ΑΝΩΤΑΤΟ ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΕΙΡΑΙΑ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΘΕΜΑ: ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΔΙΚΤΥΩΝ ΚΑΙ ΠΡΩΤΟΚΟΛΛΑ ΔΡΟΜΟΛΟΓΗΣΗΣ

ΣΠΟΥΔΑΣΤΗΣ: ΖΗΝΕΛΗΣ ΟΡΕΣΤΗΣ (Α.Μ. 30584)

ΥΠΕΥΘΥΝΟΙ ΚΑΘΗΓΗΤΕΣ: ΛΕΒΕΝΤΗΣ ΣΩΤΗΡΙΟΣ

ΤΣΕΛΙΚΗΣ ΓΕΩΡΓΙΟΣ

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

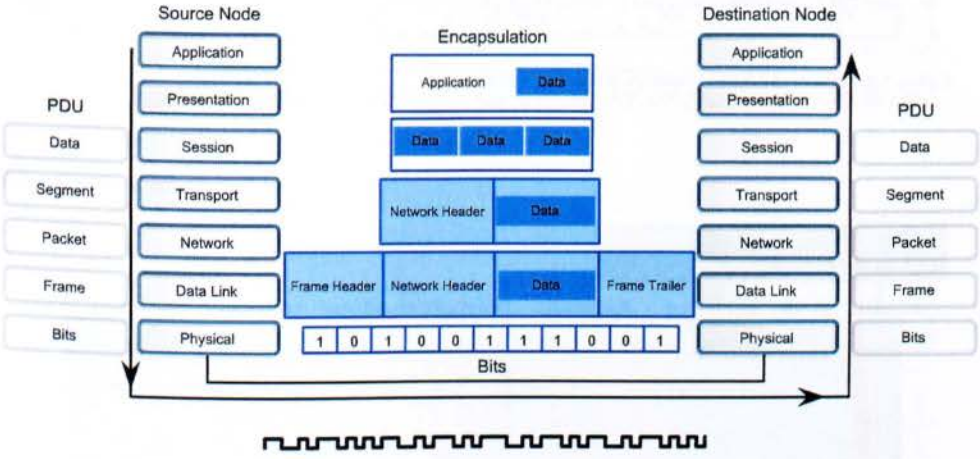
ΚΕΦΑΛΑΙΟ 1

ΤΙΤΛΟΣ: ΦΥΣΙΚΟ ΕΠΙΠΕΔΟ

1.1 ΓΕΝΙΚΑ

Τα υψηλότερα επίπεδα του πρωτόκολλου OSI προετοιμάζουν τα δεδομένα για αποστολή στον εκάστοτε προορισμό. Το φυσικό επίπεδο διαχειρίζεται πώς τα δεδομένα αυτά αποστέλλονται στο μέσο επικοινωνίας.

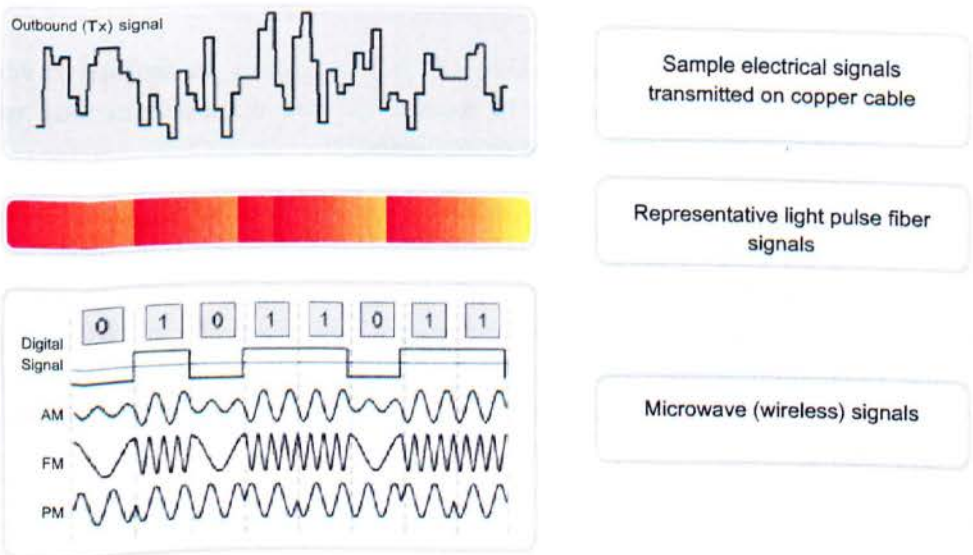
Ο ρόλος του φυσικού επίπεδου είναι να κωδικοποιεί τα δυαδικά ψηφία (binary digits) που αντιπροσωπεύουν τα frames του επιπέδου Ζεύξης σε σήματα και να διαβιβάζει, αλλά και να λαμβάνει τα σήματα μέσα στα μέσα επικοινωνίας – καλώδια χαλκού, οπτικές ίνες, αέρας (ασύρματα), που συνδέουν τις συσκευές δικτύου. Εν συντομία **ο ρόλος του φυσικού επιπέδου** είναι να παρέχει τα μέσα για τη μεταφορά σε όλα τα φυσικά μέσα του δικτύου τα bit που συνθέτουν ένα Data Link layer frame.



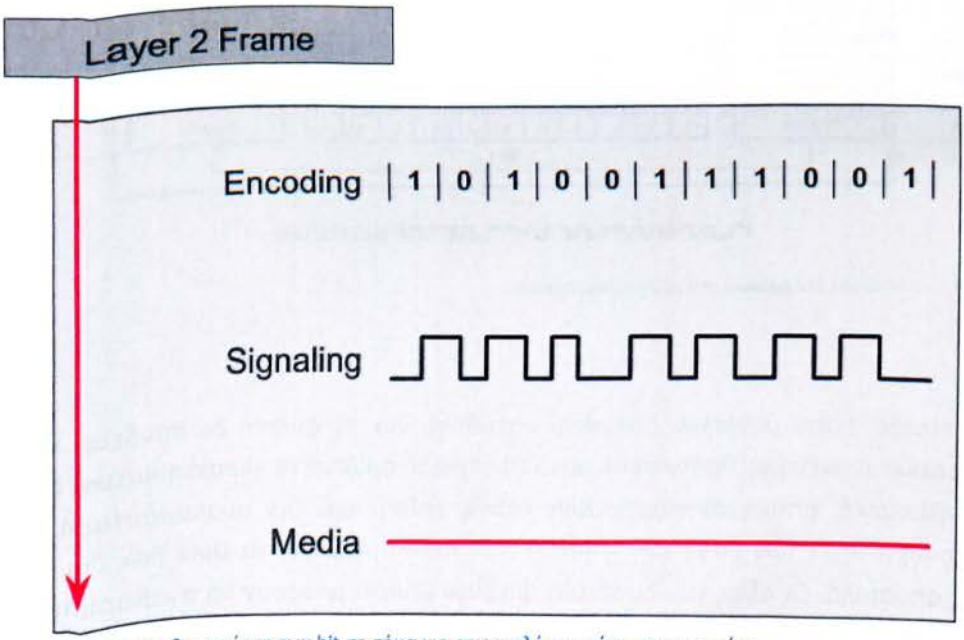
Εικόνα 1.1.1 - Αποστολή δεδομένων στο μέσο επικοινωνίας

Το επίπεδο 1 του μοντέλου OSI είναι υπεύθυνο για τη φυσική διασύνδεση των δικτυακών συσκευών. Πρότυπα σε αυτό το επίπεδο ορίζουν τα χαρακτηριστικά από την ηλεκτρική, οπτική αναπαράσταση καθώς επίσης και την αναπαράσταση σε ραδιοσυχνότητες των δυαδικών ψηφίων που περιλαμβάνουν τα Data link Frames προς αποστολή. Οι αξίες των δυαδικών ψηφίων μπορεί μπορούν να αναπαριστούν σαν ηλεκτρονικοί παλμοί, παλμοί φωτός, ή αλλαγές στα ραδιοκύματα. Τα πρωτόκολλα του φυσικού επιπέδου κωδικοποιούν τα δυαδικά ψηφία για αποστολή και τα αποκωδικοποιούν στον προορισμό.

Πρότυπα σε αυτό το επίπεδο είναι επίσης υπεύθυνα για να περιγράψουν τα φυσικά, ηλεκτρικά και μηχανικά χαρακτηριστικά των φυσικών μέσων και συνδέσμων που διασυνδέουν τις συσκευές δικτύου.

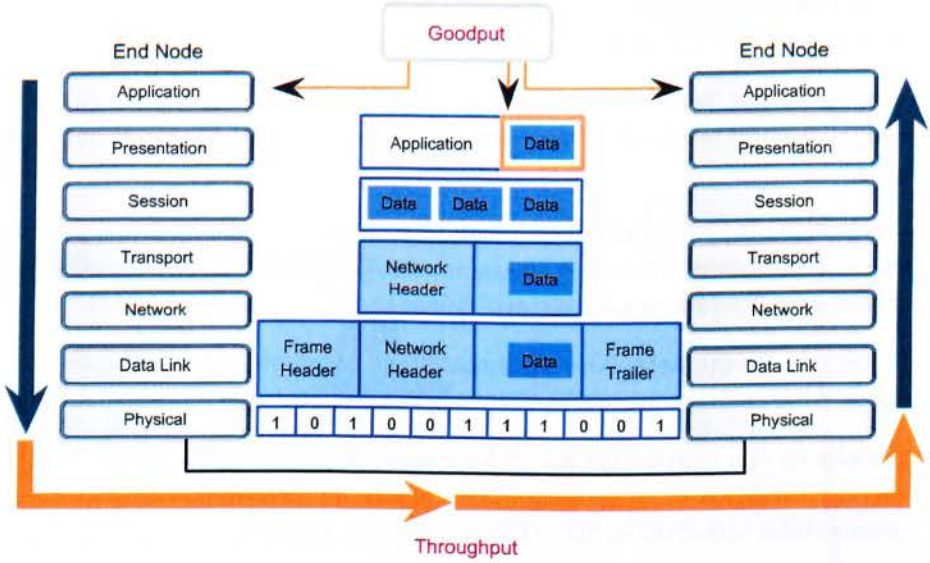


Εικόνα 1.1.2 - Αναπαράσταση σημάτων στα φυσικά μέσα



Εικόνα 1.1.3 Κωδικοποίηση των bit σε σήμα για αποστολή στο μέσω επικοινωνίας.

Ποικίλα φυσικά μέσα επικοινωνίας και Πρωτόκολλα του φυσικού επιπέδου έχουν διαφορετικές χωρητικότητες μεταφοράς δεδομένων. Το **Raw data bandwidth** είναι το θεωρητικά ανώτερο όριο μετάδοσης bit. Άλλα συγκριτικά μεγέθη είναι τα **Throughput** και **goodput,** πάντα για συγκεκριμένο χρονικό όριο.



Εικόνα 1.1.4 – Throughput και Goodput

Throughput = πραγματική απόδοση δικτύου. **Goodput** = το μέτρο της μεταφοράς των χρήσιμων δεδομένων, αφού η κίνηση από τις επικεφαλίδες των πρωτοκόλλων έχουν αφαιρεθεί (βλ. Εικόνα 1.1.4).

ΚΕΦΑΛΑΙΟ 2

ΤΙΤΛΟΣ: ΕΠΙΠΕΔΟ ΖΕΥΞΗΣ ΔΕΔΟΜΕΝΩΝ

2.1 ΓΕΝΙΚΑ

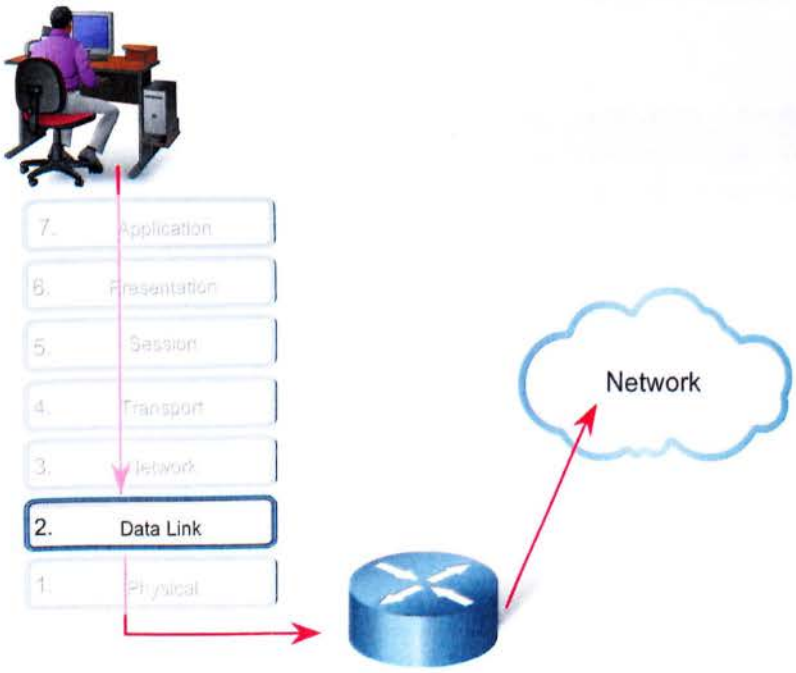
Το επίπεδο ζεύξης δεδομένων προετοιμάζει τα πακέτα από το επίπεδο δικτύου για τοποθέτηση στο φυσικό μέσο που μεταφέρει τα δεδομένα.

Το μεγάλο εύρος των μέσων επικοινωνίας δεδομένων απαιτεί αντίστοιχα ένα ευρύ φάσμα πρωτοκόλλων Ζεύξης δεδομένων για τον έλεγχο της πρόσβασης σε αυτά τα μέσα.

Η πρόσβαση στο μέσο επικοινωνίας μπορεί να είναι ομαλή και ελεγχόμενη ή μπορεί να είναι contention - based. Η λογική τοπολογία δικτύου και το φυσικό μέσο επικοινωνίας βοηθάνε να καθορίζεται ο τρόπος πρόσβασης στο φυσικό μέσο.

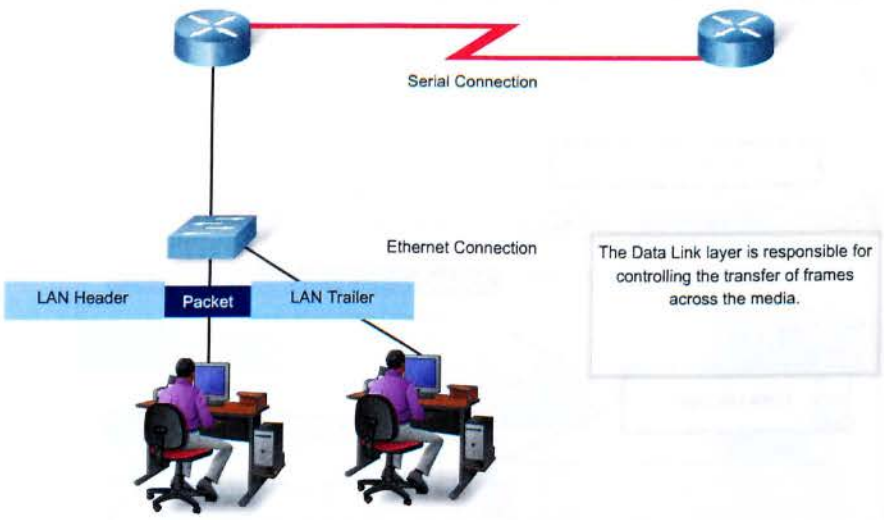
Το επίπεδο Ζεύξης Δεδομένων προετοιμάζει τα δεδομένα για τοποθέτηση στο φυσικό μέσο επικοινωνίας ενθυλακώνοντας τα Layer 3 πακέτα σε πλαίσια (frames).

Ένα πλαίσιο έχει επικεφαλίδα και πεδία που περιλαμβάνουν το Data Link Source και τις διευθύνσεις προορισμού, QoS (quality of Serevice), τον τύπο του πρωτοκόλλου, καθώς και τις τιμές ελέγχου ορθότητας του frame.



Εικόνα 2.1.1 – Επίπεδο ζεύξης δεδομένων

Το επίπεδο ζεύξης δεδομένων **είναι υπεύθυνο για τον έλεγχο της μεταφοράς των πλαισίων (frames)** κατά τη μεταφορά του στο φυσικό μέσο επικοινωνίας.



Εικόνα 2.1.2 - Το επίπεδο ζεύξης δεδομένων είναι υπεύθυνο για τον έλεγχο της μεταφοράς των πλαισίων (frames) κατά τη μεταφορά του στο φυσικό μέσο επικοινωνίας.

2.2 ΤΑ ΔΥΟ ΥΠΟΣΤΡΩΜΑΤΑ

Για να υποστηρίξει μια ευρεία ποικιλία των λειτουργιών του δικτύου, το στρώμα ζεύξης δεδομένων συχνά χωρίζεται σε δύο υποστρώματα: στο **πάνω υπόστρωμα** και στο **κάτω υπόστρωμα**.

Το πάνω υπόστρωμα καθορίζει τις διαδικασίες λογισμικού που παρέχουν υπηρεσίες στα δικτυακά πρωτόκολλα.

Το χαμηλότερο υπόστρωμα καθορίζει τις διαδικασίες πρόσβασης στα μέσα επικοινωνίας που εκτελούνται από το υλικό.

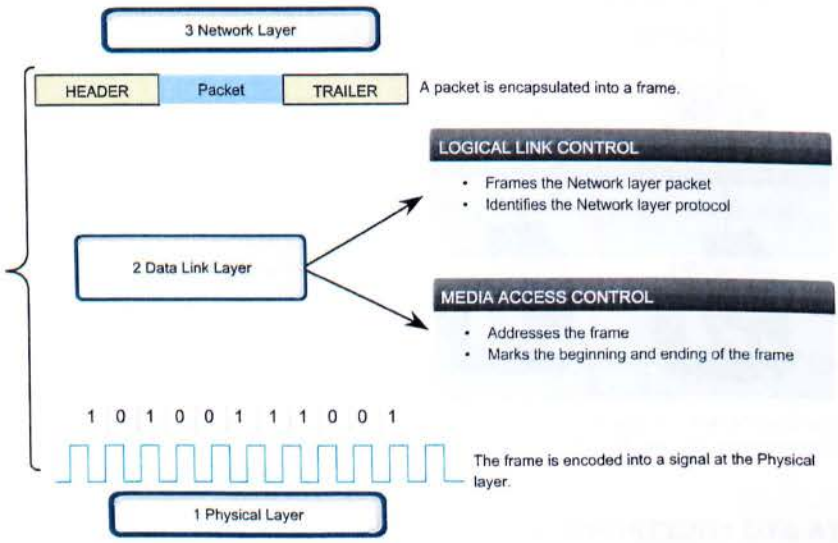
Τα δύο υποστρώματα LAN είναι:

Logical Lick Control

Το Logical Lick Control (LLC) τοποθετεί τις πληροφορίες στο πλαίσιο που προσδιορίζει το δίκτυο στρώμα πρωτοκόλλου που χρησιμοποιείται για το πλαίσιο. Οι πληροφορίες αυτές επιτρέπουν πολλαπλά Layer 3 πρωτόκολλα, όπως το IP και IPX, να χρησιμοποιούν το ίδιο interface του δικτύου και των μέσων ενημέρωσης.

Media Access Control

Το Media Access Control (MAC) παρέχει στοιχεία διευθυνσιοδότησης για το επίπεδο ζεύξης δεδομένων και την οριοθέτηση των δεδομένων σύμφωνα με τις φυσικές απαιτήσεις σήμανσης του μέσου και τον τύπο του πρωτόκολλου.



Εικόνα 2.2.1 - Logical link Control. Media Access Control

2.3 ΤΟΠΟΘΕΤΗΣΗ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΜΕΣΟ – MEDIA ACCESS CONTROL METHODS

Υπάρχουν διαφορετικοί τρόποι για να ρυθμιστεί η τοποθέτηση των πλαισίων στο μέσο. Τα πρωτόκολλα στο στρώμα ζεύξης δεδομένων καθορίζουν τους κανόνες για την πρόσβαση σε διαφορετικά μέσα. Ορισμένες μέθοδοι χρησιμοποιούν εξαιρετικά ελεγχόμενες διαδικασίες για να εξασφαλίζεται ότι τα πλαίσια τοποθετούνται με ασφάλεια στο μέσο. Αυτές οι μέθοδοι ορίζονται από εξελιγμένα πρωτόκολλα.

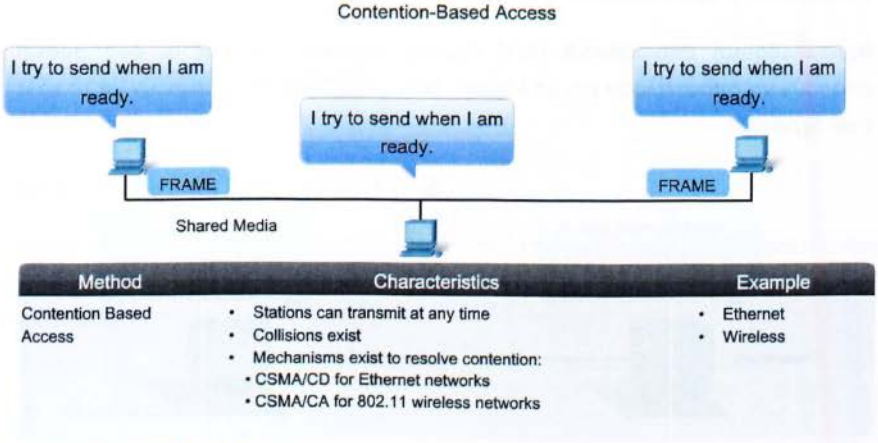
Η μέθοδος που χρησιμοποιείται εξαρτάται από:

- Την κοινή χρήση πολυμέσων - Εάν και πώς οι κόμβοι μοιράζονται το μέσα επικοινωνίας.
- Την Τοπολογία - Πώς η σύνδεση μεταξύ των κόμβων εμφανίζεται στο στρώμα ζεύξης δεδομένων

Μερικές τοπολογίες δικτύων μοιράζονται το μέσο επικοινωνίας με πολλαπλούς κόμβους. Ανά πάσα στιγμή, μπορεί να υπάρχουν μια σειρά από συσκευές που προσπαθούν να στείλουν και να λάβουν δεδομένα μέσω του δικτύου. Υπάρχουν κανόνες που διέπουν τον τρόπο που οι συσκευές αυτές μοιράζονται το κοινό μέσο επικοινωνίας.

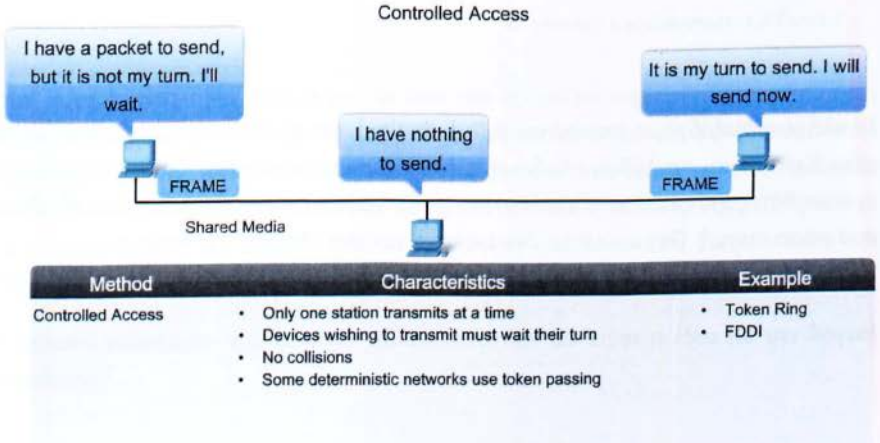
Υπάρχουν δύο βασικές μέθοδοι ελέγχου των μέσων ενημέρωσης για την κοινή πρόσβαση των μέσων ενημέρωσης:

- Contention based - Όλοι οι κόμβοι ανταγωνίζονται για τη χρήση του μέσου



Εικόνα 2.3.1 - Contention Based Access

- Ελεγχόμενη (Controlled Access) - Κάθε κόμβος έχει το δικό του χρόνο του για να χρησιμοποιήσει το μέσο



Εικόνα 2.3.2 - Controlled Access

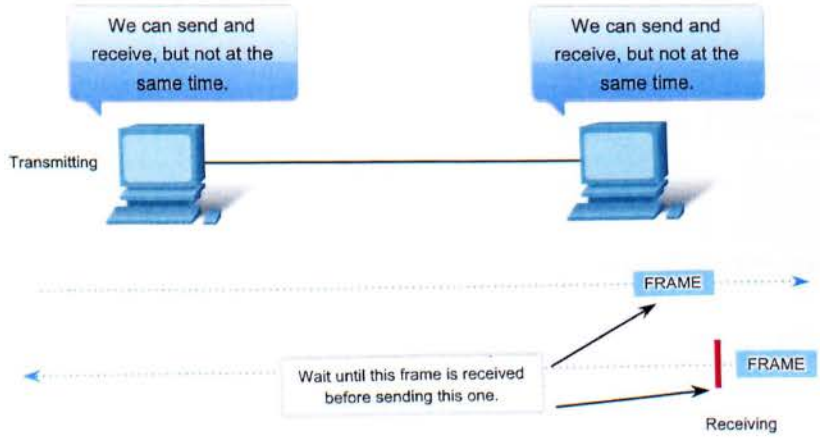
2.4 ΜΕΘΟΔΟΣ ΠΡΟΣΒΑΣΗΣ ΔΕΔΟΜΕΝΩΝ ΓΙΑ ΜΗ ΚΟΙΝΟ ΜΕΣΟ ΕΠΙΚΟΙΝΩΝΙΑΣ

Σε point to point τοπολογία συνδέονται μόνο δύο κόμβοι. Οι κόμβοι δεν έχουν να μοιραστούν το μέσο επικοινωνίας με άλλους υπολογιστές ή πρέπει να καθοριστεί αν ένα πλαίσιο προορίζεται για αυτόν τον κόμβο. Ως εκ τούτου, τα πρωτόκολλα Data link layer έχουν λίγα να κάνουν για τον έλεγχο πρόσβασης στο μέσο επικοινωνίας.

