνω λίστας.
Δεν επιτρέπονται (deny) τα πακέτα IP που προέρχονται από Τρίπολη (ip address 150.180.2.0, subnet mask 255.255.255.0) και προορίζονται για οπουδήποτε (any) σε port number ίσο (eq) με 23 (telnet).

iv) Στον Router Tripoli, interface Fe2/2

ip access-list extended 103 deny udp 62.40.3.5 255.255.255.0 150.180.2.0 255.255.255.0

Επεξήγηση της παραπάνω λίστας.
Δεν επιτρέπονται (deny) τα πακέτα UDP που προέρχονται από το PC 5 (ip address 62.40.3.5, subnet mask 255.255.255.0) και προορίζονται για την Τρίπολη (ip address 150.180.2.0, subnet mask 255.255.255.0).

4. Δ μέρος Προγραμματισμός

TCP Server

```
#include <stdio.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <unistd.h>
#include <netinet/in.h>
#include <string.h>
#include <stdlib.h>

#define SIZE 100

int main(int argc, char **argv)
{
        int connfd, pid, listenfd, len;
        struct sockaddr_in serv_addr, cli_addr;
        int port= 9000;
        char text[SIZE]="";


        connfd = socket(AF_INET,SOCK_STREAM,0); //Δημιουργία TCP socket από server

        bzero(&serv_addr, sizeof(serv_addr)) //μηδενισμός των πεδίων της δομής serv_addr
        //Εναλλακτικά η συνάρτηση memset((void*)&serv_addr,0,sizeof(serv_addr)); έχει την ίδια λειτουργία με την bzero

        serv_addr.sin_family = AF_INET; //Καθορισμός του τύπου του socket ως INTERNET socket

        serv_addr.sin_addr.s_addr = htonl(INADDR_ANY);//συνάρτηση μετατροπής IP διεύθυνσης σε long integer. Έτσι ο server μπορεί να στέλνει και να λαμβάνει από οποιαδήποτε IP address

        serv_addr.sin_port = htons(port);//συνάρτηση μετατροπής του port που ακούει ο server σε short integer

        bind(connfd,(struct sockaddr *)&serv_addr, sizeof(serv_addr));//Σύνδεση του server στο socket

        listen(connfd,10);//ο server ορίζει μια ουρά αιτήσεων με μέγεθος 10

        printf ("Server listens to port: %d\n",port);

        while(1)//ο server εκτελεί άπειρο βρόγχο
        {
                len= sizeof(cli_addr);

                Listenfd=accept (connfd,(struct sockaddr*)&cli_addr,&len);//Η συνάρτηση accept εκτελείται αυτόματα κάθε φορά που ο server λαμβάνει μια αίτηση από τον client και επιστρέφει ένα ακέραιο αριθμό ο οποίος καταχωρείται στη μεταβλητή listenfd και αφορά το socket connfd. Ουσιαστικά ο αριθμός στη listenfd είναι ο νέος αριθμός με τον οποίο θα αναφερόμαστε τώρα στο socket και θα χρησιμοποιηθεί σε όλες τις επόμενες εντολές

                if (listenfd<0)
                {
                        puts("error");
                        exit(0);
                }

                pid=fork();//δημιουργία child του server

                if (pid==0)
                {
                        close(connfd);//κλείσιμο αρχικού socket

                        recv(listenfd,text,SIZE,0);//ο server λαμβάνει πληροφορία από τον client
```

```
                printf("Server received from Client Message: %s\n", text);

                strcpy(text, "Hello from Server");

                send(listenfd, text, strlen(text),0);//o server στέλνει πληροφορία στον client

                exit(0);//τερματισμός child process του server
            }
        }

        return 0; //τερματισμός TCP server
}
```

TCP Client

```
#include <stdio.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <unistd.h>
#include <netinet/in.h>
#include <string.h>
#include <stdlib.h>

#define SIZE 512

int main(int argc, char **argv)
{
        int i, listenfd, port=9000;
        struct sockaddr_in cliaddr;
        char text[50];

        listenfd = socket(AF_INET, SOCK_STREAM,0);//Δημιουργία TCP socket από client

        bzero(&cliaddr, sizeof(cliaddr)) //μηδενισμός των πεδίων της δομής cliaddr
        //Εναλλακτικά η συνάρτηση memset((void*)& cliaddr,0,sizeof(cliaddr)); εκτελεί την ίδια λειτουργία με την bzero

        cliaddr.sin_family = AF_INET; //Καθορισμός του τύπου του socket ως INTERNET socket

        cliaddr.sin_addr.s_addr =htonl(INADDR_ANY);//συνάρτηση μετατροπής IP διεύθυνσης σε long integer

        cliaddr.sin_port =htons(port); //συνάρτηση μετατροπής του port που ακούει ο client σε short integer

        connect(listenfd,(struct sockaddr *)&cliaddr, sizeof(cliaddr));//Σύνδεση του client στο socket

        strcpy(text, "Hello from Client");

        send(listenfd, text, strlen(text),0);//o TCP client στέλνει πληροφορία (κείμενο) στον server

        recv(listenfd,text,SIZE,0);//o TCP client λαμβάνει πληροφορία (κείμενο) από τον server

        printf("Client received from Server Message: %s\n", text);

        close(listenfd);//κλείσιμο socket

        return 0; //τερματισμός TCP client
}
```

UDP Server

```
#include <stdio.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <unistd.h>
```

```
#include <netinet/in.h>
#include <string.h>
#include <stdlib.h>

#define SIZE 100

int main(int argc, char **argv)
{
        int connfd, len;
        struct sockaddr_in serv_addr;
        int port=9000;
        char text[SIZE];

        connfd = socket(AF_INET,SOCK_DGRAM,0); //Δημιουργία UDP socket από server.

        bzero(&serv_addr, sizeof(serv_addr)) //Μηδενισμός των πεδίων της δομής serv_addr

        serv_addr.sin_family = AF_INET; //Καθορισμός του τύπου του socket ως INTERNET socket

        serv_addr.sin_addr.s_addr = htonl(INADDR_ANY); //συνάρτηση μετατροπής IP διεύθυνσης σε long integer

        serv_addr.sin_port = htons(port); //συνάρτηση μετατροπής του port που ακούει ο server σε short integer

        bind(connfd,(struct sockaddr *)&serv_addr,sizeof(serv_addr));//Σύνδεση του server στο socket

        printf("Server listens to port: %d\n",port);

        len=sizeof(serv_addr);

        recvfrom(connfd, text, SIZE, 0,(struct sockaddr*)&serv_addr, &len);//ο server λαμβάνει πληροφορία (κείμενο) από τον client

        printf("Server received from Client Message: %s\n", text);

        strcpy(text, "Hello from Server");

        sendto(connfd,text,SIZE,0, (struct sockaddr*)&serv_addr,sizeof(struct sockaddr));//ο server στέλνει πληροφορία (κείμενο)
στον client

        close(connfd);//κλείσιμο socket

        exit(0);//τερματισμός server
}
```

UDP Client

```
#include <stdio.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <unistd.h>
#include <netinet/in.h>
#include <string.h>
#include <stdlib.h>

#define SIZE 512

int main(int argc, char **argv)
{
        int i, listenfd, port=9000, len;
        struct sockaddr_in cliaddr;
        char text[50];

        listenfd = socket(AF_INET, SOCK_DGRAM,0);//Δημιουργία UDP socket από client
```

```
	bzero(&cliaddr, sizeof(cliaddr));//Μηδενισμός των πεδίων της δομής cliaddr

	cliaddr.sin_family = AF_INET;

	cliaddr.sin_addr.s_addr = htonl(INADDR_ANY);//συνάρτηση μετατροπής IP διεύθυνσης σε long integer

	cliaddr.sin_port = htons(port); //συνάρτηση μετατροπής του port που ακούει ο client σε short integer

	strcpy(text, "Hello from Client");

	sendto(listenfd, text, SIZE,0,(struct sockaddr*)& cliaddr, sizeof(struct sockaddr)); //ο UDP client στέλνει πληροφορία (κείμενο) στον server

	len=sizeof(cliaddr);

	recvfrom(listenfd, text, SIZE, 0,(struct sockaddr*)&cliaddr, &len); //ο UDP client λαμβάνει πληροφορία (κείμενο) στον server

	printf("Client received from Server Message: %s\n", text);

	close(listenfd);//κλείσιμο socket

	return 0;//τερματισμός UDP client
}
```

Φεβρουάριος 2009 - Θέμα 1

α)Θέλουμε να δημιουργήσουμε ένα πρόγραμμα που να υλοποιεί ένα TCP server, με τη χρήση του Unix socket API. Η λειτουργία του server θα είναι να δέχεται μια σύνδεση από ένα client, να εκτελεί μια συνάρτηση "do_something" (δεν έχει σημασία τι λειτουργία εκτελεί η συνάρτηση αυτή) και μετά να τερματίζει. Σας δίνονται τα εξής τμήματα κώδικα σε ανακατεμένη σειρά:

```
do_something(s1);
bind(s2,(struct sockaddr *)&servaddr, sizeof(servaddr));
s3 = socket(AF_INET,SOCK_STREAM,0);
s4=accept(s5, (struct sockaddr*)&cliaddr, &sizeof(cliaddr));
bzero(&servaddr, sizeof(servaddr));
servaddr.sin_family = AF_INET;
servaddr.sin_addr.s_addr = htonl(INADDR_ANY);
servaddr.sin_port = htons(SERV_PORT);
listen(s6, LISTENQ);
```

Σας ζητείται να τα βάλετε στη σωστή σειρά έτσι ώστε να συμπληρώσετε το παρακάτω πρόγραμμα και επίσης να αντικαταστήσετε τα s1, s2, s3, s4, s5 και s6 με τα σωστά socket descriptor (listenfd ή connfd)

```
#define SERV_PORT 9000

int main(int argc, char **argv)
{
	int listenfd, connfd;
	socklen_t clilen;
	struct sockaddr_in cliaddr, servaddr;
	...
}
```

β)Ένα πρόβλημα που υπάρχει με τον παραπάνω TCP server είναι ότι δέχεται μια σύνδεση από ένα TCP Client και όταν ολοκληρώσει την εξυπηρέτηση του ο server τερματίζει. Πως μπορούμε να κάνουμε τον server να δέχεται συνδέσεις από περισσότερους του ενός πελάτες; Δώστε ψευδοκώδικα και συμπληρώστε το παραπάνω πρόγραμμα

Λύση

α)

```
#define SERV_PORT 9000

int main(int argc, char **argv)
{
```

```
        int listenfd, connfd;
        socklen_t clilen;
        struct sockaddr_in cliaddr, servaddr;

        connfd = socket(AF_INET,SOCK_STREAM,0);

        bzero (&servaddr, sizeof(servaddr));

        servaddr.sin_family = AF_INET;
        servaddr.sin_addr.s_addr = htonl(INADDR_ANY);
        servaddr.sin_port = htons(SERV_PORT);

        bind(connfd,(struct sockaddr *)&servaddr, sizeof(servaddr));

        listen(connfd, LISTENQ);

        listenfd=accept(connfd,(struct sockaddr*)&cliaddr, &sizeof(cliaddr));

        do_something(listenfd);
}
```

β) Για να μπορεί ο server να δέχεται συνδέσεις από περισσότερους από ένα πελάτες πρέπει να εκτελεί τη συνάρτηση fork() μέσα σε άπειρο βρόγχο ως εξής:

```
        while(1)//ο server εκτελεί άπειρο βρόγχο
        {

                listenfd=accept(connfd,(struct sockaddr*)&cliaddr, &sizeof(cliaddr));

                if (listenfd<0)
                {
                        puts("error");
                        exit(0);
                }

                pid=fork();//δημιουργία child του server

                if (pid==0)
                {
                        close(connfd);

                        do_something(listenfd);

                        close(listenfd);

                        exit(0);
                }
        }
```

Φεβρουάριος 2011 - Θέμα 4

α) Σας δίνεται το παρακάτω πρόγραμμα ενός TCP server που ακούει στο port 9000, γραμμένο με την χρήση του unix socket api.

```
#include <sys/types.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <sys/socket.h>
#include <stdlib.h>
#include <string.h>
#define LISTENQ 10

int main(int argc, char **argv)
{
     int     listenfd, connfd, n;
     pid_t   childpid;
     socklen_t clilen;
     struct sockaddr_in cliaddr, servaddr;
     char    buf[200];

          A

          B

          C

       for ( ; ; ) {
            D

          if ( (childpid = fork()) == 0) {
               E
          }
            F
       }
}
```

Αντιστοιχίστε τα παρακάτω τμήματα κώδικα (1-6) στις σωστές θέσεις στο παραπάνω πρόγραμμα (A-F).

1
```
bind(listenfd, (struct sockaddr *) &servaddr, sizeof(servaddr));
listen(listenfd, LISTENQ);
```

2
```
bzero(&servaddr, sizeof(servaddr));
servaddr.sin_family =  AF_INET;
servaddr.sin_addr.s_addr = htonl (INADDR_ANY);
servaddr.sin_port = htons (9000);
```

3
```
close(listenfd);
do_something();  /*Μια συνάρτηση που κάνει την κυρίως δουλειά*/
exit(0);
```

4
```
clilen = sizeof(cliaddr);
connfd = accept(listenfd, (struct sockaddr *) &cliaddr, &clilen);
```

5
```
close(connfd);
```

6
```
listenfd = socket (AF_INET, SOCK_STREAM , 0);
```

β)

i) Για ποιο λόγο το 2ο όρισμα της κλήσης accept είναι τύπου pointer σε struct sockaddr;
ii) Μπορούν να συνδεθούν παραπάνω από ένας πελάτης ταυτόχρονα στο server και γιατί ναι ή όχι;
iii) Τι υποδηλώνει η σταθερά AF_INET και σε ποια περίπτωση θα χρειαζόταν να την αλλάξουμε;
iv) Τι προσθήκες αλλαγές θα πρέπει να γίνουν στο παραπάνω πρόγραμμα ώστε να γίνει UDP server;

Απάντηση

α)

Ένας τυπικός TCP server εκτελεί τις ακόλουθες λειτουργίες (με τη σειρά που παρουσιάζονται)

- socket() - Δημιουργία του socket
- bind() - Συνδέει το socket με μια IP διεύθυνση και θύρα
- listen() - Το socket περιμένει τα μηνύματα από τους πελάτες
- accept() - Αποδοχή της σύνδεσης
- fork() - Εξυπηρέτηση του πελάτη από ένα «αφοσιωμένο» αντίγραφο του server
- read(), write() - Μεταφορά δεδομένων
- close() - Κλείσιμο του socket

Με βάση τα παραπάνω, προκύπτει το ζητούμενο πρόγραμμα του TCP server.

```
#include <sys/types.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <stdlib.h>
#include <string.h>
#define LISTENQ 10

int main (int argc, char **argv)
{
        int listenfd, connfd, n;
        pid_t childpid;
       socklen_t clilen;
        struct sockaddr_in cliaddr, servaddr;
        char buf [200];

    listenfd = socket (AF_INET, SOCK_STREAM, 0);
```

```
    bzero(&servaddr, sizeof(servaddr));
    servaddr.sin_family = AF_INET;
    servaddr.sin_addr.s_addr = htonl (INADDR_ANY);
    servaddr.sin_port = htons (9000);

    bind(listenfd, (struct sockaddr *) &servaddr, sezeof(servaddr));
    listen(listenfd, LISTENQ);

    for ( ;  ;  )  {
            clilen = sizeof(cliaddr);
            connfd = accept(listenfd, (struct sockaddr *) &cliaddr, &clilen);

            if  ( (childpid = fork() ) == 0) {
            close(listenfd);
            do_something();    /* Μια συνάρτηση που κάνει κάτι χρήσιμο
            exit(0);

            }
               close(connfd);
        }
}
```

β)

i)

Έχουμε την ακόλουθη κλήση accept

```
connfd = accept(listenfd, (struct sockaddr *) &cliaddr, &clilen);
```

Το δεύτερο όρισμα είναι ο δείκτης σε δομή cliaddr (έχει δηλωθεί προηγουμένως ως sockaddr_in). Η cliaddr περιέχει την διεύθυνση (protocol address) του client. Πιο συγκεκριμένα, μέσω του δείκτη γίνεται πρόσβαση στα εξής τρία πεδία

- sin_family: το address family (domain)
- sin_addr: η IP διεύθυνση του υπολογιστή
- sin_port: το port number

ii)

Λόγω της χρησιμοποίησης της κλήσης fork() πολλοί πελάτες μπορούν να συνδεθούν ταυτόχρονα στον server. Με την fork() ο πελάτης επικοινωνεί με ένα «αφοσιωμένο» αντίγραφο του server, ενώ ο «αρχικός» server μπορεί να δέχεται νέες κλήσεις σύνδεσης από άλλους πελάτες.

iii)

Η σταθερά AF_INET δηλώνει ότι το socket χρησιμοποιεί το Internet Domain. Κάθε socket στο Internet Domain ταυτοποιείται από την δυάδα:

- IP Address του υπολογιστή
- Port number - Θύρα επικοινωνίας

Θα χρειαζόταν να αλλάξουμε τη σταθερά AF_INET αν για τις διευθύνσεις χρησιμοποιούσαμε άλλο Domain. Π.χ. για το Unix Domain χρησιμοποιείται η σταθερά AF_UNIX.

iv)

Ένας τυπικός UDP server εκτελεί τις ακόλουθες λειτουργίες

- socket() - Δημιουργία του socket
- bind() - Συνδέει το socket με μια IP διεύθυνση και θύρα
- sendto(), recvfrom() - Μεταφορά δεδομένων

Με βάση τα παραπάνω προκύπτει το ζητούμενο πρόγραμμα ενός UDP server

```
#include <sys/types.h>
#include <netinet/in.h>
#include <arpa/inet.h>

#include <stdlib.h>
#include <string.h>

int main (int argc, char **argv)
{
        int sockfd;
         socklen_t clilen;
          struct sockaddr_in cliaddr, servaddr;
          char buf [200];

    bzero(&servaddr, sizeof(servaddr));
    servaddr.sin_family = AF_INET;
    servaddr.sin_addr.s_addr = htonl (INADDR_ANY);
    servaddr.sin_port = htons (9000);

    bind(sockfd, (struct sockaddr *) &servaddr, sezeof(servaddr));
```

```
        for ( ; ; ) {

                n = Recvfrom(sockfd, buff, 200, 0, cliaddr, &clilen);
                do_something();    /* Μια συνάρτηση που κάνει κάτι χρήσιμο
                Sendto(sockfd, buff, n, 0, cliaddr, clilen);

                }
        }
}
```

Οι αλλαγές/προσθήκες είναι οι ακόλουθες:

1. Αντί για δύο sockets listenfd και connfd, που χρησιμοποιούνται στις κλήσεις listen() και accept(), στον UDP server θα χρησιμοποιηθεί μόνο το socket sockfd για τις κλήσεις recvfrom() και sendto().
2. Στη κλήση bind() αντί για listenfd χρησιμοποιούμε το sockfd.
3. Προσθέτουμε κλήσεις recvfrom() και sendto().
4. Αφαιρούμε τη κλήση fork()
5. Αφαιρούμε τη κλήση close()

Θέμα* 1 *Άτυπης Ιούνιος 2010

1. Τι προσθήκες / αλλαγές θα πρέπει να γίνουν ώστε ο server να ακούει σε μια συγκεκριμένη ip;

Απάντηση

Στην εντολή serv_addr.***sin_addr.s_addr*** = ***htonl***(***INADDR_ANY***); αντικαθιστούμε τη σταθερά ***INADDR_ANY*** με τη συγκεκριμένη IP διεύθυνση από την οποία θέλουμε να «ακούει» ο server.

2. Ποιες από τις παραπάνω συναρτήσεις είναι blocking και ποιες όχι;

Απάντηση

Οι blocking συναρτήσεις είναι οι recv, recvfrom, send και sendto

3. Τι προσθήκες/αλλαγές θα πρέπει να γίνουν ώστε να γίνει UDP ή TCP Server;

Απάντηση

Στην εντολή connfd = ***socket***(***AF_INET***, ***SOMETHING***,0); αν η παράμετρος ***SOMETHING*** πάρει την τιμή ***SOCK_STREAM*** τότε δημιουργούμε ένα TCP Socket, ενώ αν πάρει την τιμή ***SOCK_DGRAM*** τότε δημιουργούμε ένα UDP Socket

4. Από τις bind, connect, socket, close, listen, sendto, recvfrom, read, write ποιες θα χρησιμοποιούσατε στην κατασκευή ενός UDP Server και ποιές στην κατασκευή ενός TCP Server; Μπορούν να συνδεθούν παραπάνω από ένας πελάτης ταυτόχρονα στο συγκεκριμένο Server;

Απάντηση

Σε ένα UDP Server χρησιμοποιούνται οι συναρτήσεις:

- socket
- bind
- recvfrom
- sendto
- close

Σε ένα TCP Server χρησιμοποιούνται οι συναρτήσεις:

- socket
- bind
- listen
- read
- write
- close

Στον UDP Server συνδέουμε πάντα ένα πελάτη, ενώ στον TCP Server μπορούμε να συνδέσουμε και να εξυπηρετήσουμε ταυτόχρονα πολλούς πελάτες.

β) Ποιες για να φτιάξετε ένα client για τον παραπάνω server και με ποια σειρά;

Απάντηση

Στην κατασκευή ενός UDP Client χρησιμοποιούνται οι συναρτήσεις:

- socket
- recvfrom
- sendto
- close

Στην κατασκευή ενός TCP Client χρησιμοποιούνται οι συναρτήσεις:

- socket
- connect
- write
- read
- close

5. Ε μέρος Network Simulator

Θέμα 5 Φεβρουάριος 2011

α) Έστω το παρακάτω σενάριο προσομοίωσης του ns-2

```
set ns [new Simulator]

set n0 [$ns node]
set n1 [$ns node]
set n2 [$ns node]
set n3 [$ns node]

$ns duplex-link $n0 $n1 1Mb 100ms DropTail
$ns duplex-link $n1 $n2 2Mb 50ms RED
$ns duplex-link $n0 $n3 1Mb 70ms RED
$ns duplex-link $n3 $n1 1Mb 70ms DropTail

set tcpSender [new Agent/TCP]
$ns attach-agent $n0 $tcpSender
set tcpReceiver [new Agent/TCPSink]
$ns attach-agent $n2 $tcpReceiver
$ns connect $tcpSender $tcpReceiver
set ftp1 [new Application/FTP]
$ftp1 attach-agent $tcpSender

set udpSender [new Agent/UDP]
$ns attach-agent $n3 $udpSender
set udpReceiver [new Agent/Null]
$ns attach-agent $n2 $udpReceiver
$ns connect $udpSender $udpReceiver
set cbr0 [new Application/Traffic/CBR]
$cbr0 attach-agent $udpSender
$cbr0 set rate_ 0.02Mb

$ns at 1.0 "$ftp1 start"
$ns at 0.5 "$cbr0 start"
$ns at 100 "finish"

proc finish {} {
    exit 0
}

$ns run
```

Σχεδιάστε την τοπολογία και προσδιορίστε στο σχήμα τις παραμέτρους της προσομοίωσης (αριθμήστε τους κόμβους, βάλτε την χωρητικότητα και την καθυστέρηση διάδοσης των συνδέσμων και προσδιορίστε την

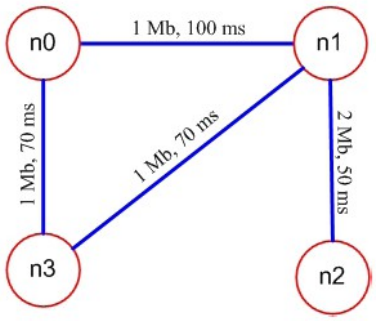
Drop Tail is a simple active queuing management (AQM) algorithm used in many routers. It doesn't differentiate traffic from different sources. As long as the queue is filled up, it will drop subsequent packets arrived. In other words, drop the tail of sequence of packets.

Random Early Detection or Random Early Drop (RED) is another AQM. It monitors the average queue size and take actions on packet (either drop or mark) based on statistical probabilities.

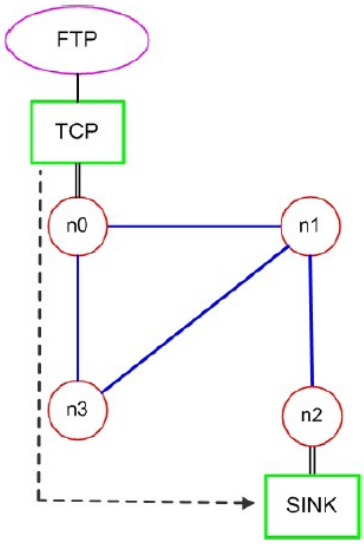
<u>Απάντηση</u>

α)

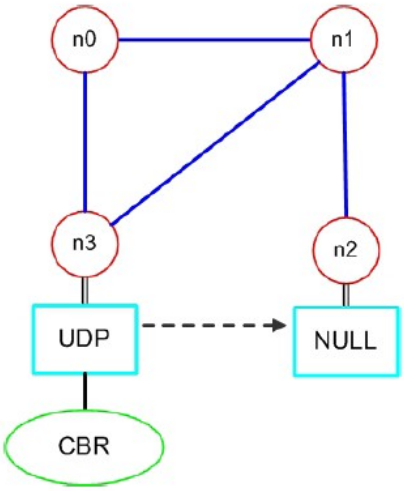
Με βάση τις 9 πρώτες εντολές προκύπτει η παρακάτω τοπολογία



Οι επόμενες 7 εντολές ορίζουν μια TCP σύνδεση από τον κόμβο n0 στο κόμβο n2. Επίσης πάνω από τη σύνδεση TCP, ορίζουν την κίνηση FTP (File Transfer Protocol).

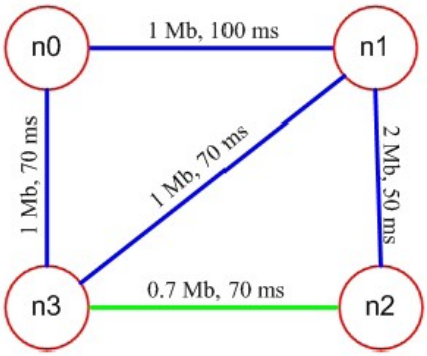


Οι επόμενες 8 εντολές ορίζουν μια UDP σύνδεση από τον κόμβο n3 στο κόμβο n2. Επίσης πάνω από τη σύνδεση UDP, ορίζουν την κίνηση CBR (Constant Bit Rate) με ρυθμό μετάδοσης 0.02 Mb.



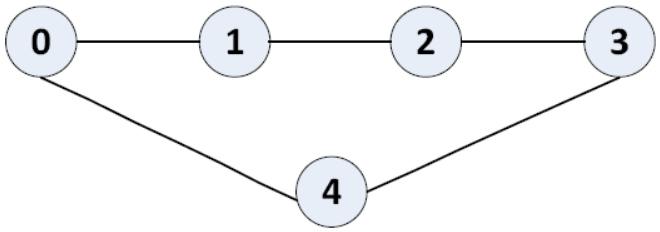
Για την προσθήκη επιπλέον συνδέσμου μεταξύ των κόμβων n2 και n3, μπορούμε να χρησιμοποιήσουμε την ακόλουθη εντολή (με ουρά RED).

```
$ns duplex-link $n2 $n3 0.7Mb 70ms RED
```



Άσκηση 2011

Να υλοποιηθεί πρόγραμμα προσομοίωσης (tcl script) μέσω του οποίου θα κατασκευάζεται η παρακάτω δικτυακή τοπολογία (5 nodes, 5 links).



Επιλέξτε χωρητικότητα των συνδέσμων (Kbits/sec) ίση με 2 * [αριθμό της ομάδα] σας, και καθυστέρηση διάδοσης των πακέτων μέσω αυτών ίση με 300 msec. Ο τύπος των ουρών που διαθέτουν αφήνετε να επιλεχθούν από εσάς.

