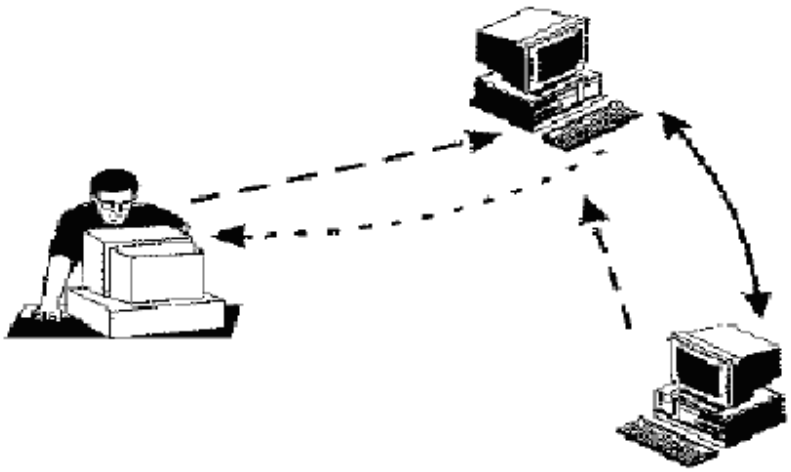
Α.Τ.Ε.Ι. ΚΡΗΤΗΣ

ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ ΕΠΙΛΟΓΗΣ

«ΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ ΚΑΙ ΔΙΚΤΥΑ Η/Υ»

ΤΙΤΛΟΣ: *ΜΕΛΕΤΗ ΜΕΤΑΔΟΣΗΣ ΔΕΔΟΜΕΝΩΝ ΣΕ ΑΣΥΡΜΑΤΑ ΤΟΠΙΚΑ ΔΙΚΤΥΑ IEEE 802.11*



ΦΟΙΤΗΤΗΣ: ΚΑΛΙΟΝΤΖΑΚΗΣ ΣΤΥΛΙΑΝΟΣ

ΕΙΣΗΓΗΤΗΣ:ΛΙΟΔΑΚΗΣ ΓΕΩΡΓΙΟΣ ΚΑΘΗΓΗΤΗΣ ΕΦΑΡΜΟΓΩΝ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΝΙΚΗΣ/ΤΟΜΕΑΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΕΡΓΑΣΤΗΡΙΟ ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ,ΔΙΚΤΥΩΝ ΚΑΙ ΕΦΑΡΜΟΓΩΝ

(COMmunication NETworks Telematic Applications – COMNETTA Group)

Χανιά Κρήτης, Φεβρουάριος 2006

ΠΕΡΙΕΧΟΜΕΝΑ

Κεφάλαιο 3: Θέματα μετάδοσης δεδομένων πολυμέσων σε IEEE 802.11 WLAN

Κεφάλαιο 4: Πειραματική μελέτη

Ευχαριστίες

Θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες στον καθηγητή εφαρμογών του Ανώτατου Τεχνολογικού Εκπαιδευτικού Ιδρύματος Χανίων Κρήτης, κ. Λιοδάκη Γεώργιο, του οποίου η βοήθεια για την παρούσα πτυχιακή εργασία ήταν πολύ σημαντική.
Τέλος ευχαριστώ την οικογένεια μου για την ψυχολογική υποστήριξη που μου προσέφεραν.

Καλιοντζάκης Στυλιανός

Κεφάλαιο 1: Εισαγωγή στα ασύρματα δίκτυα

1.1 Εισαγωγή

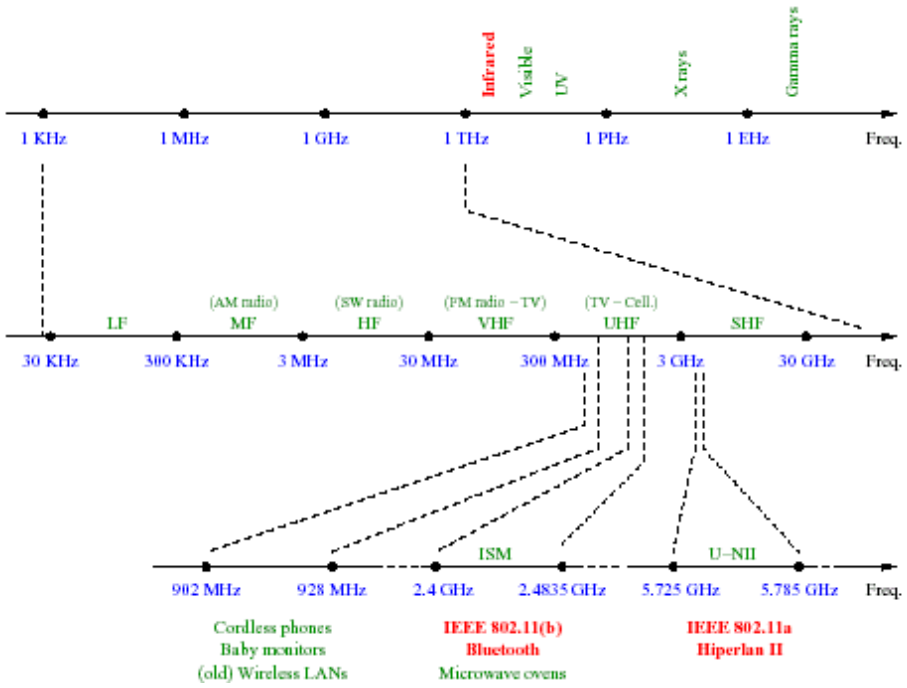
Με τον όρο ασύρματα δίκτυα επικοινωνιών καλούνται όλες οι τεχνολογικές λύσεις δικτύωσης μεταξύ υπολογιστικών συσκευών στις οποίες το φυσικό μέσο μετάδοσης των πληροφοριών είναι ραδιοσυχνότητες(RF) και με αυτό τον τρόπο για τη μετάδοσή τους δεν απαιτείται η μεσολάβηση κάποιου καλωδίου. Οι τεχνολογικές λύσεις αυτές είναι πολλές στον αριθμό και καλύπτουν ένα μεγάλο φάσμα προτύπων και τεχνολογιών όπως είναι τα δίκτυα GSM/GPRS (η τεχνολογία δηλαδή που χρησιμοποιούν τα γνωστά σε όλους μας κινητά τηλέφωνα), το LMDS, το HiperLAN, το 802.11, το Bluetooth, λύσεις που εκμεταλλεύονται το υπέρυθρο κομμάτι του φάσματος (FSO – Free Space Optics, open-air photonics) κ.λπ.

1.2 Ιστορικό

Η πρώτη προσπάθεια για τη σύνδεση των τεχνολογιών δικτύου με την επικοινωνία μέσω ραδιοκυμάτων ξεκίνησε το 1971 με την υλοποίηση ενός project του πανεπιστήμιου της Hawaii, το οποίο ονομάστηκε ALOHANET. Το ALOHANET ήταν ένα σύστημα όπου απομακρυσμένοι υπολογιστές επικοινωνούσαν μεταξύ τους μέσω ενός κεντρικού υπολογιστή χωρίς την χρησιμοποίηση των συμβατικών τηλεφωνικών καλωδίων, αλλά με τη βοήθεια ραδιοκυμάτων.

Το 1985, στην Αμερική, ο οργανισμός FCC (Federal Communications Commission) ο οποίος καθορίζει το εύρος συχνοτήτων που θα χρησιμοποιείται για κάθε τηλεπικοινωνιακή εφαρμογή - εξουσιοδότησε την κοινή χρήση του φάσματος συχνοτήτων

ISM (Instrumentation, Scientific, and Medical) στο οποίο στηρίχθηκε η μελλοντική κατασκευή όλων των τεχνολογιών WLAN.



Σχήμα 1.1

Για την κατασκευή ενός WLAN σε μία χώρα, θα πρέπει να ληφθεί υπόψη η νόμιμη χρήση των συχνοτήτων αυτών από τους αντίστοιχους οργανισμούς της συγκεκριμένης χώρας.(Σχήμα 1.1)

Στα τέλη του 1980, το IEEE ξεκίνησε την ανάπτυξη του πρώτου Standard για WLANs, το οποίο ολοκληρώθηκε τελικά το 1977 και είναι γνωστό ως IEEE 802.11. Όπως θα δούμε παρακάτω, την προσπάθεια αυτή ακολούθησαν και άλλοι οργανισμοί ώστε να επιτύχουν την καλύτερη δυνατή απόδοση των ασύρματων τοπικών δικτύων.

1.3 Σύγχρονες τεχνολογίες – πρότυπα

Για την υλοποίηση ενός ασύρματου τοπικού δικτύου μπορεί να επιλεχθεί ένα από τα πολλά Standards που οι διάφοροι οργανισμοί και εταιρίες έχουν δημιουργήσει τα τελευταία χρόνια. Στη συνέχεια αναφέρουμε τα κυριότερα.