Full Duplex και Duplex Half

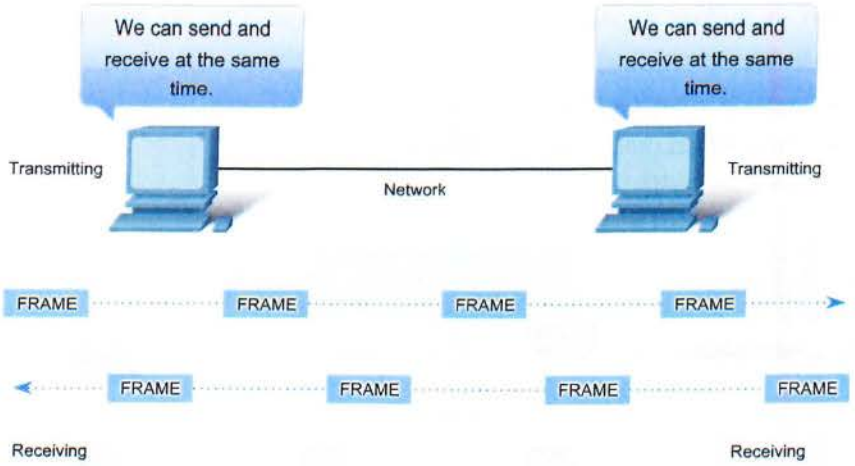
Στις Συνδέσεις point-to-point, το στρώμα ζεύξης δεδομένων πρέπει να εξετάσει αν η επικοινωνία είναι half-duplex ή full-duplex.

Ημιαμφίδρομη επικοινωνία (half duplex) σημαίνει ότι και οι δύο συσκευές μπορούν να αποστείλουν και να λάβουν δεδομένα, αλλά δεν μπορούν να το κάνουν ταυτόχρονα.



Εικόνα 2.4.1 - Ημιαμφίδρομη επικοινωνία

Σε πλήρως αμφίδρομη επικοινωνία (full duplex), και οι δύο συσκευές μπορούν να μεταδώσουν και να λάβουν δεδομένα ταυτόχρονα. Το στρώμα ζεύξης δεδομένων προϋποθέτει ότι τα μέσο επικοινωνίας είναι διαθέσιμο και για τους δύο κόμβους ανά πάσα στιγμή. Ως εκ τούτου, δεν υπάρχει ανάγκη ελέγχου - διαιτησίας.



Εικόνα 2.4.2 - Πλήρως αμφίδρομη επικοινωνία

2.5 ΛΟΓΙΚΗ ΚΑΙ ΦΥΣΙΚΗ ΤΟΠΟΛΟΓΙΑ

Η τοπολογία του δικτύου είναι η ρύθμιση ή η σχέση των συσκευών του δικτύου και των διασυνδέσεων μεταξύ τους. Οι Τοπολογίες δικτύων μπορούν να χωριστούν σε δύο επίπεδα :

- φυσικό επίπεδο
- λογικό επίπεδο.

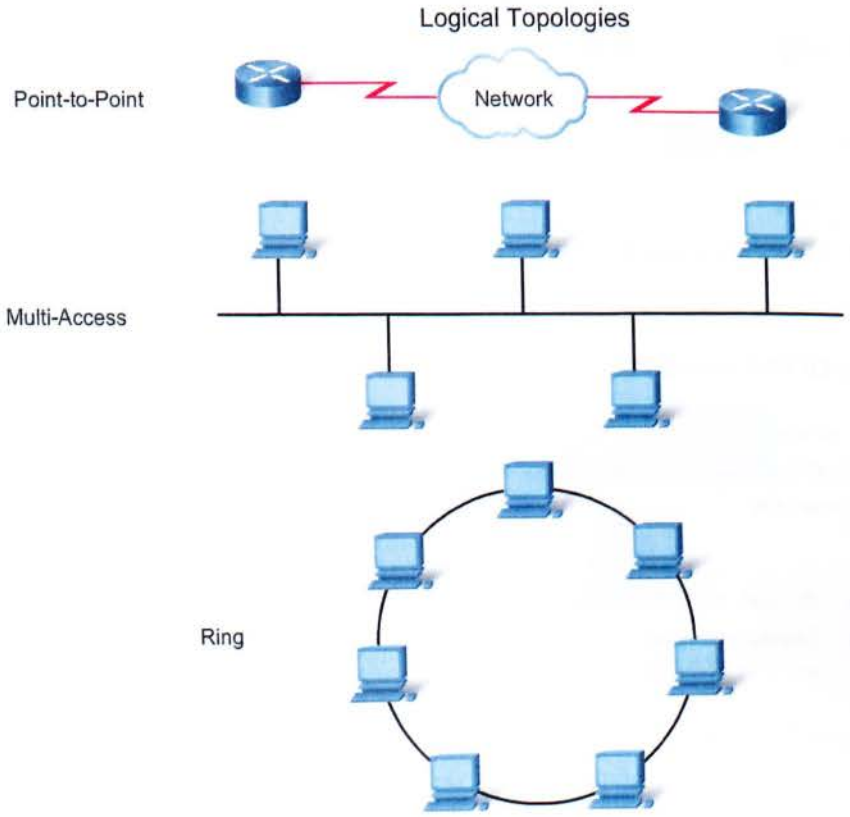
Η φυσική τοπολογία είναι μια διάταξη των κόμβων και των φυσικών συνδέσεων μεταξύ τους. Η αναπαράσταση του τρόπου που χρησιμοποιείται το μέσο για τη διασύνδεση των συσκευών.

Μια λογική τοπολογία είναι ο τρόπος που ένα δίκτυο μεταφέρει πλαίσια από έναν κόμβο στον επόμενο. Η ρύθμιση αυτή αποτελείται από εικονικές συνδέσεις μεταξύ των κόμβων ενός δικτύου ανεξάρτητα από τη φυσική τους διάταξη. Αυτά τα λογικά μονοπάτια σήμανσης ορίζονται από τα πρωτόκολλα επιπέδου ζεύξης δεδομένων. Το στρώμα ζεύξης δεδομένων "βλέπει" τη λογική τοπολογία του δικτύου κατά τον έλεγχο της πρόσβασης σε δεδομένα στα μέσα επικοινωνίας.

Η φυσική τοπολογία του δικτύου πιθανότατα δεν θα είναι η ίδια με την λογική τοπολογία.

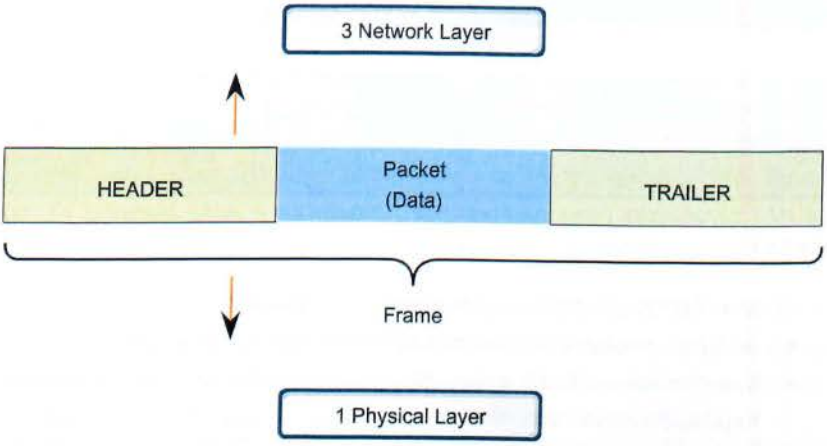
Λογικές και φυσικές τοπολογίες που χρησιμοποιούνται συνήθως στα δίκτυα είναι:

- Point-to-Point (σημείο σε σημείο)
- Multi-Access (πολλαπλής πρόσβασης)
- Ring (δαχτυλίδι)



Εικόνα 2.5.1 - Λογικές τοπολογίες

2.6 ΔΟΜΗ ΠΛΑΙΣΙΟΥ - FRAMES

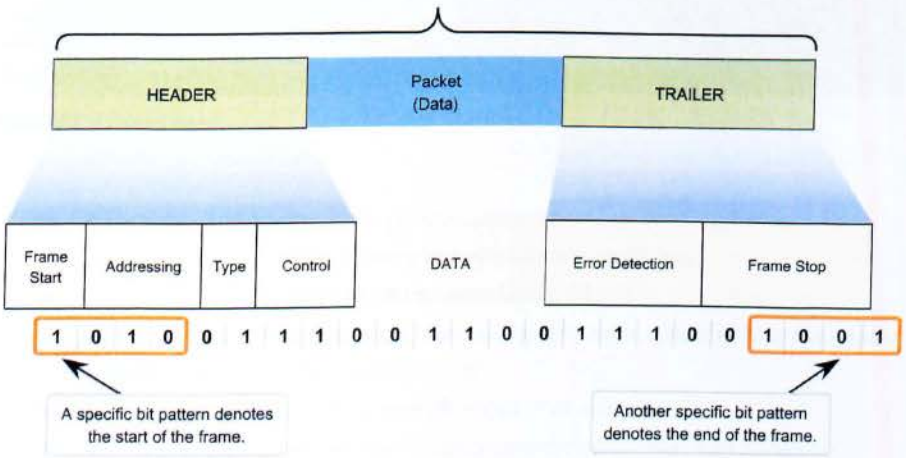


Εικόνα 2.6.1 - Δομή πλαισίου

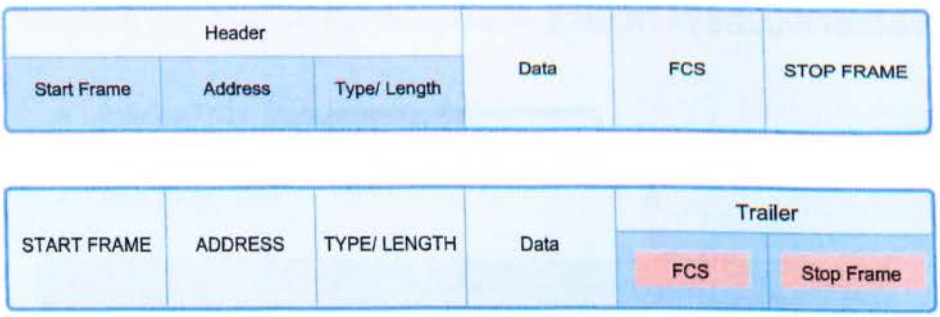
Το πλαίσιο αποτελείται από 3 μέρη.

- Την κεφαλίδα
- τα δεδομένα
- την ουρά

Η κεφαλίδα και η ουρά εμπεριέχουν συγκεκριμένες πληροφορίες, όπως αναφέρονται στην παρακάτω εικόνα.



Εικόνα 2.6.2 - Κεφαλίδα, ουρά πλαισίου



Εικόνα 2.6.3

- Start Frame - Επισημαίνει την έναρξη του πλαισίου
- Address - Υποδεικνύει την πηγή και τον προορισμό των κόμβων.
- Type/Length - Υποδεικνύει το ανώτερο στρώμα των υπηρεσιών που περιλαμβάνονται στο πλαίσιο ή πιθανώς το μέγεθος του πλαισίου. Είναι προαιρετικό πεδίο.
- FCS – Χρησιμοποιείται για έλεγχο λαθών. Η πηγή (ο αποστολέας) υπολογίζει έναν αριθμό με βάση το μέγεθος των δεδομένων του πλαισίου και τον τοποθετεί στο πεδίο FCS. Ο παραλήπτης επαναϋπολογίζει τον αριθμό αυτό με βάση τα δεδομένα του πλαισίου που δέχτηκε. Εάν οι δύο αριθμοί δε συμφωνούν το πλαίσιο διαγράφεται
- Stop Frame – Εάν δεν έχει δηλωθεί το μέγεθος του αρχείου στο πεδίο Type/Length υποδεικνύει το τέλος του πλαισίου. Το πεδίο είναι προαιρετικό.

ΚΕΦΑΛΑΙΟ 3

ΤΙΤΛΟΣ:

3.1 ΓΕΝΙΚΑ

Το Ethernet είναι μια οικογένεια τεχνολογιών δικτύωσης, που ορίζονται στα πρότυπα IEEE 802.2 και 802.3. Τα Ethernet πρότυπα καθορίζουν τόσο τα πρωτόκολλα στο Επίπεδο ζεύξης δεδομένων και τις τεχνολογίες στο φυσικό επίπεδο. Το Ethernet είναι η πιο ευρέως χρησιμοποιούμενη τεχνολογία LAN και υποστηρίζει εύρος ζώνης δεδομένων των 10, 100, 1000, ή 10.000 Mbps.

Η βασική μορφή και το πλαίσιο υποστρωμάτων IEEE στα OSI LAYER 1,2 παραμένουν σταθερά σε όλες τις μορφές του Ethernet. Ωστόσο, οι μέθοδοι για την ανίχνευση και τη διάθεση δεδομένων σχετικά με τα μέσα επικοινωνίας ποικίλλουν.

Το Ethernet χρησιμοποιεί σα μέθοδο ελέγχου πρόσβασης στο μέσο επικοινωνίας την CSMA / CD Carrier sense multiple access with collision detection. Προϋποθέτει ότι στην επικεφαλίδα του πλαισίου Ethernet εμπεριέχονται οι πληροφορίες διευθύνσεων του αποστολές και του παραλήπτη. Οι διευθύνσεις αναφέρονται στο OSI Layer 2. Όπως με τα περισσότερα πρωτόκολλα LAN, οι διευθύνσεις αυτές αντιστοιχούν στις MAC addresses. Μια διεύθυνση Ethernet MAC είναι 48 bits σε δεκαεξαδική μορφή.

3.2 ΔΟΜΗ ETHERNET FRAME

Frame

Field name	Preamble	Destination	Source	Type	Data	Frame Check Sequence
Size	8 bytes	6 bytes	6 bytes	2 bytes	46 - 1500 bytes	4 bytes

Εικόνα 3.2.1 - Ethernet frame

- Preamble - Χρησιμοποιείται για συγχρονισμό
- Destination - Η MAC διεύθυνση του παραλήπτη σε 48 bits
- Source - Η MAC διεύθυνση του αποστολέασε 48 bits
- Type - Εμπεριέχεται μία τιμή που καθορίζει ποιο πρωτόκολλο ανώτερου επιπέδου θα παραλάβει τα δεδομένα
- Data - Εμπεριέχεται το PDU, συνήθως ένα IPv4 πακέτο.
- FCS - Χρησιμοποιείται για την επαλήθευση της ορθότητας του πλαισίου.

ΚΕΦΑΛΑΙΟ 4

ΤΙΤΛΟΣ: ADDRESS RESOLUTION PROTOCOL (ARP)

4.1 ΓΕΝΙΚΑ

Το ARP πρωτόκολλο παρέχει δύο βασικές λειτουργίες:

- Συσχέτιση IPv4 διευθύνσεων με διευθύνσεις MAC
- Συντήρηση του πίνακα ARP

Συσχέτιση IPv4 διευθύνσεων με διευθύνσεις MAC

Ένα πλαίσιο για να τοποθετηθεί στο φυσικό μέσο, θα πρέπει να έχει έναν προορισμό διεύθυνσης MAC. Όταν ένα πακέτο στέλνεται στο στρώμα ζεύξης δεδομένων για να εγκλειστεί σε ένα πλαίσιο, ο κόμβος διαβάζει έναν πίνακα στη μνήμη του για να βρει την Data Link Layer διεύθυνση που έχει αντιστοιχιστεί στον IPv4 διεύθυνση προορισμού. Ο πίνακας αυτός ονομάζεται πίνακας ARP ή η μνήμη cache του ARP. Ο πίνακας ARP είναι αποθηκευμένος στη μνήμη RAM της συσκευής.

Κάθε εγγραφή, ή σειρά, του πίνακα ARP έχει ένα ζεύγος τιμών: μια διεύθυνση IP και μία διεύθυνση MAC. Καλούμε τη σχέση μεταξύ των δύο τιμών χάρτη - απλά σημαίνει ότι μπορούμε να εντοπίσουμε μια διεύθυνση IP στον πίνακα και να ανακαλύψουμε την αντίστοιχη διεύθυνση MAC. Ο πίνακας ARP αποθηκεύει προσωρινά την αντιστοίχιση των συσκευών στο τοπικό LAN.

Συντήρηση του πίνακα ARP

Ο πίνακας ARP διατηρείται δυναμικά. Υπάρχουν δύο τρόποι με τους οποίους μια συσκευή μπορεί να συγκεντρώσει τις διευθύνσεις MAC. Ένας τρόπος είναι να παρακολουθεί την κίνηση που παρατηρείται στο τοπικό τμήμα του δικτύου. Όταν ένας κόμβος λαμβάνει frames από το φυσικό μέσο, μπορεί να καταγράψει την IP προέλευσης και τη διεύθυνση MAC και να καταγράψει αυτή τη συσχέτιση στον πίνακα ARP. Καθώς τα frames μεταδίδονται στο δίκτυο, η συσκευή συμπληρώνει τον πίνακα ARP με τα ζεύγη διευθύνσεων.

Ένας άλλος τρόπος συγκέντρωσης μία διεύθυνσης MAC για μια συσκευή είναι να μεταδώσει ένα αίτημα ARP. Το πρωτόκολλο ARP στέλνει ένα broadcast Layer 2 frame σε όλες τις συσκευές στο Ethernet LAN δίκτυο. Το frame περιλαμβάνει ένα

πακέτο αίτησης ARP με την IP διεύθυνση της συσκευής προορισμού. Ο κόμβος που λαμβάνει το frame αναγνωρίζει τη συγκρίνει τη διεύθυνση αποστολής του πακέτου με τη δική του. Εάν οι δύο διευθύνσεις είναι ίδια απαντά με την αποστολή ενός πακέτου ARP Reply πίσω στον αποστολέα ως unicast frame.

Σε αυτές τις δυναμικές καταχωρήσεις στον πίνακα ARP καταχωρείται και η χρονική στιγμή καταχώρησης. Εάν μια συσκευή δεν λάβει ένα πλαίσιο από μια συγκεκριμένη συσκευή από τη στιγμή που το καθορισμένο χρονικό περιθώριο λήξει, η εγγραφή για τη συσκευή αυτή αφαιρείται από τον πίνακα ARP.

Επιπλέον, στατικές καταχωρήσεις μπορούν να εισαχθούν σε έναν πίνακα ARP, αλλά αυτό γίνεται σπάνια. Οι στατικές καταχωρήσεις στον πίνακα ARP δεν λήγουν με την πάροδο του χρόνου και πρέπει να αφαιρεθούν με το χέρι.

4.2 ΔΗΜΙΟΥΡΓΩΝΤΑΣ ΤΟ FRAME

Τι κάνει ένας κόμβος κάνει όταν χρειάζεται να δημιουργηθεί ένα frame και η μνήμη cache του πρωτοκόλλου ARP δεν περιέχει εγγραφή; Όταν το ARP λαμβάνει ένα αίτημα να χαρτογραφήσει μια διεύθυνση IPv4 με μια διεύθυνση MAC, ψάχνει για το ζεύγος διευθυνσιοδότησης στον πίνακα ARP του. Εάν το ζεύγος δεν υπάρχει, η ενθυλάκωση του πακέτου IPv4 αποτυγχάνει και οι διαδικασίες του Layer 2 ενημερώνουν το ARP να ενημερώσει ότι χρειάζεται ένα ζεύγος.

Οι υπηρεσίες ARP στη συνέχεια στέλνουν ένα πακέτο ARP Request για να ανακαλύψουν τη διεύθυνση MAC της συσκευής προορισμού στο τοπικό δίκτυο. Εάν μια συσκευή που λάβει την αίτηση έχει τη διεύθυνση IP προορισμού, απαντά με ένα πακέτο ARP Reply. Το ζεύγος καταχωρείται στον πίνακα ARP. Πακέτα για αυτήν την IPv4 διεύθυνση μπορούν τώρα να ενθυλακωθούν σε frames (πλαίσια).

Εάν καμιά συσκευή δεν αποκριθεί στο ARP Request πακέτο, το πακέτο απορρίπτεται επειδή ένα πλαίσιο δεν μπορεί να δημιουργηθεί. Αυτή η αποτυχία ενθυλάκωσης αναφέρεται στα ανώτερα στρώματα OSI της συσκευής. Εάν η συσκευή είναι μία συσκευή ενδιάμεση, όπως ένας δρομολογητής, τα ανώτερα στρώματα μπορούν να επιλέξουν να ενημερώσουν τον αποστολέα του πακέτου με ένα σφάλμα σε ένα ICMPv4 πακέτο.

ΚΕΦΑΛΑΙΟ 5

ΤΙΤΛΟΣ: ΕΠΙΠΕΔΟ ΔΙΚΤΥΟΥ – NETWORK LAYER

5.1 ΓΕΝΙΚΑ

Το πιο σημαντικό στρώμα δικτύου (OSI Layer 3) είναι το πρωτόκολλο IP (Internet Protocol).

Η δρομολόγηση IP στο Layer 3 δεν εγγυάται αξιόπιστη παράδοση ή δε δημιουργείται μια σύνδεση αποστολέα και παραλήπτη πριν τη μετάδοσή δεδομένων. Αυτή η αναξιόπιστη επικοινωνία είναι γρήγορη και ευέλικτη. Ανώτερα στρώματα πρέπει να παρέχουν μηχανισμούς για να εγγυηθούν την παράδοση των δεδομένων, αν αυτό είναι αναγκαίο.

Ο ρόλος του στρώματος δικτύου είναι να μεταφέρονται δεδομένα από μία συσκευή σε μία άλλη, ανεξάρτητα από το είδος των δεδομένων. Τα δεδομένα ενθυλακώνονται σε ένα πακέτο. Η κεφαλή του πακέτου έχει πεδία που περιλαμβάνουν τη διεύθυνση προορισμού του πακέτου.

Εάν η διεύθυνση προορισμού δεν είναι στο ίδιο δίκτυο με τη διεύθυνση της πηγής, το πακέτο προωθείται στην προεπιλεγμένη πύλη για την προώθηση στο δίκτυο προορισμού. Η πύλη είναι μια διεπαφή ενός δρομολογητή που εξετάζει τη διεύθυνση προορισμού. Αν το δίκτυο προορισμού έχει μια καταχώρηση στον πίνακα δρομολόγησης, ο δρομολογητής προωθεί το πακέτο είτε σε ένα συνδεδεμένο δίκτυο ή στην επόμενη πύλη (next – hop gateway). Αν δεν υπάρχει καταχώρηση δρομολόγησης, ο δρομολογητής μπορεί να προωθήσει το πακέτο σε μια προκαθορισμένη διαδρομή, ή να πέσει το πακέτο.

Καταχωρίσεις στον πίνακα δρομολόγησης μπορούν να ρυθμιστούν με το χέρι σε κάθε δρομολογητή για την παροχή στατικής δρομολόγησης ή οι δρομολογητές μπορεί να ανταλλάσουν πληροφορίες διαδρομών δυναμικά μεταξύ τους χρησιμοποιώντας ένα πρωτόκολλο δρομολόγησης.

5.2 ΥΠΗΡΕΣΙΕΣ LAYER 3

Το επίπεδο δικτύου, ή OSI Layer 3, παρέχει υπηρεσίες για την ανταλλαγή των δεδομένων μέσω του δικτύου μεταξύ των συσκευών. Για την επίτευξη αυτού του στόχου χρησιμοποιούνται τέσσερις βασικές διεργασίες:

- Addressing (διευθυνσιοδότηση)
- Encapsulation (ενθυλάκωση)
- Routing (δρομολόγηση)
- Decapsulation (απενθυλάκωση)

Addressing

Κατ' αρχάς, το NETWORK LAYER πρέπει να παρέχει ένα μηχανισμό για τη διευθυνσιοδότηση των συσκευών. Εάν μεμονωμένα κομμάτια δεδομένων κατευθύνονται προς μια τερματική συσκευή, η συσκευή πρέπει να έχει μια μοναδική διεύθυνση. Σε ένα IPv4 δίκτυο, όταν η διεύθυνση αυτή προστίθεται σε μια συσκευή, η συσκευή στη συνέχεια αναφέρεται ως host.

Encapsulation

Δεύτερον, το NETWORK LAYER να παρέχει ενθυλάκωση. Όχι μόνο οι συσκευές πρέπει να ταυτίζονται με μια διεύθυνση, τα ξεχωριστά κομμάτια δεδομένων τα PDU πρέπει επίσης να περιέχουν αυτές τις διευθύνσεις. Κατά τη διάρκεια της διαδικασίας ενθυλάκωσης ,το Layer 3 δέχεται το PDU του Layer 4 και προσθέτει μια κεφαλίδα Layer 3, ή ετικέτα, για τη δημιουργία του Layer 3 PDU. Όταν αναφερόμαστε στο στρώμα δικτύου, αναφερόμαστε στο PDU ως πακέτο. Όταν ένα πακέτο έχει δημιουργηθεί, η κεφαλίδα πρέπει να περιέχει, μεταξύ άλλων στοιχείων, τη διεύθυνση του παραλήπτη (host) στον οποίο έχει σταλεί. Η διεύθυνση αυτή αναφέρεται ως διεύθυνση προορισμού. Η κεφαλίδα Layer 3 περιέχει επίσης την διεύθυνση του αποστολέα. Η διεύθυνση αυτή ονομάζεται διεύθυνση πηγής. Έπειτα το πακέτο στέλνεται προς τα κάτω στο στρώμα ζεύξης δεδομένων για να προετοιμαστεί προς μεταφορά στο φυσικό μέσο.

Routing

Στη συνέχεια, το NETWORK LAYER πρέπει να παρέχει τις υπηρεσίες για να κατευθύνει αυτά τα πακέτα. Ο αποστολέας και ο παραλήπτης δεν είναι πάντα συνδεδεμένοι στο ίδιο δίκτυο. Στην πραγματικότητα, το πακέτο μπορεί να ταξιδέψει μέσω πολλών διαφορετικών δικτύων. Στην πορεία, κάθε πακέτο πρέπει να καθοδηγείται μέσω του δικτύου για να φτάσει στον τελικό προορισμό του. Οι συσκευές που συνδέουν τα δίκτυα ονομάζονται δρομολογητές (routers). Ο ρόλος του δρομολογητή είναι να επιλέξει μονοπάτια και να κατευθύνει τα πακέτα προς τον προορισμό τους. Αυτή η διαδικασία είναι γνωστή ως δρομολόγηση.