Θα εγκαθίσταται (i) μια FTP/TCP σύνδεση, (ii) μια CBR/UDP σύνδεση (CBR=constant bit rate), ανάμεσα στους κόμβους 0-3 (με αφετηρία τον κόμβο 0 και τερματισμό τον κόμβο 3). Αναλυτικά, το μέγεθος των πακέτων να είναι 1000 Bytes και για τις δύο περιπτώσεις, ενώ το rate για την CBR πηγή να είναι ίσο με τον [αριθμό της ομάδας] (σε Kbits/sec). Το πείραμα θα διαρκεί 15sec. Η κίνηση θα ξεκινάει τη χρονική στιγμή t1=0.1sec. Κατά τη χρονική στιγμή t2=5.0sec ο σύνδεσμος 4-3 θα καταρρέει και στα t3=9sec θα αποκαθίσταται η λειτουργία του. Πειράματα θα εκτελεστούν με στατική και δυναμική δρομολόγηση.

Τι παρατηρείτε στις εξής περιπτώσεις:

- Στατική δρομολόγηση + UDP
- Δυναμική δρομολόγηση + UDP
- Στατική δρομολόγηση + TCP
- Δυναμική δρομολόγηση + TCP

Οι παρατηρήσεις μπορούν να γίνουν, χρησιμοποιώντας το tracefile (.tr)

Ποιό είναι το throughput του συστήματος σε κάθε μία από αυτές τις 4 περιπτώσεις? Το throughput μετριέται σε bps και μπορεί να βρεθεί από το tracefile (.tr) ως ο λόγος των bytes που έφτασαν στον προορισμό προς τον χρόνο εκτέλεσης του πειράματος.

Απάντηση

ns_script_CBR_dynamic.tcl

```
set ns [new Simulator]

#trace files
set nf [open out.nam w]
$ns namtrace-all $nf
set tf [open out.tr w]
$ns trace-all $tf
```

```
#nodes and links
set n0 [$ns node]
set n1 [$ns node]
set n2 [$ns node]
set n3 [$ns node]
set n4 [$ns node]
# netlab137 -> bandwidth = 2*137 = 274Kb/sec
$ns duplex-link $n0 $n1 274Kb 300ms DropTail
$ns duplex-link $n1 $n2 274Kb 300ms DropTail
$ns duplex-link $n2 $n3 274Kb 300ms DropTail
$ns duplex-link $n3 $n4 274Kb 300ms DropTail
$ns duplex-link $n4 $n0 274Kb 300ms DropTail

# Agents
set udp0 [new Agent/UDP]
$ns attach-agent $n0 $udp0

set sink [new Agent/Null]
$ns attach-agent $n3 $sink

set cbr0 [new Application/Traffic/CBR]
$cbr0 set packetSize_ 1000
$cbr0 set rate_ 137Kb
$cbr0 attach-agent $udp0

$ns connect $udp0 $sink

$ns rtproto DV

proc finish {} {
        global ns nf tf
        $ns flush-trace
        close $nf
        close $tf
        exit 0
}

#enarksh kinhshs
$ns at 0.1 "$cbr0 start"
$ns rtmodel-at 5.0 down $n3 $n4
$ns rtmodel-at 9.0 up $n3 $n4
$ns at 15.0 "$cbr0 stop"
$ns at 16.0 "finish"

$ns run
```

---

ns_script_CBR_static.tcl

```
set ns [new Simulator]

#trace files
set nf [open out.nam w]
$ns namtrace-all $nf
set tf [open out.tr w]
$ns trace-all $tf

#nodes and links
set n0 [$ns node]
set n1 [$ns node]
set n2 [$ns node]
set n3 [$ns node]
set n4 [$ns node]
# netlab137 -> bandwidth = 2*137 = 274Kb/sec
```

```
$ns duplex-link $n0 $n1 274Kb 300ms DropTail
$ns duplex-link $n1 $n2 274Kb 300ms DropTail
$ns duplex-link $n2 $n3 274Kb 300ms DropTail
$ns duplex-link $n3 $n4 274Kb 300ms DropTail
$ns duplex-link $n4 $n0 274Kb 300ms DropTail

# Agents
set udp0 [new Agent/UDP]
$ns attach-agent $n0 $udp0

set sink [new Agent/Null]
$ns attach-agent $n3 $sink

set cbr0 [new Application/Traffic/CBR]
$cbr0 set packetSize_ 1000
$cbr0 set rate_ 137Kb
$cbr0 attach-agent $udp0

$ns connect $udp0 $sink

#default methodos einai static
#epipleon parousiazei problhmata
#kata thn ektelesh opote
#th metatrepoume se comment
#$ns rtproto Static

proc finish {} {
        global ns nf tf
        $ns flush-trace
        close $nf
        close $tf
        exit 0
}

#enarksh kinhshs
$ns at 0.1 "$cbr0 start"
$ns rtmodel-at 5.0 down $n3 $n4
$ns rtmodel-at 9.0 up $n3 $n4
$ns at 15.0 "$cbr0 stop"
$ns at 16.0 "finish"

$ns run
```

---

ns_script_FTP_dynamic.tcl

```
set ns [new Simulator]

#trace files
set nf [open out.nam w]
$ns namtrace-all $nf
set tf [open out.tr w]
$ns trace-all $tf

#nodes and links
set n0 [$ns node]
set n1 [$ns node]
set n2 [$ns node]
set n3 [$ns node]
set n4 [$ns node]
# netlab137 -> bandwidth = 2*137 = 274Kb/sec
$ns duplex-link $n0 $n1 274Kb 300ms DropTail
$ns duplex-link $n1 $n2 274Kb 300ms DropTail
```

```
$ns duplex-link $n2 $n3 274Kb 300ms DropTail
$ns duplex-link $n3 $n4 274Kb 300ms DropTail
$ns duplex-link $n4 $n0 274Kb 300ms DropTail

# Agents
set tcp0 [new Agent/TCP]
$ns attach-agent $n0 $tcp0

set sink [new Agent/TCPSink]
$ns attach-agent $n3 $sink

set ftp [new Application/FTP]
$ftp set packetSize_ 1000
$ftp attach-agent $tcp0

$ns connect $tcp0 $sink

$ns rtproto DV

proc finish {} {
        global ns nf tf
        $ns flush-trace
        close $nf
        close $tf
        exit 0
}

#enarksh kinhshs
$ns at 0.1 "$ftp start"
$ns rtmodel-at 5.0 down $n3 $n4
$ns rtmodel-at 9.0 up $n3 $n4
$ns at 15.0 "$ftp stop"
$ns at 16.0 "finish"

$ns run
```

---

ns_script_FTP_static.tcl

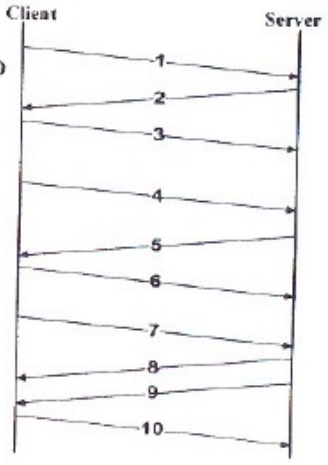
```
set ns [new Simulator]

#trace files
set nf [open out.nam w]
$ns namtrace-all $nf
set tf [open out.tr w]
$ns trace-all $tf

#nodes and links
set n0 [$ns node]
set n1 [$ns node]
set n2 [$ns node]
set n3 [$ns node]
set n4 [$ns node]
# netlab137 -> bandwidth = 2*137 = 274Kb/sec
$ns duplex-link $n0 $n1 274Kb 300ms DropTail
$ns duplex-link $n1 $n2 274Kb 300ms DropTail
$ns duplex-link $n2 $n3 274Kb 300ms DropTail
$ns duplex-link $n3 $n4 274Kb 300ms DropTail
$ns duplex-link $n4 $n0 274Kb 300ms DropTail

# Agents
set tcp0 [new Agent/TCP]
$ns attach-agent $n0 $tcp0
```

```
set sink [new Agent/TCPSink]
$ns attach-agent $n3 $sink

set ftp [new Application/FTP]
$ftp set packetSize_ 1000
$ftp attach-agent $tcp0

$ns connect $tcp0 $sink

#default methodos einai static
#epipleon parousiazei problhmata
#kata thn ektelesh opote
#th metatrepoume se comment
#$ns rtproto Static

proc finish {} {
        global ns nf tf
        $ns flush-trace
        close $nf
        close $tf
        exit 0
}

#enarksh kinhshs
$ns at 0.1 "$ftp start"
$ns rtmodel-at 5.0 down $n3 $n4
$ns rtmodel-at 9.0 up $n3 $n4
$ns at 15.0 "$ftp stop"
$ns at 16.0 "finish"

$ns run
```

6. ΣΤ μέρος Λοιπά Θέματα

Φεβρουάριος 2011 - Θέμα 2

α) Το παρακάτω σχήμα δείχνει τα πακέτα που ανταλλάσσονται κατά την έναρξη μίας TCP σύνδεσης, την ανταλλαγή πληροφορίας καθώς και κατά το κλείσιμο της σύνδεσης.



Κάθε πακέτο (1,2, …, 10) περιέχει μία από τις παρακάτω πληροφορίες:

a) Data_2 & ACK of Data_1,
b) SYN
c) ACK_FIN
d) ACK of Data_2
e) ACK_FIN
f) ACK
g) FIN
h) SYN & ACK
i) Data_1
j) FIN

Κάνετε την αντιστοίχιση μεταξύ πακέτων (1, …, 10) και της πληροφορίας που αυτά περιέχουν (a, .., j).

β) Το DSL-584T ADSL modem router είναι ένα υψηλής ταχύτητας ευρυζωνικό modem για οικιακή και επαγγελματική χρήση. Υποστηρίζει τα τελευταία standards ADSL2/+, εξασφαλίζοντας έτσι ταχύτητες εώς 24Mbps downstream και 1Mbps upstream (ADSL2+), ή 12Mbps downstream and 1Mbps upstream (ADSL2). Η συσκευή αυτή μεταξύ των άλλων έχει τα παρακάτω χαρακτηριστικά:

1. Firewall
2. Mac Adress Filtering
3. Υποστήριξη SNMP

Εξηγείστε απλά και σύντομα τι σημαίνουν τα χαρακτηριστικά 1-3.

<u>Απάντηση</u>

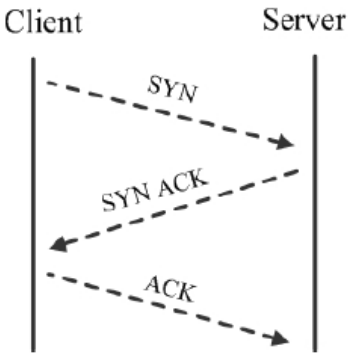
α)

Τυπικά μια TCP επικοινωνία χωρίζεται σε 3 φάσεις:

- Εγκατάσταση (έναρξη) της σύνδεσης
- Μεταφορά δεδομένων (ανταλλαγή πληροφορίας)
- Τερματισμός (κλείσιμο) της σύνδεσης

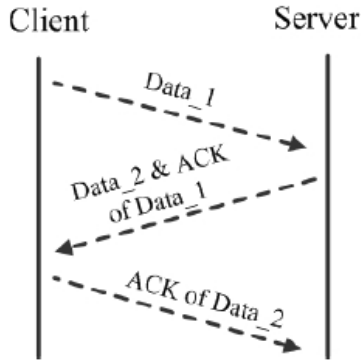
Η εγκατάσταση της σύνδεσης πραγματοποιείται με την «τριπλή» χειραψία (στέλνονται 3 πακέτα)

- Ο πελάτης (client) στέλνει ένα πακέτο SYN
- Ο εξυπηρετητής (server) απαντά με ένα SYN ACK (δηλ. επιβεβαιώνει τη λήψη του SYN)
- Ο πελάτης στέλνει ένα πακέτο ACK (δηλ. επιβεβαιώνει τη λήψη του SYN ACK)



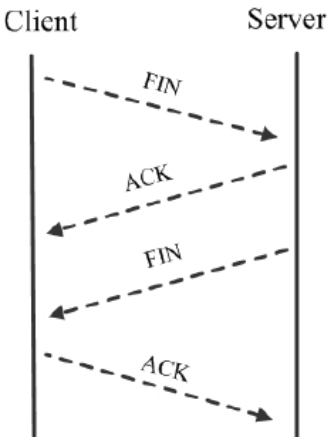
Κατά τη δεύτερη φάση το πλήθος των πακέτων που στέλνονται ποικίλλει. Στο συγκεκριμένο παράδειγμα στέλνονται 3 πακέτα

- Ο πελάτης στέλνει το πακέτο Data_1
- Ο εξυπηρετητής απαντά με το πακέτο Data_2 & ACK of Data_1
- Ο πελάτης στέλνει το πακέτο ACK of Data_2

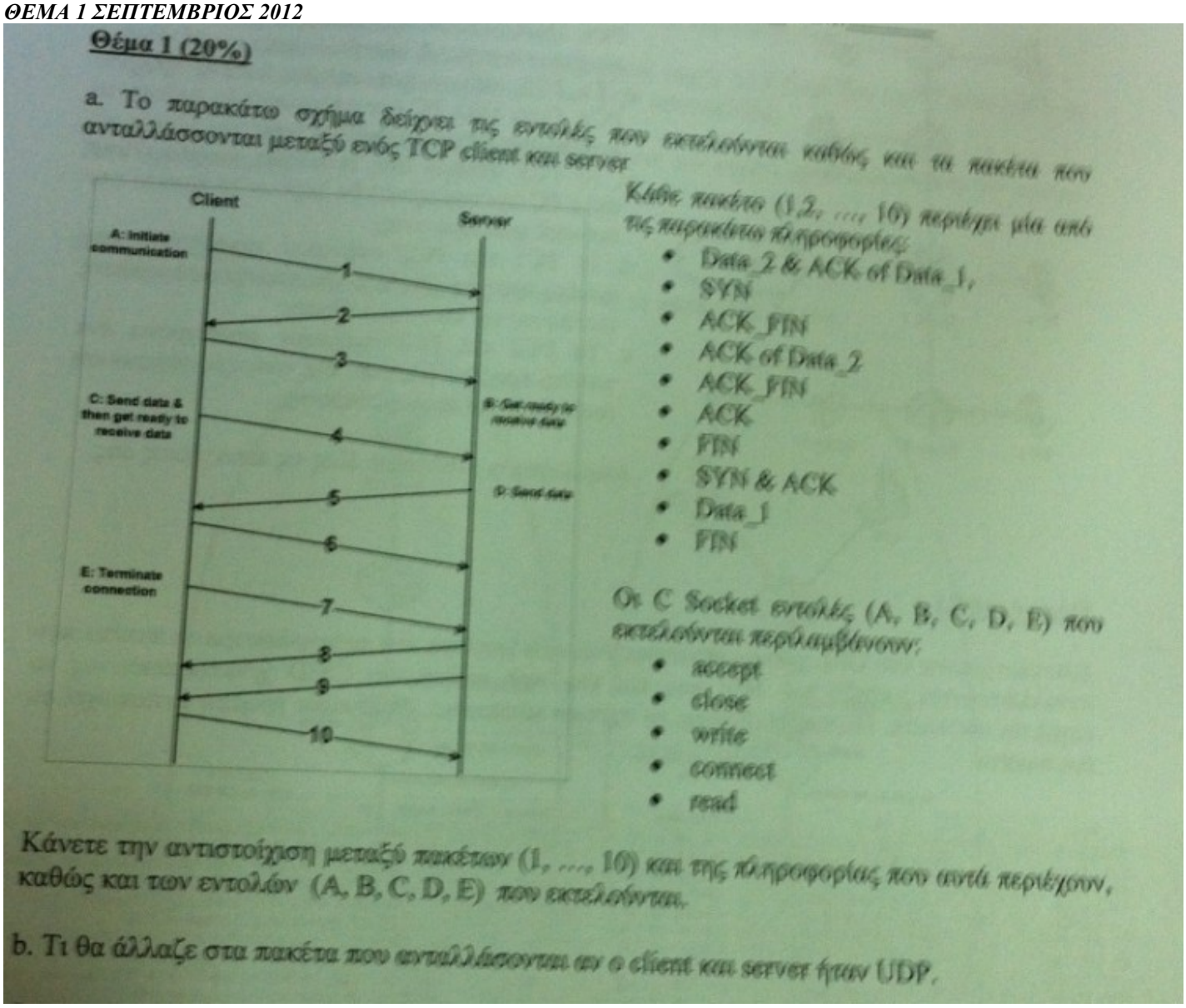


Κατά την τρίτη και τελευταία φάση πραγματοποιούνται δύο «διπλές» χειραψίες (στέλνονται 4 πακέτα)

- Ο πελάτης στέλνει ένα πακέτο FIN (δηλώνει την επιθυμία για τερματισμό της σύνδεσης)
- Ο εξυπηρετητής απαντά με ένα πακέτο ACK
- Ο εξυπηρετητής στέλνει ένα πακέτο FIN
- Ο πελάτης απαντά με ένα πακέτο ACK



ΘΕΜΑ 1 ΣΕΠΤΕΜΒΡΙΟΣ 2012



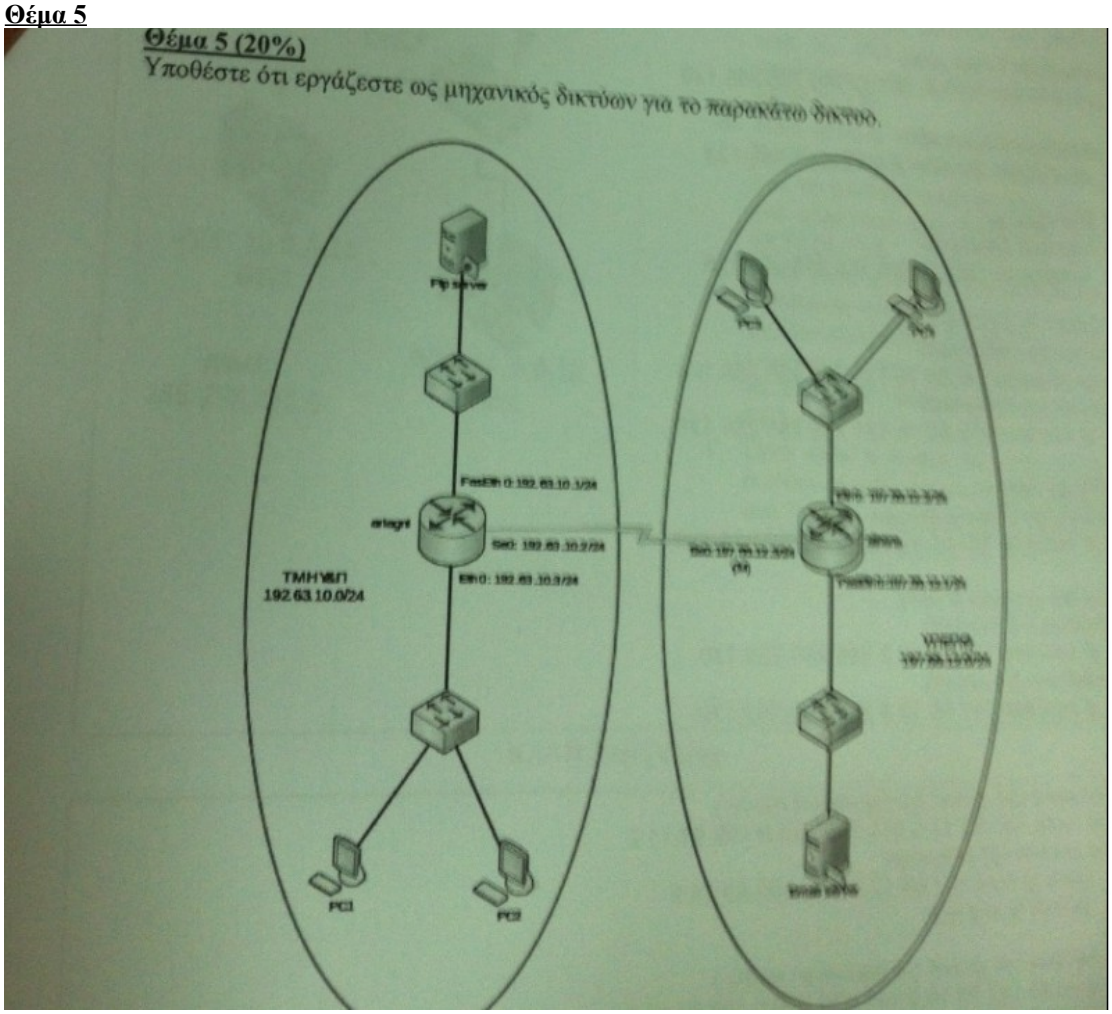
Απάντηση

A)
1<->SYN
2<->SYN_ACK
3<->ACK
4<->Data_1
5<->Data_2 & ACK of Data_1
6<->ACK of Data_2
7<->FIN
8<->ACK_FIN
9<->FIN
10<->ACK_FIN

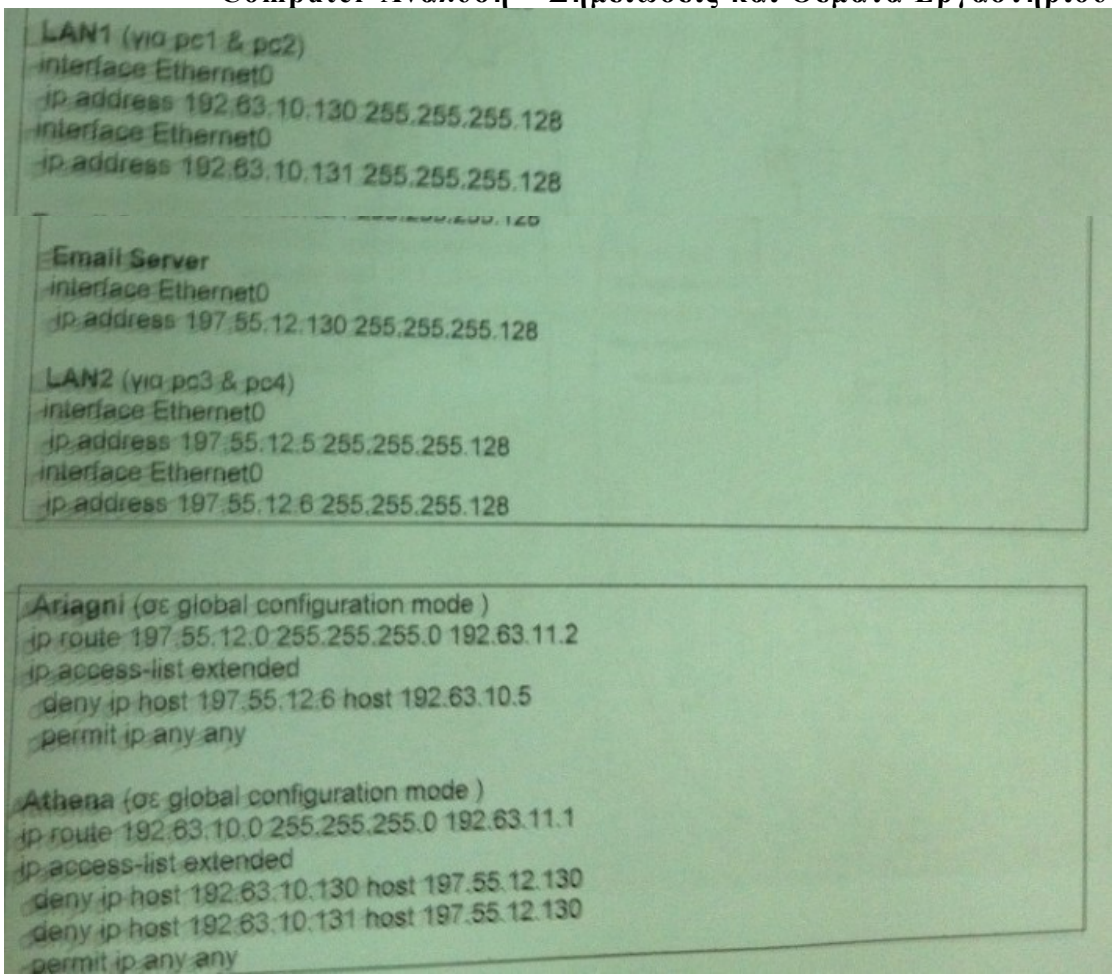
A<->connect
B<->accept
C<->write
D<->read
E<->close

b) Αν ο client και ο server ήταν UDP δεν θα υπήρχαν τα πακέτα για την εγκαθίδρυση και τον τερματισμό της σύνδεσης δηλ. τα SYN, SYN_ACK, ACK και FIN και τα πακέτα

Θέμα 5


Θέμα 5 (20%)
Υποθέστε ότι εργάζεστε ως μηχανικός δικτύων για το παρακάτω δίκτυο.
ΤΜΗΜΑ
192.63.10.0/24
PC1
PC2


Ariagni
interface Serial0/0
ip address 192.63.11.1 255.255.255.252
interface Ethernet0/0
ip address 192.63.10.129 255.255.255.128
interface Ethernet0/1
ip address 192.63.10.1 255.255.255.128
Athena
interface Serial0/0
ip address 192.63.11.2 255.255.255.252
interface Ethernet0/0
ip address 197.55.12.129 255.255.255.128
interface Ethernet0/1
ip address 197.55.12.1 255.255.255.128
FTP Server
interface Ethernet0
ip address 192.63.10.5 255.255.255.128



Εξηγείστε ποια επίδραση έχει η εφαρμογή των παραπάνω εντολών στη διασυνδεσιμότητα του δικτύου;

Απάντηση

Ariagni

Interface Serial 0/0	**Επιλέγουμε τη διεπαφή Serial 0/0 του router Ariagni**
ip address 192.63.11.1 255.255.255.252	Θέτουμε στη διεπαφή Serial 0/0 την IP 192.63.11.1 255.255.255.252
interface Ethernet 0/0	**Επιλέγουμε τη διεπαφή Ethernet 0/0 του router Ariagni**
ip address 192.63.10.129 255.255.255.128	Θέτουμε στη διεπαφή Ethernet 0/0 την IP 192.63.10.129 255.255.255.128
interface Ethernet 0/1	**Επιλέγουμε τη διεπαφή Ethernet 0/1 του router Ariagni**
ip address 192.63.10.1 255.255.255.128	Θέτουμε στη διεπαφή Ethernet 0/1 την IP 192.63.10.1 255.255.255.128

Athena

Interface Serial 0/0	**Επιλέγουμε τη διεπαφή Serial 0/0 του router Athena**
ip address 192.63.11.2 255.255.255.252	Θέτουμε στη διεπαφή Serial 0/0 την IP 192.63.11.2 255.255.255.252
interface Ethernet 0/0	**Επιλέγουμε τη διεπαφή Ethernet 0/0 του router Athena**
ip address 197.55.12.129 255.255.255.128	Θέτουμε στη διεπαφή Ethernet 0/0 την IP 197.55.12.129 255.255.255.128
interface Ethernet 0/1	**Επιλέγουμε τη διεπαφή Ethernet 0/1 του router Athena**
ip address 197.55.12.1 255.255.255.128	Θέτουμε στη διεπαφή Ethernet 0/1 την IP 197.55.12.1 255.255.255.128

FTP Server

interface Ethernet 0	**Επιλέγουμε τη διεπαφή Ethernet 0 του FTP Server**
ip address 192.63.10.5 255.255.255.128	Θέτουμε στη διεπαφή Ethernet 0 την IP 192.63.10.5 255.255.255.128