1.3.1 IEEE 802.11

Τον Ιούνιο του 1977 η IEEE οριστικοποίησε το πρώτο της Standard για WLANs. Το 802.11 Standard καθορίζει ως συχνότητα λειτουργίας τα 2.4 GHz και υποστηρίζει ρυθμούς δεδομένων της τάξεως των 1 Mbps και 2 Mbps. Για την ασύρματη μεταφορά δεδομένων καθορίζονται οι λειτουργίες και οι υπηρεσίες ενός υποστρώματος MAC και τριών διαφορετικών φυσικών στρωμάτων. Το υποστρώμα MAC έχει 2 τρόπους λειτουργίας:

- Μία κατανεμημένη (distributed) λειτουργία (CSMA/CA)
- Μια συντονισμένη (coordinated) λειτουργία (polling mode)

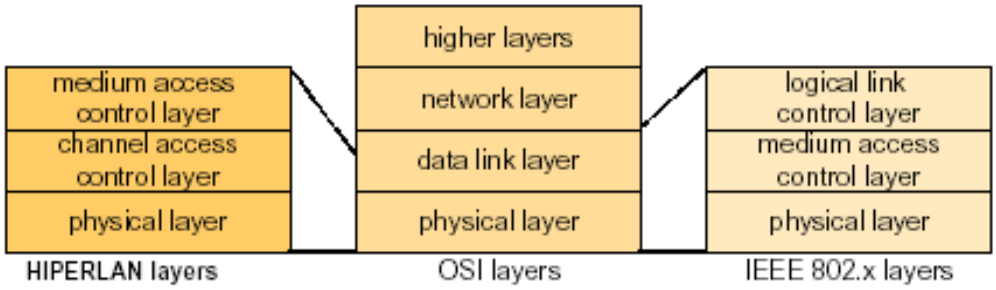
Στα τέλη του 1999 η IEEE κοινοποίησε δύο νέα συμπληρωματικά Standards για WLANs, τα 802.11a και 802.11b:

- Το 802.11a έχει καθοριστεί έτσι ώστε να υποστηρίζει ρυθμούς δεδομένων έως και 54 Mbps με χρήση της τεχνικής διαμόρφωσης OFDM (Orthogonal Frequency Division Multiplexing) στην μπάντα των 5 GHz.
- Το 802.11b είναι ουσιαστικά μια προέκταση του αρχικού 802.11 καθώς χρησιμοποιεί ως διαμόρφωση την τεχνική DSSS και λειτουργεί στα 2.4 GHz. Η διαφορά έγκειται στο γεγονός ότι μπορεί να υποστηρίξει ρυθμούς δεδομένων έως και 11 Mbps.

1.3.2 HiperLAN

Το HiperLAN καθιερώθηκε το 1996 από την ETSI (European Telecommunications Standards Institute). Η πρώτη έκδοση του Standard είναι το HiperLAN I. Το Standard αυτό

λειτουργεί στην μπάντα από 5.1 έως 5.3 GHz, ενώ ο ρυθμός σηματοδοσίας φτάνει τα 24 Mbps. Το πρωτόκολλο χρησιμοποιεί μια παραλλαγή του CSMA/CA η οποία στηρίζεται στο χρόνο ζωής του πακέτου, την προτεραιότητα των πακέτων και τις αναμεταδόσεις στο επίπεδο MAC. Στο επόμενο σχήμα (Σχήμα 1.2) δίνεται η συσχέτιση των διάφορων στρωμάτων όπως αυτά καθορίζονται από τα δύο κυριότερα Standards (HiperLAN και 802.11x) με την αρχιτεκτονική OSI.



Σχήμα 1.2

Η ETSI έχει καθορίσει και ένα νέο πρωτόκολλο που ονομάζεται HiperLAN II και λειτουργεί και αυτό στα 5 GHz (5.4 έως 5.7 GHz). Το HiperLAN II στηρίζεται στην τεχνική διαμόρφωσης OFDM (Orthogonal Frequency Digital Multiplexing), ενώ υποστηρίζει διάφορους ρυθμούς μετάδοσης (6, 9, 12, 18, 27, 36 και έναν εναλλακτικό ρυθμό των 54 Mbps). Το HiperLan II είναι ουσιαστικά ένα σύστημα ασύρματου ATM, ενώ το πρωτόκολλο που χρησιμοποιείται στο υποστρώμα MAC στηρίζεται σε μια διαφοροποιημένη λειτουργία της τεχνικής TDMA.

1.3.3 OpenAir

Το OpenAir είναι ένα Standard που αναπτύχθηκε από την εταιρία Proxim. Είναι προγενέστερο του 802.11 και χρησιμοποιεί την τεχνική του Frequency Hopping επιτυγχάνοντας ρυθμούς δεδομένων 0.8 και 1.6 Mbps (χρησιμοποιώντας τεχνικές διαμόρφωσης 2FSK και 4FSK, αντίστοιχα). Το πρωτόκολλο που χρησιμοποιείται στο υποστρώμα MAC είναι το CSMA/CA με MAC επαναμεταδόσεις και στηρίζεται στην ανταλλαγή RTS/CTS πακέτων.

1.3.4 HomeRF SWAP

Η HomeRF είναι μια ομάδα από μεγάλες εταιρίες που δημιουργήθηκε για να προωθήσει την χρήση των WLAN στο σπίτι και στα γραφεία. Η ομάδα αυτή έχει αναπτύξει ένα νέο πρωτόκολλο για τον σκοπό αυτό, το οποίο ονομάζεται SWAP (Shared Wireless Access Protocol).

Το SWAP χρησιμοποιεί στο υποστρώμα MAC ένα νέο πρωτόκολλο, το οποίο συνδυάζει χαρακτηριστικά και λειτουργίες από το DECT (ένα Standard της ETSI για ψηφιακά ασύρματα τηλέφωνα) και το 802.11. Η συχνότητα λειτουργίας είναι τα 2.4 GHz, ενώ στο φυσικό στρώμα χρησιμοποιείται η τεχνική FHSS, υποστηρίζοντας ρυθμούς δεδομένων της τάξης των 1 Mbps και 2 Mbps.

1.3.5 Bluetooth

Το Bluetooth αποτελεί μια προδιαγραφή που εκδόθηκε από το Bluetooth Special Interest Group (SIG) με την ενίσχυση μερικών από τις μεγαλύτερες εταιρίες όπως οι Ericsson, IBM, Intel, Microsoft κ.ά. Το Bluetooth δεν αποτελεί ένα πρωτόκολλο για WLAN, αλλά βρίσκει εφαρμογές στα ασύρματα προσωπικά δίκτυα WPANs (Wireless Personal Area Networks), που αποτελούν μικρότερα σε έκταση δίκτυα από τα WLANs, με ακτίνα δράσης έως 10 μέτρα. Το Bluetooth λειτουργεί στα 2.4 GHz, χρησιμοποιεί ως τεχνική διαμόρφωσης την FHSS και φτάνει σε ρυθμούς δεδομένων ως το 1 Mbps.

1.4 Οφέλη από τα ασύρματα δίκτυα

Με τα ασύρματα δίκτυα οι χρήστες μπορούν να έχουν πρόσβαση σε πληροφορίες, χωρίς να αναζητούν κάποιον τρόπο για να συνδεθούν, ενώ τα δίκτυα μπορούν να αναβαθμιστούν ή να μεταφερθούν χωρίς μετακίνηση καλωδίων. Τα ασύρματα δίκτυα παρέχουν μία σειρά από πλεονεκτήματα σε σχέση με τα παραδοσιακά ενσύρματα δίκτυα όπως:

• Αύξηση της παραγωγικότητας λόγω της ευελιξίας στην κίνηση. Τα ασύρματα δίκτυα παρέχουν πρόσβαση σε οποιοδήποτε σημείο της εταιρίας, επιτρέποντας στους χρήστες να έχουν πρόσβαση στα δεδομένα τους ακόμα και όταν δεν βρίσκονται στο χώρο του γραφείου τους.

• Ταχύτητα και ευκολία εγκατάστασης. Χωρίς την τοποθέτηση καλωδίων σε τοίχους ή δάπεδα, η εγκατάσταση ενός ασύρματου δικτύου μπορεί να είναι εξαιρετικά γρήγορη και εύκολη.

• Ευελιξία. Με τα ασύρματα δίκτυα η πληροφορία μπορεί να πάει σε σημεία όπου δεν μπορεί να φτάσει το καλώδιο.