Decapsulation

Τέλος, το πακέτο φτάνει στον παραλήπτη και υφίσταται επεξεργασία στο Layer 3. Ο παραλήπτης εξετάζει τη διεύθυνση προορισμού για να βεβαιωθεί ότι το πακέτο απευθύνεται σε αυτήν τη συσκευή. Αν η διεύθυνση είναι σωστή, τότε στο πακέτο γίνεται απενθυλάκωση από το στρώμα δικτύου και το Layer 4 PDU που περιέχεται στο πακέτο διέρχεται μέσω της κατάλληλης υπηρεσία στο στρώμα μεταφοράς (Layer4).

5.3 ΜΕΘΟΔΟΙ ΔΡΟΜΟΛΟΓΗΣΗΣ

Υπάρχουν 4 μέθοδοι δρομολόγησης/αποστολής ή αλλιώς Routing Schemes, ο καθένας με τα δικά του μοναδικά χαρακτηριστικά. Είναι, με τη σειρά που παρουσιάζονται, οι Unicast, Broadcast, Multicast. Οι ορολογίες αυτές αναφέρονται και στον τύπο των διευθύνσεων IP που χρησιμοποιούνται.

Unicast

Ο πιο συνηθισμένος τύπος για μια IP διεύθυνση είναι μια unicast διεύθυνση και είναι ο πιο διαδεδομένος τρόπος μετάδοσης πληροφορίας στο σημερινό Internet. Συνήθως αναφέρεται σε έναν μεμονωμένο αποστολέα ή παραλήπτη και μπορεί να χρησιμοποιηθεί τόσο για αποστολή όσο και παραλαβή. Συνήθως μια unicast διεύθυνση αντιστοιχίζεται με μια μόνο συσκευή, αλλά αυτό δεν σημαίνει ότι υπάρχει αντιστοιχία 1-1. Ορισμένοι υπολογιστές έχουν πολλές διαφορετικές unicast διευθύνσεις, η κάθε μια για την δικιά της ξεχωριστή χρήση. Στέλνοντας την ίδια πληροφορία σε διαφορετικές unicast διευθύνσεις, απαιτεί από τον αποστολέα να στείλει την ίδια πληροφορία τόσες φορές όσες και οι παραλήπτες του. Στην unicast δρομολόγηση κάθε router εξετάζει το destination address του λαμβανόμενου πακέτου και ψάχνει αυτήν την διεύθυνση σε έναν πίνακα, ώστε να προσδιορίσει ποια διασύνδεση να χρησιμοποιήσει ώστε το πακέτο να φτάσει πιο κοντά στον προορισμό του. Η source address του πακέτου δεν παίζει κανένα ρόλο.

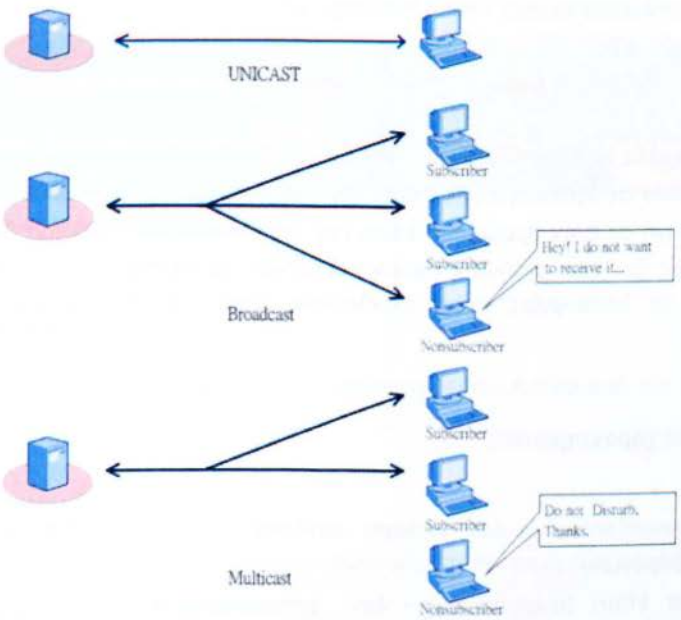
Broadcast

Η broadcast, στέλνοντας την πληροφορία σε όλους τις πιθανούς προορισμούς, δίνει τη δυνατότητα στον αποστολέα, να στείλει την πληροφορία μόνο μια φορά και όλοι οι παραλήπτες να την πάρουν. Στο IP πρωτόκολλο, η διεύθυνση 255.255.255.255 παριστάνει ένα περιορισμένο τοπικό broadcast. Για παράδειγμα, το να στείλεις σε όλες τις διευθύνσεις σε ένα τοπικό δίκτυο που αρχίζουν με 192.0.2, η directed broadcast διεύθυνση είναι 192.0.2.255 (υποθέτοντας ότι το netmask είναι 255.255.255.0). Δυστυχώς δεν υπάρχει καμία μορφή internet-wide broadcast και είναι περιορισμένο σαν τεχνολογία μόνο στα τοπικά Ethernet δίκτυα. Στο IPv6 το broadcast δεν υφίσταται σε καμία μορφή και έχει δώσει την θέση του στο multicasting.

Multicast

Μια multicast διεύθυνση αντιστοιχίζεται με ένα group από ενδιαφερόμενους χρήστες. Σύμφωνα με το RFC3171 της IANA (Internet Assigned Numbers Authority), οι διευθύνσεις 224.0.0.0 μέχρι 239.255.255.255 είναι ορισμένες ως multicast διευθύνσεις. Αυτές οι διευθύνσεις ήταν γνωστές παλαιότερα και με την ονομασία Class D. Ο αποστολέας στέλνει ένα datagram UDP πακέτο από την unicast διεύθυνση του, στην multicast διεύθυνση και οι routers αναλαμβάνουν να κάνουν αντίγραφα του πακέτου μόνο όταν χρειάζεται και να το στείλουν σε όσους παραλήπτες δήλωσαν ενδιαφέρον για το συγκεκριμένο πακέτο από τον συγκεκριμένο αποστολέα. Δεν απαιτείται προηγούμενη γνώση για το ποιοι ή πόσοι

παραλήπτες υπάρχουν στο δίκτυο. Κάθε υπολογιστής (στην ουσία κάθε εφαρμογή του υπολογιστή) που θέλει να λάβει πληροφορία από ένα multicast group, πρέπει να χρησιμοποιήσει το IGMP για να πάρει μέρος. Τα ενδιάμεσα routers πρέπει κι αυτά να χρησιμοποιούν το IGMP για να επικοινωνήσουν. Σε αντίθεση με τη unicast δρομολόγηση που αναφέραμε παραπάνω, η source address (που είναι μια απλή unicast διεύθυνση) χρησιμοποιείται για να προσδιορίσει την κατεύθυνση του data stream. Η πηγή του multicast traffic θεωρείται σαν upstream. Το router προσδιορίζει ποιες downstream διασυνδέσεις είναι προορισμοί για αυτό το multicast group και στέλνει το πακέτο μέσω των κατάλληλων διασυνδέσεων. Ο όρος reverse path forwarding χρησιμοποιείται για να περιγράψει αυτό το είδος της δρομολόγησης. Δηλαδή, το να δρομολογείς πακέτα μακριά από την πηγή, παρά κοντά από τον προορισμό.



Εικόνα 5.3.1 - Μέθοδοι δρομολόγησης

5.4 ΒΑΣΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ IP

Το πρωτόκολλο επιπέδου δικτύου προσδιορίζει την δομή του πακέτου και επεξεργασίας που χρησιμοποιούνται για τη μεταφορά των δεδομένων από τον αποστολέα στον παραλήπτη. Η λειτουργία του δε λαμβάνει υπόψη τα δεδομένα εφαρμογής (data). Αυτό επιτρέπει τη μεταφορά πακέτων για πολλούς τύπους επικοινωνίας μεταξύ πολλαπλών συσκευών.

Κάποια Network Layer Protocols είναι:

- Internet Protocol version 4 (IPv4)
- Internet Protocol version 6 (IPv6)
- Novell Internetwork Packet Exchange (IPX)
- AppleTalk
- Connectionless Network Service (CLNS/DECNet)

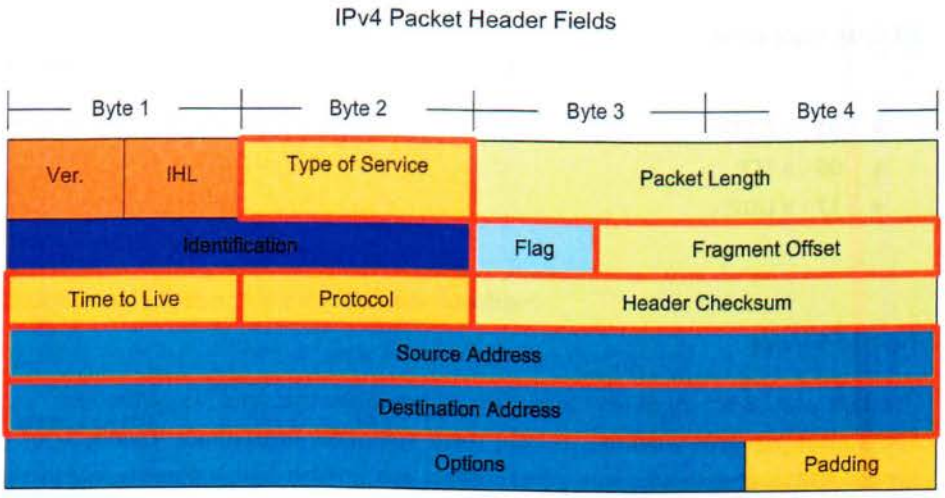
Το πρωτόκολλο Internet έχει σχεδιαστεί ως ένα πρωτόκολλο με χαμηλό overhead. Παρέχει μόνο τις λειτουργίες που είναι απαραίτητες για να παραδώσει ένα πακέτο από μια πηγή σε έναν προορισμό πάνω ένα διασυνδεδεμένο σύστημα δικτύων. Το πρωτόκολλο δεν έχει σχεδιαστεί για να εντοπίζει και να διαχειρίζεται τη ροή των πακέτων. Οι λειτουργίες αυτές εκτελούνται από άλλα πρωτόκολλα σε άλλα στρώματα.

IPv4 βασικά χαρακτηριστικά:

- Connectionless - Δεν υπάρχει σύνδεση, πριν την αποστολή πακέτων δεδομένων.
- Best Effort (αναξιόπιστη) - Δεν χρησιμοποιείται για να εγγυηθεί την παράδοση πακέτων.
- Media Independence - Λειτουργεί ανεξάρτητα από το φυσικό μέσο που φέρει τα δεδομένα.

5.5 ΔΟΜΗ ΠΑΚΕΤΟΥ IP

Σε TCP /IP δίκτυα το Network Layer PDU αναφέρεται ως IP Packet



Εικόνα 5.5.1 - Κεφαλίδα πακέτου IPv4

IP Destination Address

Περιέχει μία 32-bit δυαδική τιμή που αντιπροσωπεύει τον προορισμό των πακέτων

IP Source Address

Περιέχει μία 32-bit δυαδική τιμή που αντιπροσωπεύει την πηγή των πακέτων.

Time-to-Live

Το Time-to-Live (TTL) είναι μία 8-bit δυαδική τιμή που υποδεικνύει την υπόλοιπη "ζωή" του πακέτου. Η τιμή TTL μειώνεται με (τουλάχιστον κατά ένα) κάθε φορά που το πακέτο δέχεται επεξεργασία από έναν δρομολογητή. Όταν η τιμή γίνεται μηδέν, ο δρομολογητής δεν αποδέχεται το πακέτο ή το βγάζει εκτός «κυκλοφορίας» και αφαιρείται από τη ροή δεδομένων του δικτύου. Αυτός ο μηχανισμός αποτρέπει πακέτα που δεν μπορούν να φθάσουν στον προορισμό τους από τη διαβίβαση επ' αόριστον μεταξύ των δρομολογητών σε ένα βρόχο δρομολόγησης.

Protocol

Περιέχει μία 8-bit δυαδική τιμή και δείχνει τον τύπο του ωφέλιμου φορτίου δεδομένων που το πακέτο μεταφέρει. Επιτρέπει το στρώμα δικτύου να περάσει τα δεδομένα στο κατάλληλο ανώτερο στρώμα πρωτοκόλλου.

Κάποιες τιμές είναι:

- 01 - > ICMP
- 06 - > TCP
- 17 - > UDP

Type-of-Service

Περιέχει μια 8-bit δυαδική τιμή που χρησιμοποιείται για να καθορίσει την προτεραιότητα κάθε πακέτου. Η τιμή αυτή επιτρέπει μηχανισμό Quality – of – Service (QoS), μηχανισμός που εφαρμόζεται στα πακέτα υψηλής προτεραιότητας, όπως αυτά που μεταφέρουν δεδομένα φωνητικής τηλεφωνίας.

Fragment Offset

Ένας δρομολογητής μπορεί να χρειαστεί να τεμαχίσει ένα πακέτο κατά τη διαβίβαση από ένα μέσο σε ένα άλλο μέσο. Όταν ο κατακερματισμός συμβεί, το πακέτο IPv4 χρησιμοποιεί το Fragment Offset και τη σημαία MF στην επικεφαλίδα IP για να ανακατασκευάσει το πακέτο κατά την άφιξή του στο κεντρικό υπολογιστή προορισμού. Το Fragment Offset πεδίο προσδιορίζει τη σειρά με την οποία θα τοποθετηθεί το κάθε κομμάτι στην ανακατασκευή.

More Fragments flag

Αποτελείται από ένα bit (MF) στο πεδίο Flag . Όταν το MF= 1 τότε το κομμάτι του πακέτου εξετάζεται σε ποια σειρά πρέπει να ταξινομηθεί στην ανακατασκευή του πακέτου. Όταν το MF = 0 και το Fragment Offset έχει τιμή τότε τοποθετείται το κομμάτι ως τελευταίο στην ανακατασκευή του πακέτου. Ένα μη κατακερματισμένο πακέτο έχει MF = 0, το Fragment Offset = 0.

Don't Fragment flag

Αποτελείται από ένα bit (DF) στο πεδίο Flag. . Όταν το DF= 1 τότε δεν επιτρέπεται ο κατακερματισμός του πακέτου.

Version

Περιέχει την έκδοση της IP (πχ 4).

Header Length (IHL)

Καθορίζει το μέγεθος της επικεφαλίδας πακέτου.

Packet Length

Το πεδίο αυτό δίνει όλο το μέγεθος του πακέτου, συμπεριλαμβανομένων της επικεφαλίδας και των δεδομένων, σε bytes.

Identification

Το πεδίο αυτό χρησιμοποιείται κυρίως για τον εντοπισμό μοναδικών κομματιών ενός αρχικού πακέτου IP.

Header Checksum

Το πεδίο ελέγχου χρησιμοποιείται για τον έλεγχο σφάλματος στην επικεφαλίδα του πακέτου.

Options

Υπάρχει πρόβλεψη για επιπλέον πεδία στην επικεφαλίδα του IPv4 ώστε να παρέχονται και άλλες υπηρεσίες, αλλά αυτά χρησιμοποιούνται σπάνια.

ΚΕΦΑΛΑΙΟ 6

ΤΙΤΛΟΣ: INTERNET CONTROL MESSAGE PROTOCOL (ICMP)

6.1 ΓΕΝΙΚΑ

Το πρωτόκολλο **Internet Control Message Protocol (ICMP)** είναι ένα από τα βασικά πρωτόκολλα του διαδικτύου. Χρησιμοποιείται κυρίως από τα λειτουργικά συστήματα των ηλεκτρονικών υπολογιστών ενός δικτύου για την ανταλλαγή μηνυμάτων λάθους, όπως για παράδειγμα την έλλειψη κάποιας υπηρεσίας από έναν server ή την απουσία ενός υπολογιστή από το δίκτυο.

Το πρωτόκολλο ICMP διαφέρει από τα πρωτόκολλα TCP και UDP διότι συνήθως δεν χρησιμοποιείται από τις εφαρμογές που εκτελούνται σε κάποιον υπολογιστή, αλλά από το λειτουργικό του σύστημα. Εξαίρεση σε αυτό τον κανόνα αποτελεί το εργαλείο ping, το οποίο στέλνει μηνύματα ICMP Echo Request σε κάποιον υπολογιστή του δικτύου για να διαπιστώσει εάν ο υπολογιστής αυτός υπάρχει ή όχι και επίσης πόσο χρόνο χρειάζεται το μήνυμα να φτάσει σε αυτόν. Εάν ο υπολογιστής αυτός υπάρχει, θα απαντήσει με μηνύματα Echo Response.

6.2 ΤΕΧΝΙΚΕΣ ΛΕΠΤΟΜΕΡΕΙΕΣ

Το πρωτόκολλο ICMP έχει τυποποιηθεί στα έγγραφα RFC 792 και RFC 1122. Η έκδοση του πρωτοκόλλου που χρησιμοποιείται πιο συχνά είναι η έκδοση 4, η οποία ονομάζεται και ICMPv4 και αποτελεί μέρος του IPv4. Το IPv6 διαθέτει ένα αντίστοιχο πρωτόκολλο το οποίο ονομάζεται ICMPv6.

Τα μηνύματα ICMP κατασκευάζονται στο επίπεδο δικτύου και αποτελούν κανονικά πακέτα IP. Όπως και το πρωτόκολλο UDP, το ICMP δεν εγγυάται ότι το πακέτο θα φτάσει αξιόπιστα στον προορισμό του. Μερικές από τις πιο συνηθισμένες δικτυακές εφαρμογές χρησιμοποιούν πακέτα ICMP, όπως για παράδειγμα η εντολή traceroute. Η εντολή αυτή χρησιμοποιείται για την εύρεση όλων των κόμβων ενός δικτύου από τους οποίους πρέπει να περάσει ένα πακέτο για να φτάσει στον τελικό προορισμό του. Αυτό που κάνει ουσιαστικά είναι να στέλνει πακέτα UDP με συγκεκριμένο χρόνο ζωής (TTL – Time to Live) και να περιμένει πακέτα ICMP που να περιέχουν μήνυμα σφάλματος "ο χρόνος ζωής τελείωσε" (Time To Live exceeded in transit) ή "ο προορισμός δεν βρέθηκε" (Destination unreachable). Στο σημείο αυτό αξίζει να αναφερθεί ότι ο χρόνος ζωής (TTL - Time To Live) ενός πακέτου είναι ο μέγιστος αριθμός των κόμβων του δικτύου από τους οποίους θα πρέπει να περάσει έως ότου φτάσει στον προορισμό του. Εάν ένα πακέτο κατά την πορεία του στο δίκτυο περάσει από περισσότερους κόμβους απ' ότι αναγράφεται στο πεδίο TTL, τότε το πακέτο αυτομάτως απορρίπτεται και ο υπολογιστής ο οποίος διαπίστωσε το σφάλμα στέλνει ένα ICMP μήνυμα σφάλματος στον υπολογιστή που δημιούργησε το πακέτο. Τέλος, η εντολή ping χρησιμοποιεί επίσης το πρωτόκολλο ICMP για την λειτουργία της και συγκεκριμένα τα ICMP μηνύματα "Echo request" και "Echo reply".

6.3 ΔΟΜΗ ΠΑΚΕΤΟΥ ICMP

Στον πίνακα που ακολουθεί φαίνεται η κεφαλίδα (header) ενός πακέτου ICMP. Ακολουθεί επεξήγηση των πεδίων της ICMP κεφαλίδας. Τα πεδία της IP κεφαλίδας εξηγούνται στο υποκεφάλαιο 5.4 για το IP - Internet Protocol.

+	Bits 0–3	4–7	8–15	16–18	19–31
0	Version	IHL	TOS/DSCP/ECN	Total Length	
32	Identification			Flags	Fragment Offset
64	Time to Live		Protocol	IP Header Checksum	
96	Source Address				
128	Destination Address				
160					
192					

Πίνακας 6.3.1 - Κεφαλίδα πακέτου ICMP

- **Type**
  Ο κωδικός του τύπου μηνύματος ICMP.

- **Code**
  Το πεδίο αυτό χρησιμοποιείται ως επέκταση του προηγούμενου. Για παράδειγμα εάν το πεδίο Type περιέχει την τιμή 3 (Destination Unreachable), τότε το πεδίο αυτό μπορεί να περιέχει έναν κωδικό από το 1 έως το 15 που να δίνει τον λόγο για τον οποίο ο υπολογιστής που ψάχνουμε είναι εκτός δικτύου.

- **Checksum**
  Το πεδίο αυτό χρησιμοποιείται για τον έλεγχο σφαλμάτων κατά την μετάδοση του πακέτου.

- **ID**
  Η τιμή ID του πακέτου, η οποία επιστρέφεται στον υπολογιστή που δημιούργησε το πακέτο στην περίπτωση που έχουμε απάντηση ECHO REPLY.

- **Sequence**
  Αυτό το πεδίο περιέχει την τιμή σειράς του πακέτου και επιστρέφεται στον υπολογιστή που δημιούργησε το πακέτο στην περίπτωση που έχουμε απάντηση ECHO RE

ΛΙΣΤΑ ΜΗΝΥΜΑΤΩΝ ΕΛΕΓΧΟΥ ICMP

- 0 - Echo Reply
- 1 - Reserved
- 2 - Reserved
- 3 - Destination Unreachable
- 4 - Source Quench
- 5 - Redirect Message
- 6 - Alternate Host Address
- 7 - Reserved
- 8 - Echo Request
- 9 - Router Advertisement
- 10 - Router Solicitation
- 11 - Time Exceeded
- 12 - Parameter Problem
- 13 - Timestamp
- 14 - Timestamp Reply
- 15 - Information Request
- 16 - Information Reply
- 17 - Address Mask Request
- 18 - Address Mask Reply
- 19 - Reserved for security
- 20-29 - Reserved for robustness experiment
- 30 - Traceroute
- 31 - Datagram Conversion Error
- 32 - Mobile Host Redirect
- 33 - IPv6 Where-Are-You
- 34 - IPv6 Here-I-Am
- 35 - Mobile Registration Request
- 36 - Mobile Registration Reply
- 37 - Domain Name Request
- 38 - Domain Name Reply
- 39 - SKIP Algorithm Discovery Protocol, Simple Key-Management for Internet Protocol
- 40 - Photuris, Security failures
- 41 - ICMP for experimental mobility protocols such as Seamoby [RFC4065]
- 42-255 - Reserved

ΚΕΦΑΛΑΙΟ 7

ΤΙΤΛΟΣ: TRANSPORT LAYER – TCP (TRANSMISSION CONTROL PROTOCOL)

7.1 ΓΕΝΙΚΑ

Το **TCP** ***(Transmission Control Protocol - Πρωτόκολλο Ελέγχου Μεταφοράς)*** είναι ένα από τα κυριότερα πρωτόκολλα της Σουίτας Πρωτοκόλλων Διαδικτύου. Βρίσκεται πάνω από το IP protocol *(πρωτόκολλο IP)*. Οι κύριοι στόχοι του πρωτοκόλλου TCP είναι να επιβεβαιώνεται η αξιόπιστη αποστολή και λήψη δεδομένων, επίσης να μεταφέρονται τα δεδομένα χωρίς λάθη μεταξύ του στρώματος δικτύου (network layer) και του στρώματος εφαρμογής (application layer) και, φτάνοντας στο πρόγραμμα του στρώματος εφαρμογής, να έχουν σωστή σειρά. Οι περισσότερες σύγχρονες υπηρεσίες στο Διαδίκτυο βασίζονται στο TCP. Για παράδειγμα το SMTP (port 25), το παλαιότερο (και μη-ασφαλές) Telnet (port 23), το FTP και πιο σημαντικό το HTTP (port 80), γνωστό ως υπηρεσίες World Wide Web (WWW - Παγκόσμιος Ιστός). Το TCP χρησιμοποιείται σχεδόν παντού, για αμφίδρομη επικοινωνία μέσω δικτύου.

Αρχικά το **Transmission** ήταν **Transfer**, ένας όρος που προσδιόριζε την μεταβίβαση του ελέγχου στα άκρα του δικτύου **TCPIP** πριν αποσπαστεί το **IP**.

7.2 TCP ΕΠΙΚΕΦΑΛΙΔΑ

Τα πακέτα του πρωτοκόλλου TCP καλούνται segments (τμήματα)[2] Ένα από τα κυριότερα μέρη ενός segment είναι η TCP επικεφαλίδα (TCP header), η οποία παρέχει συγκεκριμένες πληροφορίες για το πρωτόκολλο TCP. Το ελάχιστο μέγεθος της επικεφαλίδας είναι 5 words και το μέγιστο 15 words (απουσία ή παρουσία όλων των options αντίστοιχα).

TCP επικεφαλίδα				
+	Bits 0 - 3	4 - 9	10 - 15	16 - 31
0	**Source** Port Θύρα Προέλευσης			**Destination** Port Θύρα Προορισμού
32	**Sequence** Number Αριθμός ακολουθίας			
64	**Acknowledgment** Number Αριθμός επιβεβαίωσης			
96	**Data Offset**	**Reserved**	**Flags** Σημαίες	**Window** Παράθυρο
128	**Checksum** Άθροισμα ελέγχου			**Urgent** Pointer Επείγοντα δεδομένα
160	**Options** Επιλογές (προαιρετικές)			
160/192+	**Data** Δεδομένα			

Πίνακας 7.2.1 - TCP επικεφαλίδα

- **Source Port**
  Αυτό το πεδίο προσδιορίζει την port (θύρα) του αποστολέα

- **Destination Port**
  Αυτό το πεδίο προσδιορίζει την port (θύρα) του παραλήπτη

- **Sequence Number**
  Ο sequence number (αριθμός ακολουθίας) έχει διπλό ρόλο:

  - Εαν υπάρχει η SYN flag (SYN σημαία) τότε είναι ο αρχικός αριθμός ακολουθίας (ISN - initial sequence number) και η πρώτη octet δεδομένων του πακέτου είναι ο ISN+1.
  - Αλλιώς, εαν δεν υπάρχει η SYN flag, τότε η πρώτη octet δεδομένων είναι ο αριθμός ακολουθίας.

- **Acknowledgment number**
  Όταν υπάρχει η ACK flag η τιμή αυτού του πεδίου δείχνει τον επόμενο sequence number (αριθμό ακολουθίας) που αναμένει ο αποστολέας.