LAN1 (pc1 & pc2)

interface Ethernet 0	**Επιλέγουμε τη διεπαφή Ethernet 0 του pc1**
ip address 192.63.10.130 255.255.255.128	Θέτουμε στη διεπαφή Ethernet 0 την IP 192.63.10.130 255.255.255.128
interface Ethernet 0	**Επιλέγουμε τη διεπαφή Ethernet 0 του pc2**
ip address 192.63.10.131 255.255.255.128	Θέτουμε στη διεπαφή Ethernet 0 την IP 192.63.10.131 255.255.255.128

Email Server

interface Ethernet 0	**Επιλέγουμε τη διεπαφή Ethernet 0 του Email Server**
ip address 197.55.12.130 255.255.255.128	Θέτουμε στη διεπαφή Ethernet 0 την IP 197.55.12.130 255.255.255.128

LAN2 (pc3 & pc4)

interface Ethernet 0	**Επιλέγουμε τη διεπαφή Ethernet 0 του pc3**
ip address 197.55.12.5 255.255.255.128	Θέτουμε στη διεπαφή Ethernet 0 την IP 197.55.12.5 255.255.255.128
interface Ethernet 0	**Επιλέγουμε τη διεπαφή Ethernet 0 του pc4**
ip address 197.55.12.6 255.255.255.128	Θέτουμε στη διεπαφή Ethernet 0 την IP 197.55.12.6 255.255.255.128

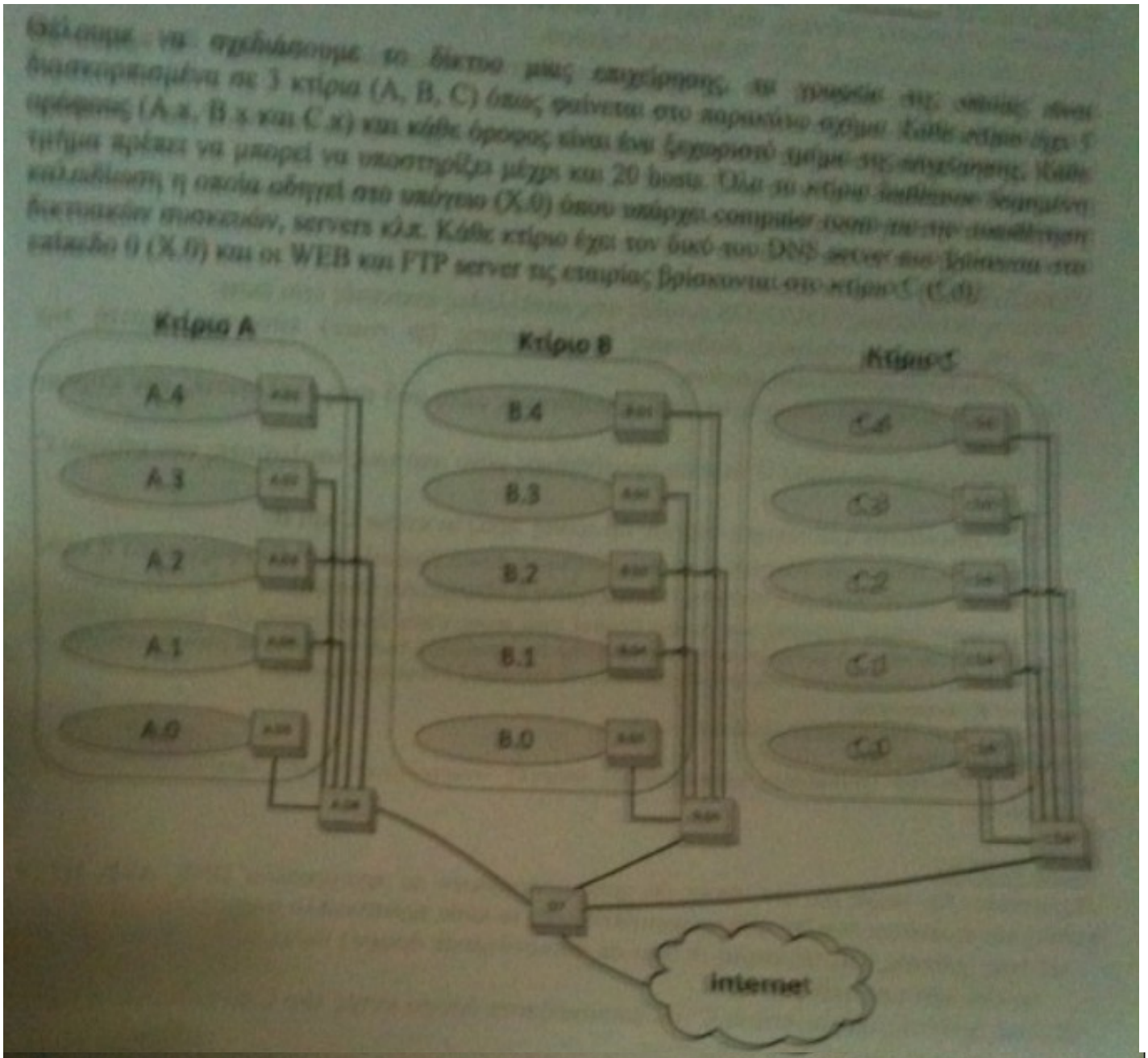
Ariagni (σε global configuration mode)

ip route 197.55.12.0 255.255.255.0 192.63.11.2	**Δημιουργούμε στατική σύνδεση του router Ariagni με το δίκτυο ΤΜΗΜΤΥ (το οποίο έχει IP 197.55.12.0 255.255.255.0) και πιο συγκεκριμένα με τη σειριακή διεπαφή του router Athena (που έχει IP την 192.63.11.2)**
ip access list extended	**Ορίζουμε εκτεταμένη λίστα προσπέλασης**
deny ip host 197.55.12.6 host 192.63.10.5 **permit ip any any**	**Απαγορεύουμε την ip κίνηση από το PC4 (IP 197.55.12.6) προς τον FTP Server (IP 192.63.10.5) και επιτρέπουμε οποιαδήποτε άλλη IP κίνηση**

Athena (σε global configuration mode)

ip route 192.63.10.0 255.255.255.0 192.63.11.1	**Δημιουργούμε στατική σύνδεση του router Athena με το δίκτυο ΤΜΗΥ&Π (το οποίο δρομολογεί έχει IP 192.63.10.0 255.255.255.0) και πιο συγκεκριμένα με τη σειριακή διεπαφή του router Ariagni (η οποία έχει IP την 192.63.11.1)**
ip access list extended	**Ορίζουμε εκτεταμένη λίστα προσπέλασης**
deny ip host 192.63.10.130 host 197.55.12.130	**Απαγορεύουμε την ip κίνηση από το PC1 (IP 192.63.10.130) στον Email Server (IP 197.55.12.130)**
deny ip host 192.63.10.131 host 197.55.12.130	**Απαγορεύουμε την ip κίνηση από το PC2 (IP 192.63.10.131) στον Email Server (IP 197.55.12.130)**
permit ip any any	**Επιτρέπουμε οποιαδήποτε άλλη IP κίνηση**

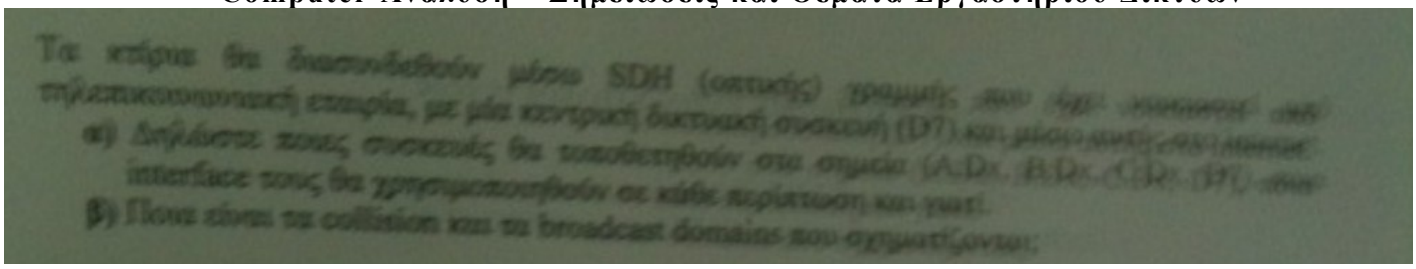
Θέματα Φεβρουάριος 2012



Θέμα 1 (15%)

Έχει αποφασιστεί ότι ο δικτυακός εξοπλισμός θα αποτελείται από:

- *Ethernet switches*, μοντέλο Cisco Catalyst 2970, κάθε ένα από τα οποία διαθέτει 24 θύρες Ethernet ταχύτητας 10/1000/1000 Mbps (υποστηρίζουν δηλαδή και τις 3 ταχύτητες).
- *Routers*, μοντέλο Cisco 7206, κάθε ένας από τους οποίους διαθέτει 5 Ethernet interfaces ταχύτητας 10 Mbps, 5 Fast Ethernet interfaces ταχύτητας 100 Mbps και 4 SDH (optical) interfaces.



Απάντηση

Θέμα 1

Η συνδεσμολογία είναι η εξής:

Κτίριο Α

Στο κτίριο Α και στα σημεία Α.D1 έως και Α.D5 θα βάλουμε 4 Ethernet switches προκειμένου να συγκεντρώσουν τους host κάθε ορόφου.

Στο σημείο Α.D6 θα τοποθετηθεί ένας Cisco Router ο οποίος θα συνδεθεί στις 5 Ethernet διεπαφές τους με τα switches κάθε ορόφου

Κτίριο Β

Στο κτίριο Β στα σημεία Β.D1 έως και Β.D5 θα θέσουμε 4 Ethernet switches προκειμένου να συγκεντρώσουν τους host κάθε ορόφου
Στο σημείο Β.D6 θα τοποθετηθεί ένας Router ο οποίος θα συνδεθεί στις 5 Ethernet διεπαφές τους με τα switches κάθε ορόφου

Κτίριο C

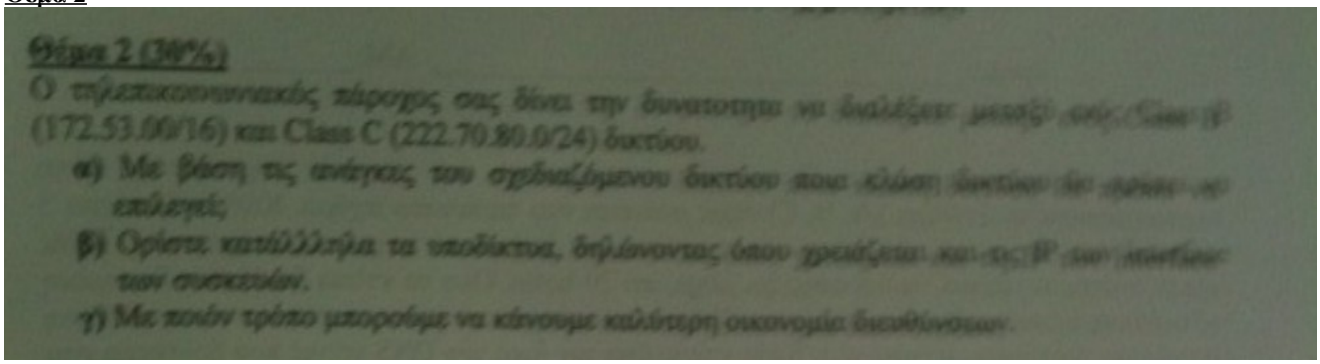
Στο κτίριο C στα σημεία C.D1 έως και C.D5 θα τοποθετηθούν ομοίως 4 Ethernet switches προκειμένου να συγκεντρώσουν τους Η/Υ κάθε ορόφου
Στο σημείο C.D6 θα τοποθετηθεί ένας Router ο οποίος θα συνδεθεί στις 5 Ethernet διεπαφές τους με τα switches κάθε ορόφου

Σημείο D

Στο σημείο D7 θα τοποθετηθεί ένας Router ο οποίος στις SDH διεπαφές του θα συνδεθεί με τους routers των σημείων Α.D6, Β.D6 και C.D6 των υπόλοιπων κτιρίων

Θεωρούμε ότι έχουμε 5 collision domain σε κάθε κτίριο όσα και τα switches. Θεωρούμε ότι έχουμε 5 broadcast domain όσοι και οι routers και άλλα 3 broadcast domain στις συνδέσεις των router των 3 κτιρίων με τον router στο σημείο D7 και 1 ακόμα broadcast domain στη σύνδεση με το Internet

Θέμα 2



Απάντηση

α)

Με βάση τις δικτυακές ανάγκες μας θα χρησιμοποιήσουμε κλάση Β διότι πρέπει να διευθυνσιοδοτήσουμε συνολικά 3 κτίρια* 5 όροφοι/κτίριο*20 υπολογιστές/όροφο=300 Η/Υ. Άρα χρειαζόμαστε 9 host bit. Με την IP 222.70.80.0/24 έχουμε μόνο 8 host bit άρα δεν φτάνουν και επιλέγουμε την 172.53.0.0./16. Άρα **172.253.sshhhhhh.hhhhhhhh**

β)

Υποδίκτυο κτιρίου Α	**Δυαδική Μορφή**
Διεύθυνση Υποδικτύου	172.253.**00** 000000.000000
1os host	172.253.**00** 000000.000001
Τελευταίος host	172.253.**00** 000000.01100100
Διεύθυνση εκπομπής	172.253.**00** 111111.111111

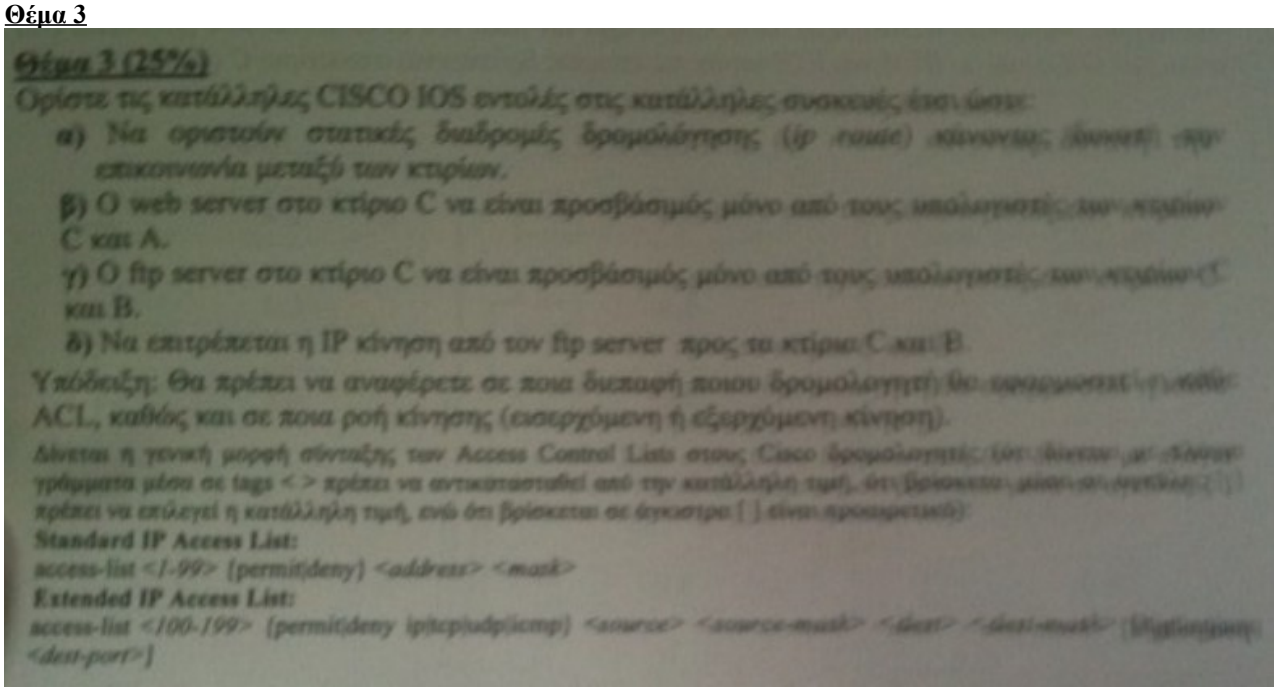
Υποδίκτυο κτιρίου Β	**Δυαδική Μορφή**

Διεύθυνση Υποδικτύου	172.253.**01** 000000.000000
1os host	172.253.**01** 000000.000001
Τελευταίος host	172.253.**01** 000000.01100100
Διεύθυνση εκπομπής	172.253.**01** 111111.111111

Υποδίκτυο κτιρίου Γ	**Δυαδική Μορφή**
Διεύθυνση Υποδικτύου	172.253.**10** 000000.000000
1os host	172.253.**10** 000000.000001
Τελευταίος host	172.253.**10** 000000.01100100
Διεύθυνση εκπομπής	172.253.**10** 111111.111111

c) Η καλύτερη οικονομία διευθύνσεων μπορεί να γίνει με το να μην αφήνουμε κενές (αχρησιμοποίητες) διευθύνσεις. Αυτό θα επιτευχθεί αν συνδέσουμε τα επιμέρους υποδίκτυα σε ένα μεγαλύτερο δίκτυο

Θέμα 3



Θέμα 3 (25%)

Ορίστε τις κατάλληλες CISCO IOS εντολές στις κατάλληλες συσκευές έτσι ώστε:

α) Να οριστούν στατικές διαδρομές δρομολόγησης (ip route) κάνοντας δυνατή την επικοινωνία μεταξύ των κτιρίων.

β) Ο web server στο κτίριο C να είναι προσβάσιμος μόνο από τους υπολογιστές των κτιρίων C και A.

γ) Ο ftp server στο κτίριο C να είναι προσβάσιμος μόνο από τους υπολογιστές των κτιρίων C και B.

δ) Να επιτρέπεται η IP κίνηση από τον ftp server προς τα κτίρια C και B.

Υπόδειξη: Θα πρέπει να αναφέρετε σε ποια διεπαφή ποιου δρομολογητή θα εφαρμοστεί (γιατί) κάθε ACL, καθώς και σε ποια ροή κίνησης (εισερχόμενη ή εξερχόμενη κίνηση).

Δίνεται η γενική μορφή σύνταξης των Access Control Lists στους Cisco δρομολογητές (οι δίνεται με δίπλα γράμματα μέσα σε tags < > πρέπει να αντικατασταθεί από την κατάλληλη τιμή, ότι βρίσκεται μέσα σε αγκύλες [ ] πρέπει να επέλεγε η κατάλληλη τιμή, ενώ ότι βρίσκεται σε άγκιστρα { } είναι προαιρετικό):

Standard IP Access List:

access-list <1-99> {permit|deny} <address> <mask>

Extended IP Access List:

access-list <100-199> {permit|deny ip|tcp|udp|icmp} <source> <source-mask> <dest> <dest-mask> [flag] [eq <dest-port>]

Απάντηση

a)

Κτίριο Α

Στο δρομολογητή A.D5 την εντολή:

access-list 100 ip static route IP διεύθυνση D7 IP διεύθυνση B.D6

access-list 100 ip static route IP διεύθυνση D7 IP διεύθυνση C.D6

Στο δρομολογητή B.D5 την εντολή:

access-list 110 ip static route IP διεύθυνση D7 IP διεύθυνση A.D6

access-list 110 ip static route IP διεύθυνση D7 IP διεύθυνση C.D6

Στο δρομολογητή C.D5 την εντολή:

access-list 120 ip static route IP διεύθυνση D7 IP διεύθυνση A.D6

access-list 120 ip static route IP διεύθυνση D7 IP διεύθυνση B.D6

b) στην εισερχόμενη κίνηση του web server C

access-list 120 permit ip IP διεύθυνση A IP διεύθυνση C

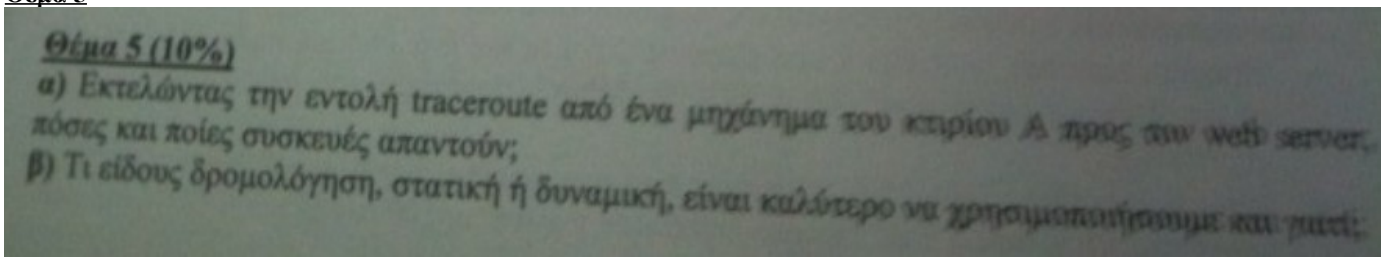
access-list 120 permit ip IP διεύθυνση C IP διεύθυνση C

c)

access-list 120 permit tcp IP διεύθυνση C IP FTP server
access-list 120 permit tcp IP διεύθυνση B IP FTP server

d)
access-list 130 permit ip IP διεύθυνση FTP server IP διεύθυνση C
access-list 130 permit ip IP διεύθυνση FTP server IP διεύθυνση B

Θέμα 5

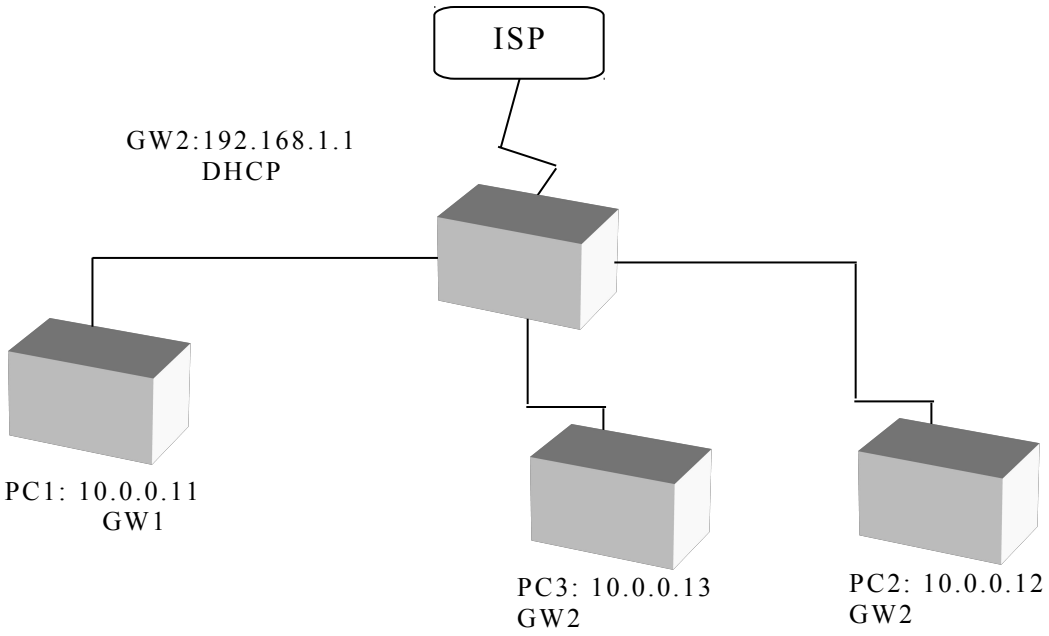

Θέμα 5 (10%)
α) Εκτελώντας την εντολή traceroute από ένα μηχάνημα του κτιρίου Α προς τον web server, πόσες και ποίες συσκευές απαντούν;
β) Τι είδους δρομολόγηση, στατική ή δυναμική, είναι καλύτερο να χρησιμοποιήσουμε και γιατί;

Απάντηση
Η εντολή traceroute χρησιμοποιείται για να εμφανίσει το μονοπάτι που ακολουθεί ένα πακέτο πληροφορίας από τον Η/Υ μας στον Η/Υ που προσδιορίζουμε. Εμφανίζει όλους τους routers μέσω των οποίων διέρχεται το πακέτο μέχρι να φράσει στον προορισμό του. Επιπλέον δείχνει πόσο χρόνο παίρνει το κάθε βήμα (hop) από τον ένα router στον άλλο.

Εκτελώντας την εντολή traceroute από ένα μηχάνημα του κτιρίου Α προς τον web server οι συσκευές που απαντούν είναι όλες που βρίσκονται στο ίδιο broadcast domain με το μηχάνημα αυτό δηλ. τα switches όλων των ορόφων του κτιρίου Α δηλ. το τα switches A.D1, A.D2, A.D3, A.D4 και A,D5 και ο router A.D6

Θα χρησιμοποιήσουμε στατική δρομολόγηση διότι στη στατική Δρομολόγηση
- Ορίζονται εξαρχής οι πίνακες δρομολόγησης και ακολούθως ξεκινά η δρομολόγηση των πακέτων από την πηγή στον προορισμό
- Οι όποιες αλλαγές απαιτούν διαχειριστική παρέμβαση
- Εύκολη στο σχεδιασμό διαχείριση
- Χρησιμοποιείται σε απλές δικτυακές τοπολογίες όπου η κίνηση του δικτύου είναι προβλέψιμη
- Ακατάλληλη για τα σημερινά δίκτυα λόγω του μεγάλου μεγέθους τους και των συχνών αλλαγών στην τοπολογία του δικτύου

Θέμα 6 Σεπτέμβριος 2012



a. Ποια είναι η source και destination διεύθυνση ενός πακέτου που φεύγει από το PC1 με προορισμό το PC3

b. Ποια είναι η source και destination διεύθυνση ενός πακέτου που φτάνει στο PC2 με αφετηρία το PC1

c. Ποια είναι η source και destination διεύθυνση ενός πακέτου που φεύγει από το PC1 με προορισμό ένα μηχάνημα στο διαδίκτυο (π.χ. 68.99.26.170)

d. Ποια είναι η source και destination διεύθυνση ενός πακέτου που φτάνει στο modem/router με προορισμό ένα μηχάνημα στο διαδίκτυο (π.χ. 68.99.26.170)

e. Ποια είναι η source και destination διεύθυνση ενός πακέτου που φτάνει στο modem/router με αφετηρία ένα μηχάνημα στο διαδίκτυο (π.χ. 68.99.26.170) και με προορισμό το PC2

f. Ποια είναι η source και destination διεύθυνση ενός πακέτου που φτάνει στο PC1 με αφετηρία ένα μηχάνημα στο διαδίκτυο (π.χ. 68.99.26.170)

Απάντηση

a

source	destination
10.0.0.11	10.0.0.13

b.

source	destination
10.0.0.11	10.0.0.12

c.

source	destination
10.0.0.11	68.99.26.170

d.

source	destination
192.168.1.1	68.99.26.170

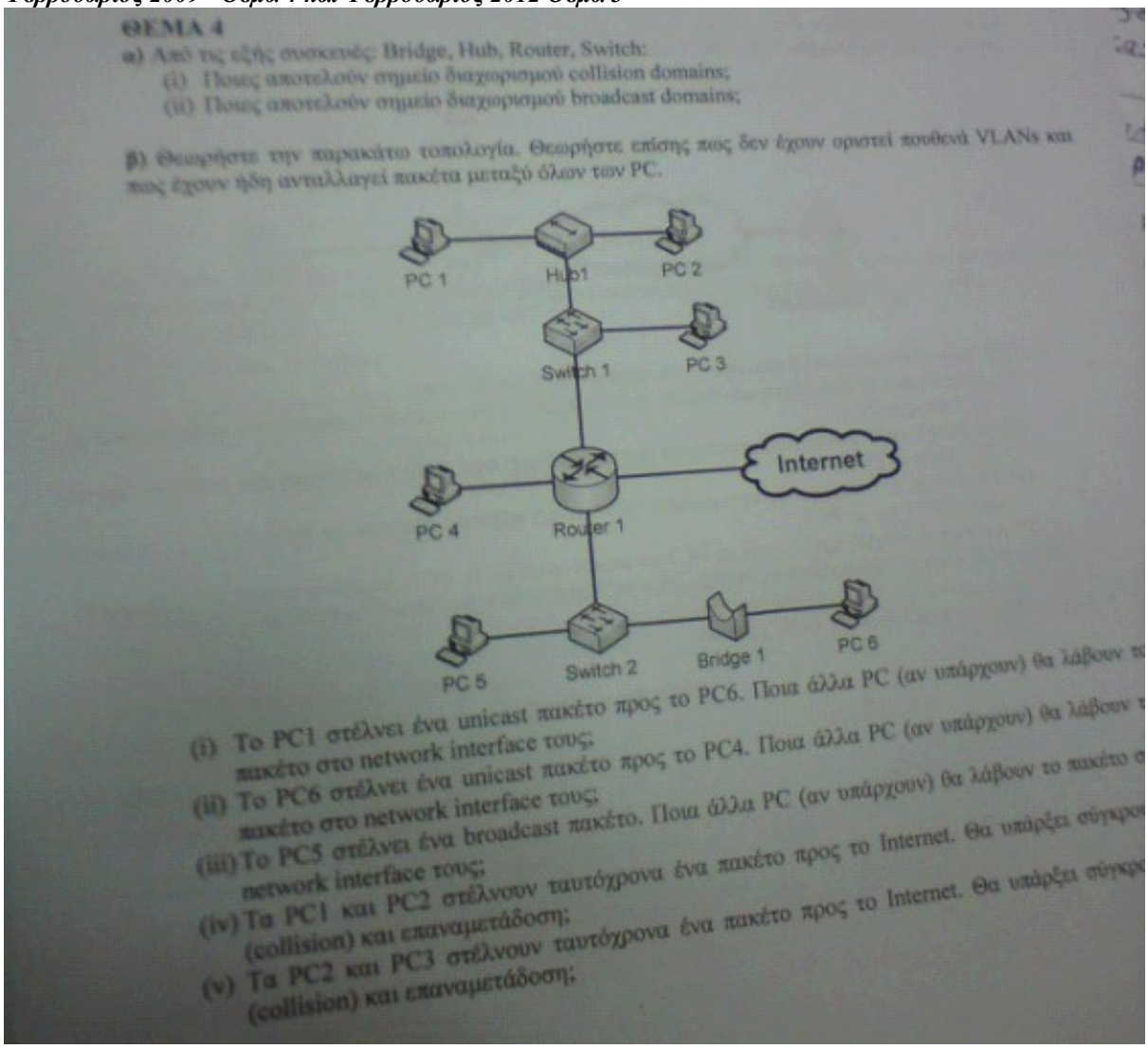
e.

source	destination
68.99.26.170	192.168.1.1

f.

source	destination
68.99.26.170	10.0.0.11

Φεβρουάριος 2009 - Θέμα 4 και Φεβρουάριος 2012 Θέμα 3



Απάντηση

α)

- ✓ Κάθε Hub αποτελεί ένα collision domain ανεξάρτητα από τον αριθμό των ports του
- ✓ Κάθε port ενός Switch/Bridge αποτελεί ένα collision domain
- ✓ Κάθε port ενός Router λειτουργεί και σαν ένα collision domain και σαν ένα broadcast domain.