• Μειωμένο κόστος εγκατάστασης και συντήρησης. Αν και το αρχικό κόστος της εγκατάστασης των ασύρματων δικτύων μπορεί να είναι μεγαλύτερο από αυτό των ενσύρματων λύσεων, μακροπρόθεσμα τα οφέλη μπορεί να είναι σημαντικά. Εάν για την ενσύρματη υλοποίηση χρειάζεται η καταβολή τελών (λ.χ. μίσθωση γραμμής από ΟΤΕ), στο ασύρματο δίκτυο δεν έχουμε τέτοια έξοδα, ενώ σημαντικά είναι και τα οφέλη από τις μεταβολές που γίνονται στο δίκτυο, οι οποίες στην περίπτωση του ασύρματου γίνονται εύκολα και ανέξοδα.

• Δυνατότητα προσαρμογής στις ανάγκες. Το ασύρματο δίκτυο μπορεί να υλοποιηθεί με μία σειρά τοπολογίες, ικανοποιώντας τις ανάγκες τόσο μικρών όσο και πολυπληθών ομάδων χρηστών ακόμα και μερικών χιλιάδων.

1.5 Εφαρμογές

Ανάλογα με τους χώρους στους οποίους μπορούμε να δούμε οφέλη από τη χρήση των WLAN συμπεριλαμβάνονται και οι παρακάτω:

Επιχειρήσεις: Με ένα WLAN οι εργαζόμενοι μπορούν να εκμεταλλευθούν το κινητό δίκτυο για e-mail, πρόσβαση σε αρχεία και αναζήτηση στο Internet, ανεξάρτητα από την περιοχή που βρίσκεται το γραφείο, αλλά και από το αν βρίσκονται στο γραφείο ή όχι.

Εκπαίδευση: Με τη χρήση WLAN από τα ακαδημαϊκά ινστιτούτα οι φοιτητές μπορούν να έχουν πρόσβαση μέσω laptops στο πανεπιστημιακό δίκτυο ενώ γίνεται πιο προσιτή και εφαρμόσιμη η τηλε-εκπαίδευση.

Υγεία: Με τη χρήση ασύρματων φορητών υπολογιστών για την επεξεργασία σε πραγματικό χρόνο, οι εργαζόμενοι στον τομέα υγείας αυξάνουν την παραγωγικότητά τους και την ποιότητα φροντίδας των ασθενών, καθώς εξαλείφονται προβλήματα όπως οι καθυστερήσεις και η γραφειοκρατία.

Επενδύσεις: Με ένα φορητό υπολογιστή ο οποίος συνδέεται με ένα ασύρματο τοπικό δίκτυο, οι επενδυτές μπορούν να δεχθούν πληροφορίες για τις τιμές απο μια βάση δεδομένων σε πραγματικό χρόνο, βελτιώνοντας έτσι την ταχύτητα και την ποιότητα των συναλλαγών.

1.6 Ασφάλεια

. Η λειτουργία ενός ασύρματου δικτύου αντιστοιχεί στα χαμηλότερα επίπεδα της αρχιτεκτονικής ενός δικτύου και δεν εμπεριέχει άλλες λειτουργίες όπως εγκατάσταση σύνδεσης από άκρο σε άκρο ή άλλες υπηρεσίες (π.χ. login) που προσφέρουν τα ανώτερα στρώματα. Για τον λόγο αυτό το μόνο θέμα που σχετίζεται με την ασφάλεια και απασχολεί τα ασύρματα δίκτυα έχει να κάνει με θέματα ασφαλείας των χαμηλότερων στρωμάτων, όπως η κρυπτογράφηση (encryption) των δεδομένων.

Για τον λόγο αυτό, έχουν υλοποιηθεί διάφορες τεχνικές κωδικοποίησης οι οποίες καθιστούν εξαιρετικά δύσκολη την λήψη της μεταδιδόμενης πληροφορίας από κάποιον χρήστη πέραν του προοριζόμενου.

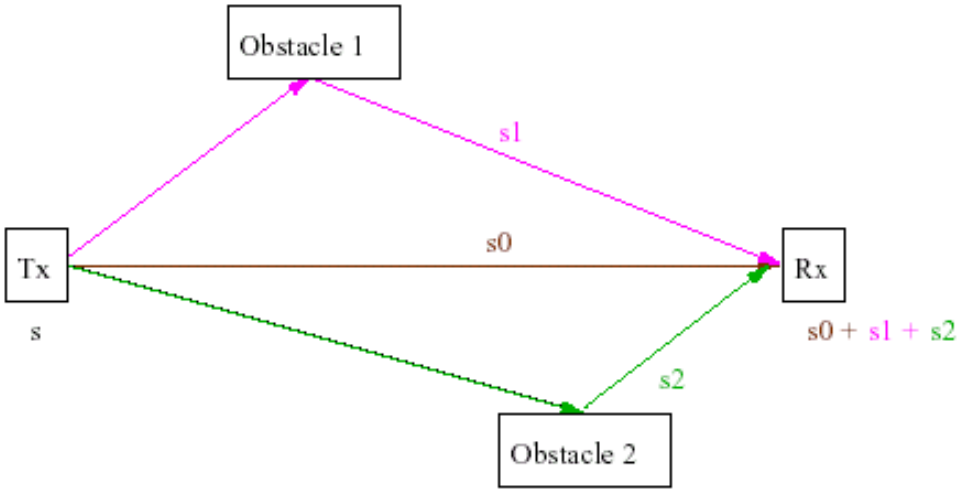
Τέτοιες τεχνικές είναι οι τεχνικές εξάπλωσης φάσματος (spread spectrum) που θα αναφερθούν με λεπτομέρεια σε επόμενο κεφάλαιο, ενώ εάν ο χρήστης απαιτεί περισσότερη ασφάλεια κατά τη μετάδοση των δεδομένων, το IEEE 802.11 Standard (το πιο διαδεδομένο ίσως πρωτόκολλο για WLAN στην περιοχή των 2.4 GHz), καθορίζει τη χρήση της κωδικοποίησης WEP (Wired Equivalent Privacy). Η κωδικοποίηση αυτή χρησιμοποιεί τον αλγόριθμο 'RSA Data Security Inc. RC4 encryption' για την κρυπτογράφηση των εκπεμπόμενων σημάτων.

1.7 Προβλήματα

Η χρήση των ηλεκτρομαγνητικών κυμάτων (ραδιοκυμάτων και υπέρυθρης ακτινοβολίας) για την μετάδοση των σημάτων κάνουν τα WLAN ευπαθή σε πολλά φαινόμενα παρεμβολής (interference) τα οποία αλλοιώνουν σε μικρότερο ή μεγαλύτερο βαθμό την επικοινωνία των ασύρματων χρηστών. Τα κυριότερα από αυτά τα προβλήματα αναφέρονται στη συνέχεια

1.7.1 Παρεμβολή λόγω πολλαπλών διαδρομών

Όπως φαίνεται και στο επόμενο σχήμα (Σχήμα 1.3) τα μεταδιδόμενα σήματα μπορούν να συνδυαστούν με τα ανακλώμενα από διάφορες επιφάνειες ή εμπόδια με αποτέλεσμα την φθορά ή καταστροφή του σήματος που ανιχνεύεται από τον δέκτη. Το φαινόμενο αυτό είναι γνωστό ως 'παρεμβολή λόγω πολλαπλών διαδρομών' ή 'πολύοδη διάδοση' (multipath propagation). Ο συνολικός χρόνος καθυστέρησης μεταξύ των ανακλώμενων σημάτων σε σχέση με το αρχικό σήμα (primary signal) αναφέρεται ως delay spread.



Σχήμα 1.3

Οι κατασκευαστές συσκευών για ασύρματα τοπικά δίκτυα ασχολούνται συνεχώς με την επεξεργασία διαφόρων τεχνικών για τον περιορισμό των προβλημάτων που προέρχονται από το συγκεκριμένο φαινόμενο, ενώ ανάμεσα στια άλλες μεθόδους που χρησιμοποιούνται είναι και οι equalization και antenna diversity.

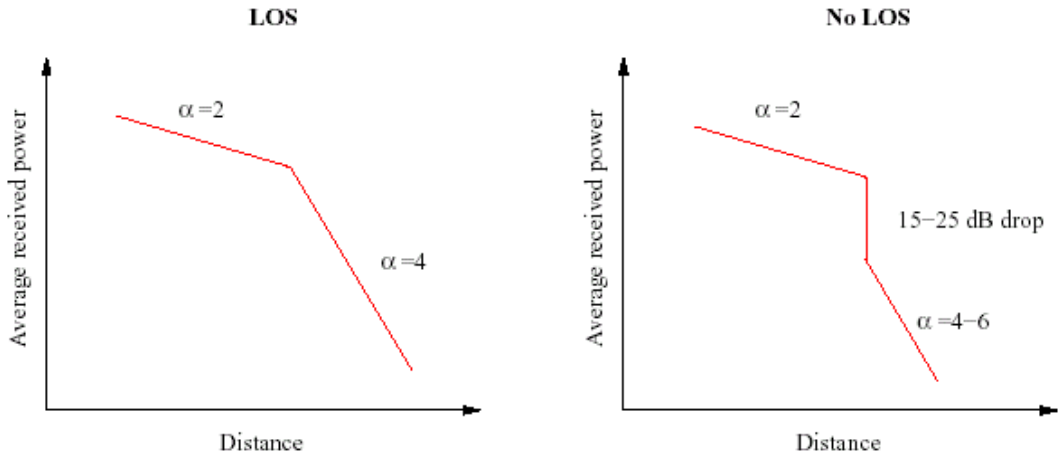
*1.7.2 **Path loss***

Το φαινόμενο του 'path loss' μεταξύ πομπού και δέκτη είναι ένα από τα σημαντικότερα στοιχεία που πρέπει να ληφθούν υπόψη κατά τον σχεδιασμό ενός WLAN.