- **Data offset**

Είναι ο αριθμός από words μεγέθους 32 bit στην επικεφαλίδα TCP (TCP header). Καθορίζει το μέγεθος της επικεφαλίδας (πολλαπλάσιο του 32) και επομένως δείχνει και την αρχή των δεδομένων.

- **Reserved**
  Πεδίο 6 bit "κρατημένων" (αγγλ. reserved) για μελλοντική χρήση. Η τιμή των bit πρέπει να είναι 0.

- **Flags** *(επίσης γνωστό ως bits ελέγχου - Control bits)*
  Περιέχει 6 bit - σημαίες:

Σημαία	Σημασία	Προέλευση ονομασίας
URG	Το πεδίο urgent pointer είναι σημαντικό	**URG**ent
ACK	Το πεδίο επιβεβαίωσης είναι σημαντικό	**ACK**nowledgment
PSH	Λειτουργία ώθησης	**PuSH**
RST	Επαναρύθμιση σύνδεσης	**ReSeT**
SYN	Συγχρονισμός αριθμών ακολουθίας	**SYN**chronize
FIN	Ο αποστολέας δεν στέλνει άλλα δεδομένα	**FIN** (=τέλος)

Πίνακας 7.2.2 - Flags

- **Window**
  Ο αριθμός από octets δεδομένων (bytes) που επιθυμεί να δεχτεί ο αποστολέας του πακέτου, αρχίζοντας από εκείνη που δείχνει το πεδίο επιβεβαίωσης (acknowledgment field).

- **Checksum**
  Το πεδίο checksum μεγέθους 16 bit χρησιμοποιείται για έλεγχο λαθών στην επικεφαλίδα και στα δεδομένα.

- **Options**
  Μεταβλητή, η οποία καθορίζει ειδικές επιλεγόμενες ρυθμίσεις και μπορεί να καταλάβει χώρο στο τέλος της επικεφαλίδας TCP (TCP header). Το μήκος τους είναι πολλαπλάσιο των 8 bit και σε το περιεχόμενο της επικεφαλίδας μετά την τελευταία επιλογή πρέπει να γεμίζει (πχ. με μηδενικά - 0). Με αυτόν τον τρόπο το data offset θα δείχνει σωστά την αρχή των δεδομένων.

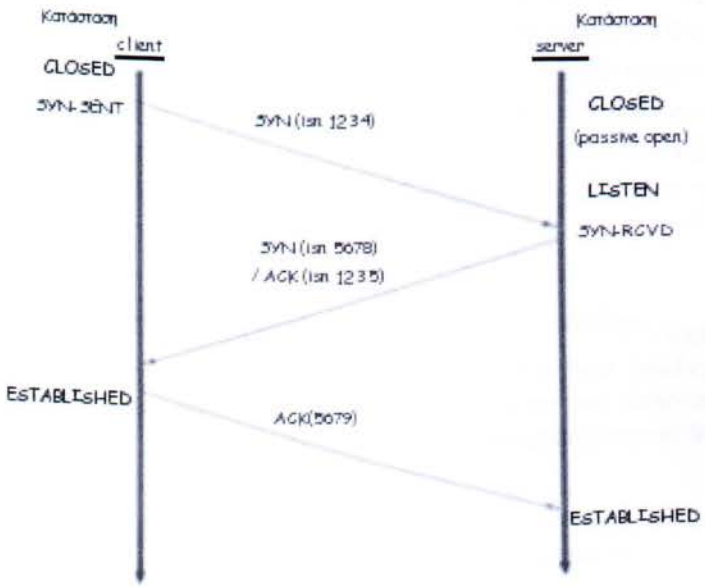
- **Urgent pointer**
  Εάν είναι ενεργοποιημένο το URG bit ελέγχου, τότε αυτό το πεδίο δείχνει τον αριθμό ακολουθίας (sequence number)της octet που βρίσκεται αμέσως μετά

το τελευταίο byte από τα επείγοντα δεδομένα. Έτσι παρουσιάζει τη θέση του τελευταίου byte με επείγοντα δεδομένα.

7.3 ΕΝΑΡΞΗ – ΤΡΙΜΕΡΗΣ ΧΕΙΡΑΨΙΑ /3 – WAY HANDSHAKE

Το πρωτόκολλο ελέγχου μεταφορών (TCP) είναι connection oriented, δηλαδή η μεταφορά δεδομένων γίνεται μέσω σύνδεσης, η οποία οριοθετείται από ένα σήμα έναρξης και ένα σήμα τέλους ή διακοπής.

Πριν να προσπαθήσει ένα πρόγραμμα-πελάτης (client) να συνδεθεί με έναν server, ο server πρέπει πρώτα να δεσμεύσει μια port και να την ανοίξει ώστε να δέχεται συνδέσεις: αυτό καλείται passive open. Όταν γίνει αυτό, ο client μπορεί να αρχίσει τη σύνδεση (active open). Για να γίνει μια σύνδεση, γίνεται μια "χειραψία" ανάμεσα στα συμμετέχοντα μέρη, το λεγόμενο **three-way handshake**:



Εικόνα 7.3.1 - 3 way handshake

Έναρξη της σύνδεσης με three-way handshake

1.Αρχικά αποστέλλεται ένα πακέτο με το SYN bit ενεργοποιημένο. Ο client θέτει το πεδίο αριθμού ακολουθίας στην TCP επικεφαλίδα (TCP header) στον αρχικό αριθμό ακολουθίας του (ISN - initial sequence number).

2.Ο server στο άλλο άκρο απαντάει:

- είτε με SYN (για να στείλει και το δικό του ISN) και ACK (που έχει το ISN+1 του client) του πρώτου πακέτου του client για να αποδεχτεί τη σύνδεση,
- ή SYN/RST για να ενημερώσει τον client ότι αρνείται τη σύνδεση και η διαδικασία σταματά.

3.Όταν ο client πάρει ένα πακέτο SYN/ACK απαντάει, αυτή τη φορά, με ένα πακέτο ACK. Σε αυτό το σημείο, τα δύο μέρη συνδέονται και μπορούν πλέον να σταλούν τα δεδομένα.

Κατά τη διάρκεια του three-way handshake, τα δύο μέρη διαπραγματεύονται επίσης όλες τις ειδικές επιλογές που θα χρησιμοποιηθούν κατά τη διάρκεια της σύνδεσης TCP, όπως ECN κ.α.

7.4 ΜΕΤΑΦΟΡΑ ΔΕΔΟΜΕΝΩΝ

Μόλις ανταλλαχθούν οι ISNs, οι εφαρμογές μπορούν να διαβιβάσουν δεδομένα η μια στην άλλη. Η ανάλυση του τρόπου με τον οποίο γίνεται η μεταφορά δεδομένων, απαιτεί εξέταση για

- έλεγχο ροής (flow control) και
- τεχνικές ελέγχου συμφόρησης (congestion avoidance).

Σε μια απλή υλοποίηση του TCP, χωρίς τους προαναφερθέντες ελέγχους, η εφαρμογή θα στείλει πακέτα στο δίκτυο προς τον παραλήπτη, εφ' όσον υπάρχουν δεδομένα να σταλούν και εφ' όσον ο αποστολέας δεν υπερβαίνει το window που του έχει υποδείξει ο παραλήπτης. Όταν ο παραλήπτης δέχεται πακέτα TCP, στέλνει επιβεβαιώσεις (acknowledgement), δείχνοντας σε ποιο σημείο του ρεύματος από byte (byte stream) βρίσκεται. Αυτές οι επιβεβαιώσεις περιέχουν επίσης το επόμενο window (παράθυρο) που καθορίζει πόσα byte επιθυμεί να δεχτεί στη συνέχεια ο παραλήπτης.

Εάν ορισμένα δεδομένα αναπαράγονται ή χάνονται, μπορεί να δημιουργηθεί ένα κενό στο ρεύμα από byte (byte stream). Ο παραλήπτης θα συνεχίσει να επιβεβαιώνει την νεότερη θέση που βρίσκεται, στο ρεύμα από byte που έχει δεχτεί.

Εάν δεν υπάρχουν δεδομένα για να σταλούν, ο αποστολέας θα βρίσκεται σε αδράνεια αναμένοντας την εφαρμογή να βάλει δεδομένα στο byte stream ή να παραλάβει δεδομένα από το άλλο άκρο της σύνδεσης.

7.5 ΕΛΕΓΧΟΣ ΡΟΗΣ

Ο έλεγχος ροής απαιτεί την επιβεβαίωση λήψης (acknowledgment) κάθε πακέτου από τον απόμακρο host πριν να σταλεί το επόμενο. Οι αλγόριθμοι για το sliding window, που χρησιμοποιούνται από το TCP, επιτρέπουν σε πολλαπλά πακέτα δεδομένων να μεταφέρονται ταυτόχρονα για να χρησιμοποιείται αποδοτικότερα το εύρος ζώνης (bandwidth) ενός δικτύου.

Για παράδειγμα, εαν ένας υπολογιστής Α στείλει 4 byte με αριθμό ακολουθίας (sequence number) 100 - συνεπώς, τα 4 bytes έχουν αριθμό ακολουθίας 100, 101, 102 και 103 - τότε ο παραλήπτης πρέπει να απαντήσει με επιβεβαίωση (acknowledgement) που φέρει sequence number 104. Αυτό πρόκειται να είναι το επόμενο byte που περιμένει στο επόμενο πακέτο. Εαν για κάποιο λόγο, τα τελευταία δύο bytes περιέχουν σφάλματα τότε η τιμή της επιβεβαίωσης θα είναι 102, εφόσον τα bytes με αριθμό 100 και 101 έχουν φτάσει με επιτυχία.

7.6 ΕΛΕΓΧΟΣ ΣΥΜΦΟΡΗΣΗΣ

Αν και το TCP συνήθως δεν ενδιαφέρεται για όσα συμβαίνουν στο διαδίκτυο (αυτό είναι εργασία που εκτελείται από IP protocol στο 3ο επίπεδο του μοντέλου OSI) πρέπει να είναι αρκετά "έξυπνο", ώστε να αντιληφθεί και να χειριστεί κατάλληλα μια συμφόρηση στο δίκτυο. Το TCP δεν μπορεί να αγνοήσει τι συμβαίνει στο διαδίκτυο μεταξύ των δύο συνδεδεμένων άκρων.

Για αυτόν τον λόγο, το TCP περιλαμβάνει διάφορους συγκεκριμένους αλγορίθμους που έχουν ως σκοπό είτε να αποφύγουν εξ αρχής τη συμφόρηση, είτε να ανταποκριθούν σε αυτή. Χρησιμοποιούνται διάφοροι μηχανισμοί για να επιτευχθεί υψηλή απόδοση και να μην υπερφορτωθεί το δίκτυο. Αυτοί οι μηχανισμοί περιλαμβάνουν:

- τον αλγόριθμο slow-start,
- τον αλγόριθμο congestion avoidance,
- τον αλγόριθμο fast retransmit και
- τον αλγόριθμο fast recovery

όπως αναφέρεται στο RFC 2001.

7.7 ΤΕΡΜΑΤΙΣΜΟΣ / 4 – WAY HANDSHAKE

Η σύνδεση τερματίζεται με ένα **four-way handshake**, με την κάθε πλευρά να τερματίζει ανεξάρτητα:

1.Όταν κάποιο άκρο επιθυμεί να κλείσει τη σύνδεση από πλευράς του, στέλνει ένα πακέτο με το FIN ενεργοποιημένο,

2.Το πακέτο αυτό επιβεβαιώνει η άλλη πλευρά με ένα ACK και

3.στη συνέχεια, στέλνει το ένα πακέτο FIN

4.Η πλευρά που ξεκίνησε τον τερματισμό, μπορεί να το επιβεβαιώσει στέλνοντας ένα πακέτο ACK.

Με αυτόν τον τρόπο, για έναν τυπικό τερματισμό χρειάζεται ένα ζεύγος πακέτων FIN και ACK για κάθε άκρο στη σύνδεση TCP. Μια σύνδεση μπορεί να είναι "half-open", δηλαδή η μία πλευρά να έχει τερματίσει, όχι όμως και η άλλη. Η πλευρά που έχει τερματίσει δεν μπορεί να στείλει πλέον δεδομένα, ενώ η άλλη μπορεί.

Τέλος, είναι δυνατό, αν και λιγότερο πιθανό, οι δύο host να στείλουν ταυτόχρονα ένα πακέτο FIN ο ένας στον άλλο. Στη συνέχεια ο καθένας επιβεβαιώνει το FIN που δέχτηκε με ένα πακέτο ACK. Στο σημείο αυτό και οι δύο διακόπτουν τη σύνδεση.

ΚΕΦΑΛΑΙΟ 8

ΤΙΤΛΟΣ: TRANSPORT LAYER - UDP (USER DATAGRAM PROTOCOL)

8.1 ΓΕΝΙΚΑ

Το πρωτόκολλο **User Datagram Protocol (UDP)** είναι ένα από τα βασικά πρωτόκολλα που χρησιμοποιούνται στο Διαδίκτυο. Μία εναλλακτική ονομασία του πρωτοκόλλου είναι **Universal Datagram Protocol**. Διάφορα προγράμματα χρησιμοποιούν το πρωτόκολλο UDP για την αποστολή σύντομων μηνυμάτων (γνωστών και ως datagrams) από τον έναν υπολογιστή στον άλλον μέσα σε ένα δίκτυο υπολογιστών.

Ένα από τα κύρια χαρακτηριστικά του UDP είναι ότι δεν εγγυάται αξιόπιστη επικοινωνία. Τα πακέτα UDP που αποστέλλονται από έναν υπολογιστή μπορεί να φτάσουν στον παραλήπτη με λάθος σειρά, διπλά ή να μην φτάσουν καθόλου εάν το δίκτυο έχει μεγάλο φόρτο. Αντιθέτως, το πρωτόκολλο TCP διαθέτει όλους τους απαραίτητους μηχανισμούς ελέγχου και επιβολής της αξιοπιστίας και συνεπώς μπορεί να εγγυηθεί την αξιόπιστη επικοινωνία μεταξύ των υπολογιστών. Η έλλειψη των μηχανισμών αυτών από το πρωτόκολλο UDP το καθιστά αρκετά πιο γρήγορο και αποτελεσματικό, τουλάχιστον για τις εφαρμογές εκείνες που δεν απαιτούν αξιόπιστη επικοινωνία.

Οι εφαρμογές audio και video streaming χρησιμοποιούν κατά κόρον πακέτα UDP. Για τις εφαρμογές αυτές είναι πολύ σημαντικό τα πακέτα να παραδοθούν στον παραλήπτη σε σύντομο χρονικό διάστημα ούτως ώστε να μην υπάρχει διακοπή στην ροή του ήχου ή της εικόνας. Κατά συνέπεια προτιμάται το πρωτόκολλο UDP διότι είναι αρκετά γρήγορο, παρόλο που υπάρχει η πιθανότητα μερικά πακέτα UDP να χαθούν. Στην περίπτωση που χαθεί κάποιο πακέτο, οι εφαρμογές αυτές διαθέτουν ειδικούς μηχανισμούς διόρθωσης και παρεμβολής ούτως ώστε ο τελικός χρήστης να μην παρατηρεί καμία αλλοίωση ή διακοπή στην ροή του ήχου και της εικόνας λόγω του χαμένου πακέτου. Σε αντίθεση με το πρωτόκολλο TCP, το UDP υποστηρίζει broadcasting, δηλαδή την αποστολή ενός πακέτου σε όλους τους υπολογιστές ενός δικτύου, και multicasting, δηλαδή την αποστολή ενός πακέτου σε κάποιους συγκεκριμένους υπολογιστές ενός δικτύου. Η τελευταία δυνατότητα χρησιμοποιείται πολύ συχνά στις εφαρμογές audio και video streaming ούτως ώστε μία ροή ήχου ή εικόνας να μεταδίδεται ταυτόχρονα σε πολλούς συνδρομητές.

Μερικές σημαντικές εφαρμογές που χρησιμοποιούν πακέτα UDP είναι οι εξής: Domain Name System (DNS), IPTV, Voice over IP (VoIP), Trivial File Transfer Protocol (TFTP) και τα παιχνίδια που παίζονται ζωντανά μέσω του Διαδικτύου.

8.2 ΔΟΜΗ UDP ΠΑΚΕΤΟΥ

Η δομή ενός πακέτου UDP περιγράφεται αναλυτικά στο αντίστοιχο πρότυπο IETF RFC 768. Στην σουίτα πρωτοκόλλων του Διαδικτύου, το UDP βρίσκεται ανάμεσα στο επίπεδο δικτύου (network layer) και στο επίπεδο συνόδου (session layer) ή εφαρμογών (application layer).

Κάθε πακέτο UDP έχει μία κεφαλίδα (header) που αναφέρει τα χαρακτηριστικά του. Η κεφαλίδα περιλαμβάνει μονάχα 4 πεδία, τα οποία είναι πολύ λίγα εάν συγκριθούν με άλλα πρωτόκολλα, όπως το TCP. Δύο από τα τέσσερα πεδία είναι προαιρετικά.

+	Bits 0 - 15	16 - 31
0	Source Port	Destination Port
32	Length	Checksum
64	Data	

Πίνακας 8.2.1 - Κεφαλίδα UDP πακέτου

Ακολουθεί μία συνοπτική εξήγηση των πεδίων:

Source port

- Η πόρτα του αποστολέα από την οποία προήλθε το πακέτο. Εάν ο παραλήπτης επιθυμεί να στείλει κάποια απάντηση, θα πρέπει να την στείλει στην πόρτα αυτήν. Το συγκεκριμένο πεδίο δεν είναι υποχρεωτικό και στις περιπτώσεις που δεν χρησιμοποιείται θα πρέπει να έχει την τιμή μηδέν.

- **Destination port**
  Η πόρτα του παραλήπτη στην οποία θα πρέπει να παραδοθεί το πακέτο.

- **Length**
  Το πεδίο αυτό έχει μέγεθος 16-bit και περιλαμβάνει το μέγεθος του πακέτου σε bytes. Το μικρότερο δυνατό μέγεθος είναι 8 bytes, αφού η κεφαλίδα αυτή καθ' αυτή καταλαμβάνει τόσο χώρο. Θεωρητικά, το μέγεθος του UDP πακέτου δεν μπορεί να ξεπερνάει τα 65,527 bytes, αλλά πρακτικά το όριο μειώνεται στα 65,507 bytes λόγω διαφόρων περιορισμών που εισάγει το πρωτόκολλο IPv4 στο επίπεδο δικτύου.

- **Checksum**
  Ένα πεδίο 16-bit το οποίο χρησιμοποιείται για επαλήθευση της ορθότητας του πακέτου στο σύνολό του, δηλαδή τόσο της κεφαλίδας όσο και των δεδομένων.

Στην συνέχεια το πακέτο UDP περνάει στο επίπεδο δικτύου, το οποίο αναλαμβάνει να το μεταδώσει στο δίκτυο υπολογιστών. Το επίπεδο αυτό τοποθετεί μία ακόμη κεφαλίδα στο πακέτο, η οποία διαφέρει ανάλογα με την έκδοση του πρωτοκόλλου που χρησιμοποιείται στο επίπεδο δικτύου (IPv4 ή IPv6).

- Για **IPv4**, το πακέτο λαμβάνει την ακόλουθη μορφή:

+	Bits 0 - 7	8 - 15	16 - 23	24 - 31
0	Source address			
32	Destination address			
64	Zeros	Protocol	UDP length	
96	Source Port		Destination Port	
128	Length		Checksum	
160	Data			

Πίνακας 8.2.2

- **Source Address, Destination Address**
  Οι διευθύνσεις IP του αποστολέα και του παραλήπτη αντίστοιχα.

- **Zeros**
  Μία ακολουθία μηδενικών, η οποία δεν παίζει κανέναν ρόλο κατά την μετάδοση του πακέτου.

- **Protocol**
  Ένας χαρακτηριστικός αριθμός που αντιστοιχεί στο πρωτόκολλο που χρησιμοποιείται. Για το UDP η τιμή που παίρνει το πεδίο αυτό είναι 17.

- **UDP Lenght**
  Το συνολικό μέγεθος του πακέτου UDP.

8.3 ΧΡΗΣΙΜΟΤΗΤΑ – ΕΦΑΡΜΟΓΕΣ UDP

Εφαρμογές UDP

Όπως αναφέρθηκε και προηγουμένως, οι εφαρμογές που χρησιμοποιούν το πρωτόκολλο UDP θα πρέπει να μπορούν να δεχτούν κάποια απώλεια πακέτων ή διάφορα σφάλματα στα πακέτα τα οποία στέλνουν. Μερικές εφαρμογές, όπως για παράδειγμα το Trivial File Transfer Protocol (TFTP) υλοποιούν δικούς τους μηχανισμούς διασφάλισης της αξιοπιστίας της επικοινωνίας. Πάντως, τις περισσότερες φορές οι εφαρμογές που χρησιμοποιούν το UDP δεν επιβάλλουν επιπρόσθετους μηχανισμούς αξιοπιστίας διότι θα παρεμποδίζονται από αυτούς και χειροτερεύει η απόδοσή τους. Κλασικό παράδειγμα τέτοιων προγραμμάτων είναι οι εφαρμογές πραγματικού χρόνου (πχ. media streaming, παιχνίδια στο διαδίκτυο, VoIP κτλ). Στην περίπτωση πάντως που μία εφαρμογή χρειάζεται αξιόπιστη μετάδοση δεδομένων, δηλαδή η πλειοψηφία των εφαρμογών του διαδικτύου, θα προτιμήσει να χρησιμοποιήσει το πρωτόκολλο TCP αντί του UDP.

Σε ένα τυπικό δίκτυο υπολογιστών, η κίνηση που προέρχεται από την μετάδοση UDP πακέτων ανέρχεται σε ένα αρκετά μικρό ποσοστό. Παρόλα αυτά όμως, το πρωτόκολλο αυτό το χρησιμοποιούν πολύ σημαντικές εφαρμογές, στην σωστή λειτουργία των οποίων βασίζεται το διαδίκτυο. Τέτοιες εφαρμογές είναι για παράδειγμα οι εξής: Domain Name System (DNS), Simple Network Management Protocol (SNMP), Dynamic Host Configuration Protocol (DHCP) και το Routing Information Protocol (RIP).

Γιατί υπάρχει το UDP; Τι εξυπηρετεί;

Το TCP λοιπόν, σύμφωνα με όσο αναφέραμε παραπάνω, φαντάζει σαν μια ιδανική λύση για την σωστή και αξιόπιστη κυρίως μεταφορά των δεδομένων μας. Γιατί χρησιμοποιούμε το UDP; Το UDP υπάρχει ακριβώς γιατί υπάρχουν εφαρμογές, όπου δεν μας ενδιαφέρει τόσο η ακεραιότητα των δεδομένων, όσο τα δεδομένα να φτάσουν όσο δυνατόν γρηγορότερα στον παραλήπτη, έστω και με κάποια απώλεια. Εκεί δηλαδή που το TCP είναι αργό και δεν μας εξυπηρετεί, έρχεται να πάρει τη θέση του το UDP. Μερικές εφαρμογές που χρησιμοποιούν το UDP είναι οι παρακάτω:

•

Εφαρμογές οι οποίες μεταδίδουν real-time audio/video, όπως IPTV, VoIP. Εδώ μας ενδιαφέρει τα δεδομένα να φτάνουν την σωστή χρονική στιγμή. Οποιαδήποτε απώλεια τους μας επηρεάζει μόνο στην ποιότητα του αναπαραγόμενου σήματος.

8.4 ΔΙΑΦΟΡΕΣ ΜΕΤΑΞΥ TCP ΚΑΙ UDP

Το πρωτόκολλο TCP λειτουργεί εγκαθιδρύοντας συνδέσεις μεταξύ του αποστολέα και του παραλήπτη των πακέτων. Από την στιγμή που μία σύνδεση εγκαθιδρυθεί με επιτυχία, όλα τα δεδομένα αποστέλλονται από τον έναν υπολογιστή στον άλλο με

την μορφή πακέτων χρησιμοποιώντας την 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 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.

ΚΕΦΑΛΑΙΟ 9

ΤΙΤΛΟΣ: ΑΝΩΤΕΡΑ ΕΠΙΠΕΔΑ ΣΤΟ OSI ΜΟΝΤΕΛΟ (UPPER LAYERS)

9.1 ΕΠΙΠΕΔΟ 5: ΣΥΝΟΔΟΥ

Το *επίπεδο συνόδου* ελέγχει τις συνόδους (δηλαδή τις ανταλλαγές δεδομένων) μεταξύ δύο υπολογιστών, του Α και του Β. Ξεκινά, διαχειρίζεται και τερματίζει τη σύνδεση μεταξύ μιας τοπικής και μιας απομακρυσμένης εφαρμογής. Αντιμετωπίζει λειτουργίες FDX (*full duplex, οι Α και Β μιλούν ταυτόχρονα από δύο κανάλια*) ή HDX (*half-duplex, μιλάει ο Α και μετά απαντάει ο Β από το ένα διαθέσιμο κανάλι*), ενώ υποστηρίζει διαδικασίες αποθήκευσης κατάστασης (checkpoint), αναβολής (adjournment), τερματισμού (αγγλ. termination) και επανεκκίνησης (restart). Αυτό το επίπεδο είναι υπεύθυνο για το ομαλό κλείσιμο της συνόδου (που είναι ιδιότητα του TCP) και επίσης για την *αποθήκευση* και *ανάκτηση κατάστασης*, λειτουργίες οι οποίες δεν χρησιμοποιούνται στην στοίβα πρωτοκόλλων του Διαδικτύου.

9.2 ΕΠΙΠΕΔΟ 6: ΠΑΡΟΥΣΙΑΣΗΣ

Το *επίπεδο παρουσίασης* μετασχηματίζει τα δεδομένα σε τυπική μορφή που την αναμένει το επίπεδο εφαρμογών. Στο επίπεδο αυτό τα δεδομένα υφίστανται κρυπτογράφηση, συμπίεση, κωδικοποίηση MIME και όποια άλλη διαμόρφωση απαιτεί η μορφή δεδομένων ή ο σχεδιαστής του πρωτοκόλλου. Παραδείγματα αποτελούν η μετατροπή αρχείων από κώδικα EBCDIC σε κώδικα ASCII και η μετατροπή της δομής των δεδομένων σε μορφή XML ή αντίστροφα (π.χ. από XML σε έγγραφο τύπου DOC).