β)

(i) **Επειδή στις unicast διευθύνσεις υπάρχει σχέση 1-1 μεταξύ της διεύθυνσης του δικτύου και ενός τελικού σημείου του δικτύου κάθε διεύθυνση προορισμού αναγνωρίζει ένα μοναδικό παραλήπτη**. Το πακέτο θα παραληφθεί αρχικά από τα PC που βρίσκονται στο ίδιο broadcast domain με το PC1 δηλ. από τα PC2 και PC3 (αυτά θα απορρίψουν το πακέτο διότι δεν τα αφορά) και στη συνέχεια αυτό θα παραληφθεί από το PC6.

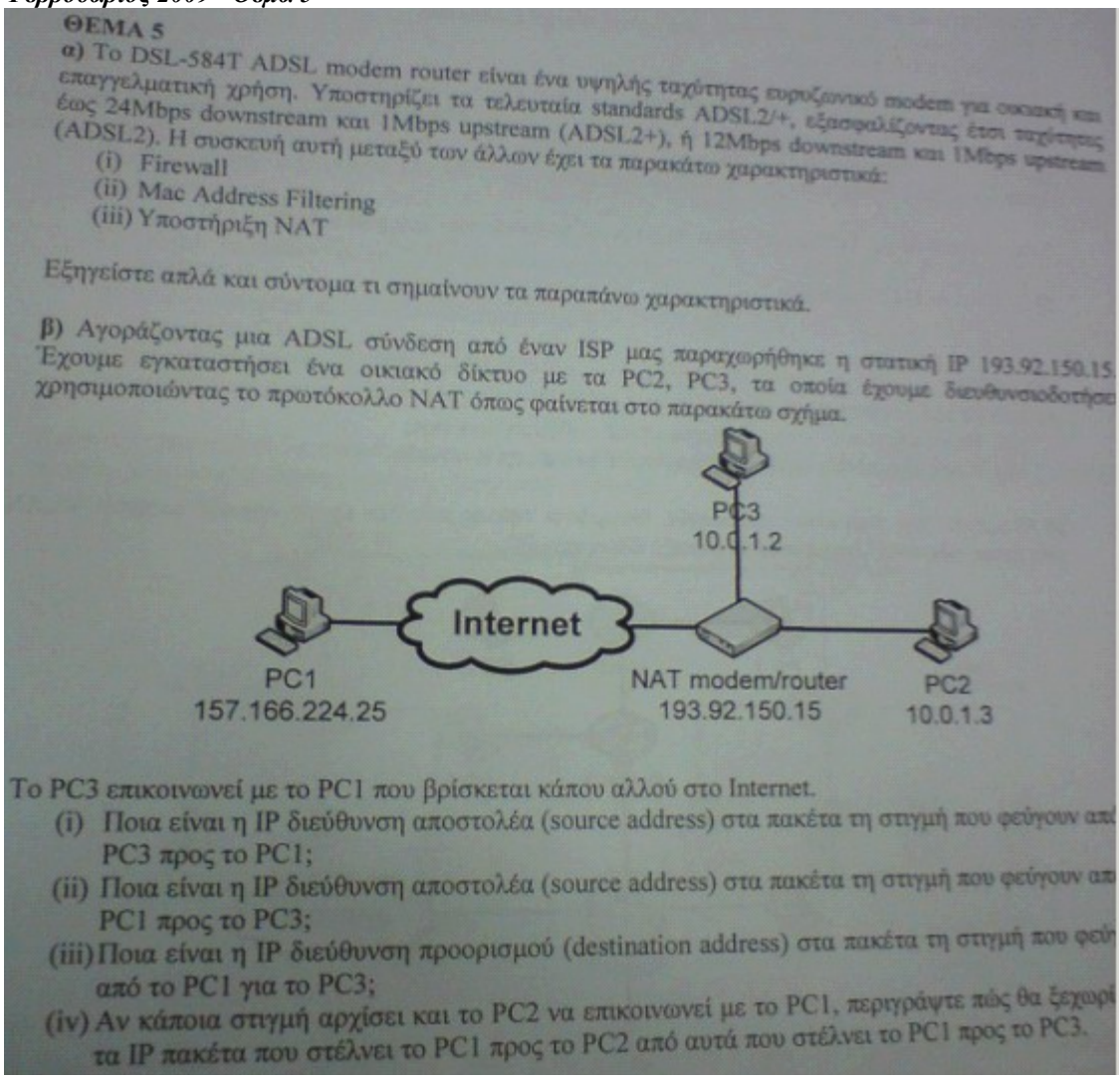
(ii) Το **πακέτο δεν θα παραληφθεί από κανένα άλλο PC**

(iii) Στις broadcast και multicast διευθύνσεις υπάρχει σχέση 1-πολλά μεταξύ της διεύθυνσης του δικτύου και της διεύθυνσης των τελικών σημείων-παραληπτών του δικτύου δηλαδή η διεύθυνση προορισμού αναγνωρίζει ένα σύνολο από παραλήπτες στους οποίους η πληροφορία στέλνεται. Συνεπώς το πακέτο που στέλνει το PC5 θα το παραλάβουν όλα τα PC που βρίσκονται στο ίδιο broadcast domain με το PC5 δηλαδή το PC6. Η διαφορά από το unicast πακέτο είναι ότι αυτό δεν θα απορριφθεί από τα PC του ίδιου broadcast domain.

(iv) Τα PC1 και PC2 ανήκουν στο ίδιο collision domain άρα θα υπάρχει σύγκρουση και επαναμετάδοση. Γενικά όταν υπάρχει ταυτόχρονη μετάδοση πακέτων από διαφορετικά PC του ίδιου collision domain, τότε τα πακέτα αυτά θα συγκρούονται και θα απαιτείται επαναμετάδοση.

(v) Τα PC2 και PC3 δεν ανήκουν στο ίδιο collision domain (λόγω του switch) άρα δεν θα υπάρχει σύγκρουση.

Φεβρουάριος 2009 - Θέμα 5



ΘΕΜΑ 5

α) Το DSL-584T ADSL modem router είναι ένα υψηλής ταχύτητας ευρυζωνικό modem για οικιακή και επαγγελματική χρήση. Υποστηρίζει τα τελευταία standards ADSL2/+, εξασφαλίζοντας έτσι ταχύτητες έως 24Mbps downstream και 1Mbps upstream (ADSL2+), ή 12Mbps downstream και 1Mbps upstream (ADSL2). Η συσκευή αυτή μεταξύ των άλλων έχει τα παρακάτω χαρακτηριστικά:

(i) Firewall
(ii) Mac Address Filtering
(iii) Υποστήριξη NAT

Εξηγείστε απλά και σύντομα τι σημαίνουν τα παραπάνω χαρακτηριστικά.

β) Αγοράζοντας μια ADSL σύνδεση από έναν ISP μας παραχωρήθηκε η στατική IP 193.92.150.15. Έχουμε εγκαταστήσει ένα οικιακό δίκτυο με τα PC2, PC3, τα οποία έχουμε διευθυνσιοδοτήσει χρησιμοποιώντας το πρωτόκολλο NAT όπως φαίνεται στο παρακάτω σχήμα.

Το PC3 επικοινωνεί με το PC1 που βρίσκεται κάπου αλλού στο Internet.

(i) Ποια είναι η IP διεύθυνση αποστολέα (source address) στα πακέτα τη στιγμή που φεύγουν από PC3 προς το PC1;
(ii) Ποια είναι η IP διεύθυνση αποστολέα (source address) στα πακέτα τη στιγμή που φεύγουν από PC1 προς το PC3;
(iii) Ποια είναι η IP διεύθυνση προορισμού (destination address) στα πακέτα τη στιγμή που φεύγουν από το PC1 για το PC3;
(iv) Αν κάποια στιγμή αρχίσει και το PC2 να επικοινωνεί με το PC1, περιγράψτε πώς θα ξεχωρίσουν τα IP πακέτα που στέλνει το PC1 προς το PC2 από αυτά που στέλνει το PC1 προς το PC3.

Απάντηση

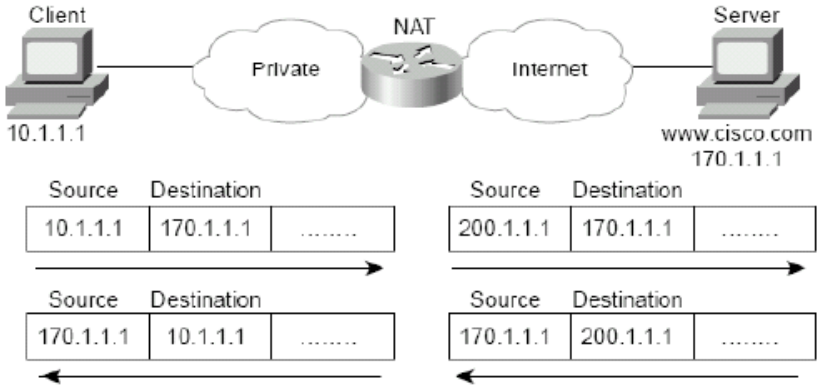
α)

Ο όρος firewall ή τείχος προστασίας χρησιμοποιείται για να δηλώσει κάποια συσκευή ή πρόγραμμα που είναι έτσι ρυθμισμένο ούτως ώστε να επιτρέπει ή να απορρίπτει πακέτα δεδομένων που περνούν από ένα δίκτυο υπολογιστών σε ένα άλλο.
Η κύρια λειτουργία ενός firewall είναι η ρύθμιση της κυκλοφορίας δεδομένων ανάμεσα σε δύο δίκτυα υπολογιστών. Συνήθως τα δύο αυτά δίκτυα είναι το Διαδίκτυο και το τοπικό/εταιρικό δίκτυο. Ένα firewall παρεμβάλλεται ανάμεσα σε δύο δίκτυα που έχουν διαφορετικό επίπεδο εμπιστοσύνης. Το διαδίκτυο έχει μικρό βαθμό εμπιστοσύνης (low level of trust), ενώ το εταιρικό δίκτυο ή το δίκτυο ενός σπιτιού διαθέτει τον μέγιστο βαθμό εμπιστοσύνης. Ένα περιμετρικό δίκτυο (perimeter network) ή μία Demilitarized Zone (DMZ) διαθέτουν μεσαίο επίπεδο εμπιστοσύνης.
Ο σκοπός της τοποθέτησης ενός firewall είναι η πρόληψη επιθέσεων στο τοπικό δίκτυο και η αντιμετώπισή τους. Παρόλα αυτά όμως, ένα firewall μπορεί να αποδειχθεί άχρηστο εάν δεν ρυθμιστεί σωστά. Η σωστή πρακτική είναι το firewall να ρυθμίζεται ούτως ώστε να απορρίπτει όλες τις συνδέσεις εκτός αυτών που επιτρέπει ο διαχειριστής του δικτύου (default-deny). Για να ρυθμιστεί σωστά ένα firewall θα πρέπει ο διαχειριστής του δικτύου να έχει μία ολοκληρωμένη εικόνα για τις ανάγκες του δικτύου και επίσης να διαθέτει πολύ καλές γνώσεις πάνω στα δίκτυα υπολογιστών. Πολλοί διαχειριστές δεν έχουν αυτά τα προσόντα και ρυθμίσουν το firewall ούτως ώστε να δέχεται όλες τις συνδέσεις εκτός από εκείνες που ο διαχειριστής απαγορεύει (default-allow). Η ρύθμιση αυτή καθιστά το δίκτυο ευάλωτο σε επιθέσεις από εξωτερικούς χρήστες.

(ii)**Το Mac Address Filtering** αναφέρεται σε μια μεθοδολογία ελέγχου πρόσβασης σύμφωνα με την οποία τα 48 bit που ανατίθενται σε κάθε κάρτα δικτύου χρησιμοποιούνται για να καθορίσουν την πρόσβαση στο δίκτυο. Οι διευθύνσεις MAC καθορίζονται αποκλειστικά για την κάθε κάρτα ώστε χρησιμοποιώντας φιλτράρισμα MAC να επιτρέπεται ή να απαγορεύεται η δικτυακή πρόσβαση σε συγκεκριμένες συσκευές με τη χρήση blacklists whitelists. Κάθε άτομο που θέλει να έχει πρόσβαση στο δίκτυο πρέπει να έχει μια whitelist για κάθε συσκευή στην οποία θέλει να έχει πρόσβαση

(iii)**Υποστήριξη NAT** σημαίνει ότι υπάρχει ένας μηχανισμός στον router για να μεταφράζει τις IP διευθύνσεις μεταξύ του global δικτύου (Internet) και ενός εσωτερικού (private) δικτύου, διότι δεν είναι δυνατή η άμεση πρόσβαση στο ιδιωτικό δίκτυο από το

δημόσιο. Ο μηχανισμός NAT αντιστοιχεί την εσωτερική διεύθυνση αποστολέα κάθε εξερχόμενου πακέτου στη διεύθυνση του router ενώ σε κάθε εισερχόμενο πακέτο που έχει ως διεύθυνση παραλήπτη τον router του δικτύου αυτή η διεύθυνση απεικονίζεται στην εσωτερική διεύθυνση κάθε συσκευής στο ιδιωτικό δίκτυο. Αυτά φαίνονται στην ακόλουθη εικόνα:



Το πλεονέκτημα του NAT είναι ότι σε συνδυασμό με την τεχνολογία PAT επιλύουν το πρόβλημα των λιγοστών IP διευθύνσεων.

β)
(i) Τα πακέτα τη στιγμή που φεύγουν από το PC3 προς το PC1 μέχρι τον NAT modem/router έχουν ως διεύθυνση αποστολέα την 10.0.1.2. (Τα πακέτα που εξέρχονται από το NAT modem/router έχουν ως source address 193.92.150.15)

(ii) Τα πακέτα τη στιγμή που φεύγουν από το PC1 προς το PC3 μέχρι τον NAT modem/router έχουν ΠΑΝΤΑ ως διεύθυνση αποστολέα την 157.166.224.24. (Ακόμα και μετά την εισαγωγή τους στο τοπικό δίκτυο αυτά διατηρούν την ίδια διεύθυνση αποστολέα)

(iii) Τα πακέτα τη στιγμή που φεύγουν από το PC1 προς το PC3 μέχρι τον NAT modem/router έχουν ως διεύθυνση παραλήπτη την 193.92.150.15. (Τα πακέτα που εισέρχονται στο NAT modem/router προς το PC3 έχουν διεύθυνση παραλήπτη την 10.0.1.2)

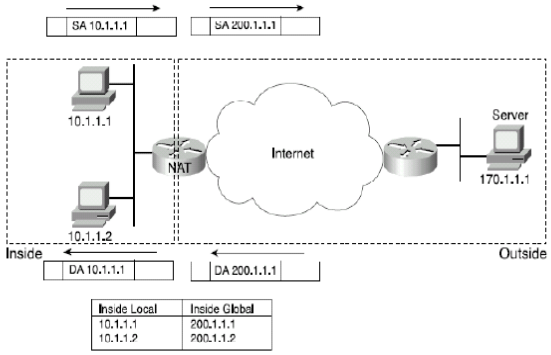
(iv) Εφαρμόζουμε το μηχανισμό PAT. Πιο συγκεκριμένα η IP διεύθυνση του PC1 είναι 157.166.224.25. Η διεύθυνση αυτή στέλνεται σε δύο διαφορετικά ports του NAT modem/router π.χ. port 1024 και 1025 όπου το ένα port π.χ. το 1024 στέλνει τα πακέτα του στο PC2 και το άλλο π.χ. το 1025 στέλνει τα πακέτα του στο PC3. Έτσι θα διαχωρίζονται τα πακέτα του PC1 προς τα PC3 και PC2

7. Z Μέρος - Ερωτήσεις Θεωρίας (Θέματα και Πιθανά Θέματα)

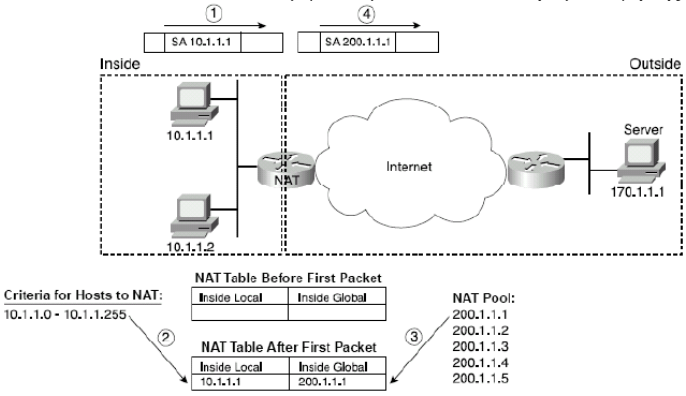
1.Ποια η διαφορά μεταξύ στατικού και δυναμικού NAT;

Απάντηση

Το στατικό NAT αντιστοιχίζει εκ των προτέρων μια ιδιωτική IP σε μια δημόσια IP



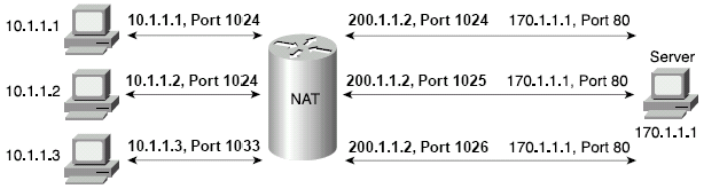
Στο δυναμικό NAT η αντιστοίχιση μιας ιδιωτικής με μια δημόσια διεύθυνση γίνεται τη στιγμή που τα πακέτα εξέρχονται ή εισέρχονται από το /στο ιδιωτικό δίκτυο σύμφωνα με τον πίνακα δρομολόγησης του router.



2.Τι γνωρίζετε για το μηχανισμό PAT; Ποια η διαφορά του από το NAT;

Απάντηση

Με την ένα προς ένα αντιστοίχιση των ιδιωτικών και δημόσιων IP διευθύνσεων του δεν επιλύεται σημαντικά το πρόβλημα των λιγοστών διευθύνσεων IP. Ο μηχανισμός Port Address Translation (PAT) επιτρέπει σε μια δημόσια διεύθυνση IP να χρησιμοποιηθεί από πολλά host σε ένα ιδιωτικό δίκτυο το οποίο είναι συνήθως ένα LAN. Η δημόσια IP διεύθυνση αντιστοιχείται σε διαφορετικά port ενός router, στα οποία έχουν αντιστοιχηθεί επίσης ιδιωτικές διευθύνσεις όπως φαίνεται και στο ακόλουθο σχήμα:



Dynamic NAT Table, With Overloading

Inside Local	Inside Global
10.1.1.1:1024	200.1.1.2:1024
10.1.1.2:1024	200.1.1.2:1025
10.1.1.3:1033	200.1.1.2:1026

Το PAT αποτελεί υποσύνολο του NAT και είναι στενά συνδεδεμένο με τις αρχές του NAT. Το PAT είναι γνωστό και ως υπερφόρτωση του NAT (NAT Overload). Στο PAT όπως αναφέραμε υπάρχει γενικά μόνο μια δημόσια διεύθυνση IP και πολλές ιδιωτικές διευθύνσεις host που συνδέονται με αυτή ενώ στο NAT κάθε δημόσια διεύθυνση IP αντιστοιχείται μόνο σε μια ιδιωτική διεύθυνση host. Το PAT λειτουργεί στο επίπεδο 3 (δικτύου) και 4 (μεταφοράς) του μοντέλου OSI ενώ το βασικό NAT λειτουργεί μόνο στο επίπεδο 3. Το πλεονέκτημα του PAT είναι ότι σε συνδυασμό με την τεχνολογία NAT επιλύουν το πρόβλημα των λιγοστών IP διευθύνσεων.

3.Ποια η διαφορά μεταξύ στατικής και δυναμικής δρομολόγησης;

Απάντηση

Στατική Δρομολόγηση

- Ορίζονται εξαρχής οι πίνακες δρομολόγησης και ακολούθως ξεκινά η δρομολόγηση των πακέτων από την πηγή στον προορισμό
- Οι όποιες αλλαγές απαιτούν διαχειριστική παρέμβαση
- Εύκολη στο σχεδιασμό διαχείριση
- Χρησιμοποιείται σε απλές δικτυακές τοπολογίες όπου η κίνηση του δικτύου είναι προβλέψιμη
- Ακατάλληλη για τα σημερινά δίκτυα λόγω του μεγάλου μεγέθους τους και των συχνών αλλαγών στην τοπολογία του δικτύου

Δυναμική Δρομολόγηση

- Η δρομολόγηση προσαρμόζεται δυναμικά στις αλλαγές στην τοπολογία του δικτύου μέσω αποστολής των routing update μηνυμάτων
- Μπορεί να χρησιμοποιηθεί ταυτόχρονα και με τη στατική δρομολόγηση

4.Ποια η διαφορά μεταξύ single και multi path δρομολόγησης;

Απάντηση

- Single Path υπάρχει ένα μοναδικό μονοπάτι μεταξύ πηγής και προορισμού
- Multi Path υπάρχουν πολλαπλά μονοπάτια μεταξύ πηγής και προορισμού. Επίσης υπάρχει καλύτερο throughput (δηλ. μεγαλύτερος αριθμός μεταφερόμενων πακέτων στη μονάδα του χρόνου), υψηλότερη αξιοπιστία και καλύτερος διαμοιρασμός του φορτίου στο δίκτυο και πολυπλεξία κίνησης μεταξύ των πολλαπλών μονοπατιών

5.Ποιές μετρικές θέλουμε να βελτιστοποιήσουμε σε ένα αλγόριθμο δρομολόγησης;

Απάντηση

- Μήκος μονοπατιού (να μειώσουμε τον αριθμό hops και το άθροισμα κόστους ανά σύνδεσμο)
- Αξιοπιστία
- Καθυστέρηση
- Εύρος ζώνης
- Φόρτος (αύξηση της χρησιμοποίησης CPU και του πλήθους των πακέτων που επεξεργάζεται ανά sec)
- Κόστος επικοινωνίας

6.Ποιός ο σκοπός ενός πρωτοκόλλου δρομολόγησης;

Απάντηση

- ✓ Μαθαίνει τις διαθέσιμες διαδρομές από μια πηγή σε ένα προορισμό
- ✓ Υπολογίζει την καλύτερη διαδρομή και την εισάγει στον πίνακα δρομολόγησης
- ✓ Αφαιρεί από τον πίνακα δρομολόγησης διαδρομές που δεν είναι πλέον έγκυρες

7.Ποιά η διαφορά μεταξύ εσωτερικού και εξωτερικού πρωτοκόλλου δρομολόγησης;

Απάντηση

Το εξωτερικό πρωτόκολλο δρομολόγησης χρησιμοποιείται για τη δρομολόγηση μεταξύ δύο διαφορετικών δικτύων (δικτύων που διαχειρίζονται από 2 διαφορετικούς οργανισμούς). Σε κάθε δίκτυο εκχωρείται ένα ξεχωριστό αναγνωριστικό (AS – Autonomous System).

Το εσωτερικό πρωτόκολλο δρομολόγησης χρησιμοποιείται σε δίκτυα των οποίων οι επιμέρους κόμβοι διαχειρίζονται από τον ίδιο οργανισμό.

8.Ποιά τα χαρακτηριστικά των δικτυακών πρωτοκόλλων;

Απάντηση

Τα δικτυακά πρωτόκολλα καθορίζουν τη λογική διευθυνσιοδότησης στο δίκτυο. Τα πακέτα που ορίζονται από το επίπεδο δικτύου αυτών των πρωτοκόλλων δρομολογούνται από τα πρωτόκολλα δρομολόγησης. Παραδείγματα δικτυακών πρωτοκόλλων IP, Novel Netware κ.λ.π.