Τα αναμενόμενα επίπεδα του path loss, τα οποία βασίζονται στην απόσταση μεταξύ του πομπού και του δέκτη, παρέχουν πολύτιμες πληροφορίες για τον καθορισμό των επιπέδων στην ισχύ της εκπομπής, στην ευαισθησία του δέκτη και στον λόγο σήματος προς θόρυβο (SNR). Το πραγματικό path loss εξαρτάται από τη συχνότητα μετάδοσης και αυξάνει εκθετικά με την αύξηση της απόστασης μεταξύ του πομπού και του δέκτη. Για τυπικές εφαρμογές σε κλειστούς χώρους, το path loss αυξάνεται περίπου 20 dB ανά 100 πόδια.

Το path loss ισοδυναμεί, ουσιαστικά, με τον λόγο της ισχύος του δέκτη προς την ισχύ του πομπού. Για μία δεδομένη ισχύ μετάδοσης (από τον πομπό), ένα μοντέλο μπορεί να χρησιμοποιηθεί για την πρόβλεψη του επιπέδου της ισχύος στον δέκτη. Το πιο απλό μοντέλο που χρησιμοποιείται, συνήθως, είναι αυτό που στηρίζεται στην εξής εκθετική σχέση: Η ισχύς του λαμβανόμενου σήματος είναι ανάλογη με την ισχύ του μεταδιδόμενου σήματος και αντιστρόφως ανάλογη με το τετράγωνο της συχνότητας μετάδοσης και την απόσταση πομπού-δέκτη υψωμένη στην δύναμη ενός παράγοντα α, ο οποίος κυμαίνεται ανάμεσα στις τιμές 2 (για ελεύθερους χώρους) και 8 (για χώρους με πολλά εμπόδια).

Οι απώλειες από το φαινόμενο αυτό εξαρτώνται άμεσα από την ύπαρξη ή μη οπτικής επαφής (LOS: Line Of Sight) ανάμεσα στον πομπό και στον δέκτη και αποδίδονται παραστατικά στο επόμενο σχήμα.(Σχήμα 1.4)



Σχήμα 1.4

1.7.3 Παρεμβολές ραδιοσημάτων

Η διαδικασία της εκπομπής και λήψης ραδιοσημάτων και σημάτων laser μέσω του αέρα καθιστά τα ασύρματα συστήματα ευπαθή από τον θόρυβο της ατμόσφαιρας και από τις μεταδόσεις άλλων συστημάτων που λειτουργούν στην ίδια μπάντα συχνοτήτων και λειτουργούν στον ίδιο φυσικό χώρο. Οι παρεμβολές από ραδιοσήματα (Radio Signal Interfernece) χωρίζονται σε:

Εσωτερικές (inward): Οι παρεμβολές αυτές προέρχονται από τις μεταδόσεις συστημάτων που χρησιμοποιούν τις ίδιες συχνότητες με αυτές ενός WLAN με το οποίο βρίσκονται στην ίδια περιοχή. Για παράδειγμα, πολλές συσκευές WLAN λειτουργούν στην περιοχή των 2.4 GHz, στην οποία λειτουργούν και οι φούρνοι μικροκυμάτων με αποτέλεσμα η μία συσκευή να παρεμβάλλεται στην άλλη, γεγονός που οδηγεί σε καθυστερήσεις και σφάλματα στην μετάδοση.

Εξωτερικές (outward): Οι παρεμβολές αυτού του είδους προκύπτουν όταν το σήμα ενός ασύρματου δικτύου διακόπτει την μετάδοση ενός άλλου γειτονικού ασύρματου συστήματος, όπως είναι ένα WLAN. Οι παρεμβολές αυτές είναι σπάνιες καθώς τα προιόντα των WLAN λειτουργούν, συνήθως, με ιδιαίτερα χαμηλή ισχύ (της τάξεως των μερικών mW).

Ένα μέρος των παρεμβολών προκύπτει, ακριβώς, από το γεγονός ότι τα προϊόντα που αποτελούν ένα WLAN λειτουργούν σε συχνότητες που δεν απαιτούν άδεια από τον FCC. Η αποφυγή και η μείωση τέτοιων παρεμβολών εναπόκειται στους κατασκευαστές των ασύρματων προϊόντων.

1.7.4 *Ασυμβατότητα συστημάτων*

Στην κατασκευή ενός WLAN θα πρέπει να ληφθεί υπόψη η ασυμβατότητα (interoperability) μεταξύ προϊόντων διαφορετικών κατασκευαστών, διαφορετικά το δίκτυο δε θα λειτουργεί σωστά. Οι λόγοι ασυμβατότητας είναι οι εξής:

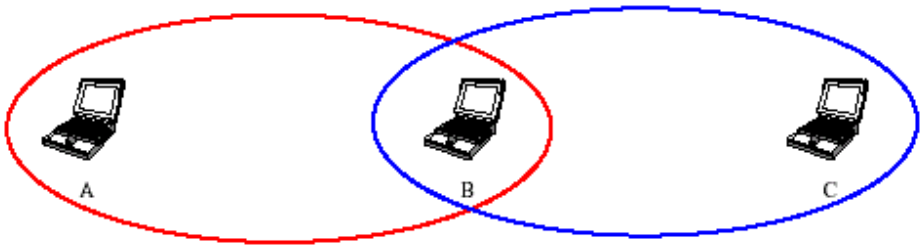
Διαφορετική τεχνολογία: Ένα σύστημα που χρησιμοποιεί την τεχνολογία διαμόρφωσης Frequency Hopping Spread Spectrum (FHSS) δε θα επικοινωνεί με ένα άλλο που βασίζεται στην τεχνολογία διαμόρφωσης Direct Sequence Spread Spectrum (DSSS).

Χρήση διαφορετικού φάσματος συχνοτήτων: Η επικοινωνία μεταξύ συσκευών που λειτουργούν σε διαφορετικές συχνότητες δεν είναι δυνατή ακόμα και αν χρησιμοποιείται η ίδια τεχνολογία.

Διαφορετική υλοποίηση: Ακόμα και να χρησιμοποιείται η ίδια τεχνολογία και το ίδιο φάσμα συχνοτήτων μπορεί να μην είναι δυνατή η επικοινωνία λόγω διαφορετικών παραμέτρων υλοποίησης από κάθε κατασκευαστή.

1.7.5 Το πρόβλημα του κρυμμένου κόμβου

Ένας συνηθισμένος περιορισμός στην απόδοση των WLAN είναι το πρόβλημα που προκύπτει από την περιορισμένη ακτίνα δράσης των ραδιοκυμάτων και είναι γνωστό ως ‘hidden node problem’. Το φαινόμενο αυτό προκύπτει όταν στο σύστημα υπάρχει ένας σταθμός που δεν μπορεί να ανιχνεύσει την μετάδοση ενός άλλου σταθμού ώστε να αναγνωρίσει ότι το μέσο χρησιμοποιείται. Στο επόμενο σχήμα (Σχήμα 1.5), ο σταθμός A θέλει να μεταδώσει στον σταθμό B, όμως δεν μπορεί να ανιχνεύσει ότι και ο σταθμός C θέλει να μεταδώσει, με αποτέλεσμα να προκύψει σύγκρουση.[1]



Σχήμα 1.5

Κεφάλαιο 2: Το πρότυπο 802.11 της IEEE για τα ασύρματα δίκτυα

2.1 Εισαγωγή

Στη σύγχρονη εποχή, η αγορά των ασύρματων δικτύων παρουσιάζει μεγάλη ανάπτυξη. Η ασύρματη τεχνολογία έχει προσεγγίσει, ή τουλάχιστον είναι ικανή να προσεγγίσει, σχεδόν κάθε τοποθεσία στην επιφάνεια της γης. Εκατομμύρια άνθρωποι επικοινωνούν καθημερινά χρησιμοποιώντας κινητά τηλέφωνα, τηλε-ειδοποιητές (pagers) και άλλα προϊόντα ασύρματης τεχνολογίας. Με την τεράστια επιτυχία που γνώρισαν οι ασύρματες τηλεπικοινωνίες και οι υπηρεσίες αποστολής και λήψης γραπτών μηνυμάτων, δεν είναι καθόλου παράξενο το γεγονός ότι η ασύρματη τεχνολογία έχει αρχίσει να εφαρμόζεται στον ιδιωτικό και στον επιχειρησιακό τομέα ολοένα και περισσότερο.