9.3 ΕΠΙΠΕΔΟ 7: ΕΦΑΡΜΟΓΩΝ

Το *επίπεδο εφαρμογών* παρέχει στον χρήστη έναν τρόπο να προσπελάσει μέσω μιας εφαρμογής τις πληροφορίες ενός δικτύου. Αυτό το επίπεδο είναι η κύρια διασύνδεση του χρήστη με την εφαρμογή και, συνεπώς, με το δίκτυο. Στο επίπεδο αυτό γίνεται η διαχείριση των κατανεμημένων εφαρμογών, η αποστολή του ηλεκτρονικού ταχυδρομείου κλπ. Παραδείγματα πρωτοκόλλων επιπέδου εφαρμογών αποτελούν τα Telnet, FTP, SMTP και http.

ΚΕΦΑΛΑΙΟ 10

ΤΙΤΛΟΣ: ΠΡΩΤΟΚΟΛΛΑ ΔΡΟΜΟΛΟΓΗΣΗΣ

10.1 ΓΕΝΙΚΑ

Τα πρωτόκολλα δρομολόγησης (routing protocols) είναι υπεύθυνα για:

- την επιλογή του καλύτερου δρόμου προς οποιοδήποτε δίκτυο/υποδίκτυο προορισμού
- την κατάλληλη ενημέρωση των πινάκων δρομολόγησης
- την ανταλλαγή πληροφοριών δρομολόγησης μεταξύ των δρομολογητών ενός δικτύου.

Υπάρχουν δυο βασικά πρωτόκολλα δρομολόγησης:

- **τα εσωτερικά πρωτόκολλα πύλης IGP (Interior Gateway Protocols)** τα οποία χρησιμοποιούνται για την επικοινωνία των δρομολογητών και την ανταλλαγή των πινάκων δρομολόγησης τους σε ένα **αυτόνομο σύστημα (autonomous system).** (π.χ RIP, OSPF) *Αυτόνομο σύστημα είναι ένα σύνολο δικτύων που εποπτεύονται από μια κοινή αρχή διαχείρισης.*
- **τα εξωτερικά πρωτόκολλα πύλης EGP (Exterior Gateway Protocols)** τα οποία χρησιμοποιούνται για την επικοινωνία των δρομολογητών και την ανταλλαγή των πινάκων δρομολόγησης τους μεταξύ αυτόνομων συστημάτων (π.χ BGP).

10.2 ΑΛΓΟΡΙΘΜΟΙ ΔΡΟΜΟΛΟΓΗΣΗΣ

Βασική λειτουργία των πρωτοκόλλων δρομολόγησης είναι η εύρεση και η επιλογή του καλύτερου δρόμου για τα δίκτυα προορισμού με τη χρήση κατάλληλων **αλγορίθμων δρομολόγησης (routing algorithms)**. Ο αλγόριθμος δρομολόγησης δημιουργεί έναν αριθμό, τον οποίο ονομάζουμε **τιμή κόστους (metric),** για κάθε διαδρομή στο δίκτυο. Η διαδρομή με το μικρότερο κόστος για τον ίδιο προορισμό καταχωρείται τελικά στον πίνακα δρομολόγησης. Ανάλογα με την υλοποίηση, ως κόστος μπορεί να χρησιμοποιηθεί ο αριθμός των δρομολογητών (hop count) που περνά το μήνυμα μέχρι να φτάσει στον προορισμό του, το εύρος ζώνης της γραμμής (bandwidth), η καθυστέρηση (delay), το φορτίο της γραμμής (load) και μια σειρά άλλων παραμέτρων ή ένας συνδυασμός από αυτές. Οι αλγόριθμοι δρομολόγησης χωρίζονται σε δυο κατηγορίες:

- **αλγόριθμοι διανύσματος απόστασης (Distance Vector Algorithms),** όπου οι πίνακες δρομολόγησης αποτελούνται από μια σειρά από προορισμούς (vectors) και κόστη τις αποστάσεις (distances) που διανύονται για την προσέγγιση του προορισμού.
- **αλγόριθμοι της κατάστασης της σύνδεσης (Link State Algorithms)**

ΚΕΦΑΛΑΙΟ 11

ΤΙΤΛΟΣ: ROUTING INFORMATION PROTOCOL (RIP)

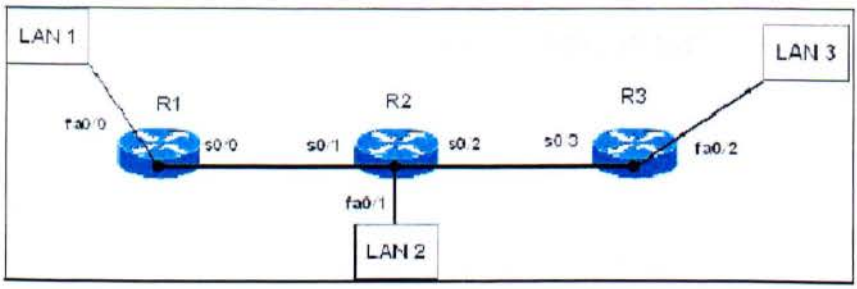
11.1 ΛΕΙΤΟΥΡΓΙΑ

Το πρωτόκολλο RIP χρησιμοποιεί τον αλγόριθμο διανύσματος απόστασης και είναι κατάλληλο για τη λειτουργία μικρών δικτύων. Στους πίνακες δρομολόγησης που προκύπτουν υπάρχουν πληροφορίες για το δρόμο και το κόστος της απόστασης προς τα δίκτυα προορισμού. Ως κόστος χρησιμοποιείται ο αριθμός των ενδιάμεσων δρομολογητών μέχρι να φτάσουμε στο δίκτυο προορισμού **(hop count).** Ο αριθμός των ενδιάμεσων δρομολογητών μέχρι το δίκτυο προορισμού μπορεί να είναι μέχρι 15.

Στο πρωτόκολλο RIP οι δρομολογητές περιοδικά (κάθε 30 δευτερόλεπτα), ανακοινώνουν ολόκληρο το περιεχόμενο του πίνακα δρομολόγησής τους, στους άμεσα γειτονικούς δρομολογητές. Ο πίνακας δρομολόγησης μπορεί να μεταδοθεί κι όταν υπάρξει κάποια αλλαγή στην τοπολογία του δικτύου. Έτσι επιτρέπεται στο κάθε δρομολογητή να βλέπει το δίκτυο του γειτονικού δρομολογητή και να προσθέτει το ανάλογο κόστος στην απόσταση που έχει ήδη προσθέσει ο δεύτερος. Το μειονέκτημα της προσέγγισης αυτής είναι ότι καθώς το δίκτυο μεγαλώνει, ανταλλάσσεται ένα μεγάλο ποσό πληροφορίας ανά τακτά χρονικά διαστήματα, ακόμα κι όταν η τοπολογία του δικτύου δεν έχει αλλάξει, με αποτέλεσμα να περιορίζεται το διαθέσιμο εύρος ζώνης και να αυξάνεται ο χρόνος σύγκλισης.

Ως χρόνος σύγκλισης (convergence time), ορίζεται ο χρόνος που περνά μέχρι όλοι οι δρομολογητές να συμφωνήσουν σχετικά με την τοπολογία του δικτύου, από τη στιγμή που θα προκύψει μια αλλαγή. Όταν αλλάζει η τοπολογία του δικτύου, εκτελείται ο αλγόριθμος δρομολόγησης και σταματά η κίνηση των δεδομένων που μεταφέρει ο δρομολογητής προς τα διάφορα interfaces του, γιατί δεν γνωρίζει αν το δίκτυο προορισμού είναι διαθέσιμο ή όχι. Άρα, όσο πιο γρήγορα γίνεται η σύγκλιση τόσο πιο γρήγορα θα μεταφερθούν τελικά τα δεδομένα προς τον προορισμό τους.

11.2 ΠΑΡΑΔΕΙΓΜΑ ΔΡΟΜΟΛΟΓΗΣΗΣ ΜΕ RIP



Εικόνα 11.2.1

Σύμφωνα με την εικόνα 11.2.1 οι πίνακες δρομολόγησης που προκύπτουν στο παραπάνω δίκτυο θα είναι:

R1

network	next hop router	metric
LAN1	connected	0
LAN2	R2	1
LAN3	R3	2

R2

network	next hop router	metric
LAN1	R1	1
LAN2	connected	0
LAN3	R3	1

R3

network	next hop router	metric
LAN1	R2	2
LAN2	R2	1
LAN3	connected	0

11.3 ΡΥΘΜΙΣΗ ΠΡΩΤΟΚΟΛΛΟΥ RIP

Υπάρχουν δυο εκδόσεις του πρωτόκολλου RIP:

- η έκδοση RIP-1, όπου δεν στέλνεται η μάσκα υποδικτύωσης μαζί με τους πίνακες δρομολόγησης (classful routing). Όλα τα δίκτυα πρέπει να έχουν τη default μάσκα,
- η έκδοση RIP-2, όπου μαζί με τους πίνακες δρομολόγησης στέλνεται και η μάσκα υποδικτύωσης (classless routing)

Η ρύθμιση του πρωτοκόλλου RIP (σε cisco routers) γίνεται με τις παρακάτω εντολές:

Router(config) #**router rip**

Router(config-router) #**network network-number**

όπου network-number, τα απ' ευθείας συνδεδεμένα δίκτυα στα interfaces του δρομολογητή.

Για την επαλήθευση του πρωτόκολλου RIP χρησιμοποιείται η εντολή:

Router **#show ip protocols**

Για την εμφάνιση του πίνακα δρομολόγησης χρησιμοποιείται η εντολή:

Router **#show ip route**

ΚΕΦΑΛΑΙΟ 12

ΤΙΤΛΟΣ: OSPF (OPEN SHORTEST PATH FIRST)

12.1 ΓΕΝΙΚΑ

Το OSPF είναι πρωτόκολλο δρομολόγησης IP δικτύων. Είναι ένα πρωτόκολλο τύπου IGP(Interior Gateway Protocol), δηλαδή διανέμει την πληροφορία εντός ενός αυτόνομου συστήματος παρότι μπορεί να στείλει και να λάβει διαδρομές και από άλλα. Βασίζεται στον αλγόριθμο του Dijkstra. Δεν υπάρχει περιορισμός στον αριθμό των hops, ενώ το RIP περιορίζεται στα 15 hops. Έχει τη δυνατότητα να σπάσει το IP δίκτυο σε πολλά υποδίκτυα διαφόρων μεγεθών, παρέχοντας μεγαλύτερη ευελιξία στον διαχειριστή και επίσης παρέχει λειτουργία αυθεντικοποίησης των μηνυμάτων δρομολόγησης. Τέλος επιτρέπει τη μεταφορά και το μαρκάρισμα των διαδρομών οι οποίες εισάγονται σε ένα αυτόνομο σύστημα από εξωτερικά πρωτόκολλα.

12.2 ΡΥΘΜΙΣΗ ΠΡΩΤΟΚΟΛΛΟΥ OSPF

Η ρύθμιση του πρωτοκόλλου **OSPF** γίνεται με τις παρακάτω εντολές σε configuration mode:

Router(config)#router ospf <process-id>	Το process-id είναι μία αριθμητική αξία τοπική στο δρομολογητή και δεν είναι απαραίτητο να ταιριάζει με άλλα process-ids που τρέχουν σε άλλους δρομολογητές
Router(config-router)#network <network or IP address> <mask> <area-id>	η εντολή αυτή χρησιμοποιείται για να αναθέτει ένα interface σε συγκεκριμένη περιοχή, όπου area-id ο αριθμός της περιοχής που θέλουμε να είναι το interface. Το mask τοποθετείται με αντίστροφη λογική σε σχέση με αυτά που έχουμε δει ως τώρα. Π.χ. ένα υποδίκτυο με subnet mask 255.255.255.0 θα πρέπει εδώ να δηλωθεί ως 0.0.0.255.

Παράδειγμα	
interface Ethernet0 ip address 192.213.11.1 255.255.255.0	*Ορίζει ip διευθύνσεις στα διάφορα interfaces του δρομολογητή*
interface Ethernet1 ip address 192.213.12.2 255.255.255.0	
interface Ethernet2 ip address 128.213.1.1 255.255.255.0	
router ospf 100	
network 192.213.0.0 0.0.0.255 area 10	*τοποθετεί και το E0 και το E1 στην ίδια περιοχή 10*
network 128.213.1.1 0.0.0.255 area 23	*τοποθετεί το E2 στην περιοχή 23*

Πίνακας 12.2.1

12.3 ΣΥΓΚΡΙΣΗ RIP vs OSPF

RIP

- Οι RIP routers μαζεύουν μεγάλο ποσό άχρηστης πληροφορίας και δημιουργούνται **λανθασμένες δρομολογήσεις** λόγω της μεγάλης **καθυστέρησης σύγκλισης**
- Οι ενημερώσεις στέλνονται **περιοδικά** ανά 30 sec, αφορούν όλη την πληροφορία δρομολόγησης και γίνονται με broadcast μετάδοση
- Το γεγονός αυτό αυτόματα κάνει το RIP ακατάλληλο για χρήση σε ασύρματα δίκτυα
- Ακατάλληλο πρωτόκολλο για **μεγάλα δίκτυα** ή δίκτυα που αλλάζουν **αρκετά γρήγορα και συχνά**
- Η σύγκλιση μπορεί να πάρει αρκετά λεπτά, οι δρομολογητές κάνουν timeout πληροφορία που δεν έχει ληφθεί πρόσφατα
- Οι αποφάσεις δρομολόγησης λαμβάνονται με βάση μόνο των **αριθμό των συνδέσεων** και όχι το κόστος – εύρος της κάθε σύνδεσης. Έτσι προτιμάται μια **κοντινή διαδρομή** έστω και αν υπάρχει μακρύτερη με περισσότερο εύρος.

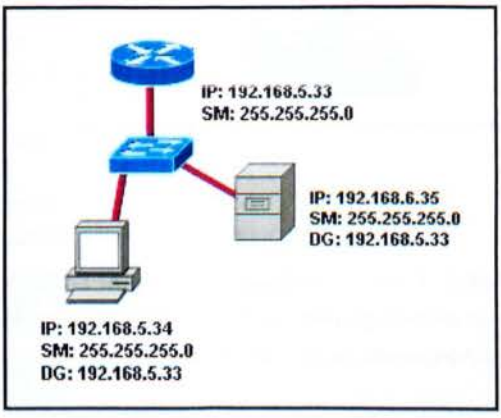
OSPF

- Έχει καλύτερη - γρηγορότερη **σύγκλιση**, διότι οι αλλαγές προωθούνται **άμεσα και όχι περιοδικά.**
- Αλλαγές στη δρομολόγηση συμβαίνουν άμεσα και όχι περιοδικά
- Οι ενημερώσεις στέλνονται μόνο **σε περίπτωση αλλαγής** και γίνονται με ip multicast μετάδοση
- Λιγότερο **overhead** στο δίκτυο, ιδιότητα σημαντική για μεγάλα δίκτυα
- Οι αποφάσεις δρομολόγησης λαμβάνονται με βάση το κόστος των συνδέσεων και έτσι προτιμάται η αληθινά βέλτιστη διαδρομή
- Το αντίτιμο που πληρώνουμε για τις περισσότερες δυνατότητες του πρωτοκόλλου είναι η **πολυπλοκότητα** στην ρύθμιση και στην άρση βλαβών
- Επίσης απαιτείται περισσότερη **επεξεργαστική ισχύς** και μνήμη στους δρομολογητές.

ΚΕΦΑΛΑΙΟ 13

ΤΙΤΛΟΣ: ΣΕΝΑΡΙΑ – ΕΡΩΤΗΣΕΙΣ

1.



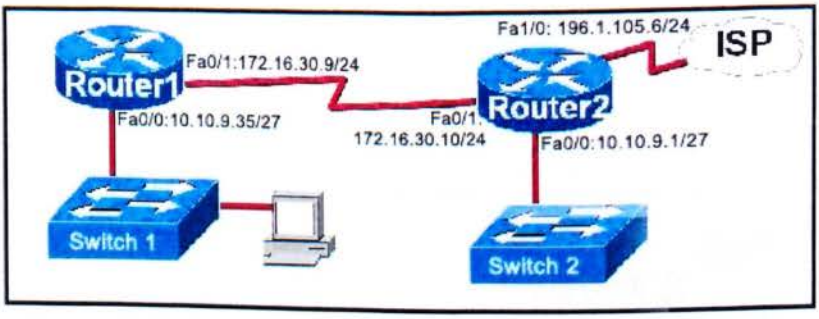
Εικόνα 13.1

Ένας χρήστης από τον υπολογιστή δεν μπορεί να συνδεθεί στον server. Όλα τα καλώδια έχουν ελεγχθεί για τη σωστή λειτουργία τους, καθώς και για τη σύνδεσή τους στις συσκευές. Όλες οι συσκευές έχουν ip διευθύνσεις. Ωστόσο ο χρήστης δεν μπορεί να συνδεθεί με τον server. Η εντολή ping δεν ανταποκρίνεται. Τι μπορεί να φταίει;

A. Το interface του router δεν έχει ρυθμιστεί με μία default gateway.
B. Το switch δεν έχει ρυθμιστεί με μία IP διεύθυνση και default gateway.
C. Το pc και ο server είναι σε διαφορετικά λογικά δίκτυα.
D. Το pc δεν γνωρίζει την MAC διεύθυνση του switch.

Απάντηση: Η μάσκα υποδικτύου /24 δηλώνει ότι ο χρήστης είναι στο δίκτυο 192.168.5.0 και ο server στο 192.168.6.0

2.



Εικόνα 13.2

Ο Χρήστης αποσυνδέθηκε από το switch 2 και συνδέθηκε στο switch 1. Ποιος συνδυασμός IP address, subnet mask, και default gateway πρέπει να δηλωθεί στο Pc του χρήστη ώστε να του επιτραπεί να λειτουργήσει μέσα στο δίκτυο;

A. IP address: 10.10.9.37 Subnet mask: 255.255.255.240 Default gateway: 10.10.9.35
B. IP address: 10.10.9.37 Subnet mask: 255.255.255.224 Default gateway: 10.10.9.35
C. IP address: 10.10.9.29 Subnet mask: 255.255.255.248 Default gateway: 10.10.9.35
D. IP address: 10.10.9.32 Subnet mask: 255.255.255.224 Default gateway: 10.10.9.35
E. IP address: 10.10.9.37 Subnet mask: 255.255.255.224 Default gateway: 196.1.105.6
F. F. IP address: 10.10.9.63 Subnet mask: 255.255.255.224 Default gateway: 10.10.9.35

Απάντηση:

Address

10.10.9.35
00001010.00001010.00001001.00100011

Netmask

255.255.255.224 = 27
11111111.11111111.11111111.11100000

Network

10.10.9.32/27
00001010.00001010.00001001.00100000

Broadcast

10.10.9.63
00001010.00001010.00001001.00111111

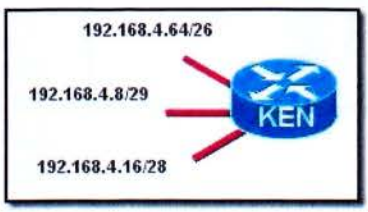
First IP

10.10.9.33
00001010.00001010.00001001.00100001

Last IP

10.10.9.62
00001010.00001010.00001001.00111110

3.



Εικόνα 13.3

Ποια διεύθυνση είναι broadcast διεύθυνση για ένα από τα υποδίκτυα που φαίνονται στην εικόνα;

A. 192.168.4.3/29
B. 192.168.4.15/29
C. 192.168.4.65/26
D. 192.168.4.255/24

Απάντηση:

Address

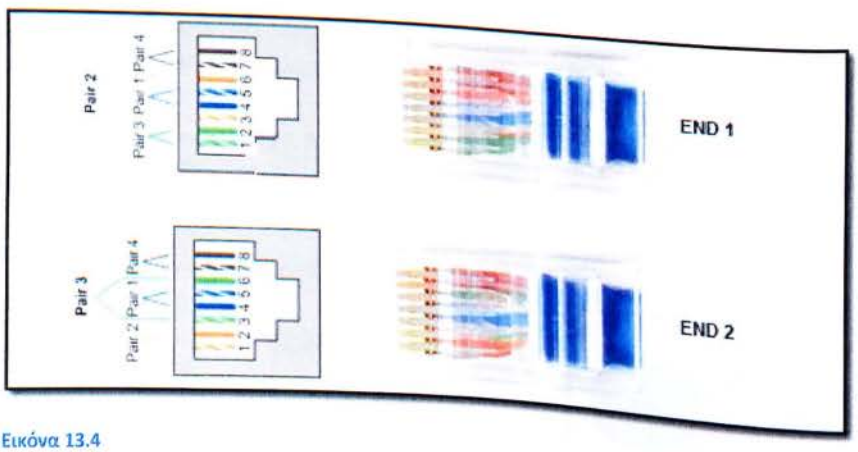
192.168.4.15
11000000.10101000.00000100.00001111

Netmask

255.255.255.248 = 29
11111111.11111111.11111111.11111000

Τα 3 τελευταία bit είναι όλα 1. Οπότε είναι broadcast διεύθυνση αφού η μάσκα είναι /29.

4.



Εικόνα 13.4

Ένας σπουδαστής εργάζεται στο εργαστήριο και επιλέγει ένα καλώδιο, όπως φαίνεται. Ποιες συνδέσεις μπορούν με επιτυχία να γίνουν με αυτό το καλώδιο;

A. Σύνδεση ενός υπολογιστή στην port console ενός δρομολογητή
B. Σύνδεση δύο δρομολογητών μέσω των θυρών Ethernet
C. Σύνδεση δύο switch μαζί με ταχύτητες Gigabit
D. Σύνδεση ενός υπολογιστή με ένα switch με ταχύτητες Gigabit
E. Σύνδεση δύο συσκευών με τον ίδιο τύπο διασύνδεσης σε ταχύτητες Fast Ethernet

Απάντηση: Το καλώδιο είναι τύπου Ethernet Crossover

Address

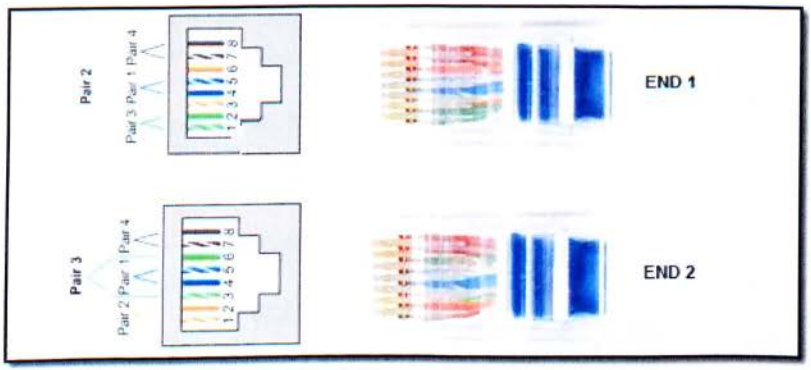
192.168.4.15
11000000.10101000.00000100.00001111

Netmask

255.255.255.248 = 29
11111111.11111111.11111111.11111000

Τα 3 τελευταία bit είναι όλα 1. Οπότε είναι broadcast διεύθυνση αφού η μάσκα είναι /29.

4.



Εικόνα 13.4

Ένας σπουδαστής εργάζεται στο εργαστήριο και επιλέγει ένα καλώδιο, όπως φαίνεται. Ποιες συνδέσεις μπορούν με επιτυχία να γίνουν με αυτό το καλώδιο;

A. Σύνδεση ενός υπολογιστή στην port console ενός δρομολογητή
B. Σύνδεση δύο δρομολογητών μέσω των θυρών Ethernet
C. Σύνδεση δύο switch μαζί με ταχύτητες Gigabit
D. Σύνδεση ενός υπολογιστή με ένα switch με ταχύτητες Gigabit
E. Σύνδεση δύο συσκευών με τον ίδιο τύπο διασύνδεσης σε ταχύτητες Fast Ethernet

Απάντηση: Το καλώδιο είναι τύπου Ethernet Crossover

5.

Το Ethernet λειτουργεί σε ποια στρώματα τους OSI μοντέλου;

A. Network layer
B. Transport layer
C. Physical layer
D. Application layer
E. Session layer
F. F. Data-link layer

6.

Ποιος είναι ο πρωταρχικός σκοπός της ενθυλάκωσης πακέτων σε πλαίσια;

A. Παρέχει διαδρομές (routes) για όλο το internetwork
B. Μορφοποιεί τα δεδομένα για την παρουσίαση στο χρήστη
C. Διευκολύνει την είσοδο και την έξοδο των δεδομένων στο φυσικό μέσο επικοινωνίας
D. Προσδιορίζει τις υπηρεσίες για τα τα δεδομένα που μεταφέρονται

7.

Τι τύπου IP διεύθυνση χρησιμοποιείται σε ένα unicast packet?

A. Συγκεκριμένης συσκευής
B. Ομάδα συσκευών
C. Της προεπιλεγμένης πύλης
D. Της broadcast address του δικτύου

8.

Ποια είναι η MAC διεύθυνση προορσιμού σε ένα multicast Ethernet πλαίσιο?

A. Η MAC δεύθυνση του αποστολέα
B. Η MAC δεύθυνση του παραλήπτη
C. Μία διεύθυνση που ξεκινάει με 01-00-5E δε δεκαεξαδική μορφή
D. Μία 48-bit σε δεκαεξαδική μορφή διεύθυνση παρουσιαζόμενη ως FF-FF-FF-FF-FF-FF

9.

Ένας υπολογιστής αποκτά διεύθυνση IP από έναν διακομιστή DHCP. Εάν ο υπολογιστής αποσυνδεθεί από το δίκτυο λόγω επισκευής, τι συμβαίνει με τη ρύθμιση της IP διεύθυνσης;

A. Η ρύθμιση είναι μόνιμη και δεν αλλάζει τίποτα.
B. Η μίσθωση της διεύθυνση ανανεώνεται αυτόματα από τον διακομιστή DHCP μέχρι το PC να ξαναεπιστρέψει στο δίκτυο.
C. Η διεύθυνση είναι διαθέσιμη για στον διακομιστή DHCP για επαναχρησιμοποίηση σε άλλους υπολογιστές, αφού η μίσθωση λήξει.
D. Η ρύθμιση για τον υπολογιστή αποθηκεύεται από το διακομιστή DHCP ώστε να του ξαναδοθεί η ίδια IP όταν ο υπολογιστής επιστρέψει στο δίκτυο

10.