9.Ποιές οι διαφορές μεταξύ IP και MAC διευθύνσεων;

Απάντηση

Κάθε κάρτα δικτύου χαρακτηρίζεται από μια MAC διεύθυνση. Η MAC διεύθυνση χαρακτηρίζει μοναδικά ένα Η/Υ σε ένα τοπικό δίκτυο (LAN) και χρησιμοποιείται για δρομολόγηση στο Data Link Layer του μοντέλου OSI (2ο επίπεδο). Αντίθετα η IP διεύθυνση χαρακτηρίζει μοναδικά ένα Η/Υ στο διαδίκτυο και χρησιμοποιείται για δρομολόγηση στο Network Layer του μοντέλου OSI (3ο επίπεδο). Η MAC διεύθυνση χαρακτηρίζει την κάρτα δικτύου και δεν μπορεί να αλλαχθεί από το χρήστη, ενώ η IP διεύθυνση μπορεί να αλλάξει καθ΄ςω ο Η/Υ μετακινείται σε άλλο δίκτυο. Τα δίκτυα IP κρατάνε μια αντιστοίχιση μεταξύ της IP διεύθυνσης μιας συσκευής και της MAC διεύθυνσης της συσκευής. Αυτή η αντιστοίχηση είναι γνωστή σαν ARP cache ή ARP table

10 (Θ). Ποια η διαφορά μεταξύ των πρωτοκόλλων TCP και UDP

Απάντηση

Το πρωτόκολλο TCP είναι το πιο συχνά χρησιμοποιούμενο πρωτόκολλο στο Internet. Ο λόγος γιαυτό είναι ότι το TCP προσφέρει διόρθωση σφαλμάτων. Όταν χρησιμοποιείται το πρωτόκολλο TCP τότε υπάρχει «εγγυημένη παράδοση» της πληροφορίας. Αυτό οφείλεται κατά μεγάλο μέρος σε μια μέθοδο που ονομάζεται έλεγχος ροής. Ο έλεγχος ροής αποφασίζει πότε τα δεδομένα θα επαναμεταδοθούν και διακόπτει την ροή των δεδομένων μέχρι να σταλούν επιτυχώς τα προηγούμενα πακέτα. Αυτό το κάνει διότι κατά την αποστολή ενός πακέτου μπορεί να γίνει σύγκρουση (collision). Όταν συμβεί αυτό ο πελάτης (client) ζητά από τον εξυπηρετητή (server) να ξαναστείλει το πακέτο έτσι ώστε το όλο ληφθέν πακέτο να είναι ολοκληρωμένο και ταυτόσημο με αυτό που μεταδόθηκε
Το πρωτόκολλο UDP είναι επίσης ένα συχνά χρησιμοποιούμενο πρωτόκολλο στο Internet. Παρόλαυτα το UDP δεν χρησιμοποιείται ποτέ για τη μετάδοση σημαντικών δεδομένων όπως π.χ. ιστοσελίδες, πληροφορίες για βάσεις δεδομένων κ.λ.π. Το UDP χρησιμοποιείται συνήθως για την αποστολή audio και video. Τα αρχεία αυτής της μορφής όπως π.χ. Windows Media audio files, Real Player κ.λ.π. χρησιμοποιούν το UDP διότι προσφέρει ταχύτητα. Ο λόγος που το UDP είναι πιο γρήγορο από το TCP είναι διότι δεν υπάρχει έλεγχος ροής ή διόρθωση λαθών. Τα δεδομένα που στέλνονται στο Internet επηρεάζονται από συγκρούσεις και υπάρχουν λάθη. Το UDP ασχολείται μόνο με την ταχύτητα. Αυτός είναι ό βασικός λόγος που τα μέσα μετάδοσης audio και video δεν είναι υψηλής ποιότητας.

11 (Θ). Τι γνωρίζετε για την εντολή ping;
Απάντηση
Η εντολή **ping** χρησιμοποιείται για να ελέγξουμε την IP διεύθυνση προορισμού που θέλουμε να προσπελάσουμε-προσεγγίσουμε και να καταγράψουμε το αποτέλεσμα. Η εντολή **ping** δείχνει εάν αποκρίθηκε ο παραλήπτης (προορισμός) και πόσος χρόνος μεσολάβησε μέχρι να ληφθεί η απάντηση. Αν υπάρχει σφάλμα στην επικοινωνία με τον παραλήπτη η εντολή **ping** εμφανίζει μήνυμα σφάλματος. Οι λόγοι που χρησιμοποιούμε την εντολή ping είναι οι ακόλουθοι:

- Να κάνουμε ping στον Η/Υ μας (με διεύθυνση και όχι με όνομα host) για να ελέγξουμε ότι το TCP/IP λειτουργεί (Κάνοντας ping στον Η/Υ μας δεν επιβεβαιώνει ότι η κάρτα δικτύου λειτουργεί)
- Να κάνουμε ping στον Η/Υ σε ένα τοπικό router για να ελέγξουμε αν ο router λειτουργεί
- Να κάνουμε ping πέρα από τον τοπικό router.

12(Θ). Τι γνωρίζετε για την εντολή netstat;
Απάντηση
Η εντολή netstat αποτελεί ένα χρήσιμο εργαλείο για τον έλεγχο για τον έλεγχο της διαμόρφωσης του δικτύου και της δραστηριότητας σε αυτό, ουσιαστικά χρησιμοποιείται για την απεικόνιση στατιστικών πληροφοριών ενός δικτύου TCP / IP.

13.Να περιγράψετε τις συσκευές Hub, Switch-Bridge και Router
Απάντηση
Hub
Είναι μια συσκευή στην οποία συνδέονται δικτυακοί κόμβοι μέσω καλωδίων συνεστραμμένων ζευγών ή οπτικής ίνας ώστε να δρουν σαν ένα ενιαίο τμήμα. Κυρίως χρησιμοποιείται σε τοπικά δίκτυα ethernet. Τα Hubs λειτουργούν στο φυσικό επίπεδο του μοντέλου OSI. Η συσκευή είναι μια μορφή αναμεταδότη πολλαπλών θυρών. Το hub λαμβάνει ένα σήμα και το κάνει broadcast σε όλα τα ports του. Στην πραγματικότητα το hub είναι ένας repeater με περισσότερες από μία ports.

Switch-Bridge
Το bridge/switch διαβάζει ένα σήμα και βρίσκει το MAC-address της κάρτας δικτύου στο οποίο απευθύνεται το πακέτο, στη συνέχεια κατευθύνει το πακέτο στο κατάλληλο port. Το MAC-address είναι ένας κωδικός που έχει λάβει η κάρτα δικτύου από το εργοστάσιο και είναι μοναδικός. Το bridge χρησιμοποιείται πολλές φορές για να γεφυρώσει ασύμβατα δίκτυα π.χ. ένα ενσύρματο δίκτυο με ένα ασύρματο (συνήθως βέβαια αυτό γίνεται μέσω router ο οποίος πρέπει να διαθέτει τα κατάλληλα interfaces). Το switch λειτουργεί στο 2ο επίπεδο του μοντέλου TCP/IP, διαχειρίζεται πλαίσια (frames) και τα δρομολογεί εντός του τοπικού δικτύου.

Router
Ο Router λειτουργεί στο 3ο επίπεδο του μοντέλου TCP/IP και χρησιμοποιείται για τη σύνδεση δικτύων διαφορετικού τύπου καθώς και δικτύων με διαφορετικό χώρο διευθύνσεων. Ο router διαβάζει τη διεύθυνση IP του κάθε πακέτου που λαμβάνει και κάνοντας AND με την subnet mask του ξεκαθαρίζει εάν ο παραλήπτης ανήκει στο ίδιο δίκτυο με το router ή σε διαφορετικό. Εάν ανήκει στο ίδιο το στέλνει στον παραλήπτη, εάν ανήκει σε διαφορετικό το προωθεί σε άλλον router με βάση ένα εσωτερικό πίνακα που κρατάει στην "μνήμη" του. Εάν το πακέτο ανήκει σε άγνωστο δίκτυο, π.χ. Internet το πακέτο ταξιδεύει στον default gateway που συνήθως είναι ένας άλλος Router, ή ένα PC που κάνει IP forwarding και λειτουργεί σαν router, και με την ίδια διαδικασία καταλήγει στον παραλήπτη. Ο router διαχειρίζεται πακέτα και τα δρομολογεί μεταξύ διαφορετικών δικτύων

14.Τι γνωρίζετε για τα VLAN (Virtual Lan);
Απάντηση
Είναι μια μέθοδος δημιουργίας ανεξάρτητων λογικών δικτύων μέσα σε ένα φυσικό δίκτυο. Έχει ως στόχο τη δημιουργία ενός ιδιωτικού εύρους (private scope) στις επικοινωνίες Η/Υ καθώς και την ασφαλή επέκταση ενός ιδιωτικού δικτύου σε ένα ανασφαλές δίκτυο όπως το Internet. Οι σύνδεσμοι μεταξύ των κόμβων σε ένα ιδιωτικό VLAN δημιουργούνται μέσω εικονικών κυκλωμάτων μεταξύ των host ενός μεγαλύτερου δικτύου Τα ιδιωτικά VLAN συχνά εγκαθίστανται από οργανισμούς για να δώσουν απομακρυσμένη πρόσβαση (remote access) σε ένα ασφαλές δίκτυο οργανισμού (organizational network). Γενικά ένα VLAN έχει πιο πολύπλοκη τοπολογία από μια σύνδεση σημείο προς σημείο.

Τα πλεονεκτήματα του είναι η:

- ✓ Μείωση της κίνησης στο δίκτυο
- ✓ Αύξηση της ασφάλειας
- ✓ Μείωση σε απαιτήσεις hardware

15(Θ).Τι γνωρίζετε για την εντολή traceroute;

Απάντηση

Η εντολή traceroute χρησιμοποιείται για να εμφανίσει το μονοπάτι που ακολουθεί ένα πακέτο πληροφορίας από τον Η/Υ μας στον Η/Υ που προσδιορίζουμε. Εμφανίζει όλους τους routers μέσω των οποίων διέρχεται το πακέτο μέχρι να φράσει στον προορισμό του. Επιπλέον δείχνει πόσο χρόνο παίρνει το κάθε βήμα (hop) από τον ένα router στον άλλο.

16(Θ). Να περιγράψτε τη λειτουργία των πρωτοκόλλων ARP και DNS

Απάντηση

ARP

Τα τοπικά δίκτυα (LAN) λειτουργούν τυπικά με διευθύνσεις MAC και δεν γνωρίζουν τίποτα για διευθύνσεις IP. Για να είναι εφικτή η επικοινωνία μεταξύ δύο υπολογιστών πρέπει ο καθένας να γνωρίζει τη διεύθυνση MAC του άλλου. Η λύση που χρησιμοποιείται είναι να σταλεί ένα πακέτο εκπομπής που ρωτά: Σε ποιον ανήκει η διεύθυνση IP 147.102.240.1; Το πακέτο θα φτάσει με εκπομπή (broadcast) σε κάθε Η/Υ του δικτύου 147.102.240.0 (Με μάσκα υποδικτύου 255.255.255.0) και καθεμία από αυτές θα ελέγξει αν απευθύνεται στη δική της διεύθυνση IP. Μόνο η μηχανή με τη σωστή διεύθυνση IP θα ανταποκριθεί με μονο-εκπομπή (unicast) δίνοντας τη διεύθυνση Mac αυτής. Το πρωτόκολλο που διατυπώνει αυτή την ερώτηση, απαντάει και λαμβάνει την απάντηση είναι το ARP.
Εν συντομία η λειτουργία του ARP είναι η εξής:

- Ο Α γνωρίζει τη διεύθυνση IP του Β και θέλει να μάθει τη φυσική του διεύθυνση MAC
- Ο Α εκπέμπει μια αίτηση ARP που περιέχει την IP διεύθυνση του Β
- Όλοι οι Η/Υ είναι υποχρεωμένοι να ακούν για ερωτήσεις ARP και να απαντούν
- Ο Β λαμβάνει το πακέτο ARP και απαντά με τη φυσική του διεύθυνση
- Ο Α καταχωρεί το ζεύγος IP-φυσική διεύθυνση σε προσωρινή μνήμη
- Οι καταχωρήσεις εκπνέουν χρονικά μετά από μερικά λεπτά και η πληροφορία διαγράφεται

DNS

Κάθε μηχάνημα – host του Διαδικτύου μπορεί να αναγνωριστεί από την IP διεύθυνσή του, που είναι ένας δυαδικός αριθμός των 32 bits. Το ίδιο το δίκτυο (και συγκεκριμένα το επίπεδο διαδικτύου) καταλαβαίνει μόνο τις IP διευθύνσεις. Οι άνθρωποι, όμως, μπορούν πιο εύκολα να θυμούνται ονόματα και όχι δυαδικούς αριθμούς. Για αυτό το λόγο τις περισσότερες φορές τα προγράμματα σπάνια απευθύνονται στους host του Διαδικτύου χρησιμοποιώντας την IP διεύθυνση, αλλά κάνουν χρήση συμβολικών ονομάτων, με την μορφή ακολουθιών ASCII χαρακτήρων. **Για την αντιστοίχηση μεταξύ των δυαδικών διευθύνσεων και των διευθύνσεων σε μορφή ASCII χαρακτήρων χρησιμοποιείται ένα πρωτόκολλο του στρώματος εφαρμογών, το DNS (Domain Name System)**. Το πρωτόκολλο DNS χρησιμοποιεί το UDP και συγκεκριμένα την θύρα 53.
Το DNS είναι:
1.Ένα ιεραρχικό σύστημα ονοματολογίας των κόμβων του Internet.
2. Μία κατανεμημένη βάση δεδομένων που υλοποιείται σε ένα πλήθος διακομιστών DNS και περιέχει τις αντιστοιχίες ονομάτων host – διευθύνσεων IP.
3.Ένα πρωτόκολλο Επιπέδου Εφαρμογής (Πρότυπο TCP/IP) επιτρέπει σε δύο υπολογιστές να επικοινωνούν μεταξύ τους με τη χρήση ονομάτων μέσω των διακομιστών DNS.

Συνοπτικά το ARP μεταφράζει μια IP address (π.χ. 192.168.0.1) σε μια MAC address (e.g. 00:11:12:13:14:15) ενώ το DNS μεταφράζει ένα όνομα (π.χ. Example Web Page) σε μια IP address (e.g. 212.178.0.19)

17 (Θ). Ποια η διαφορά μεταξύ unicast, broadcast και anycast διευθύνσεων

Απάντηση

- ✓ Στις **unicast** διευθύνσεις υπάρχει σχέση 1-1 μεταξύ της διεύθυνσης του δικτύου και ενός τελικού σημείου του δικτύου. Κάθε διεύθυνση προορισμού αναγνωρίζει ένα μοναδικό παραλήπτη
- ✓ Στις **broadcast and multicast** υπάρχει σχέση 1 προς πολλά μεταξύ της διεύθυνσης του δικτύου και της διεύθυνσης των τελικών σημείων-παραληπτών του δικτύου. Η διεύθυνση προορισμού αναγνωρίζει ένα σύνολο από παραλήπτες στους οποίους η πληροφορία στέλνεται
- ✓ Στις **anycast** διευθύνσεις υπάρχει επίσης μια σχέση 1 προς πολλά μεταξύ της διεύθυνσης του δικτύου και της διεύθυνσης των τελικών σημείων-παραληπτών του δικτύου: κάθε διεύθυνση προορισμού αναγνωρίζει ένα σύνολο παραληπτών αλλά μόνο ένας από αυτούς επιλέγεται σε μια δεδομένη χρονική στιγμή για να λάβει πληροφορία από ένα οποιοδήποτε παραλήπτη
- ✓ Στο IPv4 έχουμε τις unicast, broadcast και multicast διευθύνσεις. Στο IPv6 έχουμε unicast, multicast και anycast. Στο IPv6 οι broadcast διευθύνσεις δεν χρησιμοποιούνται πλέον διότι έχουν αντικατασταθεί από τις multicast διευθύνσεις.

18 (Θ). Τι γνωρίζετε για το πρωτόκολλο ARP

Απάντηση

Το **Address Resolution Protocol (ARP)** είναι **χρήσιμο στην αντιστοίχιση διευθύνσεων του επιπέδου δικτύου (IP διευθύνσεων) με τις MAC διευθύνσεις του χαμηλότερου επιπέδου**. Είναι ευρέως διαδεδομένο, καθώς απαντάται σχεδόν σε όλα τα σύγχρονα τοπικά δίκτυα που συνδυάζουν το πρωτόκολλο Ethernet με τη σουίτα πρωτοκόλλων TCP/IP. Με απλά λόγια, κάθε κόμβος του δικτύου που επιθυμεί να επικοινωνήσει με έναν άλλο κόμβο του δικτύου για τον οποίο γνωρίζει μόνο την IP διεύθυνση, κάνει χρήση του εν λόγω πρωτοκόλλου για να εντοπίσει την hardware διεύθυνση του προορισμού.

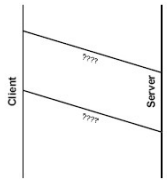
19. Τι γνωρίζετε για το σετ πρωτοκόλλων Universal Plug and Play (UPnP)

Απάντηση

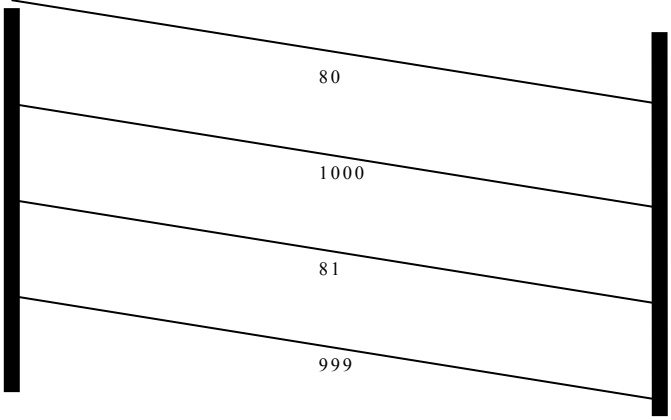
Το **Universal Plug and Play (UPnP) σετ πρωτοκόλλων** είναι ένα διεθνές στάνταρντ του οργανισμού ISO, που αποσκοπεί στην επικοινωνία μεταξύ συσκευών σχεδόν οποιουδήποτε τύπου με τρόπο διάφανο προς το χρήστη, χωρίς να απαιτείται οποιαδήποτε ρύθμιση εκ μέρους του (plug and play). Η λειτουργία του στηρίζεται σε ανοιχτά, ήδη διαθέσιμα standards. Μπορεί να χρησιμοποιηθεί σε οικιακό περιβάλλον, όπου ο χρήστης δεν έχει απαραίτητα προχωρημένες τεχνικές γνώσεις, καθώς και σε επιχειρησιακό περιβάλλον, όπου υπάρχει η ανάγκη για μείωση του διαχειριστικού κόστους που επιφέρει η δικτύωση. Το UPnP επιτρέπει τη διασύνδεση μιας μεγάλης ποικιλίας συσκευών. Υπολογιστές, οικιακές & καταναλωτικές συσκευές (από βιντεοκάμερες και συστήματα ήχου & εικόνας μέχρι ψυγεία & φούρνοι) μπορούν να συνδεθούν ενσύρματα ή ασύρματα σε ένα δίκτυο που υποστηρίζει το σετ πρωτοκόλλων UPnP. Χρησιμοποιείται IP διευθυνσιοδότηση, που προφανώς δεν εφαρμόζεται χειροκίνητα αλλά με χρήση του πρωτοκόλλου DHCP (αν είναι διαθέσιμο) ή μιας παρόμοιας διαδικασίας που ονομάζεται AutoIP. Τα πρωτόκολλα που χρησιμοποιούνται για την ανακοίνωση των υπηρεσιών κάθε συσκευής είναι το Simple Service Discovery Protocol (SSDP) για την αρχική ενημέρωση των υπολοίπων συσκευών του δικτύου και η γλώσσα eXtensive Markup Language (XML) για την αναλυτική παρουσίαση των χαρακτηριστικών και των δυνατοτήτων της.

20. Τι γνωρίζετε για το port knocking; Καταγράψτε ένα πιθανό port knocking sequence σε μια μορφή όπως η παρακάτω όπου κάθε διαγώνια γραμμή αντιστοιχεί στην αποστολή ενός πακέτου

Απάντηση



Κάθε υπολογιστής που ανήκει στο Internet μπορεί να παίξει το ρόλο του διακομιστή (server). Μπορεί δηλαδή να είναι σε θέση να δεχτεί αιτήματα σε συγκεκριμένες θύρες (ports) τις οποίες έχει προηγουμένως ρυθμίσει κατάλληλα ώστε να δέχονται αιτήματα. Ένας υποψήφιος εισβολέας ενός υπολογιστικού συστήματος θα μπορούσε να ερευνήσει ένα προς ένα τα διαθέσιμα ports προκειμένου να εντοπίσει πιθανά ανοιχτά και στη συνέχει να βρει διόδους εκμετάλλευσης της κατάστασης. Η παραπάνω διαδικασία είναι γνωστή με την ονομασία port scanning. **Το port knocking αποσκοπεί στην παρεμπόδιση του επιτιθέμενου που προσπαθεί να κάνει χρήση της πιο πάνω μεθόδου. Όταν χρησιμοποιείται η εν λόγω μέθοδος όλα τα ports ενός υπολογιστή εμφανίζονται ως κλειστά**. Μόνο όταν κάποιος επιχειρήσει μια ακολουθία «χτυπημάτων» σε συγκεκριμένες πόρτες με συγκεκριμένη σειρά, αλλάζει η ρύθμιση του φράγματος ασφαλείας του υπολογιστικού συστήματος για να επιτρέψει την επικοινωνία με συγκεκριμένες θύρες που μέχρι νωρίτερα εμφανίζονταν ως κλειστές. Το πλήθος των διαθέσιμων θυρών κάνει την τυχαία εύρεση της ορθής ακολουθίας «χτυπημάτων» ουσιαστικά αδύνατη.
Η πιο κλασική μορφή port knocking κάνει χρήση πακέτων συγχρονισμού (SYN) που στέλνονται διαδοχικά προς τις κατάλληλες θύρες. Αν π.χ. η ακολουθία θυρών που «ξεκλειδώνει» το φράγμα ασφαλείας έχει οριστεί σε 80 – 1000 – 81 – 999 τότε μια επιτυχής αποστολή μηνυμάτων απεικονίζεται με τον ακόλουθο τρόπο:



21. Ποιο πρωτόκολλο χρησιμοποιεί η εφαρμογή traceroute; Τι πακέτα ανταλλάσσονται και ποιος ο ρόλος του πεδίου TTL;

Απάντηση

Η εφαρμογή traceroute χρησιμοποιεί το πρωτόκολλο UDP. Σε ορισμένα περιβάλλοντα όμως, δίνεται η επιλογή και για χρήση του ICMP (Windows) και ακόμη και του TCP (BSD, MacOS). Στην πιο συνηθισμένη περίπτωση του UDP, τα πακέτα που χρησιμοποιούνται είναι τα UDP datagrams, με προορισμούς ports 33434 έως 33534.

Το πεδίο TTL ορίζει το μέγιστο αριθμό βημάτων (hops) που επιτρέπεται να ταξιδέψει ένα πακέτο, πριν διαγραφεί. Στόχος του πεδίου είναι να αποτρέψει την κατάσταση κατά την οποία ένα πακέτο κυκλοφορεί για πάντα ανάμεσα στους δρομολογητές του δικτύου, χωρίς να φτάνει ποτέ στον προορισμό του. Πολλά τέτοια «ορφανά» πακέτα θα μπορούσαν να προκαλέσουν πολύ σύντομα συμφόρηση και κατάρρευση του δικτύου. **Αν και στη θεωρία το πεδίο TTL αποσκοπούσε στην αποθήκευση ενός χρονικού διαστήματος σε δευτερόλεπτα, στην πράξη μετρά απλά τον αριθμό των βημάτων που έχει διανύσει ένα πακέτο**. Αυτό επιτυγχάνεται με την μείωση της τιμής στο πεδίο TTL κατά μία μονάδα από κάθε δρομολογητή που προωθεί το πακέτο προς τον επόμενο κόμβο του δικτύου. Κάθε δρομολογητής που διαπιστώνει πως η τιμή του πεδίου TTL έχει γίνει ίση με μηδέν πριν φτάσει στον προορισμό του, καταστρέφει το πακέτο και αντί αυτού στέλνει ένα πακέτο ICMP τύπου 11 προς τον αποστολέα για να τον ενημερώσει για το συμβάν.

22. Τι εννοούμε με τον όρο Network interface ενός υπολογιστή;

Απάντηση

Network interface ενός υπολογιστή είναι η διασύνδεση του υπολογιστή με ένα δίκτυο. Σε έναν υπολογιστή μπορούν να υπάρχουν διασυνδέσεις με περισσότερα του ενός δίκτυα και επομένως ο συγκεκριμένος υπολογιστής να έχει περισσότερα από ένα network interfaces.

Εκτελώντας την εντολή ifconfig –a η οποία επιστρέφει τα network interfaces σε έναν υπολογιστή, μπορούμε να βρούμε τις subnet masks για όλα τα interfaces του zenon. Χαρακτηριστική είναι η περίπτωση ενός κοινού ADSL δρομολογητή, που είθισται να περιλαμβάνει τουλάχιστον δύο network interfaces. Το πρώτο είναι ένα LAN interface (συνήθως Ethernet) για τη σύνδεση του υπολογιστή στον δρομολογητή. Το δεύτερο είναι ένα WAN interface για τη σύνδεση του δρομολογητή με το ADSL δίκτυο κορμού.

23. Ποιος ο βασικός σκοπός του πρωτοκόλλου CDP;

Απάντηση

Το πρωτόκολλο CDP είναι ένα δικτυακό πρωτόκολλο επιπέδου δεδομένων (Data Link Layer) το οποίο χρησιμοποιείται από τους δρομολογητές και τον εξοπλισμό της εταιρείας Cisco. Η κυριότερη χρήση του αφορά στην ανακάλυψη άλλων συσκευών στο δίκτυο, αλλά και ανταλλαγή πληροφοριών (έκδοση του λειτουργικού συστήματος και η IP διεύθυνση της συσκευής κτλ) μεταξύ των συσκευών αυτών, με την προϋ πόθεση ότι αυτές υποστηρίζουν το πρωτόκολλο. Μια επιπλέον δυνατότητα του πρωτοκόλλου –όπως αυτή υλοποιήθηκε αργότερα- είναι η μεταφορά δεδομένων που αφορούν στη δρομολόγηση πακέτων του δικτύου (On-Demand Routing). Για την απενεργοποίηση του πρωτοκόλλου αρκεί να δώσουμε την εντολή "no cdp run". Για να δώσουμε την παραπάνω εντολή, πρέπει να βρισκόμαστε σε privilledged mode.

24. Ποιο πρωτόκολλο θα χρησιμοποιήσουμε σε ένα δίκτυο που αποτελείται από αρκετά Cisco switches για να ρυθμίσουμε κάθε switch ξεχωριστά;

Απάντηση

Το πρωτόκολλο που μπορούμε να χρησιμοποιήσουμε είναι το VTP ή VLAN Trunk Protocol. Μπορούμε να ορίσουμε το VLAN στον κεντρικό VTP server και το πρωτόκολλο θα φροντίσει να το διανείμει σε όλα τα switches αυτόματα μειώνοντας σημαντικά το φόρτο διαχείρισης.

25. Ποιες οι βασικές χρήσεις των Console και Auxiliary Port σε ένα Cisco δρομολογητή;

Απάντηση

Console Port. Παρέχει έναν τρόπο για να συνδέει ένα τερματικό-υπολογιστή με το router έτσι ώστε να δουλέψει πάνω σε αυτό. Το console port χρησιμοποιείται από τους administrators για να συνδεθούν πάνω στο router κατευθείαν χωρίς να υπάρχει network connection. Ένα μειονέκτημά του είναι κάποιος υπεύθυνος θα πρέπει να βρίσκεται στην ίδια τοποθεσία με το router έτσι ώστε να γίνει η σύνδεση.

Auxiliary Port: Οι περισσότεροι Cisco δρομολογητές έχουν και ένα δεύτερο port στο πίσω μέρος που ονομάζεται auxiliary port. Όπως το console port, έτσι και αυτό παρέχει απευθείας σύνδεση με το router. Όμως διαφέρει από το console port στο ότι το auxiliary port παρέχει έναν connector τύπο που επιτρέπει τη σύνδεση modem πάνω σε αυτόν. Αυτό έχει ως σκοπό να μπορείς να συνδεθείς στο router απομακρυσμένα (dialup) και να μπορούν να αντιμετωπιστούν προβλήματα χωρίς τη φυσική παρουσία ανθρώπου.

26. Ποια η διαφορά ενός Collision από ένα Broadcast Domain

Απάντηση

Collision Domain: Ένα collision domain είναι ένα φυσικό τμήμα δικτύου όπου τα πακέτα δεδομένων μπορούν «να συγκρουστούν» το ένα με το άλλο για την αποστολή σε ένα κοινό μέσο, και ιδιαίτερα στο πρωτόκολλο Ethernet.