Έτσι λοιπόν, καθώς τα προϊόντα ασύρματης δικτύωσης κατακλύζουν όλο και περισσότερο την αγορά και καθώς ο αριθμός των υλοποιήσεων ασύρματων δικτύων μεγαλώνει συνεχώς, είναι απαραίτητη η ύπαρξη ενός ή περισσοτέρων αποδεκτών μηχανισμών και προτύπων (standards), τα οποία θα προσδιορίζουν λύσεις με τις οποίες θα αντιμετωπίζονται τα διάφορα προβλήματα που διέπουν τα ασύρματα δίκτυα. Σε αυτά περιλαμβάνονται ο καθορισμός της τοπολογίας ενός ασύρματου τοπικού δικτύου, πρωτόκολλα διαμοιρασμού ενός κοινού μέσου μετάδοσης (Medium Access Control - MAC issues), θέματα ελέγχου και ασφάλειας των χρηστών, κ.α.

Το πρότυπο 802.11 της IEEE για τα ασύρματα δίκτυα αποτελεί ένα τέτοιο μηχανισμό. Το τμήμα αυτό εισάγει τον αναγνώστη στις βασικές έννοιες και αρχές λειτουργίας του προτύπου 802.11. Το πρότυπο 802.11 περιορίζεται στα δύο πρώτα επίπεδα του δικτυακού μοντέλου αναφοράς OSI, ήτοι, στο φυσικό επίπεδο (ΦΕ) και στο επίπεδο σύνδεσης δεδομένων (ΕΣΔ). Για την ακρίβεια, δεν καλύπτει ολόκληρο το ΕΣΔ, αλλά το *πρώτο μισό* του, δηλαδή το *υπο-επίπεδο πρόσβασης στο μέσο* (MAC Layer).

2.2 Το φυσικό επίπεδο

Το πρότυπο 802.11 ορίζει τρία διαφορετικά φυσικά επίπεδα. Η ύπαρξη περισσότερων από ένα επιλογών για το φυσικό επίπεδο επιτρέπει στους σχεδιαστές συστημάτων να επιλέγουν κάθε φορά την τεχνολογία εκείνη, η οποία ταιριάζει καλύτερα με το κόστος, την απόδοση και το προφίλ των λειτουργιών μιας συγκεκριμένης εφαρμογής.Ειδικότερα, το πρότυπο προσδιορίζει ένα οπτικό ΦΕ που χρησιμοποιεί υπέρυθρες ακτίνες για τη μετάδοση δεδομένων και δύο ΦΕ ραδιοσυχνότητας (RF-based), τα οποία λειτουργούν στην περιοχή συχνοτήτων των 2,4 GHz (από 2,4 - 2,4835 GHz) του ISM.

Στο σχήμα 2.1 απεικονίζονται τα επίπεδα που καλύπτονται από το πρότυπο.

<table>
<tr><td colspan="2">802.2</td><td colspan="2">Υπο-επίπεδο Ελέγχου Λογικών Καναλιών (LLC sublayer)</td><td rowspan="2">Επίπεδο Σύνδεσης Δεδομένων</td></tr>
<tr><td colspan="2">802.11</td><td colspan="2">Υπο-επίπεδο Προσπέλασης Μέσου (MAC sublayer)</td></tr>
<tr><td>Υπέρυθρο ΦΕ</td><td>Direct Sequence ΦΕ</td><td>FH (Frequency Hop) ΦΕ</td><td>Φυσικό Επίπεδο</td></tr>
</table>

Σχήμα 2.1

Οι δύο διαφορετικές τεχνολογίες ΦΕ ραδιοσυχνότητας που απεικονίζονται στο παραπάνω σχήμα, ανήκουν στην κατηγορία των τεχνικών *διασποράς φάσματος (spread spectrum techniques)* οι οποίες όμως δεν καλύπτονται εδώ. Αναφορικά μόνο, οι τεχνολογίες διασποράς φάσματος που προσδιορίζει το 802.11 για τα δύο ΦΕ ραδιοσυχνότητας είναι η *τεχνική διασποράς φάσματος άμεσης ακολουθίας (Direct Sequence Spread Spectrum - DSSS)* και η *τεχνική διασποράς φάσματος αναπήδησης συχνότητας (Frequency Hopping Spread Spectrum - FHSS)*

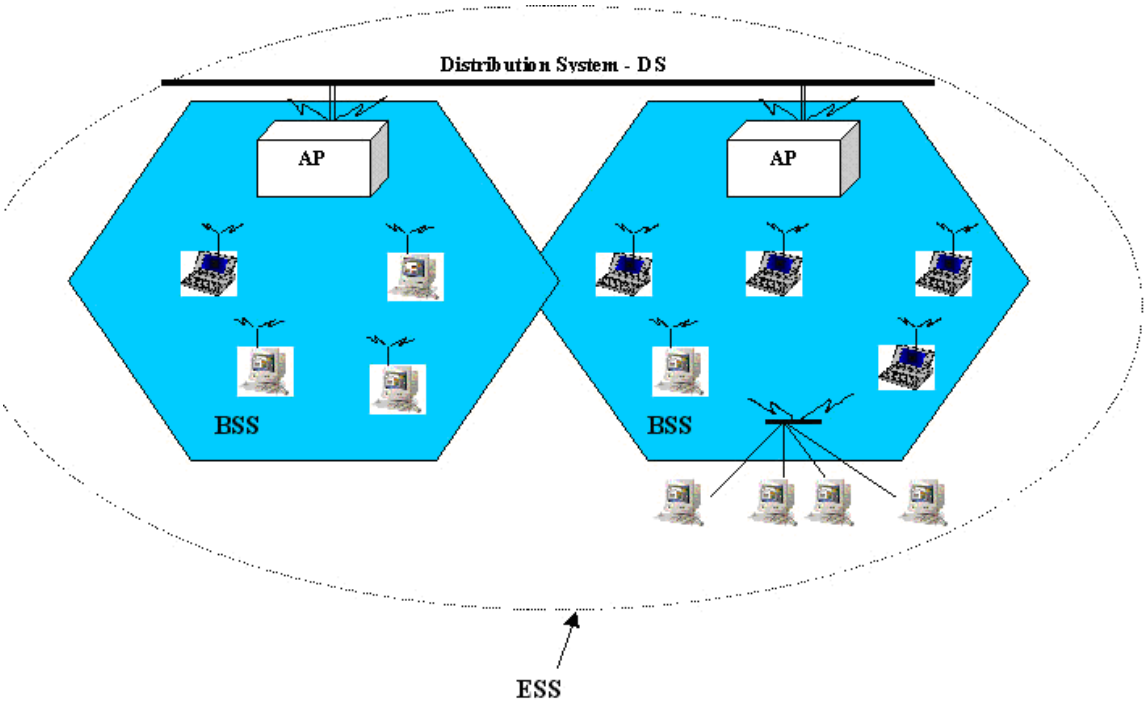
Το μικρό εύρος κάλυψης που έχει το υπέρυθρο ΦΕ το καθιστά κατάλληλο μόνο για εφαρμογές κλειστού χώρου, όπως ένα μικρό γραφείο, ένα δωμάτιο, κλπ. Αντίθετα, οι άλλοι δύο τύποι ΦΕ μπορούν να χρησιμοποιηθούν σε εφαρμογές όπου υπάρχει η ανάγκη

κάλυψης μεγάλων περιοχών (ανοικτών ή κλειστών), όπως είναι μια πανεπιστημιούπολη, τα κτίρια μιας επιχείρησης, κλπ.

2.3 Αρχιτεκτονική του πρότυπου IEEE 802.11

Ένα ασύρματο δίκτυο 802.11 βασίζεται σε μια κυψελοειδής αρχιτεκτονική, σύμφωνα με την οποία, ολόκληρο το σύστημα διαιρείται σε περιοχές ή *κελιά* με το κάθε κελί να ελέγχεται από ένα *Σταθμό - Βάσης (Base Station)*. Στην ορολογία του 802.11 ένα κελί ονομάζεται *Βασικό Σύνολο Υπηρεσιών (Basic Service Set - BSS)* και ο σταθμός βάσης, *Σημείο Πρόσβασης (Access Point - AP)*. Παρόλο που ένα δίκτυο μπορεί να αποτελείται από ένα μόνο κελί, οι περισσότερες δικτυακές εγκαταστάσεις 802.11 συνήθως αποτελούνται από πολλά κελιά με τα σημεία πρόσβασης να βρίσκονται συνδεδεμένα σε μια ραχοκοκαλιά, η οποία ονομάζεται *Σύστημα Διανομής (Distribution System - DS)* και η οποία μπορεί να είναι είτε ένα ενσύρματο (π.χ.Ethernet), είτε ένα ασύρματο δίκτυο.