Ποια προεπιλεγμένη μάσκα υποδικτύωσης παρέχει τον περισσότερο χώρο για σύνδεση συσκευών σε ένα δίκτυο;

A. 255.0.0.0
B. 255.255.0.0
C. 255.255.255.0
D. 255.255.255.252

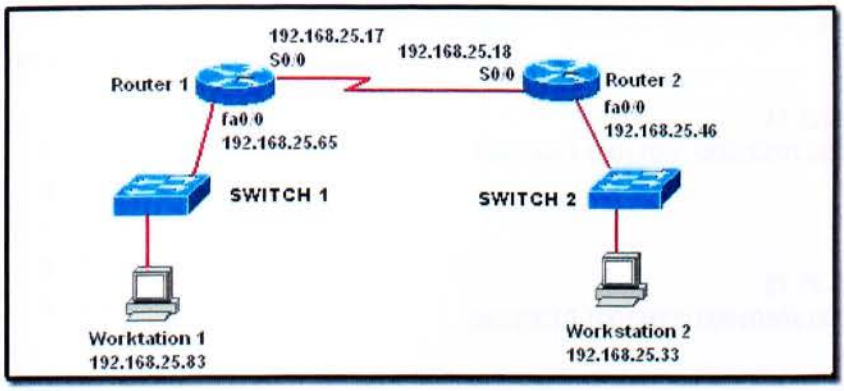
Απάντηση: Τα διαθέσιμα bit είναι 24. Οπότε 2^24 – 2 = 16777214 διαθέσιμες IP διευθύνσεις προς χρήστες. Αφαιρέσαμε 2 γιατί η μία είναι η broadcast διεύθυνση και η άλλη η διεύθυνση του δικτύου.

11.

Ποια πληροφορία προστίθεται κατά την ενθυλάκωση στο OSI Layer 3;

A. Η MAC προορισμού και αποστολής
B. Το application protocol προορισμού και αποστολής
C. Ο αριθμός της θύρας προορισμού και αποστολής
D. Η IP address προορισμού και αποστολής

12.



Εικόνα 13.5

Ένας διαχειριστής δικτύου έχει διαμορφώσει ένα δίκτυο υποδικτύων από το αρχικό δίκτυο 192.168.0.0/28. Το Workstation 1 δεν είναι σε θέση να επικοινωνήσει με το Workstation 2. Ποια είναι η αιτία αυτής της απώλειας των επικοινωνιών;

A. Το workstation 1 και το workstation 2 είναι στο ίδιο υποδίκτυο
B. Οι σειριακές συνδέσεις χρησιμοποιούν διευθύνσεις από το LAN υποδίκτυα.
C. Το Workstation 1 δεν είναι στο ίδιο δίκτυο με τη διεπαφή LAN του Router 1
D. Αν χρησιμοποιούνται routers στο δίκτυο, δεν χρειάζεται να υπάρξουν υποδίκτυα.

Απάντηση: Η τελευταία IP του δικτύου είναι η 192.168.25.78. Επομένως το Workstation 1 βρίσκεται σε άλλο δίκτυο.

Address
192.168.25.65
11000000.10101000.00011001.01000001

Netmask

255.255.255.240 = 28
11111111.11111111.11111111.11110000

Network

192.168.25.64/28
11000000.10101000.00011001.01000000

Broadcast

192.168.25.79
11000000.10101000.00011001.01001111

First IP

192.168.25.65
11000000.10101000.00011001.01000001

Last IP

192.168.25.78
11000000.10101000.00011001.01001110

13.

Μια εταιρεία πρέπει να επεκτείνει το LAN σε έξι διαφορετικά κτίρια. Προκειμένου να περιοριστεί το ποσό της εξασθένησης του σήματος στο τοπικό δίκτυο, τι είδος φυσικού μέσου επικοινωνίας θα ήταν το καλύτερο να χρησιμοποιηθεί μεταξύ των κτιρίων;

A. αέρα (ασύρματο)
B. ομοαξονικό καλώδιο
C. οπτική ίνα
D. θωρακισμένο καλώδιο συνεστραμμένου ζεύγους
E. αθωράκιστο καλώδιο συνεστραμμένου ζεύγους

14.

Ποιοι παράγοντες πρέπει να λαμβάνονται υπόψη κατά την επιλογή του κατάλληλου καλωδίου για τη σύνδεση ενός υπολογιστή σε ένα δίκτυο;

A. τύπος του διαύλου συστήματος
B. μοντέλο μητρικής
C. απόσταση του καλωδίου λειτουργίας
D. ταχύτητα μετάδοσης
E. τον κατασκευαστή του υπολογιστή

15.

Ποιος είναι ο όρος που χρησιμοποιείται για να περιγράψει τα δεδομένα στο στρώμα πρωτοκόλλου μεταφοράς δεδομένων (transport);

A. bits
B. packets
C. segments
D. frames
E. data streams

16.

Τι χρησιμοποιούν οι δρομολογητές για να διαλέξουν τις καλύτερες διαδρομές, ώστε να αποστείλουν πακέτα δεδομένων;

A. Πίνακες ARP
B. Πίνακες Bridging
C. Πίνακες Routing
D. Πίνακες Switching

Απάντηση: Οι δρομολογητές αποθηκεύουν πίνακες Routing (δρομολόγησης) που αντιστοιχούν τις διευθύνσεις δικτύου με την καλύτερη διεπαφή εξόδου.

17.

Ποια επίπεδα του μοντέλου OSI συνδυάζονται σε άλλα επίπεδα του μοντέλου TCP / IP;

A. Network
B. Presentation
C. Internet
D. Data link
E. Application
F. Physical
G. Session
H. Network access
I. Transport

Απάντηση: Τα επίπεδα στο OSI Presentation και Session συνδυάζονται στο επίπεδο Application του TCP / IP. Τα επίπεδα στο OSI Data link και Physical συνδυάζονται στο επίπεδο Network του TCP / IP.

18.

Τι μπορεί να συμβεί όταν το TTL είναι 1;

A. Το πακέτο μπορεί να παραδοθεί επιτυχώς, εάν προορίζεται για ένα άμεσα συνδεδεμένο δίκτυο.
B. Το πακέτο θα απορριφθεί από τον επόμενο δρομολογητή, εκτός εάν ο δρομολογητής έχει μία διεπαφή στο προοριζόμενο δίκτυο.
C. Το πακέτο θα επιστρέψει στον αποστολέα.
D. Το πακέτο θα επιστρέψει στον προηγούμενο δρομολογητή.

Απάντηση: Όταν το TTL είναι 1, έχει ένα σταθμό που απομένει είτε να παραδοθεί είτε να απορριφθεί. Το IP δεν παρέχει ειδοποίηση επιστροφής από πακέτα που απορρίπτονται.

19.

Το IP είναι ασυνδεσιστρεφής (connectionless). Δεν πραγματοποιείται σύνδεση πριν την αποστολή μεταξύ αποστολέα και παραλήπτη. Συνήθως μπορεί να χαθεί ένα πακέτο κατά τη διάρκεια της διαδρομής του. Εάν τα πακέτα χαθούν, πώς θα ολοκληρωθεί το τελικό μήνυμα;

A. Το πρωτόκολλα δρομολόγησης, όπως το RIP, είναι προσανατολισμένα σε σύνδεση (connection oriented) και θα ειδοποιήσουν τον αποστολέα.
B. Ο παραλήπτης περιμένει το πακέτο και θα στείλει αίτημα αποστολής στον αποστολέα εάν το πακέτο δε φτάσει.
C. Το IP header εμπεριέχει τον αποστολέα, ώστε το πακέτο να μπορεί να επιστραφεί στον αποστολέα από το δρομολογητή που έλαβε το πακέτο όταν το TTL ισούταν με 0.

Απάντηση: Ο παραλήπτης περιμένει το πακέτο και θα στείλει αίτημα αποστολής στον αποστολέα εάν το πακέτο δε φτάσει. Το IP είναι connectionless, επομένως δεν υπάρχει μηχανισμός αξιοπιστίας ενσωματωμένος στο πρωτόκολλο. Τα πρωτόκολλα δρομολόγησης, όπως το RIP, χρησιμοποιούνται από τους δρομολογητές για να μοιράζονται τις πληροφορίες δρομολόγησης. Δεν εμπλέκονται σε μηχανισμό αξιοπιστίας TCP / IP.

20.

Γιατί το ICMPv4 είναι ένα σημαντικό πρωτόκολλο που λειτουργεί με το IPv4; Ποιοι είναι οι τύποι μηνυμάτων ICMP;

Απάντηση: Το IPv4 είναι ένα μη αξιόπιστο (best effort) πρωτόκολλο. Το ICMPv4 παρέχει τα μέσα για προβλήματα δικτύου, όπως χαμένα πακέτα ή συμφόρηση δικτύου να αναφέρονται στο δίκτυο αποστολής ή στον χρήστη αποστολής. Τα μηνύματα περιέχουν:

Host Conformation
Unreachable Destination or Service
Time Exceeded
Route Redirection
Source Quench

21.

Ένας χρήστης έχει συνδέσει δύο pc με ένα καλώδιο (peer to peer). Για να συνδέσει και ένα τρίτο pc στο δίκτυο αγοράζει ένα hub και δύο καλώδια straight – through, ώστε το κάθε pc να είναι συνδεδεμένο με το hub. Ποιο θα είναι το αποτέλεσμα αυτής της αναβάθμισης του δικτύου;

A. Και τα 3 pc θα συνδεθούν επιτυχώς στο hub.
B. 2 pc θα συνδεθούν επιτυχώς στο hub.
C. 1 pc θα συνδεθεί επιτυχώς στο hub.
D. Κανένα pc δε θα συνδεθεί επιτυχώς στο hub.

Απάντηση: Μόνο τα pc που συνδέονται με straight – through καλώδια θα συνδεθούν επιτυχώς στο hub. Το τρίτο pc συνδέθηκε με το αρχικό καλώδιο που είναι ένα crossover καλώδιο κατάλληλο για peer to peer δίκτυα.

22.

Ένας διαχειριστής δικτύου σε μια εταιρεία παραγωγής ειδών από ξύλο αντιμετωπίζει προβλήματα στην πτέρυγα Α του κτιρίου. Οι συσκευές είναι ίδιες σε όλες τις πτέρυγες και μοιάζουν όλες να λειτουργούν κανονικά, αλλά η ταχύτητα του δικτύου έχει μειωθεί σημαντικά στην Α πτέρυγα. Οι πωλήσεις έχουν αυξηθεί σημαντικά και οι μηχανές στον όροφο παραγωγής δουλεύουν στο μέγιστο. Ο διαχειριστής του δικτύου είναι κάτω από μεγάλη πίεση, ώστε να ανεβάσει την ταχύτητα σε επιθυμητό επίπεδο. Προσπαθώντας να λύσει το πρόβλημα καταλήγει σε μία λίστα από πιθανά αίτια του προβλήματος. Ποια είναι τα τρίτα πρώτα αίτια σε βαρύτητα που δημιουργούν αυτή τη χαμηλή απόδοση του δικτύου;

A. Η Α πτέρυγα έχει τους περισσότερους χρήστες στο δίκτυο.
B. Ο επιστάτης σφουγγαρίζει τον όροφο της πτέρυγας Α κάθε Τετάρτη στις 16:00. Οι άλλες πτέρυγες σφουγγαρίζονται τη νύχτα.
C. Κάποιο εργαζόμενοι στην πτέρυγα Α έχουν φέρει ψυγεία και φούρνους μικροκυμάτων κοντά στο χώρο εργασίας.
D. Η Α πτέρυγα έχει δίκτυο τα τελευταία 3 χρόνια. Οι άλλες πτέρυγες έχουν δίκτυο τα τελευταία 4 χρόνια.
E. Οι χρήστες στην πτέρυγα Α είναι κοντά στον όροφο παραγωγής.
F. Η Α πτέρυγα έχει καλώδια CAT 5, ενώ οι άλλες πτέρυγες έχουν καλώδια CAT 5 και ασύρματη σύνδεση.

Απάντηση: A: Η Α πτέρυγα αφού έχει τους περισσότερους χρήστες, μπορεί να δημιουργείται περισσότερη κίνηση δεδομένων στο φυσικό μέσο (καλώδια) και τα πακέτα να απορρίπτονται. C: Οι συμπιεστές ψυγείων και οι φούρνοι μικροκυμάτων μπορούν να δημιουργήσουν παρεμβολές στο δίκτυο. E: Επειδή οι πωλήσεις αυξήθηκαν μπορεί να υπάρχει ηλεκτρομαγνητική παρεμβολή από τις μηχανές. Για το D και το F: ίσα ίσα που είναι παράγοντες που έχουν θετικό πρόσημα στην απόδοση του δικτύου. Για το B: Δεν επηρεάζει

23.

Ποιες διευθύνσεις είναι έγκυρες IP διευθύνσεις αξιοποιήσιμες από χρήστες, εφόσον η μάσκα υποδικτύου είναι η 255.255.255.248;

A. 192.168.200.87
B. 192.10.10.104
C. 223.168.210.100
D. 220.100.100.154
E. 200.152.2.160
F. 196.123.142.190

Απάντηση: Με μάσκα υποδικτύου 255.255.255.248 σημαίνει ότι τα δίκτυα θα αυξάνουν σε βήματα των 8. Με άλλα λόγια, οι διευθύνσεις δικτύου θα είναι 0, 8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240 και 248. Επομένως:

A: δεν θα ήταν σωστό. 192.168.200.87 θα ήταν η broadcast διεύθυνση του δικτύου 192.168.200.80

B: δεν θα ήταν σωστό. 194.10.10.104 θα ήταν διεύθυνση δικτύου

C: 223.168.210.100 είναι σωστό, είναι χρήστης στο δίκτυο 223.168.210.96.

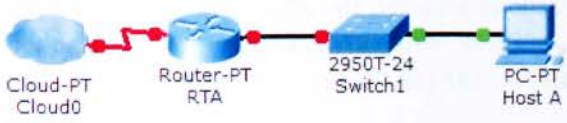
D: 220.100.100.154 είναι σωστό, είναι χρήστης στο δίκτυο 220.100.100.152.

E: δεν θα ήταν σωστό. 200.152.2.160 θα ήταν διεύθυνση δικτύου

F: 196.123.142.190 είναι σωστό, είναι χρήστης στο δίκτυο 192.123.142.184.

24.

Ο χρήστης A στο σχήμα έχει διεύθυνση IP 10.118.197.55/20. Πόσες συσκευές δικτύου μπορούν να προστεθούν στο ίδιο υποδίκτυο;



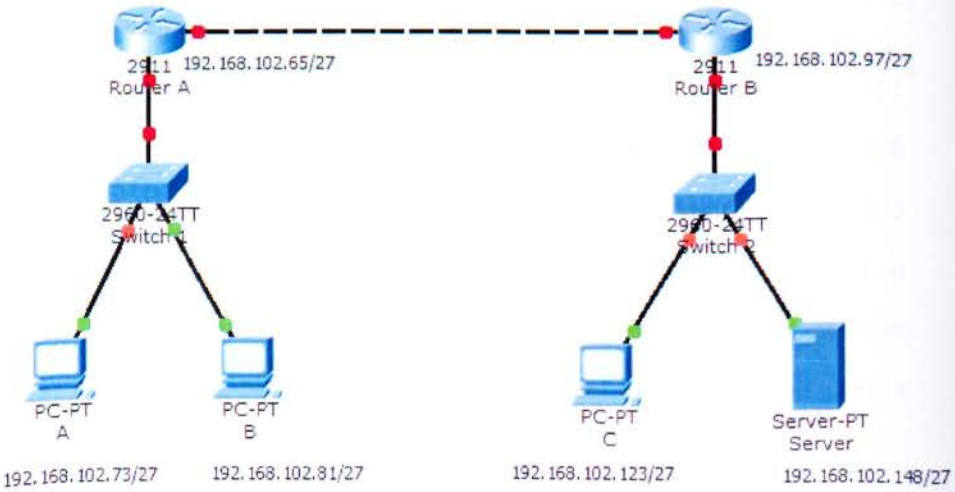
Εικόνα 13.6

A. 253
B. 509
C. 1021
D. 2045
E. 4093

Απάντηση: Η μάσκα υποδικτύου /20 μπορεί να φιλοξενήσει 4096 IP διευθύνσεις. Αφαιρούμε 1 για τη διεύθυνση δικτύου, αφαιρούμε 1 για τη broadcast διεύθυνση και αφαιρούμε άλλη μία για τον Χρήστη Α που ήδη χρησιμοποιεί μία διεύθυνση. Οπότε 4093 διευθύνσεις διαθέσιμες προς χρήση.

25.

Οι συσκευές έχουν ρυθμιστεί με στατική IP διεύθυνση στο δίκτυο 192.168.102.0. Όλοι οι χρήστες μπορούν να επικοινωνήσουν μεταξύ τους, αλλά δεν μπορούν να επικοινωνήσουν με το server. Τι δημιουργεί το πρόβλημα;



Εικόνα 13.7

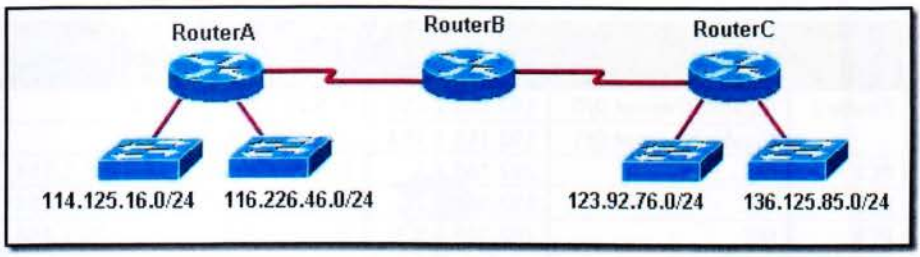
A. Η IP διεύθυνση του server είναι εκτός του υποδικτύου.
B. Η IP διεύθυνση του server είναι μια broadcast διεύθυνση.
C. Η IP διεύθυνση του server είναι μια διεύθυνση δικτύου (network address).
D. Στο switch που συνδέεται ο server δεν έχει ανατεθεί IP address.

Απάντηση: Χρησιμοποιώντας την μάσκα υποδικτύου /27 σημαίνει ότι τα δίκτυα θα αύξαναν κατά 32. Οπότε οι διευθύνσεις δικτύων είναι: 192.168.102.0, 192.168.102.32, 192.168.102.64, 192.168.102.96,

192.168.102.128, 192.168.102.160, 192.168.102.192, 192.168.102.224. Η επιλογή Α είναι σωστή επειδή η IP διεύθυνση του server 192.168.102.147 ανήκει στο δίκτυο 192.168.102.128 και όχι στο 192.168.102.96.

26.

Ποιες ενέργειες θα λάβουν χώρα όταν ο RouterA χάσει τη σύνδεση με το δίκτυο 114.125.16.0;



Εικόνα 13.8

A. Ο RouterB θα συμπεριλάβει το δίκτυο 123.92.76.0 και 136.125.85.0 στην ενημέρωση με το RouterA.

B. Κατά τη διάρκεια του επόμενου διαστήματος ενημέρωσης, ο RouterB θα στείλει ένα RIP update και στις δύο θύρες που περιλαμβάνουν το απρόσιτο δίκτυο.

C. Κατά τη διάρκεια του επόμενου διαστήματος ενημέρωσης, ο RouterC θα στείλει μια ενημέρωση προς τον RouterB δηλώνοντας ότι το δίκτυο 114.125.16.0 είναι προσβάσιμο σε 2 hops.

D. Ο Router C θα μάθει την απώλεια της σύνδεσης με το δίκτυο 114.125.16.0 από το RouterB.

E. Ο RouterB θα συμπεριλάβει το δίκτυο 123.92.76.0 και 136.125.85.0 κατά την ενημέρωση προς τον RouterC.

Απάντηση: A: Ο πιο κοντινός Router στον RouterA είναι ο RouterB. Επομένως στην επόμενη ενημέρωση RIP ο RouterA θα μάθει τη διαδρομή από το RIP Update που θα του στείλει ο RouterB. D: Στην ίδια λογική ο πιο κοντινός Router στον RouterC είναι ο RouterB.

ΠΡΑΚΤΙΚΟ ΜΕΡΟΣ

Παράδειγμα 1

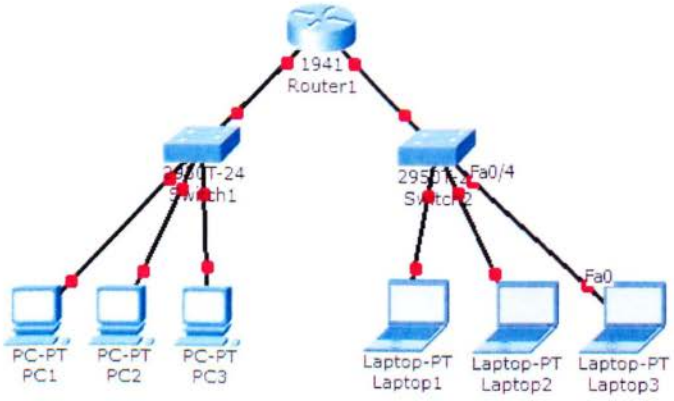
ΤΙΤΛΟΣ: ΕΞΕΡΕΥΝΗΣΗ ICMP ΚΑΙ ARP ΣΤΟ PACKET TRACER

ΔΕΔΟΜΕΝΑ ΑΣΚΗΣΗΣ

Συσκευή	Διεπαφή	IP διεύθυνση	Μάσκα Υποδικτύου	Προεπιλεγμένη πύλη
Router1	GigabitEthernet 0/0	192.168.2.254	255.255.255.0	N/A
	GigabitEthernet 0/1	192.168.1.254	255.255.255.0	N/A
PC1	NIC	192.168.1.1	255.255.255.0	192.168.1.254
PC2	NIC	192.168.1.2	255.255.255.0	192.168.1.254
PC3	NIC	192.168.1.3	255.255.255.0	192.168.1.254
Laptop1	NIC	192.168.2.1	255.255.255.0	192.168.2.254
Laptop2	NIC	192.168.2.2	255.255.255.0	192.168.2.254
Laptop3	NIC	192.168.2.3	255.255.255.0	192.168.2.254

Πίνακας Παρ1.1

- Όλες οι συνδέσεις χρησιμοποιούν καλώδια COPPER straight – through.
- Το δίκτυο μας: Αποτελείται από 1 Router. Το Router συνδέει τα δύο δίκτυα. Το 192.168.1.0 με το 192.168.2.0.
- Σε κάθε δίκτυο υπάρχει ένα switch. Σε κάθε switch έχουν συνδεθεί 3 τερματικές συσκευές.
- Ρυθμίζουμε το Packet tracer ώστε να μας εμφανίζει μόνο τα δεδομένα ARP και ICMP.
- Οι πίνακες ARP είναι άδειοι



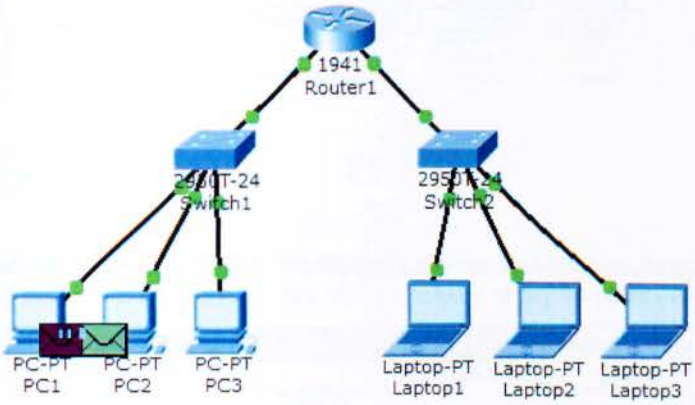
Εικόνα Παρ1.1

Σενάριο άσκησης: Θα εκτελέσουμε την εντολή PING από το PC1 με προορισμό το Laptop3. Στόχος μας είναι να εστιάσουμε στη δημιουργία και στην κίνηση των πακέτων ARP και ICMP.

ΕΚΤΕΛΕΣΗ ΑΣΚΗΣΗΣ

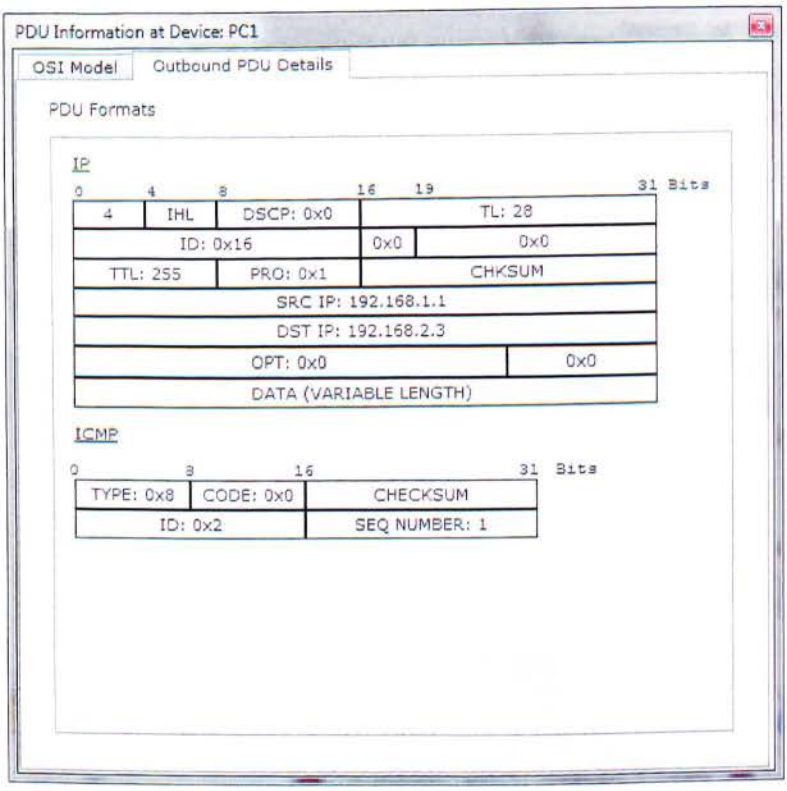
Βήμα 1. Εκτελούμε την εντολή PING από το PC1 με προορισμό το Laptop3.