Broadcast Domain: Ένα broadcast domain είναι ένα λογικό τμήμα ενός δικτύου υπολογιστών, στο οποίο όλοι οι κόμβοι μπορούν να φθάσουν ο ένας στον άλλο από τη broadcast μετάδοση στο data link layer. Ένα broadcast domain μπορεί να είναι μέσα στο ίδιο τοπικό LAN ή μπορεί να καθοδηγηθεί προς άλλα τμήματα του τοπικού LAN.

27(Θ). Τι είναι Zombie process;

Απάντηση

Zombie process είναι μια διεργασία που έχει ολοκληρώσει την εκτέλεση της αλλά εξακολουθεί να υπάρχει στον πίνακα διεργασιών (δηλαδή διατηρείται εγγραφή γιαυτή στον πίνακα διεργασιών). Σε αντίθεση με τις κανονικές διεργασίες, η εντολή kill δεν έχει καμία επίδραση σε μια zombie process.

28(Θ). Διαφορά bridge-switch

Απάντηση

Οι γέφυρες χρησιμοποιούνται για τη διασύνδεση 2 LANs μεταξύ τους ενώ τα switch χρησιμοποιούνται για τη σύνδεση 2 workstations μεταξύ τους. Μια γέφυρα εκτελεί φιλτράρισμα και διαχειρίζεται τη ροή κυκλοφορίας που διέρχεται μέσω αυτής. Η βασική διαφορά μεταξύ γέφυρας και switch είναι ο αριθμός των δικτύων που μπορεί να συνδέσει κάθε συσκευή. Επειδή τα switches έχουν περισσότερα από 2 interfaces μπορούν να συνδέσουν 3 ή περισσότερα δίκτυα μεταξύ τους. Συγκεντρωτικά οι διαφορές είναι οι ακόλουθες:

1. Ένα switch είναι βασικά μια γέφυρα (bridge) με περισσότερα από 2 interfaces ή ports
2. Τα Switches μπορούν να συνδέσουν περισσότερα από 2 δίκτυα
3. Οι γέφυρες χρησιμοποιούνται συνήθως 2 LANs ενώ τα switches χρησιμοποιούνται συνήθως για σύνδεση workstations μεταξύ τους

29 (Θ). Τι γνωρίζετε για την εντολή Nslookup

Απάντηση

Το Nslookup.exe είναι ένα εργαλείο διαχείρισης γραμμής εντολών για τον έλεγχο και την αντιμετώπιση προβλημάτων των διακομιστών DNS. Το εργαλείο αυτό εγκαθίσταται μαζί με το πρωτόκολλο TCP/IP μέσω του Πίνακα Ελέγχου (Control Panel). Πιο συγκεκριμένα το nslookup χρησιμοποιείται για να θέτει ερωτήσεις σε ένα DNS domain nameserver για την αναζήτηση και την εύρεση διευθύνσεων IP υπολογιστών στο internet. Μετατρέπει ένα όνομα host ή ένα όνομα domain σε διεύθυνση IP

30 (Θ). Τι κάνει η συνάρτηση inet_aton();

Απάντηση

Η συνάρτηση inet_aton() με πλήρες *format int inet_aton(const char *cp, struct in_addr *addr)* μετατρέπει την Internet host address cp από τον standard συμβολισμό a.b.c.d σε δυαδικά δεδομένα (binary data) και την αποθηκεύει στη δομή addr. Η συνάρτηση inet_aton() επιστρέφει μη μηδενική τιμή αν η διεύθυνση είναι έγκυρη αλλιώς επιστρέφει μηδέν

31(Θ). Τι κάνει η συνάρτηση inet_ntoa();

Απάντηση

Η συνάρτηση inet_ntoa με πλήρες format *char *inet_ntoa(struct in_addr in)* μετατρέπει την Internet host address που βρίσκεται στην παράμετρο από δυαδικά δεδομένα στον standard συμβολισμό a.b.c.d.

32(Θ). Τι κάνει η συνάρτηση inet_pton();

Απάντηση

Η συνάρτηση inet_pton με πλήρες format *int inet_pton(int af, const char *restrict src, void *restrict dst)* μετατρέπει μια διεύθυνση από την standard μορφή της ως αλφαριθμητικό είτε σε τύπο της δομής struct in_addr ή της δομής struct in6_addr είτε σε δυαδική αναπαράσταση. Το όρισμα af προσδιορίζει την οικογένεια της διεύθυνσης (υποστηρίζονται οι οικογένειες AF_INET [IP6] και AF_INET6). Το όρισμα src είναι το αλφαριθμητικό όρισμα που περιλαμβάνει τη διεύθυνση. Το όρισμα dst είναι ο buffer που αποθηκεύεται η διεύθυνση στη δυαδική της αναπαράσταση.

33(Θ). Ποια τα χαρακτηριστικά ενός καναλιού;

Απάντηση

Ένα κανάλι έχει χωρητικότητα η οποία εκφράζει το μέγιστο ρυθμό μετάδοσης δεδομένων μέσα από το κανάλι, εύρος ζώνης που δείχνει ποιες συχνότητες διέρχονται μέσα από το κανάλι, εισάγει παραμόρφωση και θόρυβο στο εισερχόμενο σήμα και περιγράφεται από την κρουστική του απόκριση.

34(Θ). Τι γνωρίζετε για το πρωτόκολλο PUpnP;

Απάντηση

Το portable Universal Plug and Play (PUPnP) προσφέρει στους developers ένα API και ανοικτό κώδικα (open source code) για την κατασκευή control points, συσκευών και γεφυρών (bridges) που είναι συμβατές με την έκδοση 1.0 του Universal Plug and Play Device Architecture Specification και υποστηρίζει πολλά λειτουργικά συστήματα όπως Linux, *BSD, Solaris κ.λ.π.

35(Θ). Ποια η διαφορά getserverbyport και getserverbyname

Απάντηση

Η συνάρτηση **getserverbyname** έχει το format struct servent *getservbyname(const char *name, const char *proto); ενώ η συνάρτηση getserverbyport έχει το format struct servent *getservbyport(int port, const char *proto);

Η συνάρτηση **getservbyname**() επιστρέφει τη δομή τύπου servent για τη γραμμή του από το φάκελο /etc/services που ταιριάζει με την υπηρεσία που χρησιμοποιεί το πρωτόκολλο proto. Αν το πεδίο proto είναι NULL τότε ταιριάζει οποιοδήποτε πρωτόκολλο

Η συνάρτηση getservbyport() επιστρέφει μια servent structure για τη γραμμή που ταιριάζει με τη θύρα (port) που δίνεται.

36(Θ). Ποια η διαφορά μεταξύ access και trunk port

Απάντηση

Ένα port μπορεί είτε access είτε trunk port. Τα trunk ports δηλώνονται σε ένα switch όταν υλοποιείται κάποιο VLAN και μέσω αυτών πραγματοποιείται η μεταφορά δεδομένων μεταξύ των switches που υλοποιούν ένα VLAN. Υλοποιούν δηλαδή το trunk link. Τα access ports χρησιμοποιούνται για να γίνει η μεταφορά δεδομένων εσωτερικά στο VLAN.

37 Ποιο από τα TCP/UDP χρησιμοποιούν συνήθως οι υπηρεσίες HTTP, SNMP, BitTorrent; Για ποιο λόγο πιστεύετε πως έγινε η κάθε επιλογή;

Απάντηση

- Το HTTP χρησιμοποιεί το TCP πρωτόκολλο. Το HTTP πρωτόκολλο προϋποθέτει για τις περισσότερες εφαρμογές πως υπάρχει αξιόπιστη μεταφορά δεδομένων μεταξύ των hosts. Το TCP πρωτόκολλο προσφέρει αξιοπιστία εφόσον είναι connection-based σε σχέση με το connectionless UDP.
- Το SNMP (Simple Network Management Protocol) χρησιμοποιεί το UDP πρωτόκολλο. Πρόκειται για Administrative Protocol που χρησιμοποιείται για να καταγράφει την κατάσταση συσκευών σε ένα δίκτυο. Για τη συγκεκριμένη εφαρμογή, το μέγεθος των μηνυμάτων που ανταλλάσσονται είναι σχετικά μικρό και δεν συμφέρει ο φόρτος που επιφέρει στο δίκτυο η εγκατάσταση την σύνδεσης που απαιτεί το TCP πρωτόκολλο.
- Το SMPT (Simple Mail Transfer Protocol) πρωτόκολλο χρησιμοποιεί το TCP, εφόσον στη συγκεκριμένη εφαρμογή η αξιοπιστία είναι πολύ σημαντική.
- Το BitTorrent πρωτόκολλο χρησιμοποιείται για την peer-to-peer μεταφορά σχετικά μεγάλου όγκου δεδομένων. Εγκαθιδρύει πολλές συνδέσεις ανά δύο hosts από τις οποίες μεταφέρονται τα δεδομένα. Με βάση αυτό, είναι λογικό να προτιμά το connection-oriented πρωτόκολλο TCP, το οποίο προσφέρει αξιοπιστία κατά τη μεταφορά δεδομένων.

38. Να περιγράψτε το πρωτόκολλο DHCP

Απάντηση

- Το Dynamic Host Configuration Protocol (DHCP) είναι ένα πρωτόκολλο δικτύου που χρησιμοποιείται για να ρυθμίσουμε συσκευές του δικτύου έτσι ώστε να μπορούν να επικοινωνούν μεταξύ τους
- Είναι ένα πρωτόκολλο Client-Server
- Ένας πελάτης DHCP χρησιμοποιεί το πρωτόκολλο DHCP για να αποκτήσει πληροφορίες ρύθμισης παραμέτρων όπως μια διεύθυνση IP, μια προεπιλεγμένη διαδρομή και μια ή περισσότερες διευθύνσεις διακομιστή DNS από ένα διακομιστή DHCP
- Ο πελάτης DHCP χρησιμοποιεί αυτές τις παραμέτρους για να ρυθμίσει τις παραμέτρους του υπολογιστή στον οποίο τρέχει. Μόλις ολοκληρωθεί η διαδικασία διαμόρφωσης ο Η/Υ είναι σε θέση να επικοινωνήσει στο διαδίκτυο

Υπάρχουν δύο τρόποι με τους οποίους μπορεί να αποδοθεί μια IP διεύθυνση στους πελάτες:

1. **Χειροκίνητη καταχώρηση**: Ο διαχειριστής του συστήματος καταχωρεί τις IP διευθύνσεις χειροκίνητα, συνήθως σε ένα αρχείο.

2. **Πρωτόκολλο Δυναμικής Καταχώρησης IP διευθύνσεων (DHCP - Dynamic Host Configuration Protocol):** Το DHCP επιτρέπει σε έναν πελάτη να αποκτήσει μια IP διεύθυνση αυτόματα και επίσης να μάθει επιπλέον πληροφορίες, όπως την διεύθυνση του δρομολογητή πρώτου άλματος (first hop router) καθώς και την διεύθυνση του DNS εξυπηρετητή του.

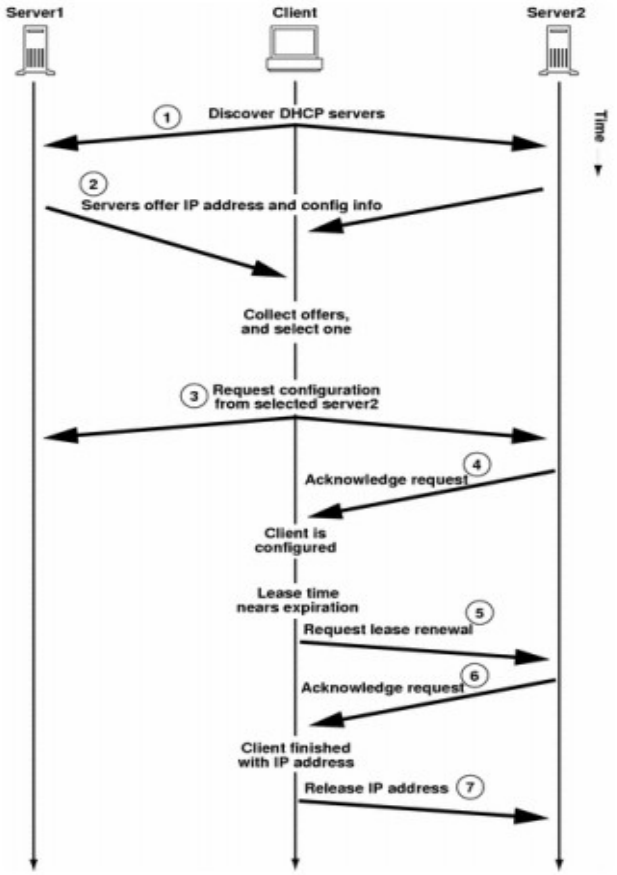
Ένας πελάτης που έχει μόλις φτάσει σε ένα δίκτυο επιθυμεί να λάβει μια IP διεύθυνση. Στην περίπτωση αυτή το πρωτόκολλο DHCP είναι μια διαδικασία τεσσάρων βημάτων:

1. **Ανακάλυψη Εξυπηρετητή DHCP**: Η πρώτη εργασία ενός μόλις αφικνούμενου πελάτη είναι να βρει έναν Εξυπηρετητή DHCP με τον οποίο θα αλληλεπιδράσει. Αυτό το επιτυγχάνει στέλνοντας ένα μήνυμα ανακάλυψης DHCP προς όλους τους υπολογιστές του δικτύου. Όταν ένας υπολογιστής συνδέεται στο δίκτυο , εκπέμπει (broadcast) ένα ειδικό πλαίσιο ελέγχου (control frame) που ονομάζεται DHCPDISCOVER και έχει ως στόχο να εντοπίσει τους διαθέσιμους DHCP servers που είναι συνδεδεμένοι στο τοπικό δίκτυο οι οποίοι μπορεί να είναι περισσότεροι από ένας .

2. **Προσφορά Εξυπηρετητή DHCP**: Ένας DHCP Εξυπηρετητής, που έχει λάβει το μήνυμα ανακάλυψης DHCP από τον πελάτη, του απαντά με ένα μήνυμα προσφοράς DHCP, το οποίο περιέχει μεταξύ άλλων πληροφοριών την προσφερόμενη IP διεύθυνση και το χρόνο για τον οποίο θα είναι έγκυρη. Δεδομένου ότι υπάρχει δυνατότητα το μήνυμα ανακάλυψης DHCP να έχει ληφθεί από περισσότερους του ενός DHCP εξυπηρετητές, ο πελάτης μπορεί να επιλέξει ανάμεσα σε πολλά μηνύματα προσφοράς DHCP. Επίσης Κάθε φορά που ένας DHCP server δέχεται ένα τέτοιο μήνυμα ανταποκρίνεται στέλνοντας στον υπολογιστή πελάτη ένα μήνυμα που ονομάζεται DHCPOFFER και περιλαμβάνει μια ελεύθερη IP διεύθυνση και ένα σύνολο παραμέτρων διαμόρφωσης (configuration parameters) οι οποίες είναι και οι πιο κατάλληλες για αυτόν τον πελάτη . Σε ορισμένες περιπτώσεις ο DHCP server πριν αποδώσει την IP διεύθυνση στον DHCP client πραγματοποιεί έναν έλεγχο για να διαπιστώσει εάν αυτή η διεύθυνση χρησιμοποιείται ήδη από κάποιον άλλο υπολογιστή . Αυτός ο έλεγχος γίνεται με τη βοήθεια ειδικών πρωτοκόλλων όπως είναι το ARP (address resolution protocol) και το ICMP (interface control message protocol)

3. **Αίτηση DHCP**: Ο πελάτης επιλέγει μία προσφορά εξυπηρετητή DHCP και ενημερώνει τον αντίστοιχο εξυπηρετητή.

4. **Βεβαίωση λήψης DHCP (DHCP ACK):** Ο DHCP εξυπηρετητής απαντά στον πελάτη βεβαιώνοντας τις παραμέτρους της προσφοράς του προς εκείνον. Όταν ο πελάτης λάβει τη βεβαίωση λήψης DHCP, η αλληλεπίδραση με τον DHCP εξυπηρετητή έχει ολοκληρωθεί και ο πελάτης μπορεί να χρησιμοποιήσει την IP διεύθυνση για όσο χρόνο είναι έγκυρη. Επειδή ωστόσο ο πελάτης ενδέχεται να επιθυμεί τη χρήση της συγκεκριμένης διεύθυνσης περισσότερο χρόνο από όσο του έχει εκχωρηθεί, το πρωτόκολλο DHCP παρέχει έναν μηχανισμό που του επιτρέπει να ανανεώσει το χρόνο χρήσης της IP διεύθυνσης.


Server1
Client
Server2
Time
1 Discover DHCP servers
2 Servers offer IP address and config info
Collect offers, and select one
3 Request configuration from selected server2
4 Acknowledge request
Client is configured
Lease time nears expiration
5 Request lease renewal
6 Acknowledge request
Client finished with IP address
Release IP address 7

39. Ποια η διαφορά μεταξύ registered και dynamic ports

Απάντηση

Για να επικοινωνήσει ένα Η/Υ που ζητά μια υπηρεσία (client) με ένα άλλο Η/Υ που παρέχει υπηρεσίες (server), ο server ορίζει μια θύρα (port) στην οποία «ακούει». Η θύρα αυτή είναι ένας 16-bit αριθμός άρα ορίζονται συνολικά 65536 θύρες (από 0 έως 65535). Οι πρώτες 1024 θύρες θεωρούνται πασίγνωστες (well known ports) και αντιστοιχούν σε γνωστές εφαρμογές. Οι θύρες 1024 έως 49151 χρησιμοποιούνται από διάφορες εφαρμογές αλλά προηγείται δέσμευση τους μέσω διαδικασίας εγγραφής (registered ports) ενώ οι θύρες από 49152 έως 65535 χρησιμοποιούνται ελεύθερα (dynamic ports)

40. Ποιες από τις παραπάνω συναρτήσεις είναι blocking και ποιες όχι;

ssize_t send(int *socket*, const void **buffer*, size_t *length*, int *flags*);
ssize_t recv(int *socket*, void **buffer*, size_t *length*, int *flags*);
int connect(int sockfd, const struct sockaddr *serv_addr, socklen_t addrlen);
int accept(int s, struct sockaddr *addr, socklen_t *addrlen);
int sendto(int s, const void *msg, size_t len, int flags, const struct sockaddr *to, socklen_t tolen);
int recvfrom(int s, void *buf, size_t len, int flags, struct sockaddr *from, socklen_t *fromlen);

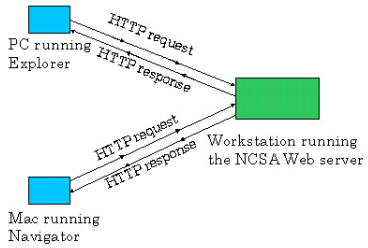
Απάντηση

Μια συνάρτηση είναι blocking όταν το πρόγραμμα δεν συνεχίζει να εκτελείται προτού λάβει μια απάντηση. Η συνάρτηση send, που εκτελείται από ένα TCP Server και/ή TCP Client για να στείλει δεδομένα στο socket, είναι blocking διότι αν δεν ληφθεί επιβεβαίωση από την άλλη πλευρά δηλ. από τον παραλήπτη, ο αποστολέας περιμένει και δεν συνεχίζει να εκτελείται. Επίσης η συνάρτηση recv που εκτελείται από ένα TCP Server και/ή TCP Client λαμβάνει δεδομένα από το socket και είναι blocking διότι αν δεν υπάρχουν δεδομένα από την άλλη πλευρά δηλ. από τον αποστολέα, ο παραλήπτης περιμένει συνεχώς μέχρι να λάβει δεδομένα και δεν συνεχίζει να εκτελείται. Αντίστοιχα οι συναρτήσεις sendto και recvfrom που εκτελούνται από ένα UDP Server και/ή UDP Client και έχουν ανάλογη λειτουργία με τις προηγούμενες είναι επίσης blocking συναρτήσεις.

41(Θ). Τι γνωρίζετε για το πρωτόκολλο HTTP;

Απάντηση

Το πρωτόκολλο HTTP (Hypertext Transfer Protocol) είναι το σύνολο των κανόνων για την μεταφορά του υπερκειμένου(hypertext) (το οποίο μπορεί να αντιστοιχεί σε αρχεία κειμένου, γραφικών, εικόνας, ήχου, video ή οποιουδήποτε multimedia αρχείου) μέσα στον Παγκόσμιο Ιστό (World Wide Web).
Το HTTP ορίζει τον τρόπο με τον οποίο οι πελάτες του Ιστού (π.χ. οι browsers) ζητούν (request) Ιστοσελίδες από τους εξυπηρετητές του Ιστού (π.χ. τους Web servers) και πως οι εξυπηρετητές μεταφέρουν τις Ιστοσελίδες στους πελάτες. Η βασική ιδέα της του πρωτοκόλλου αυτού φαίνεται στο παρακάτω σχήμα.



Όταν ο χρήστης ζητά μία Ιστοσελίδα, ο browser στέλνει ένα μήνυμα HTTP αίτησης (HTTP request), για τα διάφορα αντικείμενα της σελίδας, στον εξυπηρετητή. Ο εξυπηρετητής όταν λάβει το μήνυμα αυτό ανταποκρίνεται με μηνύματα HTTP απόκρισης (HTTP response) στα οποία περιέχονται τα αιτούμενα αντικείμενα.
Το HTTP χρησιμοποιεί το TCP ως πρωτόκολλο μεταφοράς. Αφού ο πελάτης εγκαταστήσει μία σύνδεση TCP με τον εξυπηρετητή αρχίζει την αποστολή μηνυμάτων – αιτήσεων προς αυτόν και τη λήψη μηνυμάτων – αποκρίσεων από αυτόν. Λόγω της χρήσης του TCP το HTTP δεν χρειάζεται να ασχοληθεί καθόλου με τη μεταφορά των δεδομένων. Το μόνο που πρέπει να κάνει είναι να στείλει τις αιτήσεις μέσω της TCP σύνδεσης και να περιμένει τις αποκρίσεις. Το TCP εγγυάται την αξιόπιστη μεταφορά των δεδομένων καθώς και τον έλεγχο της συμφόρησης.

42. Τι γνωρίζετε για το πρωτόκολλο SMTP;

Απάντηση

Το SMTP (Simple Mail Transfer Protocol) είναι το πρωτόκολλο του στρώματος εφαρμογών που χρησιμοποιείται για την μεταφορά των μηνυμάτων του ηλεκτρονικού ταχυδρομείου. Το SMTP χρησιμοποιεί ως πρωτόκολλο του στρώματος μεταφοράς το TCP και συγκεκριμένα τη θύρα 25 και βασικά έχει δύο τμήματα: την πλευρά του πελάτη (client side), που είναι ο εξυπηρετητής ταχυδρομείου του αποστολέα και την πλευρά του εξυπηρετητή (server side), που είναι ο εξυπηρετητής ταχυδρομείου του παραλήπτη. Ο κάθε εξυπηρετητής ταχυδρομείου μπορεί να παίξει το ρόλο είτε του πελάτη είτε του εξυπηρετητή: όταν αποστέλλει ένα μήνυμα έχει το ρόλο του πελάτη, ενώ όταν δέχεται μηνύματα έχει το ρόλο του εξυπηρετητή.

43 (Θ). Ένας νέος κόμβος συνδέθηκε σε ένα υποδίκτυο και θέλει να επισκεφθεί μια σελίδα που δεν έχει ξαναεπισκεφθεί. Περιγράψτε τη σειρά με την οποία θα χρησιμοποιήσει τα πρωτόκολλα DNS, ARP, HTTP για να το κατορθώσει. Θεωρήστε ότι ο χρήστης έχει δώσει χειροκίνητα κατάλληλη IP διεύθυνση στον κόμβο.

Απάντηση

Έστω ότι ένας χρήστης ζητά από τον browser να εμφανιστεί η σελίδα που έχει ως URL το http://www.ntua.gr/index.htm. Για να μπορέσει το μηχάνημα του χρήστη να στείλει μία HTTP αίτηση στον εξυπηρετητή Ιστού (Web server) www.ntua.gr, **το μηχάνημα του χρήστη πρέπει να μάθει την IP διεύθυνση του www.ntua.gr**. Αυτό γίνεται ως εξής:

- στο μηχάνημα του χρήστη, που λειτουργεί ως DNS πελάτης, ο browser αποσπά από το URL και περνά στον DNS πελάτη το www.ntua.gr
- Ως μέρος της DNS **ερώτησης (query)** ο DNS πελάτης στέλνει το όνομα του host (www.ntua.gr) στον DNS εξυπηρετητή
- Για να μπορέσει ο DNS εξυπηρετητής να βρει την IP διεύθυνση του host (www.ntua.gr) εκτελεί το πρωτόκολλο ARP και μαθαίνει τη φυσική διεύθυνση MAC του host. Ακολούθως επιστρέφεται το ζεύγος (IP, Φυσική διεύθυνση) από τον DNS εξυπηρετητή (server)
- Ο DNS πελάτης λαμβάνει την **απάντηση (reply) από τον** DNS εξυπηρετητή και μετά ο browser ανοίγει μία σύνδεση TCP με τον εξυπηρετητή HTTP που βρίσκεται στην συγκεκριμένη διεύθυνση IP
- Ο HTTP πελάτης (browser) εγκαθιστά μία σύνδεση **TCP** στην **θύρα 80** του εξυπηρετητή HTTP
- Στη συνέχεια ο πελάτης HTTP στέλνει ένα μήνυμα HTTP αίτησης ζητώντας το αρχείο index.htm
- Ο εξυπηρετητής στέλνει το αρχείο index.htm στον πελάτη μέσω ενός HTTP μηνύματος απόκρισης
- Ο HTTP εξυπηρετητής κλείνει την TCP σύνδεση (στην πραγματικότητα η TCP σύνδεση κλείνει όταν επιβεβαιωθεί η λήψη του αρχείου από τον πελάτη)
- Ο πελάτης HTTP (browser) λαμβάνει το αρχείο index.htm, κλείνει τη σύνδεση και απεικονίζει τα περιεχόμενά του στην οθόνη του χρήστη

44. Ποιες αρχιτεκτονικές εφαρμογών γνωρίζετε και να τις περιγράψετε;

Απάντηση

- Client-server
- Peer-to-peer (P2P)
- Hybrid of client-server and P2P

Α) Αρχιτεκτονική Client-server

Server:

- Τρέχει πάντα σε host (always-on host)
- Χρησιμοποιεί μόνιμες διευθύνσεις IP (permanent IP address)
- Χρησιμοποιούνται συμπλέγματα διακομιστών για την κλιμάκωση

Clients:

- Επικοινωνεί με τον server
- Μπορεί να είναι περιοδικά συνδεδεμένος
- Μπορεί να έχει δυναμικές διευθύνσεις
- Οι client δεν επικοινωνούν απευθείας μεταξύ τους

Β) Αρχιτεκτονική Peer-to-peer (P2P)

- Δεν βρίσκεται πάντα σε server (no always-on server)
- Αυθαίρετα τερματικά συστήματα επικοινωνούν άμεσα
- Οι κόμβοι συνδέονται περιοδικά και αλλάζουν τις IP διευθύνσεις τους
- Παρουσιάζουν μεγάλη δυνατότητα κλιμάκωσης αλλά είναι δύσκολα στη διαχείριση τους

Γ)Υβριδική Αρχιτεκτονική client-server και P2P

Εφαρμόζεται στο Skype

- Εφαρμογή voice-over-IP P2P
- Κεντρικοποιημένος (centralized) server: finding address of remote party:
- Σύνδεση client-client: απευθείας (όχι μέσω server)

Instant messaging

- το chatting μεταξύ 2 χρηστών είναι το P2P
- centralized service: client presence detection/location
  - user registers its IP address with central server when it comes online
  - user contacts central server to find IP addresses of buddies

45. Τι γνωρίζετε για τα πρωτόκολλα POP3 και IMAP

Απάντηση

Η διεθνής πρακτική στη χρήση του ηλεκτρονικού ταχυδρομείου (e-mail) στο Internet, έδειξε πως η πιο ευέλικτη λειτουργία της υπηρεσίας περιγράφεται από το παρακάτω μοντέλο:

- ο χρήστης διαθέτει τον προσωπικό του λογαριασμό σε έναν διακομιστή (mail server) κάπου στο Internet.
- χρησιμοποιεί εφαρμογές σε **γραφικό-παραθυρικό περιβάλλον** (Netscape Messenger, Microsoft Outlook, κλπ.) για να έχει:
  - **εύκολη και γρήγορη πρόσβαση** στο ηλεκτρονικό του γραμματοκιβώτιο (mailbox), τόσο για την αποστολή όσο και για τη λήψη των ηλεκτρονικών μηνυμάτων του.
  - **δυνατότητα οργάνωσης της αλληλογραφίας** του σε "φακέλους" για την καλύτερη διαχείρισή της.
- είναι πολύ σημαντικό και πρακτικό για το χρήστη, η πρόσβαση στο γραμματοκιβώτιό του να είναι **ομοιόμορφη** και **ανεξάρτητη από τον τρόπο σύνδεσής του στο Internet**. Αυτό καλύπτει:
  - τις πιθανές γεωγραφικές μετακινήσεις του χρήστη.
  - τον τρόπο πρόσβασης στο Internet(σύνδεση σε τοπικό δίκτυο ή σύνδεση με τηλεφωνική κλήση).