Το σύνολο όλων των δια-συνδεδεμένων ασύρματων δικτύων, μαζί με τα σημεία πρόσβασης και το σύστημα διανομής, ονομάζεται *Εκτεταμένο Σύνολο Υπηρεσιών (Extended Service Set - ESS)* και όσον αφορά τα ανώτερα επίπεδα του δικτυακού μοντέλου αναφοράς OSI, σύμφωνα με το πρότυπο, θα πρέπει να θεωρείται ως ένα **ενιαίο** τοπικό δίκτυο κατηγορίας 802. Στο σχήμα 2.2 απεικονίζεται η αρχιτεκτονική ενός δικτύου 802.11.



Σχήμα2.2

Το πρότυπο ορίζει επίσης και την έννοια της *πύλης (Portal)*. Η *πύλη* είναι μια συσκευή που χρησιμοποιείται για τη δια-σύνδεση ενός δικτύου 802.11 με ένα άλλο δίκτυο κατηγορίας IEEE 802.11. Η λειτουργία της μπορεί να παρομοιαστεί με τη λειτουργία ενός *δρομολογητή (router),* ο οποίος είναι ικανός να δια-συνδέει διαφορετικά δίκτυα. Η λειτουργικότητα μιας *πύλης* μπορεί να βρίσκεται είτε σε ξεχωριστή συσκευή, είτε να είναι ενσωματωμένη με το σημείο πρόσβασης.

2.4 Το επίπεδο σύνδεσης δεδομένων

Σε ένα δίκτυο 802.11, το υπο-επίπεδο προσπέλασης μέσου (MAC layer), είναι υπεύθυνο για την εκτέλεση των παρακάτω λειτουργιών.

- Για τον έλεγχο της πρόσβασης των σταθμών στο κοινό μέσο μετάδοσης
- Για τη λειτουργία του *κατακερματισμού και της επανασυναρμολόγησης (fragmentation and reassembly)*
- Για τη λειτουργία της *αναμετάδοσης πακέτου (packet retransmission)*
- Για τη λειτουργία της *επιβεβαίωσης λήψης (acknowledges)*.

2.5 Έλεγχος της πρόσβασης στο κοινό μέσο

Η τεχνική που χρησιμοποιείται από το ΕΣΔ στο 802.11 είναι **παρόμοια** με μια από τις βασικότερες μεθόδους ελέγχου πρόσβασης στο μέσο, την *Μέθοδο πολλαπλής πρόσβασης με ανίχνευση φέροντος σήματος και αποφυγή συγκρούσεων (Carrier Sense Multiple Access with Collision Avoidance - CSMA/CA.*

Σύμφωνα με τη μέθοδο αυτή, ένας σταθμός ο οποίος θέλει να μεταδώσει «αφουγκράζεται» πρώτα το μέσο μετάδοσης, για να διαπιστώσει εάν είναι κατειλημμένο. Εάν είναι, τότε δε μεταδίδει, περιμένει ένα τυχαίο χρονικό διάστημα και προσπαθεί ξανά. Εάν είναι ελεύθερο, τότε στέλνει **πρώτα** ένα ειδικό σήμα για να προειδοποιήσει ότι **πρόκειται** να μεταδώσει και στη συνέχεια, αν δε συμβεί καμιά σύγκρουση, στέλνει τα δεδομένα του. Με τον τρόπο αυτό οι υπολογιστές αντιλαμβάνονται πότε υπάρχει πιθανότητα σύγκρουσης, κάτι που τους επιτρέπει να **αποφεύγουν** τις συγκρούσεις μετάδοσης (εξού και η ονομασία της μεθόδου). Ωστόσο, η αποστολή του ειδικού σήματος μετάδοσης, αυξάνει την κίνηση, υποβαθμίζοντας την απόδοση ολόκληρου του δικτύου.

Παρόλο που αυτοί οι μηχανισμοί είναι αρκετά αποδοτικοί στα παραδοσιακά ενσύρματα δίκτυα, αυτό δε θα μπορούσαμε να πούμε ότι ισχύει και στα ασύρματα δίκτυα, για τους παρακάτω λόγους:

- Η υλοποίηση ενός μηχανισμού ανίχνευσης συγκρούσεων θα απαιτούσε την υλοποίηση ενός *αμφίδρομου πομποδέκτη*, που θα μπορούσε να στέλνει και να λαμβάνει δεδομένα ταυτόχρονα, κάτι που θα αύξανε κατά πολύ το κόστος υλοποίησης.
- Σε ένα ασύρματο δίκτυο δε θα ήταν σωστό να υποθέσουμε ότι **όλοι** οι σταθμοί μπορούν να «ακούσουν» όλους τους υπόλοιπους, μια πολύ βασική υπόθεση στις μεθόδους πρόσβασης με ανίχνευση φέροντος. Ακόμη και αν κάποιος σταθμός που επιθυμεί να μεταδώσει ανιχνεύσει το κανάλι ελεύθερο, αυτό δε σημαίνει απαραίτητα ότι αυτό είναι ελεύθερο γύρω από την περιοχή του δέκτη (αυτό το επιχείρημα αναλύεται αναλυτικότερα παρακάτω, στο τμήμα *Δέσμευση του καναλιού*).

Λόγω των παραπάνω προβλημάτων, το πρότυπο 802.11 χρησιμοποιεί μια μέθοδο αποφυγής συγκρούσεων (Collision Avoidance mechanism), παράλληλα με ένα σύστημα *θετικής επιβεβαίωσης λήψης (Positive Acknowledgement Scheme)*, που περιγράφεται παρακάτω.

2.5.1 Ανίχνευση των Συγκρούσεων (collision detection)

Ένας σταθμός ο οποίος επιθυμεί να μεταδώσει, ελέγχει αρχικά το μέσο (τον αέρα στην περίπτωσή μας). Αν είναι κατειλημμένο, τότε αναβάλει τη μετάδοση για αργότερα. Αν είναι ελεύθερο, τότε περιμένει να δει αν θα **παραμείνει** ελεύθερο για ένα συγκεκριμένο χρονικό διάστημα, το οποίο ονομάζεται **DIFS (Distributed Inter Frame Space - βλέπε παρακάτω)** και στη συνέχεια μεταδίδει το πακέτο που περιέχει τα δεδομένα. Ο δέκτης από την άλλη, λαμβάνοντας το πακέτο ελέγχει να δει εάν αυτό περιέχει τυχόν λάθη και αν όχι τότε στέλνει πίσω στον πομπό μια επιβεβαίωση λήψης (Acknowledgement - ACK).

Παραλαβή της επιβεβαίωσης λήψης από τον πομπό σημαίνει ότι το πακέτο παραδόθηκε στον προορισμό του χωρίς να συγκρουστεί με κάποιο άλλο. Αν ο αποστολέας δεν παραλάβει μια επιβεβαίωση, τότε θεωρεί ότι συνέβη μια σύγκρουση και επαναλαμβάνει τη μετάδοση του πακέτου, μέχρις ότου είτε λάβει την επιβεβαίωση, είτε ακυρώσει τη μετάδοση μετά από έναν αριθμό προσπαθειών.

2.5.2 Δέσμευση του καναλιού

Μέχρις αυτό το σημείο δε μιλήσαμε ακόμη για τον τρόπο με τον οποίο μπορεί ένας σταθμός να σιγουρευτεί ότι **όντως** το μέσο μετάδοσης είναι ελεύθερο προτού μεταδώσει. Το πρότυπο 802.11 προσδιορίζει ένα μηχανισμό *εικονικής ανίχνευσης φέροντος (virtual carrier sense mechanism)*, με τον οποίο εξασφαλίζεται ότι **όλοι** οι σταθμοί που μοιράζονται το ίδιο μέσο θα γνωρίζουν ότι κάποιος σταθμός μεταδίδει ακόμη και αν αυτοί είναι «κρυμμένοι».