Σημείωση: Με το μωβ χρώμα είναι τα δεδομένα του ICMP. Με τον πράσινο φάκελο είναι το ARP request.

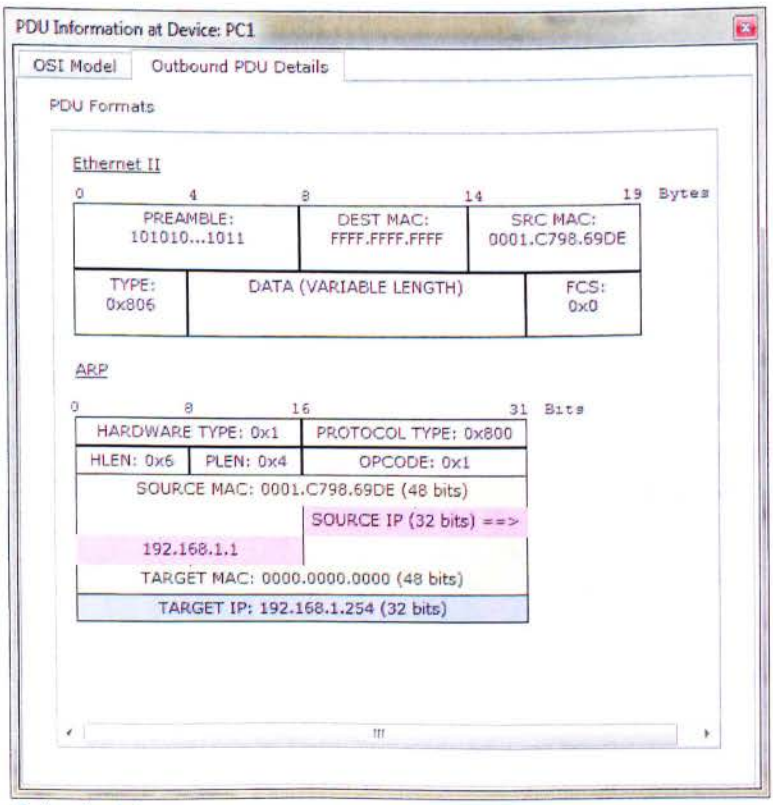


Εικόνα Παρ1.2

Παρατηρήσεις: Δημιουργείται το ICMP πακέτο. Δεν υπάρχει στον πίνακα ARP η αντιστοίχιση της διεύθυνσης αποστολής IP με τη διεύθυνση MAC του παραλήπτη. Δημιουργείται το ARP Request. Επειδή η διεύθυνση αποστολής βρίσκεται σε άλλο δίκτυο στο ARP Request καταχωρείται ως TARGET IP η IP του Interface GigabitEthernet 0/1 που είναι η προεπιλεγμένη πύλη. Η TARGET MAC διεύθυνση αποτελείται από 48 μηδενικά bits, αφού πρόκειται για ARP Request frame.

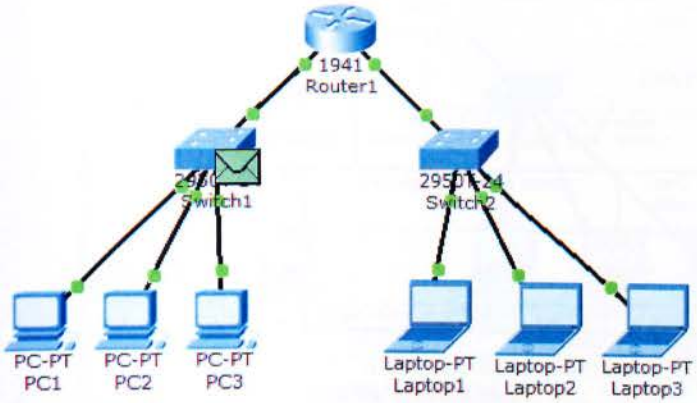


Εικόνα Παρ1.3



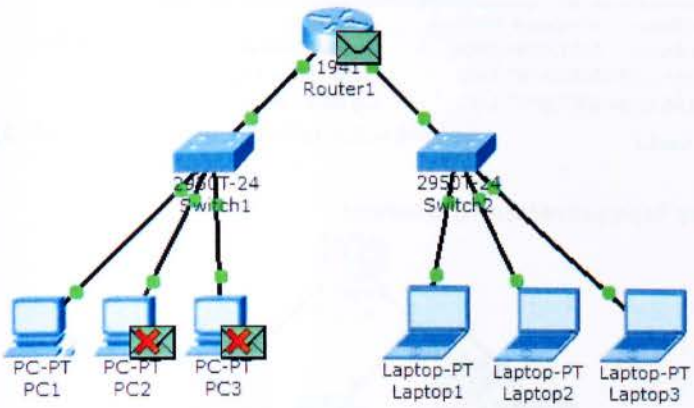
Εικόνα Παρ1.4

Βήμα 2: Το ARP request στέλνεται στο switch1 χωρίς να αλλάζει.



Εικόνα Παρ1.5

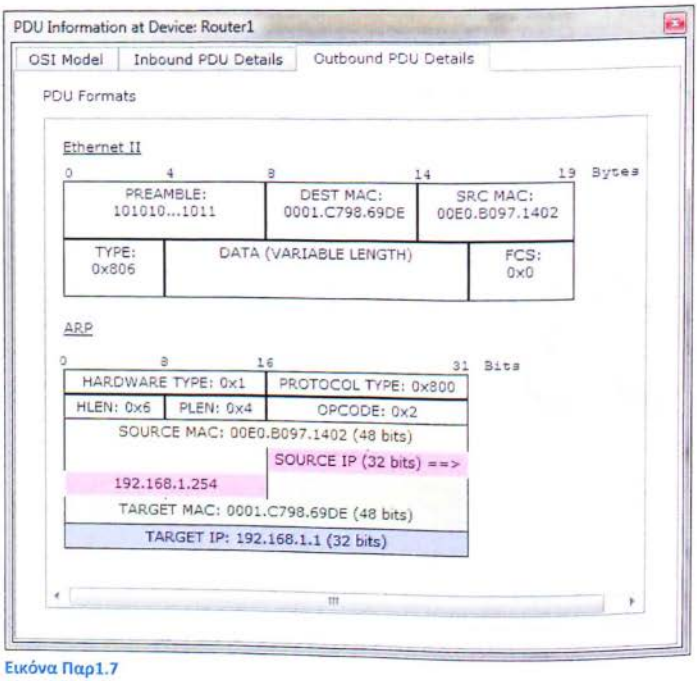
Βήμα 3: Το Switch1 στέλνει το ARP Request σε όλα τα Port που έχουν συνδεθεί συσκευές, εκτός από την Port από την οποία προήλθε το Arp Request.



Εικόνα Παρ1.6

Παρατηρήσεις: Τα ARP request απορρίπτονται από το PC2 και PC3. Το Router1 αποδέχεται το ARP Request αφού η TARGET IP είναι η IP του interface GigabitEthernet 0/1. Δημιουργεί το ARP Reply με TARGET IP την IP του PC1 και

TARGET MAC τη MAC του PC1. Τη MAC του PC1 την έμαθε επειδή στο ARP Request που δέχτηκε ήταν η MAC του αποστολέα. Ο πίνακας ARP του Router1 ανανεώθηκε.



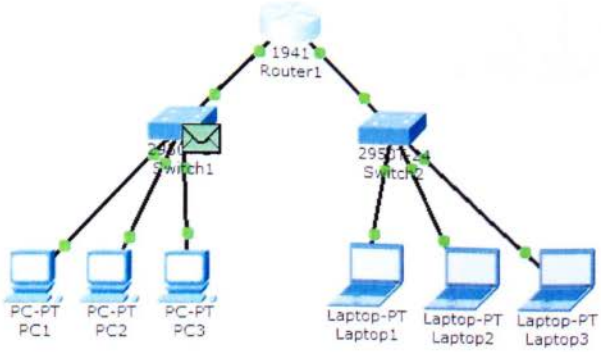
Εικόνα Παρ1.7

ARP Table for Router1

IP Address	Hardware Address	Interface
192.168.1.1	0001.C798.69DE	GigabitEthernet0/1
192.168.1.254	00E0.B097.1402	GigabitEthernet0/1
192.168.2.254	00E0.B097.1401	GigabitEthernet0/0

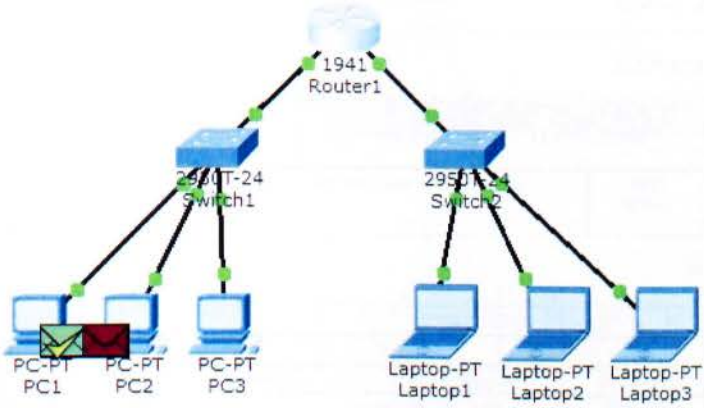
Εικόνα Παρ1.8

Βήμα 4: Το Arp Reply μεταφέρεται στο Switch1



Εικόνα Παρ1.9

Βήμα 5: Το Switch1 διαβάζοντας το MAC table του στέλνει το Arp Reply στο PC



Εικόνα Παρ1.10

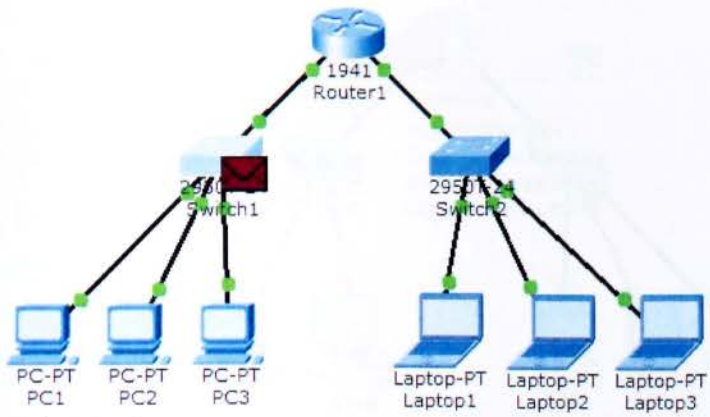
Παρατηρήσεις: Ο Arp table του PC1 έχει ανανεωθεί. Πλέον το ICMP frame μπορεί να αποσταλεί αφού έγινε η αντιστοίχιση στον Arp table του PC1 της IP του interface GigabitEthernet 0/1 του Router1 και της MAC.

ARP Table for PC1

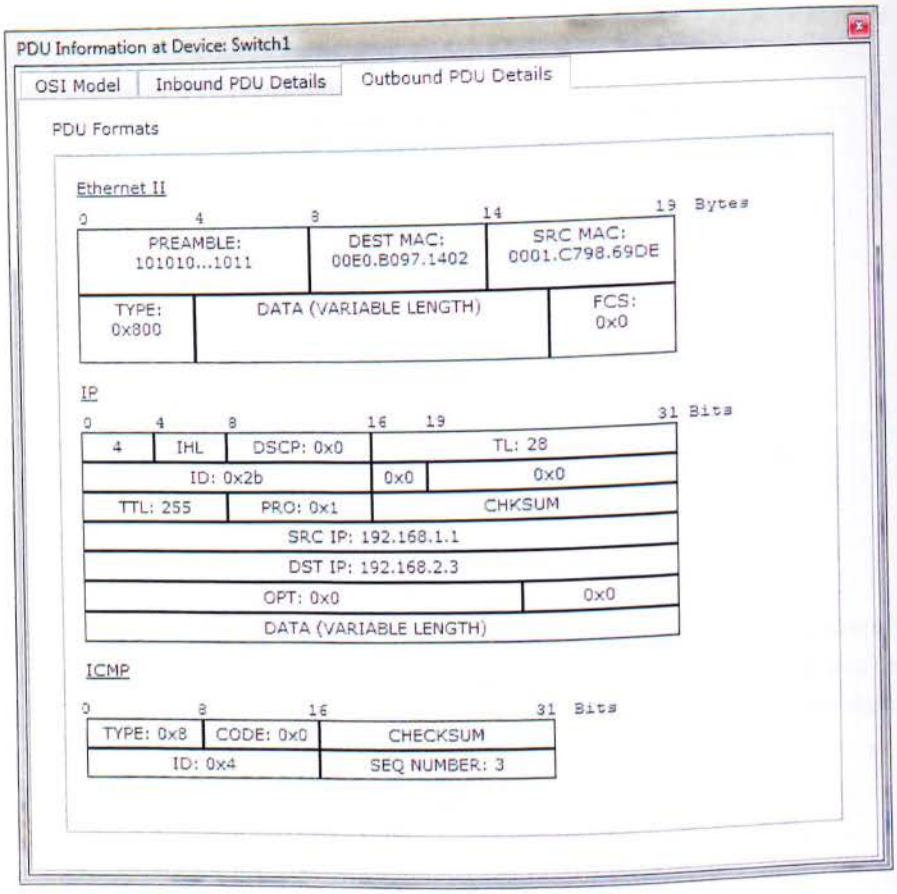
IP Address	Hardware Address	Interface
192.168.1.254	00E0.B097.1402	FastEthernet0

Εικόνα Παρ1.11

Βήμα 6: Το ICMP frame αποστέλλεται στο Switch1.

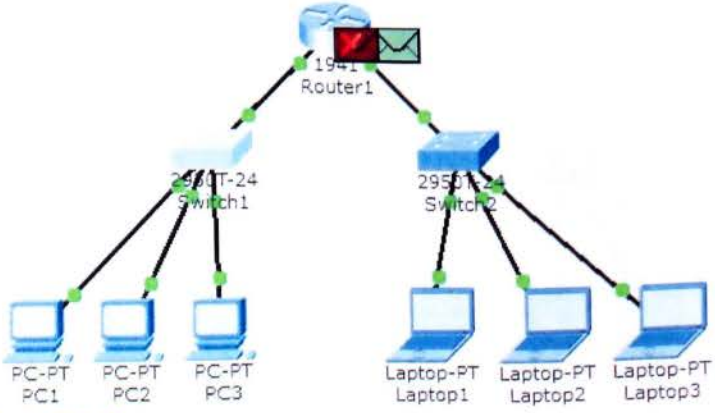


Εικόνα Παρ1.12



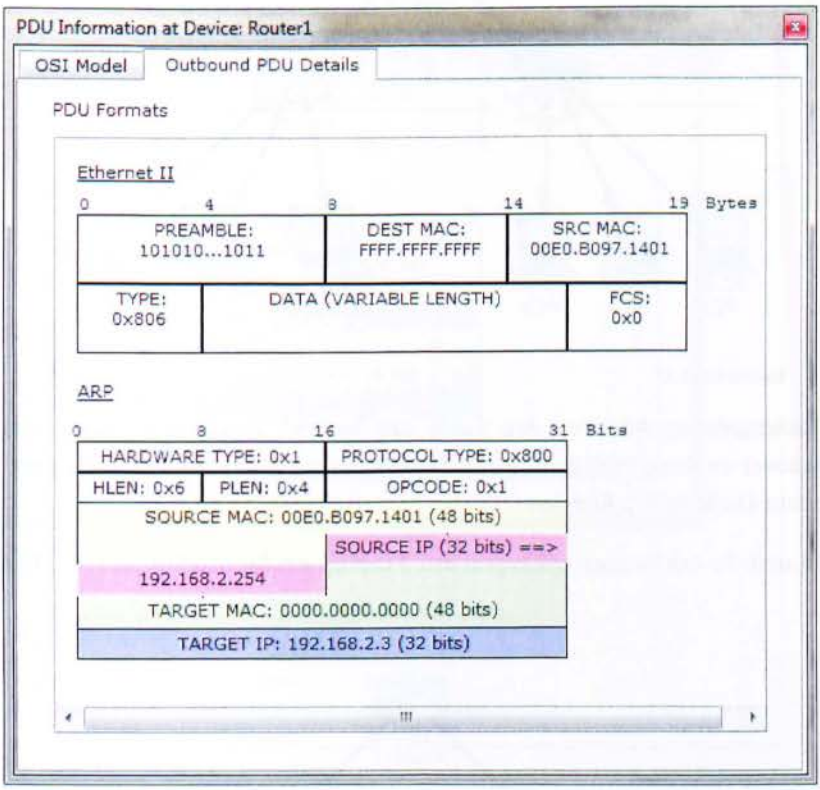
Εικόνα Παρ1.13

Βήμα 7: Το ICMP πακέτο αποστέλλεται στο Router1.



Εικόνα Παρ1.14

Παρατηρήσεις: Το ICMP frame δεν μπορεί να αποσταλεί στο Laptop3, γιατί ο Router1 δεν γνωρίζει τη MAC διεύθυνση του Laptop3. Για αυτό το λόγο ετοιμάζεται να σταλεί στο δίκτυο 192.168.2.0 ένα ARP Request .



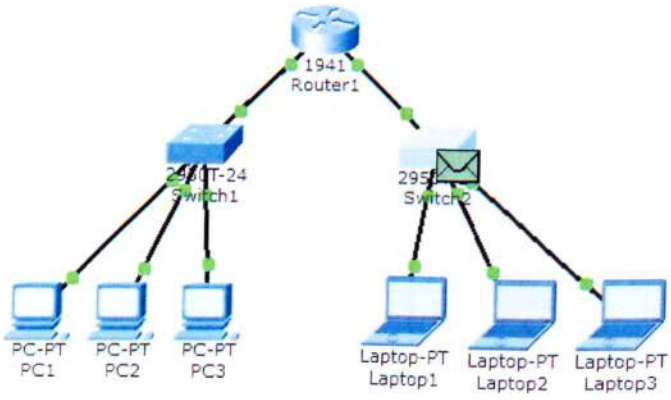
Εικόνα Παρ1.15

ARP Table for Router1

IP Address	Hardware Address	Interface
192.168.1.1	0001.C798.69DE	GigabitEthernet0/1
192.168.1.254	00E0.B097.1402	GigabitEthernet0/1
192.168.2.254	00E0.B097.1401	GigabitEthernet0/0
192.168.2.3	Incomplete	GigabitEthernet0/0

Εικόνα Παρ1.16

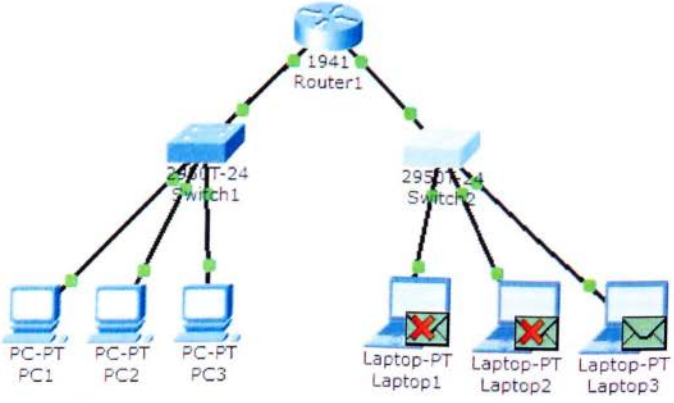
Βήμα 8: Το ARP Request αποστέλλεται στο Switch2.



Εικόνα Παρ1.17

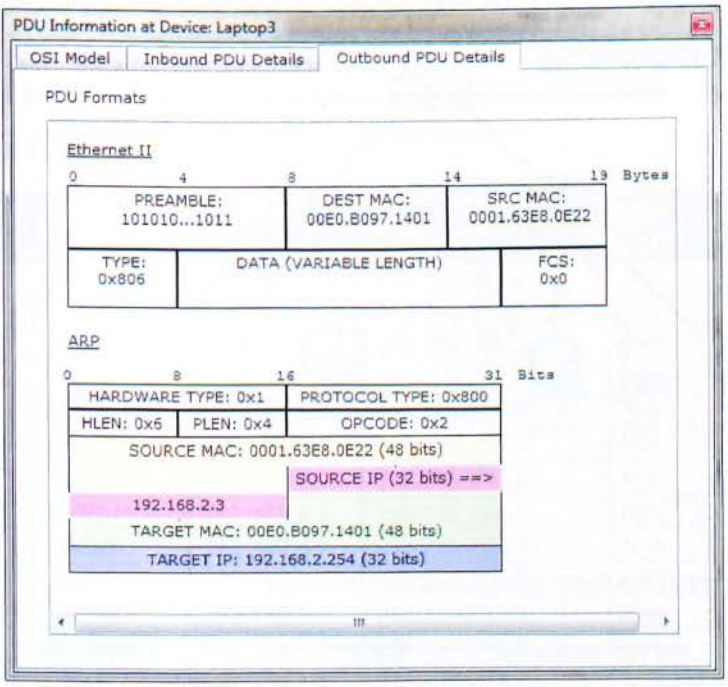
Παρατηρήσεις: Αφού ο Arp Table του Switch2 είναι κενός θα στείλει το ARP Request σε όσες Port είναι συνδεδεμένες συσκευές, εκτός από την Port από την οποία έλαβε το Arp Request.

Βήμα 9: Το Arp Request στέλνεται στα 3 Laptop και όχι στο Router1 (multicast).



Εικόνα Παρ1.18

Παρατηρήσεις: Το ARP Request απορρίφθηκε από το Laptop1 και Laptop 2 και έγινε δεκτό από το Laptop3, αφού η TARGET IP του ARP Request ήταν η IP του Laptop3. Το ARP Reply δημιουργήθηκε με τη TARGET IP να είναι η IP του interface GigabitEthernet 0/0 του Router1 και η TARGET MAC του interface GigabitEthernet 0/0 του Router1, που ήταν και ο αποστολέας στο ARP Request. Το ARP Table του Laptop 3 έχει ενημερωθεί



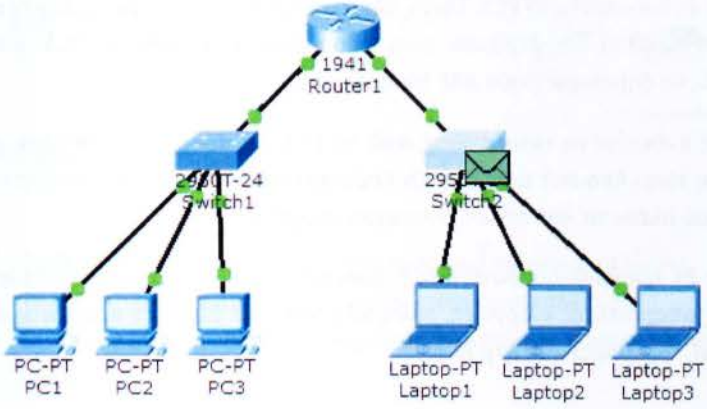
Εικόνα Παρ1.19

ARP Table for Laptop3

IP Address	Hardware Address	Interface
192.168.2.254	00E0.B097.1401	FastEthernet0

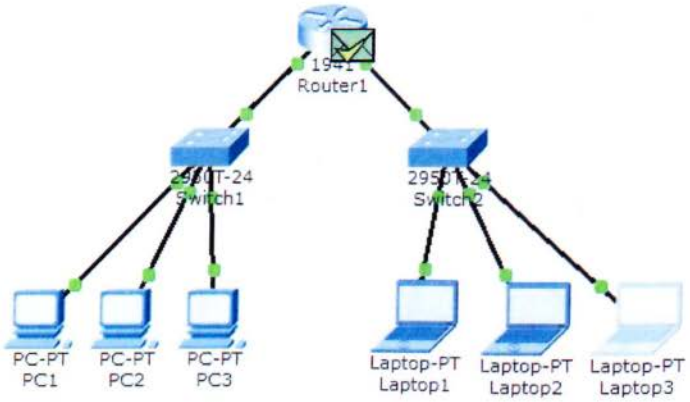
Εικόνα Παρ1.20

Βήμα 10: Το ARP Reply αποστέλλεται στο Switch2



Εικόνα Παρ1.21

Βήμα 11: Το Arp Reply αποστέλλεται στο Router1.



Εικόνα Παρ1.22

Παρατηρήσεις: Ο Arp Table του Router1 ενημερώθηκε

ARP Table for Router1

IP Address	Hardware Address	Interface
192.168.1.1	0001.C798.69DE	GigabitEthernet0/1
192.168.1.254	00E0.B097.1402	GigabitEthernet0/1
192.168.2.254	00E0.B097.1401	GigabitEthernet0/0
192.168.2.3	0001.63E8.0E22	GigabitEthernet0/0

Εικόνα Παρ1.23

ΣΥΜΠΕΡΑΣΜΑ ΑΣΚΗΣΗΣ

Το Arp Reply το αποδέχεται ο Router1. Δεν το αποστέλλει στο PC1, γιατί το TARGET IP και το TARGET MAC συμφωνούν με το GigabitInterface 0/0 του Router 1. Το ICMP πακέτο δε θα φτάσει ποτέ στο PC1. Όμως πλέον οι ARP tables ενημερώθηκαν και τα επόμενα ICMP πακέτα θα φτάσουν στον προορισμό τους από το PC1 προς το Laptop3, χωρίς να δημιουργηθούν ARP frames.

Επομένως: Σε ενδεχόμενη εντολή Ping από το PC1 με προορισμό το Laptop 3 η πρώτη ένδειξη είναι Request time out. Οι επόμενες αποστολές ICMP packets είναι επιτυχείς, αφού πλέον τα ARP tables είναι ενημερωμένα.

Παρατήρηση: Σε πραγματικές συνθήκες ο δρομολογητής (Router) αποθηκεύει στη μνήμη του τις απαραίτητες ενέργειες, όπως να στείλει με βάση το παράδειγμά μας το ICMP packet, αφού λάβει το Arp Reply.