Τις παραπάνω ανάγκες προσπάθησε να καλύψει αρχικά το πρωτόκολλο **POP3**. Η μοναδική αλλά βασική έλλειψη του POP3 έγκειται στο ότι όταν η εφαρμογή του χρήστη συνδέεται με τον διακομιστή **μεταφέρει το γραμματοκιβώτιο στο σύνολό του** στον Η/Υ που βρίσκεται ο χρήστης. Τα **μειονεκτήματα** που προκύπτουν είναι:

- **καθυστέρηση** στη μεταφορά πληροφοριών (ειδικά όταν το γραμματοκιβώτιο είναι μεγάλο και η σύνδεση γίνεται με τηλεφωνική κλήση).
- **έλλειψη ασφάλειας**, διότι τα μηνύματα του χρήστη παραμένουν τοπικά στον Η/Υ που χρησιμοποίησε και είναι ορατά από οποιονδήποτε άλλο χρησιμοποιήσει τον ίδιο Η/Υ (εκτός αν τα σβήνει κάθε φορά αφού τα διαβάσει).
- **μη διαθεσιμότητα** των μηνυμάτων από άλλα σημεία του Internet, αν δεν έχει επιλέξει την παραμονή των μηνυμάτων στο διακομιστή. Τότε όμως, μεταφέρει κάθε φορά και τα παλιά μηνύματα.

Το πρωτόκολλο **IMAP** υλοποιήθηκε για να καλύψει τα παραπάνω κενά. Η βασική διαφορά με το POP3 είναι ότι όταν η εφαρμογή του χρήστη συνδέεται με τον διακομιστή **μεταφέρονται μόνο οι τίτλοι (subjects) των μηνυμάτων** στον Η/Υ που βρίσκεται ο χρήστης. Τα αντίστοιχα **πλεονεκτήματα** είναι:

- **γρήγορη μεταφορά** πληροφοριών διότι όσο μεγάλο και να είναι το γραμματοκιβώτιο μεταφέρεται μόνο μια γραμμή κειμένου για κάθε περιεχόμενο μήνυμα.
- **Ασφάλεια** στην ανάγνωση των μηνυμάτων, διότι παραμένουν πάντα στο διακομιστή και τα διαβάζει μόνο όποιος γνωρίζει τον προσωπικό κωδικό (password) του χρήστη.
- **Διαθεσιμότητα** των μηνυμάτων από οποιοδήποτε σημείο του Internet, αρκεί να ρυθμιστεί η εφαρμογή (netscape messenger, microsoft outlook) του χρήστη με τα προσωπικά του στοιχεία (username, password, e-mail address, mail server).

46. Τι γνωρίζετε για τις συνδέσεις HTTP

Απάντηση

Μη Μόνιμες (Nonpersistent) συνδέσεις HTTP

- Το πολύ 1 αντικείμενο μπορεί να στέλνεται σε μια TCP σύνδεση
- Τα μη μόνιμα στοιχεία HTTP:
  - Απαιτούν 2 RTTs για κάθε αντικείμενο
  - Υπάρχει overhead σε κάθε σύνδεση TCP
  - Οι browsers ανοίγουν παράλληλες συνδέσεις TCP συνδέσεις για να φέρουν αναφερόμενα αντικείμενα

Persistent HTTP

- Πολλαπλά objects μπορεί να σταλούν σε μια μοναδική TCP σύνδεση μεταξύ client και server.
- Τα μόνιμα στοιχεία HTTP
  - Ο server αφήνει τη σύνδεση ανοιχτή μετά την αποστολή απάντησης
  - Τα υπόλοιπα μηνύματα HTTP μεταξύ του ίδιου client/server στέλνονται μέσω της ανοιχτής σύνδεσης
  - Ο client στέλνει αιτήσεις αμέσως μόλις συναντήσει ένα αναφερόμενο αντικείμενο
  - Υπάρχει μόνο ένα RTT για όλα τα αναφερόμενα αντικείμενα

47.Ποια η διαφορά μεταξύ "μεταγωγής κυκλώματος" και "μεταγωγής εικονικού κυκλώματος"

Απάντηση

Η μεταγωγή εικονικού κυκλώματος είναι ένα είδος της μεταγωγής πακέτων όπου τα πακέτα ενός κόμβου ακολουθούν όλα την ίδια διαδρομή και φτάνουν στη σωστή σειρά με αποτέλεσμα να υπάρχει μικρός υπολογιστικός και επικοινωνιακός φόρτος. Η μεταγωγή κυκλώματος είναι μια τεχνική μεταγωγής στην οποία κάθε σύνδεσμος σπάει σε μικρότερα κομμάτια καθένα από τα οποία αντιστοιχείται αποκλειστικά σε μια και μόνο σύνοδο.

Πλήρης Απάντηση

- Κατά κανόνα, τα δεδομένα για να φτάσουν από την πηγή στον προορισμό τους χρησιμοποιούν πολλούς ενδιάμεσους κόμβους
- Η τεχνική αυτή ονομάζεται *μεταγωγή* και τα δίκτυα που τη χρησιμοποιούν ονομάζονται δίκτυα μεταγωγής *(switching networks)*
- Είδη Μεταγωγής:
  - Μεταγωγή Κυκλώματος
  - Μεταγωγή Πακέτου
    - Μεταγωγή Πακέτου με χρήση datagrams (αυτοδύναμα πακέτα)

- Μεταγωγή Πακέτου με χρήση Εικονικών Κυκλωμάτων

Μεταγωγή Κυκλώματος (Circuit switching)

- Υπάρχει αποκλειστικό επικοινωνιακό μονοπάτι (δημιουργείται φυσικό κύκλωμα) ανάμεσα σε 2 σταθμούς (αποστολέα και παραλήπτη)
- 3 φάσεις:
  - Αποκατάσταση κυκλώματος
  - Μεταφορά δεδομένων
  - Αποσύνδεση κυκλώματος
- Πρέπει να κρατηθεί χωρητικότητα καναλιού και εσωτερική χωρητικότητα μεταγωγής για αποκατάσταση σύνδεσης
- Οι μεταγωγείς πρέπει να έχουν τη νοημοσύνη να επινοούν μια διαδρομή μέσω του δικτύου
- Η αποκατάσταση του κυκλώματος είναι χρονοβόρα
- Η χωρητικότητα του καναλιού είναι κατειλημμένη για όλη τη διάρκεια της σύνδεσης
- Αν δεν υπάρχουν δεδομένα, η χωρητικότητα σπαταλιέται
- Όταν αποκατασταθεί το κύκλωμα το δίκτυο είναι ουσιαστικά διάφανο στους χρήστες
- Η επικοινωνία μεταξύ δύο μερών γίνεται εφόσον υπάρχει φυσικό κύκλωμα το οποίο συνδέει αποστολέα και παραλήπτη.
- Παράδειγμα: Τηλεφωνικό Δίκτυο

Μεταγωγή Πακέτου (Packet Switching)

- Τα δεδομένα μεταδίδονται σε μικρά πακέτα
- Το μήνυμα τεμαχίζεται από την πηγή
- Κάθε πακέτο περιέχει ένα τμήμα των δεδομένων συν την πληροφορία ελέγχου
- Σε κάθε κόμβο της διαδρομής το πακέτο παραλαμβάνεται, αποθηκεύεται προσωρινά και στέλνεται στον επόμενο κόμβο

Πλεονεκτήματα Μεταγωγής Πακέτου έναντι Μεταγωγής Κυκλώματος

- Η αποδοτικότητα της γραμμής είναι μεγαλύτερη, επειδή μια απλή σύνδεση κόμβου-με-κόμβο μπορεί να μοιράζεται δυναμικά σε πολλά πακέτα κάθε στιγμή
- Μπορεί να εκτελέσει μετατροπή ρυθμού δεδομένων. Δυο σταθμοί διαφορετικών ρυθμών δεδομένων μπορούν να ανταλλάξουν πακέτα επειδή ο καθένας συνδέεται στον κόμβο με το δικό του ρυθμό δεδομένων
- Στα δίκτυα Μεταγωγής Κυκλώματος μια κλήση μπορεί να μπλοκαριστεί. Σε ένα δίκτυο Μεταγωγής Πακέτου τα πακέτα εξακολουθούν να γίνονται αποδεκτά, αλλά αυξάνει η καθυστέρηση παράδοσης
- Μπορούν να χρησιμοποιηθούν προτεραιότητες. Πακέτα με προτεραιότητα που βρίσκονται σε κάποιο κόμβο μπορούν να σταλούν πρώτα, έχοντας μικρότερη καθυστέρηση

Μεταγωγή Πακέτου με χρήση Εικονικών Κυκλωμάτων (virtual circuit switching)

- Η επικοινωνία μεταξύ δύο μερών ξεκινά αφού βρεθεί και προκρατηθεί μονοπάτι από τον αποστολέα προς τον παραλήπτη.
- Η επικοινωνία γίνεται με την ανταλλαγή πακέτων (ειδικά πακέτα αίτησης κλήσης και αποδοχής κλήσης).
- Κάθε πακέτο δρομολογείται σύμφωνα με το πεδίο VCI (virtual circuit identifier)
  - Δεν χρειάζεται να αποφασιστεί ποια διαδρομή θα ακολουθήσει κάθε πακέτο ξεχωριστά
- Όλα τα πακέτα χρησιμοποιούν το ίδιο μονοπάτι.

48.Ποιοι είναι οι βασικοί τύποι γραμμών επικοινωνίας και σε τι διαφέρουν?

Απάντηση

Οι βασικοί τύποι γραμμών επικοινωνίας στα δίκτυα υπολογιστών, είναι η γραμμή από σημείο προς σημείο (point to point line), η γραμμή πολλαπλών σημείων (multipoint ή multi-drop line) και η επικοινωνία
ευρείας εκπομπής. Η γραμμή από σημείο προς σημείο, συνδέει δύο συγκεκριμένες τερματικές διατάξεις, και η πληροφορία μεταφέρεται από τη μια διάταξη στην άλλη. Το μήκος της γραμμής μπορεί να ποικίλλει, ενώ το είδος της μετάδοσης μπορεί να είναι μονόπλευρης (simplex), ημίπλευρης (half duplex) ή αμφίπλευρης (full duplex) κατεύθυνσης. Η γραμμή πολλαπλών σημείων, συνδέει δύο ή περισσότερες τερματικές διατάξεις σε μια γραμμή επικοινωνίας. Σε αυτόν τον τύπο γραμμής επικοινωνίας, η πληροφορία είναι δυνατόν να ξεκινά από ένα σημείο και να καταλήγει σε άλλα γνωστά σημεία. Ένα παράδειγμα τέτοιας σύνδεσης, αποτελεί και η συνδρομητική τηλεόραση όπου ο πομπός γνωρίζει από πριν τους δέκτες. Το σχήμα αυτό επιτρέπει την επικοινωνία μεταξύ απλών τερματικών διατάξεων, με χαμηλούς ρυθμούς μετάδοσης, που δεν διαθέτουν αποθηκευτικές δυνατότητες. Συνηθέστερη όμως είναι η χρησιμοποίηση του σχήματος αυτού, στην περίπτωση σύνθετων τερματικών διατάξεων, που διαθέτουν αποθηκευτικά μέσα, και μεταδίδουν σε υψηλούς ρυθμούς μετάδοσης. Τέλος, η γραμμή εκπομπής είναι μια απλή γραμμή επικοινωνίας, η οποία χρησιμοποιείται από όλες τις τερματικές διατάξεις που θέλουν να επικοινωνήσουν μεταξύ τους. Ένα κλασσικό παράδειγμα αυτού του είδους επικοινωνίας, είναι οι ραδιοφωνικές και οι τηλεοπτικές (μη συνδρομητικές) εκπομπές, όπου, ο κάθε ένας που διαθέτει ένα δέκτη (ραδιόφωνο ή τηλεόραση), μπορεί να ακούσει το πρόγραμμα που μεταδίδεται. Στο σχήμα αυτό, ο πομπός δεν γνωρίζει τον αριθμό των δεκτών μιας περιοχής, ο οποίος θεωρητικά μπορεί να είναι άπειρος. Αντίθετα, στη συνδρομητική η καλωδιακή τηλεόραση, όσοι λαμβάνουν το πρόγραμμα, είναι νόμιμα εγγεγραμμένοι συνδρομητές, στην εταιρεία παροχής της αντίστοιχης υπηρεσίας.

49.Τι σημαίνει πολυπλεξία στη μετάδοση δεδομένων;

Απάντηση

Η τεχνική της πολυπλεξίας (multiplexing) μπορεί να ορισθεί ως η διαδικασία μεταφοράς περισσότερων από ένα σημάτων χρησιμοποιώντας την ίδια γραμμή επικοινωνίας. Με τον τρόπο αυτό είναι δυνατή η χρήση του ιδίου μέσου μετάδοσης από πολλούς υπολογιστές, οι οποίοι μπορούν να χρησιμοποιήσουν το ίδιο κανάλι για την εκπομπή και τη λήψη της πληροφορίας, χωρίς τα σήματα που εκπέμπονται από αυτούς, να αλληλεπιδρούν μεταξύ τους. Αυτή η από κοινού χρήση των εγκατεστημένων γραμμών μεταφοράς, μειώνει δραστικά το κόστος εγκατάστασης του δικτύου, και επιτρέπει την καλύτερη εκμετάλλευση της χωρητικότητας του καναλιού.

50.Ποια είναι τα χαρακτηριστικά της πολυπλεξίας επιμερισμού συχνότητας;

Απάντηση

Στην πολυπλεξία επιμερισμού συχνότητας (Frequency Division Multiplexing - FDM), το εύρος ζώνης (bandwidth) του μέσου μετάδοσης υποδιαιρείται σε πολλές μικρότερες ζώνες συχνότητας, οι οποίες ονομάζονται λογικά κανάλια. Κάθε ένα από αυτά τα κανάλια αποδίδεται σε κάθε ένα από τους σταθμούς του συστήματος, οι οποίοι μπορούν να εκπέμψουν ταυτόχρονα, ο καθένας στο δικό του ξεχωριστό κανάλι, πάνω στο οποίο έχει την αποκλειστική χρήση.

51. Σε τι διαφέρουν και σε τι μοιάζουν οι τεχνικές πολυπλεξίας επιμερισμού συχνότητας και χρόνου;

Απάντηση

Η βασική διαφορά που υφίσταται ανάμεσα στην πολυπλεξία επιμερισμού συχνότητας και στην πολυπλεξία επιμερισμού χρόνου, είναι ο διαφορετικός τρόπος κατανομής του καναλιού στους σταθμούς του δικτύου. Στην πολυπλεξία επιμερισμού συχνότητας τα σήματα διαχωρίζονται στην περιοχή συχνοτήτων και εκπέμπονται ταυτόχρονα, ενώ στην πολυπλεξία επιμερισμού χρόνου, τα σήματα διαχωρίζονται χρονικά αλλά εκπέμπονται στην ίδια περιοχή συχνοτήτων, και χρησιμοποιώντας ολόκληρο το εύρος ζώνης του μέσου μετάδοσης. Από πρακτική άποψη, η πολυπλεξία επιμερισμού χρόνου, φαίνεται πως υπερτερεί της πολυπλεξίας επιμερισμού συχνότητας, σε δύο βασικά σημεία. Το πρώτο σημείο, είναι η καθαρά ψηφιακή φύση του εξοπλισμού που χρησιμοποιείται – και που σε γενικές γραμμές περιλαμβάνει ένα πολυπλέκτη και ένα συλλέκτη – η οποία οδηγεί σε αξιόπιστη κατασκευαστική απλότητα και σε αποδοτική λειτουργία (αυτό δεν ισχύει για τον εξοπλισμό που χρησιμοποιείται στην πολυπλεξία επιμερισμού συχνότητας, και ο οποίος είναι καθαρά αναλογικός). Το δεύτερο σημείο αφορά την απουσία ανεπιθύμητων φαινομένων που εμφανίζονται στην πολυπλεξία επιμερισμού συχνότητας, όπως είναι η διασταύρωση σημάτων (cross-talk) και ο θόρυβος ενδοδιαμόρφωσης. Αυτά τα φαινόμενα οφείλονται στην ταυτόχρονη μετάδοση πολλών σημάτων σε διαφορετικές ζώνες συχνοτήτων, κάτι που δε συμβαίνει στην πολυπλεξία επιμερισμού χρόνου, όπου σε κάθε χρονική στιγμή, μόνο ένα σήμα διαρρέει το κανάλι.

52. Τι είναι η στατιστική πολυπλεξία?

Απάντηση

Η στατιστική πολυπλεξία αποτελεί μια βελτίωση της πολυπλεξίας επιμερισμού χρόνου, και έχει ως στόχο να μειώσει τα προβλήματα που παρουσιάζονται σε αυτή. Το πιο βασικό από αυτά τα προβλήματα είναι η αναποτελεσματική χρήση της χωρητικότητας της γραμμής εξόδου, σε περιπτώσεις κατά τις οποίες υπάρχουν τερματικά που δεν στέλνουν δεδομένα στο κανάλι. Επειδή η πολυπλεξία επιμερισμού χρόνου χρησιμοποιείται κατά κύριο λόγο στη σύγχρονη μετάδοση, είναι προφανές πως εάν κάποιο τερματικό δεν έχει να στείλει δεδομένα, θα λάβει χώρα αποστολή εικονικών χαρακτήρων (dummy characters), προκειμένου να διατηρηθεί ο συγχρονισμός ανάμεσα στον πομπό και στο δέκτη. Αυτό όμως σημαίνει κακή διαχείριση της χωρητικότητας του καναλιού επικοινωνίας. Σε αντίθεση με τη συνήθη πολυπλεξία επιμερισμού χρόνου όπου η χωρητικότητα της γραμμής εξόδου του πολυπλέκτη ισούται με το άθροισμα της χωρητικότητας των γραμμών εισόδου που συνδέονται σε αυτόν, στη στατιστική πολυπλεξία (statistical multiplexing), χρησιμοποιείται μια γραμμή εξόδου, με μικρότερη χωρητικότητα. Αυτή η μέθοδος ονομάζεται συγκέντρωση (concentration), ενώ οι πολυπλέκτες οι οποίοι λειτουργούν με τον τρόπο αυτό, ονομάζονται στατιστικοί πολυπλέκτες ή συγκεντρωτές (concentrators). Αυτοί οι πολυπλέκτες λειτουργούν με το μέσο όρο των ροών κυκλοφορίας δεδομένων των γραμμών εισόδου που συνδέονται σε αυτούς, και χρησιμοποιούνται κυρίως στην ασύγχρονη μετάδοση δεδομένων (asynchronous data transmission) όπου τα μηνύματα έρχονται από τα τερματικά με τυχαίο ρυθμό, και αποθηκεύονται προσωρινά μέχρι τελικά να σταλούν όλα μαζί, μέσα από τη μια και μοναδική γραμμή εξόδου. Επειδή το μήκος του κάθε μηνύματος γενικά μπορεί να είναι οποιοδήποτε, λαμβάνει χώρα προσθήκη επί του μηνύματος ενός προθέματος (prefix), που περιέχει τη διεύθυνση του αποστολέα και του παραλήπτη, καθώς επίσης και οτιδήποτε σχετικό με την προτεραιότητα διακίνησης του μηνύματος από σημείο σε σημείο.

53. Σε τι διαφοροποιείται η στατιστική πολυπλεξία, από την πολυπλεξία επιμερισμού χρόνου?

Απάντηση

Όπως έχει ήδη αναφερθεί στην προηγούμενη παράγραφο, η βασική διαφορά που υφίσταται ανάμεσα στην πολυπλεξία επιμερισμού χρόνου και στη στατιστική πολυπλεξία, είναι η τιμή της χωρητικότητας της μιας και μοναδικής γραμμής εξόδου του πολυπλέκτη, η οποία, στην περίπτωση της συνήθους πολυπλεξίας επιμερισμού χρόνου, ισούται με το άθροισμα των χωρητικοτήτων των γραμμών εισόδου που συνδέονται στον πολυπλέκτη, ενώ στη στατιστική πολυπλεξία, η χωρητικότητα αυτή έχει μικρότερη τιμή. Πιο συγκεκριμένα, ο πολυπλέκτης λειτουργεί με το μέσο όρο των χωρητικοτήτων των γραμμών εισόδου, κάτι που σημαίνει πως για να λειτουργήσει σωστά αυτό το σχήμα, θα πρέπει ο μέσος φόρτος της γραμμής κάθε τερματικής διάταξης, να είναι σχετικά μικρός, έτσι ώστε να είναι δυνατή η ταυτόχρονη μεταφορά δεδομένων από όλες τις τερματικές διατάξεις. Η στατιστική πολυπλεξία εφαρμόζεται πολύ πιο αποτελεσματικά στην ασύγχρονη μετάδοση δεδομένων, όπου ο ρυθμός αποστολής δεδομένων από τις τερματικές διατάξεις προς τον πολυπλέκτη είναι τυχαίος και ακανόνιστος. Αυτό σημαίνει πως αν και στην πραγματικότητα ο ρυθμός αποστολής δεδομένων από τις τερματικές διατάξεις, είναι ίσος με το μέσο όρο των ρυθμών μεταφοράς όλων των σταθμών, στην πράξη, εάν κάποιοι άλλοι σταθμοί δεν στέλνουν δεδομένα, η τερματική διάταξη μπορεί να ζητήσει και να πάρει μεγαλύτερο ποσοστό χωρητικότητας του καναλιού. Με τον ίδιο τρόπο όμως ενδέχεται να λάβει χώρα μείωση της διαθέσιμης χωρητικότητας προς τον κάθε σταθμό, κάτι που

γίνεται σε περιπτώσεις κατά τις οποίες η κυκλοφορία στο δίκτυο είναι αυξημένη. Αυτό βεβαίως δεν ισχύει στη συνήθη πολυπλεξία επιμερισμού χρόνου, όπου ο ρυθμός μεταφοράς δεδομένων από τον τερματικό σταθμό προς τον πολυπλέκτη, είναι σταθερός και προκαθορισμένος.

54. Τι γνωρίζετε για το επίπεδο Συνδέσμου μετάδοσης δεδομένων (`data link layer`)

Απάντηση

Το επίπεδο αυτό του μοντέλου OSI παρέχει τις παρακάτω λειτουργίες:

- Επιτρέπει σε μία συσκευή να εισέλθει στο δίκτυο, να στέλνει και να λαμβάνει μηνύματα.
- Προσφέρει μία φυσική διεύθυνση ώστε τα δεδομένα της συσκευής να στέλνονται στο δίκτυο.
- Συνεργάζεται με το λογισμικό δικτύου της συσκευής κατά την αποστολή και λήψη μηνυμάτων.
- Προσφέρει τη δυνατότητα ανίχνευσης λαθών.

Κοινά δικτυακά τα οποία λειτουργούν στο επίπεδο 2 περιλαμβάνουν:

- Κάρτες δικτύου
- Ehternet και Token-Ring Switches
- Γέφυρες (Bridges)

Οι κάρτες δικτύου έχουν μια διεύθυνση επιπέδου 2 ή μια διεύθυνση MAC. Το Switch χρησιμοποιεί τη διεύθυνση αυτή για να φιλτράρει και να προωθεί την κίνηση με σκοπό την αποφυγή της συμφόρησης και συγκρούσεων σε κάποιο τομέα του δικτύου.

Οι γέφυρες και τα switches λειτουργούν με παρόμοιο τρόπο. Παρόλα αυτά οι γέφυρες είναι ένα κομμάτι λογισμικού, ενώ τα switches χρησιμοποιούν τα ASICs (Application-Specific Integrated Circuits) για να εκτελέσουν το έργο τους σε σχετικό hardaware.

55. Τι γνωρίζετε για το επίπεδο μεταφοράς (`transport layer`)

Απάντηση

Το επίπεδο μεταφοράς του μοντέλου προσφέρει end-to-end επικοινωνία μεταξύ των τελικών συσκευών μέσω ενός δικτύου. Ανάλογα με την εφαρμογή, το επίπεδο μεταφοράς προσφέρει αξιόπιστη, συνδεσμοστρεφής ή ασυνδεσμική, και όσο το δυνατόν βέλτιστη επικοινωνία.

Μερικές από τις λειτουργίες που προσφέρονται από το επίπεδο αυτό είναι οι εξής:

- ταυτοποίηση εφαρμογής
- ταυτοποίηση του client
- επιβεβαίωση παράδοσης και ακεραιότητας του μηνύματος
- τμηματοποίηση των δεδομένων για την μεταφορά
- έλεγχος της ροής δεδομένων με σκοπό την αποφυγή υπερχείλισης μνήμης
- εγκαθίδρυση και συντήρηση και των δύο άκρων του εικονικού κυκλώματος
- ανίχνευση σφαλμάτων κατά την μετάδοση
- διάταξη των πακέτων δεδομένων στη σωστή σειρά στον παραλήπτη
- πολυπλεξία πολλαπλών διαμοιραζόμενων συνόδων πάνω από ένα μοναδικό φυσικό σύνδεσμο

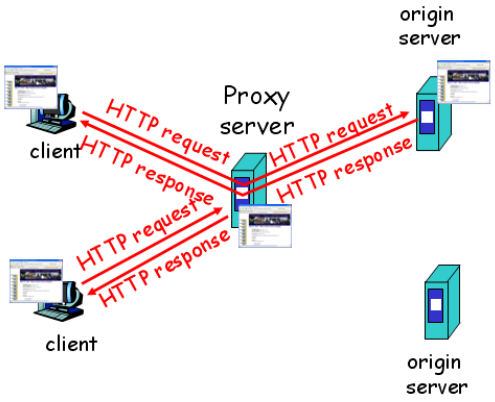
Τα πιο γνωστά πρωτόκολλα μεταφοράς είναι το συνδεσμοστρεφές TCP (Trsansmission Control Protocol) και το ασυνδεσμικό UDP (User Datagramm Protocol).