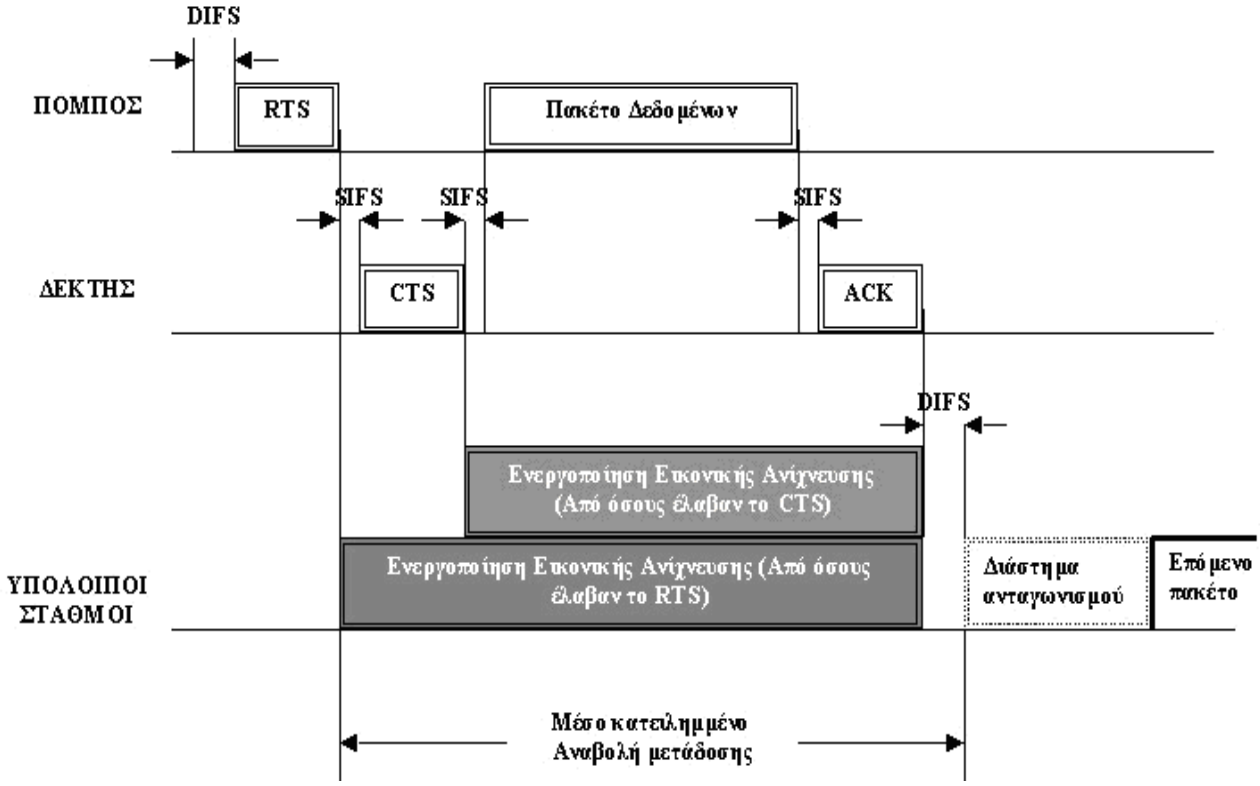
Για να κατανοήσουμε καλύτερα την παραπάνω έννοια, ας φανταστούμε την ακόλουθη περίπτωση. Θεωρείστε ότι έχουμε ένα ασύρματο δίκτυο που έχει μια αρχιτεκτονική παρόμοια με αυτή του σχήματος 8. Έστω ότι υπάρχουν τρεις σταθμοί στο κάθε κελί, ο Α, ο Β και ο Γ. Ο Α και ο Β έστω ότι αποτελούν απλούς σταθμούς, ενώ ο Γ αποτελεί ένα *σημείο πρόσβασης (AP)*. Φανταστείτε το ακόλουθο σενάριο: ο Α μπορεί να επικοινωνήσει με τον Γ, ο Β μπορεί να επικοινωνήσει με τον Γ, αλλά ο Α δε μπορεί να επικοινωνήσει απευθείας με τον Β, γιατί απέχουν τέτοια απόσταση ο ένας από τον άλλο που δεν είναι δυνατή η άμεση επικοινωνία (το σήμα δε μπορεί να διαδοθεί από τον Α στον Β). Οπότε, αν σε μια δεδομένη χρονική στιγμή και ο Α και ο Β θέλουν να μεταδώσουν, θα ανιχνεύσουν και οι δύο το μέσο ελεύθερο, αφού ο ένας δε μπορεί να «ακούσει» τον άλλο. Στη συγκεκριμένη περίπτωση θα υπάρξει σύγκρουση στην *περιοχή του δέκτη,* γιατί μπορεί ο Α να μη μπορεί να επικοινωνήσει με τον Β, αλλά και οι δύο είναι σε θέση να επικοινωνήσουν με το σημείο πρόσβασης, το Γ. Στην περίπτωση αυτή λέμε ότι ο σταθμός Β είναι «κρυμμένος» από το σταθμό Α και αντίστροφα.

Ο μηχανισμός εικονικής ανίχνευσης φέροντος λειτουργεί ως εξής: ένας σταθμός που επιθυμεί να μεταδώσει και έχει ανιχνεύσει το μέσο ελεύθερο (τουλάχιστον στην περιοχή γύρω από αυτόν), στέλνει πρώτα ένα μικρό πακέτο που ονομάζεται **RTS (Request To Send - Αίτηση για αποστολή)** και το οποίο περιέχει τη **διεύθυνση αποστολής**, τη **διεύθυνση προορισμού** και το **χρονικό διάστημα της όλης διαδικασίας** (το χρόνο δηλαδή που απαιτείται για την αποστολή του πακέτου δεδομένων και της λήψης της

επιβεβαίωσης από το δέκτη). Στη συνέχεια, ο δέκτης ελέγχει εάν το μέσο είναι **όντως** ελεύθερο (και στη δική του περιοχή δηλαδή) και αν είναι, τότε αποστέλλει ένα άλλο πακέτο μικρού μεγέθους που ονομάζεται **CTS (Clear To Send - Αποστολή Δεκτή)** το οποίο περιέχει τις ίδιες πληροφορίες με το πακέτο RTS. Σε αντίθετη περίπτωση δεν αποστέλλει τίποτε.

Όλοι οι σταθμοί που λαμβάνουν το RTS ή / και το CTS, ενεργοποιούν έναν ειδικό δείκτη που ονομάζεται *δείκτης εικονικής ανίχνευσης (virtual sense indicator),* ο οποίος καλείται **NAV - από το Network Allocation Vector.** Η ενεργοποίηση διαρκεί για το χρονικό διάστημα που αναφέρεται στο CTS (ή το RTS) και χρησιμοποιείται παράλληλα με την *φυσική ανίχνευση φέροντος* από τους σταθμούς όταν αυτοί ανιχνεύουν το καλώδιο.

Η μέθοδος αυτή μειώνει κατά πολύ την πιθανότητα συγκρούσεων στην περιοχή του δέκτη, γιατί ακόμη και οι «κρυμμένοι» από τον πομπό σταθμοί (που δε μπορούν να λάβουν το RTS δηλαδή) θα λάβουν σίγουρα το πακέτο CTS και θα θεωρήσουν το μέσο κατειλημμένο για το χρονικό διάστημα που αναφέρεται σ' αυτό. Επίσης, η αποστολή του πακέτου RTS προφυλάσσει τον **δέκτη** από συγκρούσεις στην **περιοχή του πομπού** κατά τη διάρκεια αποστολής της επιβεβαίωσης λήψης (ACK), γιατί το RTS θα ληφθεί σίγουρα από όλους τους σταθμούς που είναι «κρυμμένοι» από το δέκτη. Στο παρακάτω σχήμα δίδεται ένα χρονοδιάγραμμα των ενεργειών που λαμβάνουν χώρα κατά τη διάρκεια της επικοινωνίας μεταξύ δύο σταθμών.



Σχήμα 2.3

Στο παραπάνω σχήμα (Σχήμα 2.3) μπορούμε να διακρίνουμε και τα διάφορα χρονικά διαστήματα που μεσολαβούν πριν και μετά τις μεταδόσεις των πλαισίων. Οι χρόνοι αυτοί, κατά λέξη, ονομάζονται *δια-πλαισιακά διαστήματα (Inter-Frame Spaces - IFS)* και ανήκουν σε διάφορες κατηγορίες:

- **Short IFS - SIFS (Δια-πλαισιακό διάστημα μικρής διάρκειας):** Ο χρόνος αυτός χρησιμοποιείται για το διαχωρισμό των μεταδόσεων που ανήκουν σε ένα διάλογο μεταξύ δύο σταθμών (π.χ. πακέτο δεδομένων και ACK) και αποτελεί το μικρότερο από τους δια-πλαισιακούς χρόνους. Έχει σταθερή τιμή, η οποία διαφέρει ανά ΦΕ, και υπολογίζεται με τέτοιον τρόπο, ώστε ο πομπός να έχει αρκετό χρόνο να μεταβεί σε κατάσταση λήψης, για να μπορέσει να λάβει και να αποκωδικοποιήσει το εισερχόμενο πακέτο (π.χ. ACK ή CTS) από το δέκτη. Για

παράδειγμα, για τα ΦΕ τεχνολογίας διασποράς φάσματος αναπήδησης συχνότητας, ο χρόνος αυτός ορίζεται στα 28 μsec.