Παράδειγμα 2

ΤΙΤΛΟΣ: ΕΞΕΡΕΥΝΗΣΗ ΠΡΩΤΟΚΟΛΛΟΥ ΔΡΟΜΟΛΟΓΗΣΗΣ RIP. ΡΥΘΜΙΣΗ CISCO ROUTERS ΣΕ CLI ΣΤΟ PACKET TRACER.

ΔΕΔΟΜΕΝΑ ΑΣΚΗΣΗΣ

Συσκευή	Διεπαφή	IP διεύθυνση	Μάσκα Υποδικτύου	Προεπιλεγμένη πύλη
R1	**Fa0/0**	192.168.1.1	255.255.255.0	N/A
	Fa0/1	192.168.2.1	255.255.255.0	N/A
R2	**Fa0/0**	192.168.2.2	255.255.255.0	N/A
	S0/0/0	192.168.7.1	255.255.255.0	N/A
	S0/0/1	192.168.3.1	255.255.255.0	N/A
R3	**Fa0/0**	192.168.4.1	255.255.255.0	N/A
	S0/0/0	192.168.5.1	255.255.255.0	N/A
	S0/0/1	192.168.3.2	255.255.255.0	N/A
R4	**Fa0/0**	192.168.6.1	255.255.255.0	N/A
	S0/0/0	192.168.7.2	255.255.255.0	N/A
	S0/0/1	192.168.5.2	255.255.255.0	N/A
	Fa0/0	192.168.6.1	255.255.255.0	N/A
PC1	**NIC**	192.168.1.10	255.255.255.0	192.168.1.1
PC3	**NIC**	192.168.4.10	255.255.255.0	192.168.4.1
PC4	**NIC**	192.168.6.10	255.255.255.0	192.168.6.1

Πίνακας Παρ2.1

Εικόνα Παρ2.1

- Τα R2, R3, R4 συνδέονται μεταξύ τους με 2 σειριακά καλώδια.
- Το R3 με το PC3 συνδέονται Copper cross over καλώδιο
- Οι υπόλοιπες συνδέσεις πραγματοποιούνται με Copper straight – through καλώδια.

Τα Routing tables έχουν ως εξής:

Routing Table for R1

Type	Network	Port	Next Hop IP	Metric
C	192.168.1.0/24	FastEthernet0/0	---	0/0
C	192.168.2.0/24	FastEthernet0/1	---	0/0
S	192.168.3.0/24	FastEthernet0/1	---	1/0
S	192.168.4.0/24	FastEthernet0/1	---	1/0
S	192.168.5.0/24	FastEthernet0/1	---	1/0
S	192.168.6.0/24	---	192.168.2.2	1/0
S	192.168.7.0/24	---	192.168.2.2	1/0

Εικόνα Παρ2.2

Routing Table for R2

Type	Network	Port	Next Hop IP	Metric
C	192.168.2.0/24	FastEthernet0/0	---	0/0
C	192.168.3.0/24	Serial0/0/1	---	0/0
C	192.168.7.0/24	Serial0/0/0	---	0/0

Εικόνα Παρ2.3

Routing Table for R3

Type	Network	Port	Next Hop IP	Metric
C	192.168.3.0/24	Serial0/0/1	---	0/0
C	192.168.4.0/24	FastEthernet0/0	---	0/0
C	192.168.5.0/24	Serial0/0/0	---	0/0
S	192.168.1.0/24	---	192.168.3.1	1/0

Εικόνα Παρ2.4

Routing Table for R4

Type	Network	Port	Next Hop IP	Metric
C	192.168.5.0/24	Serial0/0/1	---	0/0
C	192.168.6.0/24	FastEthernet0/0	---	0/0
C	192.168.7.0/24	Serial0/0/0	---	0/0

Εικόνα Παρ2.5

Σκοπός άσκησης

- Να δούμε στην πράξη πώς ένας πίνακας δρομολόγησης μπορεί να περιέχει ταυτόχρονα και να αξιοποιεί δυναμικές και στατικές διαδρομές.

Εισαγωγή:

Οι δρομολογητές (routers) μπορούν να μάθουν για την ύπαρξη απομακρυσμένων δικτύων στατικά ή δυναμικά. Η άσκηση αυτή επικεντρώνεται πώς απομακρυσμένα δίκτυα προστίθενται στον πίνακα δρομολόγησης χρησιμοποιώντας στατικές διαδρομές μαζί με δυναμικό πρωτόκολλο δρομολόγησης. Οι στατικές διαδρομές ρυθμίζονται από τον διαχειριστή του δικτύου και εμπεριέχουν:

- Τη διεύθυνση δικτύου
- Τη μάσκα υποδικτύου του απομακρυσμένου δικτύου
- Την IP διεύθυνση του αμέσως επόμενου δρομολογητή ή τη διεπαφή εξόδου του τοπικού δρομολογητή

Τα πρωτόκολλα δυναμικής δρομολόγησης επιτρέπουν στους δρομολογητές αυτόματα να μαθαίνουν την ύπαρξη απομακρυσμένων δικτύων με τη βοήθεια άλλων δρομολογητών. Τα δίκτυα και το καλύτερο μονοπάτι προς κάθε δίκτυο προστίθενται στον πίνακα δρομολόγησης καθώς ανακαλύπτονται μέσω από το πρωτόκολλο δρομολόγησης.

ΕΚΤΕΛΕΣΗ ΑΣΚΗΣΗΣ

Εργασία 1: Ορίστε το RIP ως πρωτόκολλο δυναμικής δρομολόγησης σε R2, R3, και R4.

Βήμα 1. Ορίστε το Rip σε R2

Επιλέγουμε το R2 στο workspace. Επιλέγουμε την καρτέλα CLI. Πληκτρολογούμε:

Password:**cisco**

R2>**enable**

Password: **class**

R2#**configure terminal**

R2(config)#**router rip**

R2(config-router)#**network 192.168.2.0**

R2(config-router)#**network 192.168.3.0**

R2(config-router)#**network 192.168.7.0**

R2(config-router)#**end**

Βήμα 2. Ορίστε το RIP σε R3.

Επιλέγουμε το R3 στο workspace. Επιλέγουμε την καρτέλα CLI. Πληκτρολογούμε:

Password:**cisco**

R3>**enable**

Password: **class**

R3#**configure terminal**

R3(config)#**router rip**

R3(config-router)#**network 192.168.3.0**

R3(config-router)#**network 192.168.4.0**

R3(config-router)#**network 192.168.5.0**

R3(config-router)#**end**

Βήμα 3. Ορίστε το RIP σε R4.

Επιλέγουμε το R4 στο workspace. Επιλέγουμε την καρτέλα CLI. Πληκτρολογούμε:

Password:**cisco**

R4>**enable**

Password: **class**

R4#**configure terminal**

R4(config)#**router rip**

R4(config-router)#**network 192.168.5.0**

R4(config-router)#**network 192.168.6.0**

R4(config-router)#**network 192.168.7.0**

R4(config-router)#**end**

Εργασία 2: Επαληθεύστε τις στατικές και δυναμικές διαδρομές.

Βήμα 1. Επαληθεύστε τον πίνακα δρομολόγησης σε κάθε δρομολογητή.

Επιλέγουμε το R1 στο workspace. Επιλέγουμε την καρτέλα CLI. Πληκτρολογούμε:

Password:**cisco**

R1>**enable**

Password: **class**

R1#**show ip route**

ΠΑΡΑΤΗΡΗΣΗ: Ο πίνακας δρομολόγησης πρέπει να δείχνει τις άμεσα συνδεδεμένες διαδρομές και τις στατικές διαδρομές, αλλά δεν υπάρχουν δυναμικές διαδρομές σε απομακρυσμένα δίκτυα.

Επαναλαμβάνουμε το προηγούμενο βήμα σε R2, R3, και R4.

ΠΑΡΑΤΗΡΗΣΗ: Οι πίνακες δρομολόγησης στους άλλους δρομολογητές πρέπει να δείχνουν τις άμεσα συνδεδεμένες διαδρομές και συνδυασμούς από στατικές και δυναμικές διαδρομές προς απομακρυσμένα δίκτυα.

Βήμα 2. Εξερευνήστε τον πίνακα δρομολόγησης στο R1.

Από το CLI, πληκτρολογούμε:

R1#**show ip route**

Υπάρχουν στατικές διαδρομές στον πίνακα δρομολόγησης; Εάν ναι, ποιες είναι;

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/1
S    192.168.3.0/24 is directly connected, FastEthernet0/1
S    192.168.4.0/24 is directly connected, FastEthernet0/1
S    192.168.5.0/24 is directly connected, FastEthernet0/1
S    192.168.6.0/24 [1/0] via 192.168.2.2
S    192.168.7.0/24 [1/0] via 192.168.2.2
R1#
```

Εικόνα Παρ2.6

Βήμα 3. Εκτελούμε Ping από το R3 σε PC1.

Επιλέγουμε το R3 στο workspace. Επιλέγουμε την καρτέλα CLI. Πληκτρολογούμε:

R3#**ping 192.168.1.10**

Ήταν το ping επιτυχές;

```
R3#ping 192.168.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
```

Εικόνα Παρ2.7

ΠΑΡΑΤΗΡΗΣΗ: Εάν το ping δεν είχε επιτυχία ελέγξτε τους πίνακες δρομολόγησης και στους 3 δρομολογητές για να συμπεράνετε το πρόβλημα.

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.2.0/24 is directly connected, FastEthernet0/0
C    192.168.3.0/24 is directly connected, Serial0/0/1
R    192.168.4.0/24 [120/1] via 192.168.3.2, 00:00:00, Serial0/0/1
R    192.168.5.0/24 [120/1] via 192.168.3.2, 00:00:00, Serial0/0/1
                    [120/1] via 192.168.7.2, 00:00:01, Serial0/0/0
R    192.168.6.0/24 [120/1] via 192.168.7.2, 00:00:01, Serial0/0/0
C    192.168.7.0/24 is directly connected, Serial0/0/0
```

Εικόνα Παρ2.8

```
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

S    192.168.1.0/24 [1/0] via 192.168.3.1
R    192.168.2.0/24 [120/1] via 192.168.3.1, 00:00:04, Serial0/0/1
C    192.168.3.0/24 is directly connected, Serial0/0/1
C    192.168.4.0/24 is directly connected, FastEthernet0/0
C    192.168.5.0/24 is directly connected, Serial0/0/0
R    192.168.6.0/24 [120/1] via 192.168.5.2, 00:00:19, Serial0/0/0
R    192.168.7.0/24 [120/1] via 192.168.3.1, 00:00:04, Serial0/0/1
                    [120/1] via 192.168.5.2, 00:00:19, Serial0/0/0
```

Εικόνα Παρ2.9

ΣΥΜΠΕΡΑΣΜΑ:

- Ο R3 μπορεί να επικοινωνήσει με το δίκτυο 192.168.1.0 που βρίσκεται ο PC1.

S 192.168.1.0/24 [1/0] via 192.168.3.1

R 192.168.2.0/24 [120/1] via 192.168.3.1, 00:00:04, Serial0/0/1.

- Ο R2 δεν μπορεί να επικοινωνήσει με το δίκτυο 192.168.1.0 που βρίσκεται ο PC1.

Δεν υπάρχει διαδρομή προς το 192.168.1.0

Εργασία 3: Εισάγετε στατική διαδρομή στο R2 ώστε να επικοινωνεί με το τοπικό δίκτυο του R1.

Ακολουθήστε τα βήματα για να εισάγετε στατική διαδρομή στο R2 ώστε να επικοινωνεί με το τοπικό δίκτυο του R1

Βήμα 1. Εισάγουμε στατική διαδρομή στο R2 .

Επιλέγουμε το R2 στο workspace. Επιλέγουμε την καρτέλα CLI. Πληκτρολογούμε:

Password:**cisco**

R2>**enable**

Password: **class**

R2#**show ip route**

ΠΑΡΑΤΗΡΗΣΗ: Ο πίνακας δρομολόγησης δείχνει άμεσα συνδεδεμένες διαδρομές, αλλά δεν υπάρχουν στατικές διαδρομές σε απομακρυσμένα δίκτυα.

R2#**configure terminal**

R2(config)#**ip route 192.168.1.0 255.255.255.0 FastEthernet 0/0**

R2(config)#**end**

Βήμα 2. Εξερευνήστε τον πίνακα δρομολόγησης στο R2.

Επιλέγουμε το R2 στο workspace. Επιλέγουμε την καρτέλα CLI. Πληκτρολογούμε:

R2#**show ip route**

```
R2#
%SYS-5-CONFIG_I: Configured from console by console
show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

S    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
C    192.168.3.0/24 is directly connected, Serial0/0/1
R    192.168.4.0/24 [120/1] via 192.168.3.2, 00:00:11, Serial0/0/1
R    192.168.5.0/24 [120/1] via 192.168.3.2, 00:00:11, Serial0/0/1
                    [120/1] via 192.168.7.2, 00:00:16, Serial0/0/0
R    192.168.6.0/24 [120/1] via 192.168.7.2, 00:00:16, Serial0/0/0
C    192.168.7.0/24 is directly connected, Serial0/0/0
```

Εικόνα Παρ2.10

Υπάρχουν στατικές διαδρομές στον πίνακα δρομολόγησης; Εάν ναι, ποιες είναι;

S 192.168.1.0/24 is directly connected, FastEthernet0/0

Βήμα 3. Εκτελούμε την εντολή Ping από το R3 στο PC1.

Επιλέγουμε το R3 στο workspace. Επιλέγουμε την καρτέλα CLI. Πληκτρολογούμε:

R3#**ping 192.168.1.10**

Ήταν το ping επιτυχές?

```
R3#ping 192.168.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/12 ms
```

Εικόνα Παρ2.11

ΣΥΜΠΕΡΑΣΜΑ: Ναι ήταν επιτυχές. Πλέον ο R3 έχει πρόσβαση στο δίκτυο 192.168.1.0 λόγω της στατικής διαδρομής που προσθέσαμε στον R2

S 192.168.1.0/24 is directly connected, FastEthernet0/0

Εργασία 4: Δείτε τα RIP routing updates σε simulation mode.

Ακολουθήστε τα παρακάτω βήματα:

Βήμα 1. Αλλαγή από Realtime σε Simulation mode

- Έξω από το workspace στην κάτω δεξιά γωνία βρίσκεται το κουμπί με όνομα **Realtime**.
- Επιλέξτε την καρτέλα **Simulation** που βρίσκεται πάνω δεξιά και πίσω από το **Realtime**.
- Τώρα βρίσκεστε σε simulation mode.

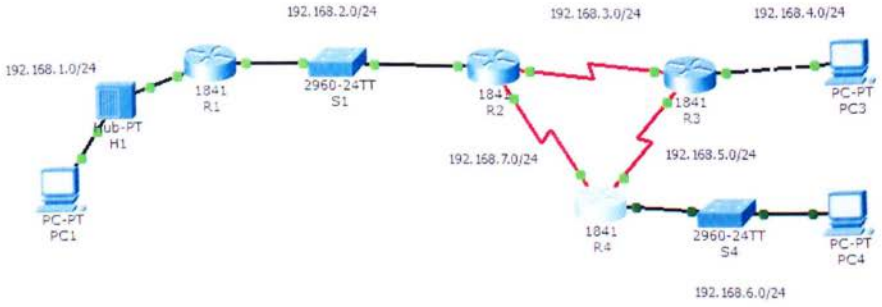
Βήμα 2. Φιλτράρετε την κίνηση ώστε να είναι ορατά μόνο τα πακέτα RIP.

- Από το simulation mode, επιλέξτε το κουμπί entitled **Edit Filters**
- Επιλέγουμε στο κουτί entitled **Show All/None** να καθαρίσουν οι επιλογές.
- Επιλέγουμε στο κουτί entitled **RIP**.

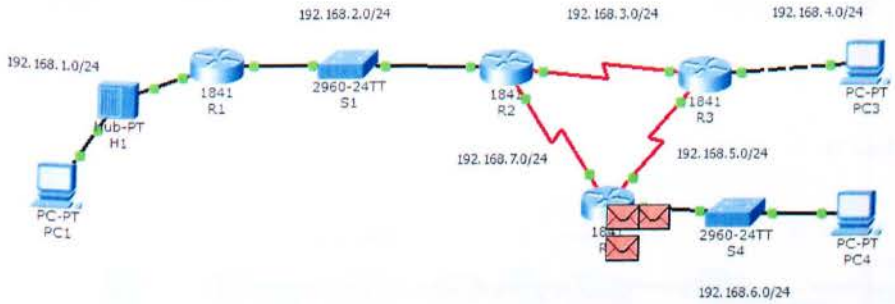
Βήμα 3. Αρχίστε το simulation.

- Για να αρχίσει η ροή επιλέγουμε στο κουμπί entitled **Auto Capture / Play.**
- Με αυτό θα αρχίσει η ροή από τα RIP updates μεταξύ των δρομολογητών.
- Παρατηρήστε ότι το R1 δεν στέλνει RIP updates και επίσης απορρίπτει τα RIP updates που λαμβάνει.

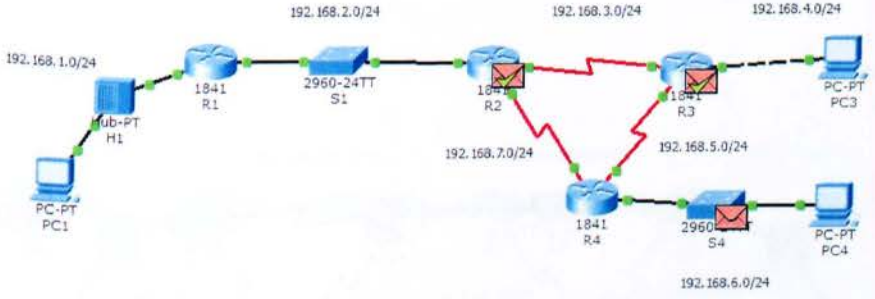
ΠΑΡΑΤΗΡΗΣΗ:Σε κατάσταση simulation, επιλέγουμε ένα από τα πακέτα που έχουν απορριφθεί από το R1.



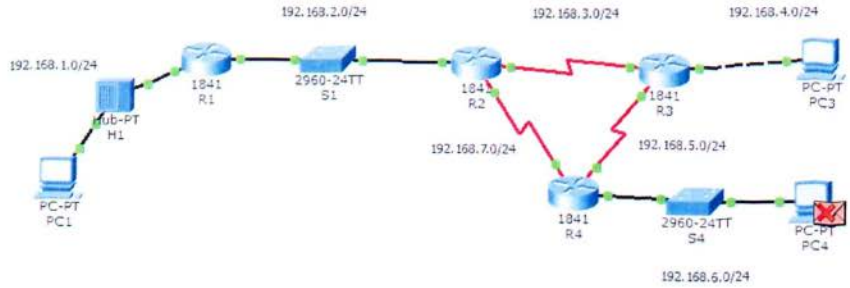
Εικόνα Παρ2.12



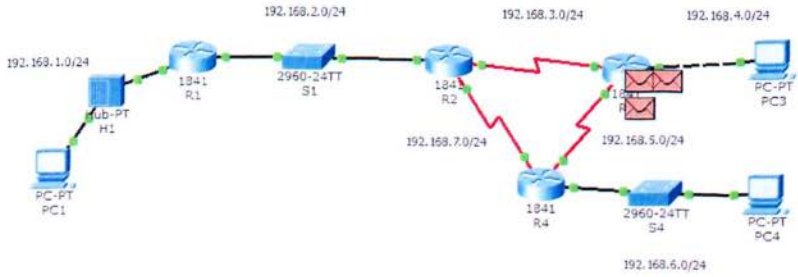
Εικόνα Παρ2.13



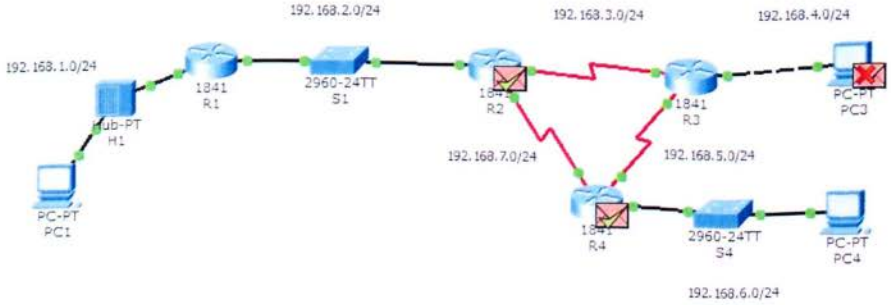
Εικόνα Παρ2.14



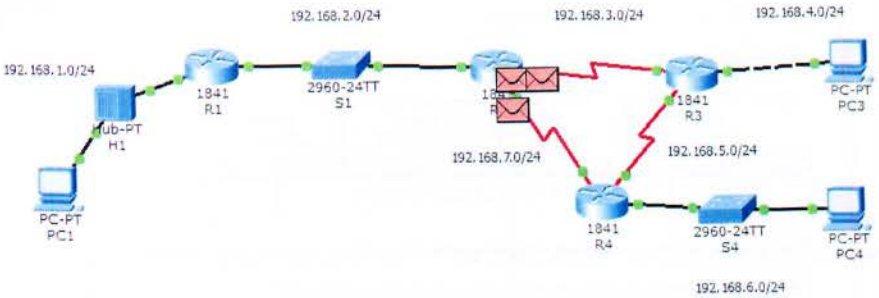
Εικόνα 2.15



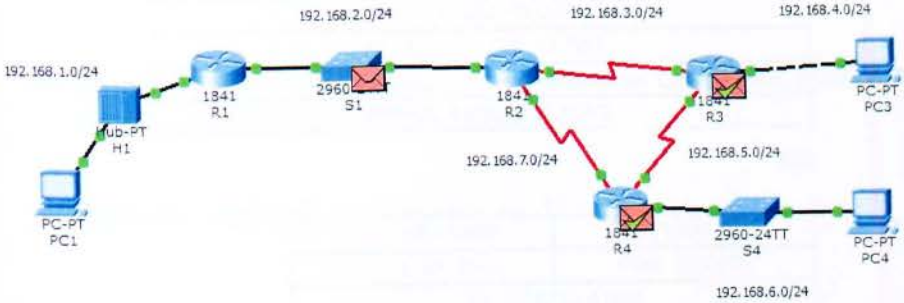
Εικόνα 2.16



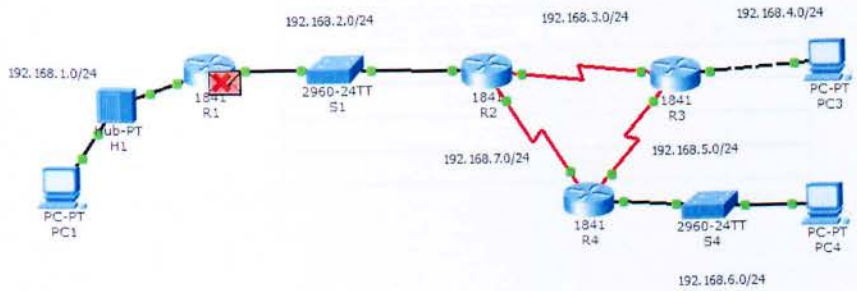
Εικόνα 2.17



Εικόνα 2.18



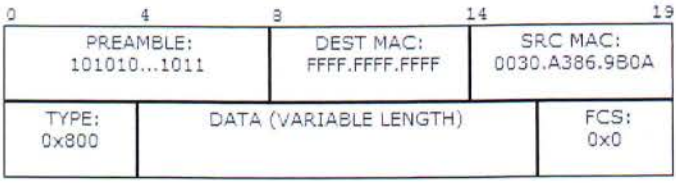
Εικόνα 2.19



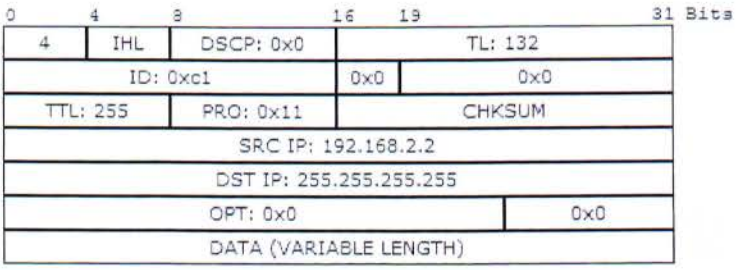
Εικόνα 2.20

PDU Formats

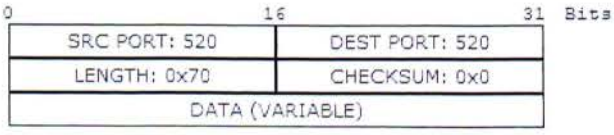
Ethernet II



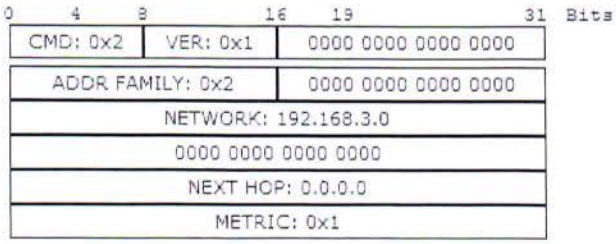
IP



UDP



RIP v.1



Εικόνα 2.21

Ο R1 αρχίζει και διαβάζει τα δεδομένα από το Layer 1. Στο Layer 4 στο UDP απορρίπτει το πακέτο και δεν προχωράει στο Layer 7 που βρίσκονται τα δεδομένα του RIP v1. Επειδή δεν έχει οριστεί λειτουργία RIP στο R1 η πόρτα 520 είναι κλειστή. Επομένως ούτε δέχεται ενημερώσεις RIP ούτε αποστέλλει ενημερώσεις RIP σε άλλους δρομολογητές.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- **Δίκτυα Υπολογιστών.** Andrew S.Tanenbaum. Εκδόσεις Κλειδάριθμος

- **Cisco CCNA Routing and Switching 200-120 Foundation Learning Guide Library.** Anthony Sequeira, John Tiso. Εκδόσεις Ciscopress

- **Network Fundamentals: CCNA Exploration Companion Guide**. Mark Dye, Rick McDonald, Antoon Rufi. Εκδόσεις Ciscopress

- **Routing Protocols and Concepts: CCNA Exploration Companion. Guide Rick Graziani, Allan Johnson.** Εκδόσεις Ciscopress

- **Wikipedia:** http://www.en.wikipedia.org