56. Τι γνωρίζετε για τον proxy server και γενικά για το web caching;

Απάντηση

Ο proxy server μόλις λάβει αίτηση από κάποιον client μπορεί να τον εξυπηρετήσει απευθείας χωρίς τη μεσολάβηση του τελικού (origin) server. Συγκεκριμένα μόλις ο proxy server λάβει αίτηση από ένα client ελέγχει την cache του για το αν υπάρχει σε αυτή το

ζητούμενο αντικείμενο. Αν ναι το δίνει κατευθείαν στον client, αλλιώς το παίρνει από τον origin server όπως δείχνει και η ακόλουθη εικόνα:



Τα πλεονεκτήματα του web-caching είναι τα εξής:

- Μειώνει το χρόνο απόκρισης στις αιτήσεις του client, δηλ. η απάντηση στον client είναι πιο γρήγορη
- Μειώνει το φόρτο κυκλοφορίας στις γραμμές

57. Ποια τα επίπεδα του IP και ποια πρωτόκολλα λειτουργούν σε κάθε ένα επίπεδο;

Απάντηση

✓ Εφαρμογής (Application): υποστηρίζει δικτυακές εφαρμογές
  - Πρωτόκολλα FTP, SMTP, HTTP

✓ Μεταφοράς (transport): επεξεργάζεται μεταφορά δεδομένων
  - Πρωτόκολλα TCP, UDP

✓ Δικτύου (network): Δρομολόγηση datagrams από αποστολέα σε παραλήπτη
  - Πρωτόκολλο IP και πρωτόκολλα δρομολόγησης

✓ Συνδέσμου Δεδομένων (link): μεταφορά δεδομένων μεταξύ γειτονικών δικτυακών στοιχείων
  - Πρωτόκολλα PPP, Ethernet

✓ Φυσικό (physical): μετάδοση bits στο φυσικό μέσο (καλώδιο)

58. Ποια η λειτουργία του επιπέδου δικτύου (link layer) ;

Απάντηση

✓ ;Έλεγχος Ροής (flow control):
  - Ελέγχεται η ροή κυκλοφορίας μεταξύ διαδοχικών κόμβων

✓ Ανίχνευση Λαθών (error detection):
  - Σφάλματα θορύβου.
  - Ο δέκτης ανιχνεύει σφάλματα
    - Στέλνει σήμα στον αποστολέα είτε να επαναμεταδώσει το μήνυμα είτε απορρίπτει το πακέτο

✓ Διόρθωση λαθών (error correction):
  - Ο δέκτης αναγνωρίζει και διορθώνει λάθη χωρίς να καταφεύγει σε αναμετάδοση

✓ Γραμμές half-duplex και full-duplex
  - Με γραμμές half duplex, οι κόμβοι μπορούν να μεταδίδουν ταυτόχρονα και στις 2 κατευθύνσεις

59. Τι γνωρίζετε για τις γραμμές του πρωτοκόλλου MAC ;

Απάντηση

Υπάρχουν 2 τύποι γραμμών (“links”)

✓ point-to-point
  - PPP για προσπέλαση dial-up
  - point-to-point γραμμή μεταξύ Ethernet switch και host

✓ broadcast
  - old-fashioned Ethernet
  - upstream HFC
  - 802.11 wireless LAN

60.

Θεωρήστε ένα τοπικό δίκτυο (LAN) με εύρος διευθύνσεων 150.139.131.0/24 στο οποίο είναι συνδεδεμένοι οι υπολογιστές ενός εργαστηρίου χρησιμοποιώντας τις κάρτες δικτύου Ethernet. Ένα PC στο εργαστήριο (PC1), στο οποίο έχει αποδοθεί η IP διεύθυνση 150.139.131.11 θέλει να επικοινωνήσει για πρώτη φορά με ένα άλλο PC του εργαστηρίου (PC2) το οποίο έχει τη διεύθυνση 150.139.131.7. Περιγράψτε τη διαδικασία με την οποία το PC1 θα ανακαλύψει, γνωρίζοντας μόνο την IP διεύθυνση του PC2, για ποιο μηχάνημα πρόκειται (ποια είναι η MAC διεύθυνση της κάρτας δικτύου του) ώστε να στείλει τα δεδομένα στο Ethernet επίπεδο. Περιγράψτε πώς απλοποιείται η διαδικασία τις επόμενες φορές που το PC1 θα θελήσει να επικοινωνήσει με το PC2.

Απάντηση

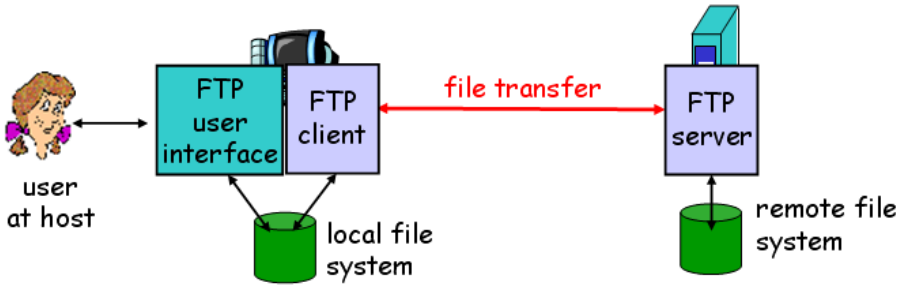
Τα δίκτυα TCP/IP χρησιμοποιούν τόσο τις IP διευθύνσεις όσο και τις MAC διευθύνσεις των συνδεδεμένων Η/Υ. Η διεύθυνση IP που έχει αντιστοιχηθεί σε ένα Η/Υ μπορεί να αλλάξει, αλλά η διεύθυνση MAC είναι σταθερή και δεν αλλάζει ποτέ. Οι Η/Υ που συνδέονται στο ίδιο TCP/IP τοπικό δίκτυο μπορούν να ανακαλύπτουν τη διεύθυνση MAC των άλλων Η/Υ του δικτύου στο οποίο είναι συνδεδεμένοι. Αυτό είναι εφικτό μέσω του πρωτοκόλλου ARP (Address Resolution Protocol). Με το πρωτόκολλο ARP κάθε Η/Υ διατηρεί μια λίστα με τις IP και MAC διευθύνσεις για κάθε συσκευή με την οποία έχει επικοινωνήσει πρόσφατα. Το πρωτόκολλο ARP μετατρέπει μια διεύθυνση IP στην αντίστοιχη φυσική διεύθυνση δικτύου. Το πρωτόκολλο ARP λειτουργεί στο 2ο επίπεδο του μοντέλου OSI.

Στο συγκεκριμένο παράδειγμα όταν το PC1, με IP 150.139.131.11, θέλει να επικοινωνήσει για 1η φορά με το 2ο PC του εργαστηρίου με IP 150.139.131.7, πρέπει πρώτα να εντοπίσει την διεύθυνση MAC του 2ου PC. Αυτές οι αντιστοιχήσεις διεύθυνση IP- διεύθυνση MAC λαμβάνονται από την **ARP cache** που υπάρχει σε κάθε PC. Αν η διεύθυνση του 2ου PC με το οποίο θέλουμε να γίνει η επικοινωνία δεν υπάρχει στην cache του 1ου PC, τότε το 1ο PC δεν μπορεί να στείλει απευθείας μηνύματα στο 2ο, αλλά πρέπει να λάβει πρώτα μια νέα αντιστοίχηση (δηλ. να προσθέσει στην cache του την αντιστοίχηση IP-MAC του 2ου PC). Για να γίνει αυτό το 1ο PC (με IP 150.139.131.11) στέλνει (broadcasts) ένα μήνυμα (που περιλαμβάνει την IP του 2ου PC μαζί με μια ARP αίτηση) σε όλο το τοπικό δίκτυο. Το 2ο PC που έχει τη δοθείσα IP (δηλ. την IP 150.139.131.7) στέλνει μια απάντηση ARP δηλ στέλνει τη διεύθυνση MAC του), επιτρέποντας στο 1ο PC (με IP 150.139.131.11) να ενημερώσει την cache του και να προχωρήσει πλέον στην αποστολή του μηνύματος στο 2ο PC.

Τις επόμενες φορές που το PC1 θέλει να επικοινωνήσει με το PC 2 τότε, όπως αναφέραμε και πιο πριν, η αντιστοίχηση της IP-MAC θα υπάρχει στην cache του 1ου PC οπότε θα γνωρίζει την IP διεύθυνση και τη MAC διεύθυνση του 2ου PC και μπορεί να στείλει απευθείας πλέον μήνυμα σε αυτό.

61. Δώστε παράδειγμα εφαρμογής για το πρωτόκολλο `FTP` ;

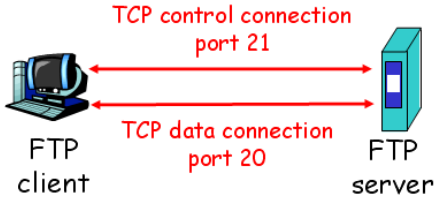
Απάντηση



- Μεταφορά αρχείων από/προς τον server (remote host)
- Μοντέλο client/server
  - *client:* αυτός που αρχικοποιεί τη μεταφορά (either to/from remote)
  - *server:* remote host

- Ο FTP client επικοινωνεί με τον FTP server στο port 21, Το πρωτόκολλο μεταφοράς είναι TCP
- Ο client αναγνωρίζεται μέσω ελέγχου γραμμής
- Ο client στέλνει εντολές στον server μέσω της γραμμής
- Όταν ο server εντολές μεταφοράς αρχείων ανοίγει μια 2η TCP σύνδεση με τον client
- Όταν μεταφέρει ένα αρχείο κλείνει τη σύνδεση
- Ο server ανοίγει άλλη TCP σύνδεση για να μεταφέρει άλλο αρχείο

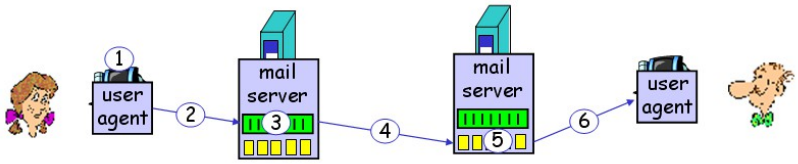
Η επικοινωνία φαίνεται στο ακόλουθο σχήμα:



62. Δώστε παράδειγμα εφαρμογής για το πρωτόκολλο SMTP ;
Απάντηση

1. Ο χρήστης Α στέλνει ένα μήνυμα σε μια διεύθυνση π.χ. bob@someschool.edu
2. Το μήνυμα τοποθετείται στην ουρά μηνυμάτων (message queue) του χρήστη Β (παραλήπτης)
3. Η πλευρά πελάτη του SMTP ανοίγει TCP σύνδεση με τον mail server του χρήστη Α
4. Ο πελάτης SMTP στέλνει το μήνυμα του Α μέσω της σύνδεσης TCP
5. Ο mail server του Β τοποθετεί το μήνυμα στο mailbox του χρήστη Β
6. Ο χρήστης Β ζητά να διαβάσει το μήνυμα

Τα βήματα φαίνονται στο ακόλουθο σχήμα:



63. Δώστε παράδειγμα εφαρμογής για το πρωτόκολλο HTTP όταν θέλουμε να προσπελάσουμε το URL www.someSchool.edu/someDepartment/home.index που περιλαμβάνει κείμενο και αναφορές σε 10 εικόνες jpeg
Απάντηση

1a. Ο πελάτης HTTPαρχικοποιεί τη σύνδεση TCP στον server HTTP (process) στο www.someSchool.edu στο port 80

1b. Ο HTTP server στο host www.someSchool.edu περιμένει για την TCP σύνδεση στο 80. Αποδέχεται τη σύνδεση και ειδοποιεί τον πελάτη client

2 Ο πελάτης HTTP client στέλνει μηνύματα αίτησης HTTP (request message) (περιέχει την URL) στο TCP connection socket. Το μήνυμα υποδηλώνει ότι ο πελάτης θέλει τη σελίδα someDepartment/home.index

3 Ο HTTP server λαμβάνει μηνύματα αίτησης, σχηματίζει απαντητικό μήνυμα (response message) που περιλαμβάνουν το ζητούμενο αντικείμενο και στέλνει το μήνυμα στο socket

4. Ο HTTP server κλείνει τη σύνδεση TCP

5 Ο HTTP πελάτης λαμβάνει την απάντηση με το αρχείο html, εμφανίζει το html. Σαρώνει το αρχείο html, εντοπίζει 10 αναφερόμενα αντικείμενα jpeg

6 Τα βήματα 1-5 επαναλαμβάνονται για καθένα από τα 10 αντικείμενα jpeg

64. Ποια τα χαρακτηριστικά των μέσων μετάδοσης;
Απάντηση
Έχουν δύο βασικά χαρακτηριστικά:

- Εύρος ζώνης (bandwidth): ορίζεται ως η διαφορά μεταξύ των τιμών της μέγιστης και ελάχιστης συχνότητας.
- Χωρητικότητα (capacity): ορίζεται ως ο μέγιστος ρυθμός με τον οποίο μπορούν να αποσταλούν ή να παραληφθούν δεδομένα, χωρίς να προκύψουν σφάλματα κατά τη διάρκεια της μετάδοσης.

65. Πως γίνεται ο διαχωρισμός δικτύων με βάση τη γεωγραφική διασπορά;
Απάντηση

- Τοπικά Δίκτυα (LAN – Local Area Networks): Δίκτυα στο επίπεδο ενός κτηρίου ή ενός συγκροτήματος κτηρίων.

- Μητροπολιτικά Δίκτυα (MAN – Metropolitan Area Networks): Δίκτυα στο επίπεδο ενός μεγάλου αστικού κέντρου, ή ενός συνόλου μικρότερων δήμων που συνήθως έχουν τη μορφή ενός ή πολλαπλών δακτυλίων και συμπληρωματικών υποδομών πρόσβασης.
- Δίκτυα Ευρείας Ζώνης (WAN – Wide Area Networks): Δίκτυα εθνικού ή και υπερεθνικού επιπέδου που συνήθως έχουν τη μορφή αραιού πλέγματος με κόμβους σε μεγάλα αστικά κέντρα.

66.Ποιές οι διαφορές μεταξύ LAN και WAN;
Απάντηση

LAN

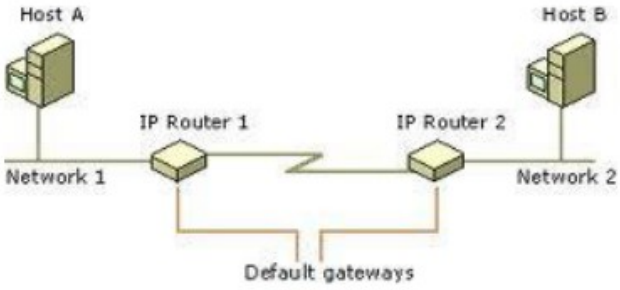
- Καλύπτει μικρή γεωγραφική περιοχή
- Διασυνδέει σταθμούς εργασίας, εξυπηρετητές, εκτυπωτές κ.α.
- Για την διασύνδεση των συσκευών στο LAN χρησιμοποιείται κάποιο switch

WAN

- Καλύπτει μεγάλη γεωγραφική περιοχή
- Διασυνδέει μεταξύ τους διαφορετικά τοπικά δίκτυα
- Για την διασύνδεση των διαφορετικών τοπικών δικτύων χρησιμοποιείται συνήθως κάποιος router

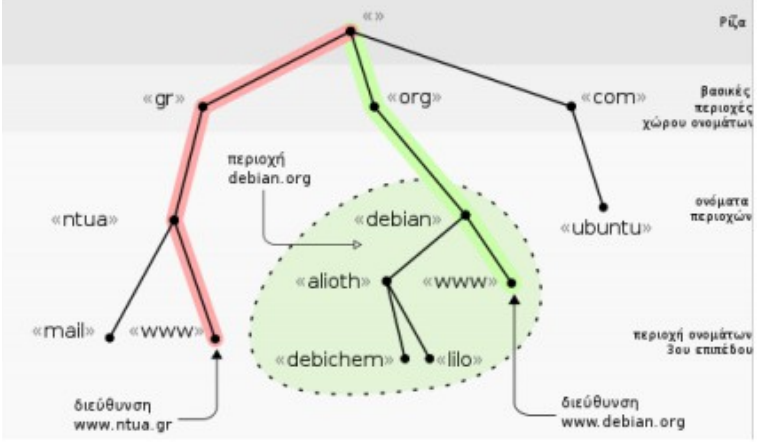
67.Τι ονομάζεται Gateway;
Απάντηση

- Σε ένα δίκτυο υπολογιστών, μια πύλη (gateway)είναι ένας κόμβος (δρομολογητής) που χρησιμεύει ως ένα σημείο πρόσβασης σε άλλο δίκτυο.
- Η προεπιλεγμένη πύλη (default gateway) είναι ο κόμβος στο δίκτυο υπολογιστών που το δικτυακό λογισμικό (network stack στο λειτουργικό) χρησιμοποιεί όταν η IP διεύθυνση δεν ταιριάζει με καμία άλλη στον πίνακα δρομολόγησης.

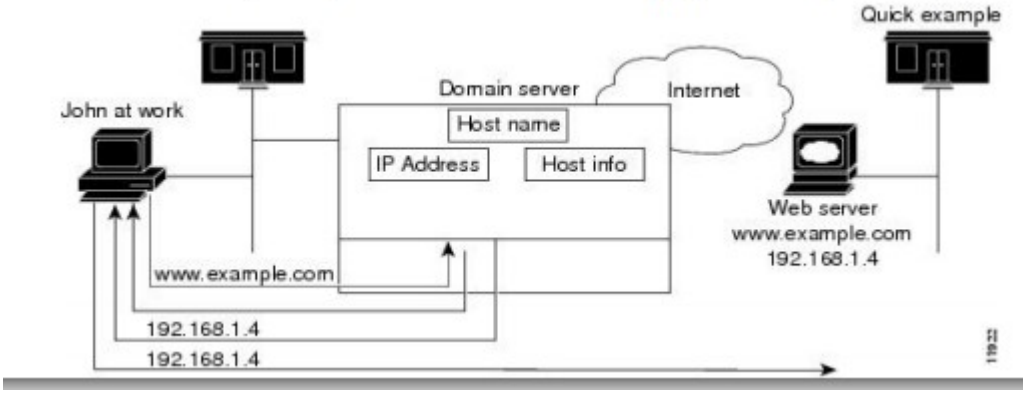


68.Τι είναι το DNS;
Απάντηση

- Το Domain Name System ή DNS (Σύστημα Ονομάτων Τομέων ή Χώρων ή Περιοχών) είναι ένα ιεραρχικό σύστημα ονοματοδοσίας για υπολογιστές, υπηρεσίες και οποιοδήποτε άλλο δικτυακό πόρο συνδέεται σε δίκτυο με πρωτόκολλο IP.



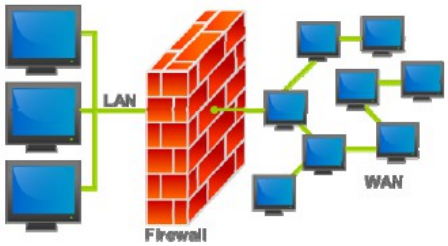
- Το πρωτόκολλο DNS μπορεί και αντιστοιχίζει ονόματα με διευθύνσεις IP



68.Τι είναι το Firewall, Mac Address Filtering και το SNMP;

Απάντηση

1. Το Firewall (Τείχος προστασίας) είναι κάποια συσκευή ή πρόγραμμα που έχει την δυνατότητα (με κατάλληλες ρυθμίσεις) να επιτρέπει ή να απορρίπτει πακέτα δεδομένων που περνούν από ένα δίκτυο σε άλλο. Τα Firewalls χρησιμοποιούνται συχνά για την προστασία των δικτύων υπολογιστών από μη εξουσιοδοτημένη πρόσβαση.



2. MAC address filtering είναι η μέθοδος προστασίας δικτύου όπου η πρόσβαση στο δίκτυο βασίζεται στην MAC address κάθε κάρτας δικτύου. Όπως είναι γνωστό, κάθε κάρτα δικτύου έχει μοναδική MAC address. Επομένως, η MAC address filtering επιτρέπει ή απαγορεύει πρόσβαση στο δίκτυο σε συγκεκριμένες συσκευές.

3. Το SNMP (Simple Network Management Protocol) είναι ένα πρωτόκολλο διαχείρισης δικτύων. Χρησιμοποιείται για την παρακολούθηση και τη διαχείριση των δικτυακών συσκευών.

69.Ποια η διαφορές μεταξύ μιας MAC address και μιας IP address;

Απάντηση

- Κάθε κάρτα δικτύου (network adapter) χαρακτηρίζεται από μια MAC διεύθυνση (48 bits)
- Η MAC διεύθυνση χαρακτηρίζει «μοναδικά» ένα υπολογιστή σε ένα τοπικό δίκτυο (LAN). Χρησιμοποιείται για την δρομολόγηση στο Data Link layer του OSI (2ο επίπεδο του μοντέλου OSI)
- Η IP διεύθυνση χαρακτηρίζει «μοναδικά» ένα υπολογιστή στο διαδίκτυο. Χρησιμοποιείται για την δρομολόγηση στο Network layer του OSI (3ο επίπεδο του μοντέλου OSI)
- Η MAC διεύθυνση χαρακτηρίζει την κάρτα δικτύου και δεν μπορεί να αλλαχθεί από τον χρήστη, ενώ η IP διεύθυνση μπορεί (και ίσως πρέπει) να αλλάξει καθώς ο υπολογιστής μετακινείται από ένα δίκτυο σε άλλο
- Τα IP δίκτυα κρατάνε μια αντιστοίχηση μεταξύ της IP διεύθυνσης μιας συσκευής και της MAC διεύθυνσης της συσκευής. Αυτή η αντιστοίχηση είναι γνωστή σαν ARP cache ή ARP table

70.Ποιές οι διαφορές μεταξύ TCP και UDP πρωτοκόλλου;

Απάντηση

Θεωρία

Ποιές οι διαφορές μεταξύ TCP και UDP πρωτοκόλλου;

Απάντηση

Το πρωτόκολλο TCP λειτουργεί εγκαθιδρύοντας συνδέσεις μεταξύ του αποστολέα και του παραλήπτη των πακέτων. Από τη στιγμή που μία σύνδεση εγκαθιδρυθεί με επιτυχία, όλα τα δεδομένα αποστέλλονται από τον ένα υπολογιστή στον άλλο με την μορφή πακέτων χρησιμοποιώντας τη σύνδεση αυτή. Τα κύρια **χαρακτηριστικά του TCP** είναι τα εξής:

- **Αξιοπιστία**- Το TCP χρησιμοποιεί διάφορους μηχανισμούς ούτως ώστε να διασφαλιστεί ότι τα πακέτα που μεταδίδονται από τον αποστολέα θα φτάσουν σίγουρα στον παραλήπτη και στην σωστή σειρά. Οι μηχανισμοί αυτοί περιλαμβάνουν την επιβεβαίωση λήψης πακέτου από τον παραλήπτη, την επαναποστολή πακέτων που χάθηκαν και τον καθορισμό ενός ελάχιστου χρονικού διαστήματος μέσα στο οποίο κάθε αποστελλόμενο πακέτο θα πρέπει να έχει παραληφθεί (timeout). Στην περίπτωση που χαθεί κάποιο πακέτο, ο αποστολέας προσπαθεί και πάλι να το ξαναστείλει. Επίσης, εάν ο παραλήπτης διαπιστώσει ότι ένα πακέτο δεν του έχει έρθει, τότε θα ζητήσει από τον αποστολέα να του το ξαναστείλει.
- **Σειρά πακέτων**- Εάν δύο πακέτα αποσταλούν σε μία σύνδεση το ένα μετά το άλλο, τότε το πρωτόκολλο TCP εγγυάται ότι θα φτάσουν στον παραλήπτη με την ίδια σειρά με την οποία στάλθηκαν. Στην περίπτωση που λείπει ένα πακέτο και έρθουν μελλοντικά πακέτα, τότε αυτά κατακρατούνται στην προσωρινή μνήμη (buffer) μέχρις ότου φτάσει το πακέτο που λείπει. Τότε αναδιατάσσονται και εμφανίζονται με την σωστή σειρά στον παραλήπτη.
- **Βαρύτητα**- Το πρωτόκολλο TCP θεωρείται ιδιαίτερα βαρύ, δεδομένου του γεγονότος ότι χρειάζονται τουλάχιστον 3 πακέτα για την εγκαθίδρυση της σύνδεσης, πριν ακόμη μεταδοθεί οποιοδήποτε πακέτο δεδομένων. Επίσης, οι μηχανισμοί αξιοπιστίας που υλοποιεί το κάνουν ακόμη πιο βαρύ, πράγμα που έχει φυσικά σημαντικό αντίκτυπο στην ταχύτητα μετάδοσης δεδομένων.
- **Το TCP χρησιμοποιεί ένα μηχανισμό τριπλής χειραψίας (three-way handshake)** πριν αρχίσει να μεταδίδει δεδομένα ενώ το UDP στέλνει δεδομένα κατευθείαν χωρίς να χρησιμοποιεί τέτοιο μηχανισμό, συνεπώς το UDP δεν εισάγει καμία καθυστέρηση στην εγκαθίδρυση μιας σύνδεσης. Αυτή η επιλογή χρειάζεται σε εφαρμογές που ανταλλάσσουν δεδομένα μικρού όγκου και σποραδικά

Το UDP είναι ένα πιο απλό και ελαφρύ πρωτόκολλο, στο οποίο δεν υπάρχει η έννοια της σύνδεσης. Κάθε πακέτο UDP διανύει το δίκτυο ως μία ξεχωριστή αυτόνομη μονάδα και όχι ως μία σειρά πακέτων σε μία σύνδεση, όπως στο TCP. Τα κύρια **χαρακτηριστικά του UDP** είναι τα εξής:

- **Αναξιόπιστο**- Κατά την αποστολή ενός πακέτου, ο αποστολέας δεν είναι σε θέση να γνωρίζει εάν το πακέτο θα φτάσει σωστά στον προορισμό του ή εάν θα χαθεί μέσα στο δίκτυο. Δεν έχει προβλεφθεί η δυνατότητα επιβεβαίωσης λήψης πακέτου από τον παραλήπτη, ούτε η επαναμετάδοση ενός χαμένου πακέτου.
- **Δεν υπάρχει σειρά**- Τα πακέτα UDP, σε αντίθεση με το TCP, δεν αριθμούνται και κατά συνέπεια δεν υπάρχει κάποια συγκεκριμένη σειρά με την οποία θα πρέπει να φτάσουν στον παραλήπτη.
- **Ελαφρύ**- Το πρωτόκολλο αυτό καθ' αυτό είναι πολύ ελαφρύ σε σύγκριση με το TCP διότι δεν εφαρμόζει όλους τους μηχανισμούς αξιόπιστης επικοινωνίας που υπάρχουν στο δεύτερο. Αυτό έχει ως συνέπεια να είναι αρκετά πιο γρήγορο.
- **Datagrams**- Κάθε πακέτο UDP ονομάζεται επίσης και "datagram", θεωρείται δε ως μεμονωμένη οντότητα που θα πρέπει να μεταδοθεί ολόκληρη. Κατά συνέπεια δεν υφίσταται η έννοια της διοχέτευσης πακέτων μέσα σε ένα κανάλι/σύνδεση.
- **Χαμηλό overhead επικεφαλίδων -Τ**ο τμήμα TCP έχει 20 bytes επικεφαλίδα ενώ το UDP έχει μόνο 8 bytes επικεφαλίδα. Το TCP χρειάζεται περισσότερα πεδία επικεφαλίδας προκειμένου νε εγγυηθεί την αξιοπιστία ενώ το UDP που δεν διασφαλίζει αξιοπιστία χρειάζεται λιγότερα πεδία.
- **Broadcast και multicast-** Επειδή το πρωτόκολλο TCP είναι προσανατολισμένο τη σύνδεση (connection-oriented protocol) δεν υποστηρίζει broadcast και multicast. Συνεπώς εφαρμογές που απαιτούν αυτό τον τύπο υπηρεσίας πρέπει να χρησιμοποιήσουν το UDP ως πρωτόκολλο μετάδοσης.