- **Point Coordination IFS - PIFS (Δια-πλαισιακό διάστημα συντονισμού σημείου):** Ο χρόνος αυτός χρησιμοποιείται από τα σημεία πρόσβασης (που εδώ ονομάζονται *συντονιστές σημείου*), όταν θέλουν να προσπελάσουν το μέσο μετάδοσης **πριν** από τους άλλους σταθμούς. Η τιμή του είναι λίγο μεγαλύτερη από του SIFS, δηλαδή 78 μsec.
- **Distributed IFS - DIFS (Κατανεμημένο δια-πλαισιακό διάστημα):** Ο χρόνος αυτός είναι το **επιπλέον** χρονικό διάστημα που μεσολαβεί προτού ένας σταθμός - που έχει ανιχνεύσει το μέσο ως ελεύθερο - προβεί σε οποιαδήποτε αποστολή πακέτου. Η τιμή του ορίζεται λίγο μεγαλύτερη από του PIFS, ήτοι 128 μsec.
- **Extended IFS - EIFS (Εκτεταμένο δια-πλαισιακό διάστημα):** Το χρονικό αυτό διάστημα είναι το μεγαλύτερο από όλα και χρησιμοποιείται από ένα σταθμό ο οποίος έχει λάβει ένα πακέτο το οποίο δε μπόρεσε να αποκωδικοποιήσει, π.χ. λόγω της ύπαρξης λαθών. Ο χρόνος αυτός είναι απαραίτητος, για να εμποδίσει ένα σταθμό, ο οποίος δε μπόρεσε να αποκωδικοποιήσει π.χ. ένα πακέτο RTS ή CTS, να συγκρουστεί με πακέτα ενός διαλόγου που βρίσκεται σε εξέλιξη.

2.6 Κατακερματισμός και επανασύνδεση

Στα τοπικά δίκτυα με καλώδιο (π.χ.Ethernet) τα πακέτα έχουν μέγεθος μερικών εκατοντάδων bytes. Στο Ethernet για παράδειγμα, το μέγιστο μέγεθος πακέτου φτάνει περίπου τα 1500 bytes. Ωστόσο, σε ένα ασύρματο δίκτυο, τα μεγάλα πακέτα δεν αποτελούν πλεονέκτημα για τους εξής λόγους:

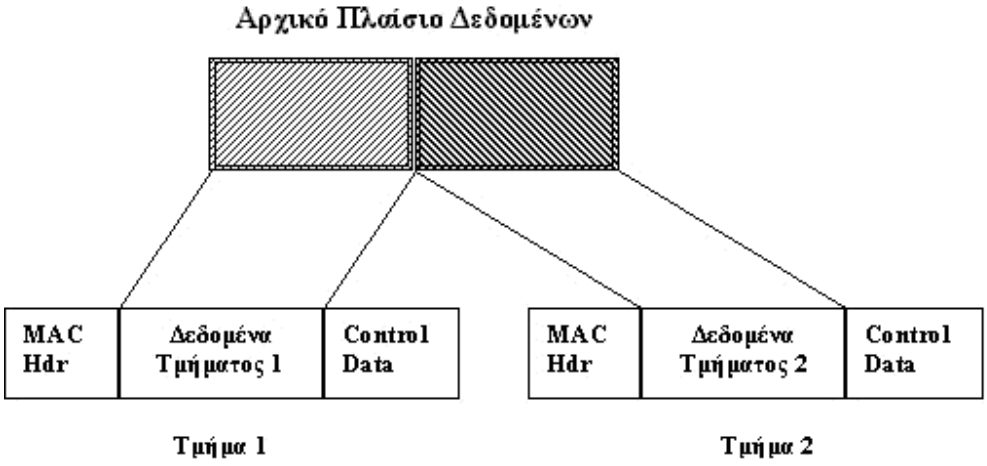
- Λόγω του υψηλότερου ρυθμού λαθών στα ασύρματα περιβάλλοντα (bit-error rate), η πιθανότητα ένα πακέτο να περιέχει λάθη αυξάνεται σύμφωνα με το μέγεθός του.

- Στην περίπτωση όπου ένα πακέτο καταστραφεί, είτε λόγω μιας σύγκρουσης, είτε λόγω εξωτερικών παρεμβολών, όσο μικρότερο είναι το μέγεθός του, τόσο μικρότερη είναι και η επιβάρυνση που απαιτείται για την αναμετάδοσή του.
- Στα συστήματα αναπήδησης συχνότητας, η συχνότητα μετάδοσης αλλάζει συνεχώς. Κατά συνέπεια, όσο μικρότερο είναι το μέγεθος ενός πακέτου, τόσο μικρότερη είναι και η πιθανότητα ότι η μετάδοσή του θα αναβληθεί για μετά την αναπήδηση.

Από την άλλη, όμως, δεν είναι λογικό να δημιουργηθεί ένα πρωτόκολλο το οποίο δε θα μπορεί να χειριστεί πακέτα μεγάλου μεγέθους (π.χ. πακέτα μεγέθους Ethernet - 1500 bytes), γιατί τότε δε θα μπορούσε να υπάρξει δια-σύνδεση των δικτύων 802.11 με τα άλλα δίκτυα της κατηγορίας 802.11 .

Η λύση που προτείνει το 802.11 είναι ένας *μηχανισμός κατακερματισμού και επανασυναρμολόγησης*, όπου τα πακέτα που είναι μεγαλύτερα σε μέγεθος από αυτό που μπορεί να δεχθεί το δίκτυο *κατακερματίζονται* σε μικρότερου - επιτρεπτού μεγέθους **τμήματα (fragments).** Ο μηχανισμός αυτός βασίζεται σε ένα μηχανισμό *μετάδοσης - και - αναμονής (Send - and - wait),* όπου ένας σταθμός αφού μεταδώσει ένα τμήμα δεν επιτρέπεται να προβεί στη μετάδοση ενός νέου τμήματος προτού, είτε λάβει την επιβεβαίωση από το δέκτη, είτε εγκαταλείψει τη μετάδοση του τμήματος μετά από έναν αριθμό προσπαθειών και ακυρώσει τη μετάδοση ολόκληρου του πλαισίου.

Στο παρακάτω σχήμα (Σχήμα 2.4) απεικονίζεται ένα πλαίσιο το οποίο έχει κατακερματιστεί σε δύο μικρότερα για να μπορέσει να μεταδοθεί σε ένα δίκτυο 802.11. Ο πομπός θα πρέπει να περιμένει να λάβει συνολικά δύο επιβεβαιώσεις, μία για το καθένα τμήμα.



Σχήμα 2.4

2.7 Εισαγωγή ενός σταθμού στο δίκτυο

Όταν ένας σταθμός θέλει να αποκτήσει πρόσβαση σε ένα BSS (είτε λόγω εκκίνησής του, είτε επειδή εισέρχεται στην περιοχή που καλύπτεται από το κελί, κλπ) το πρώτο μέλημά του είναι να συγχρονιστεί με το σημείο πρόσβασης του κελιού. Υπάρχουν δύο τρόποι να το επιτύχει αυτό.

- *Παθητική Σάρωση (passive scanning):* Στην περίπτωση αυτή ο σταθμός απλά περιμένει να λάβει ένα *πλαίσιο - φάρο (beacon frame)*, από το σημείο πρόσβασης. Το πλαίσιο - φάρος, είναι ένα πλαίσιο που μεταδίδεται περιοδικά από το σημείο πρόσβασης και περιέχει πληροφορίες συγχρονισμού. Οι σταθμοί που επιθυμούν να συγχρονιστούν με το BSS χρησιμοποιούν τις πληροφορίες που υπάρχουν στο πλαίσιο αυτό.
- *Ενεργητική σάρωση (active scanning):* Στην περίπτωση αυτή ο σταθμός προσπαθεί μόνος του να εντοπίσει ένα σημείο πρόσβασης μεταδίδοντας *πλαίσια*

αίτησης εξερεύνησης (probe request frames) και περιμένοντας να λάβει *πλαίσια απάντησης εξερεύνησης (probe response frames)* από κάποιο σημείο πρόσβασης.

***Επικύρωση χρήστη (authentication process*)**

Άπαξ και ένας σταθμός εντοπίσει και συγχρονιστεί με το σημείο πρόσβασης, προχωρά στη διαδικασία επικύρωσης, η οποία αφορά την επικοινωνία μεταξύ του σταθμού και του σημείου πρόσβασης, ώστε να διαπιστωθεί η γνώση ενός μυστικού κωδικού πρόσβασης.

Συσχέτιση χρήστη (association process)

Μετά την επικύρωση του, ο σταθμός εισέρχεται στη διαδικασία συσχέτισης, με την οποία ανταλλάσσονται πληροφορίες σχετικά με τους σταθμούς και τις δυνατότητες του BSS, και με την οποία το *σύστημα διανομής* (distribution system - DS) μπορεί να ενημερώνεται για την τρέχουσα θέση του σταθμού. Μόνο αφού ολοκληρωθεί και αυτή η διαδικασία μπορεί ο σταθμός να μεταδώσει και να λάβει πλαίσια στο δίκτυο.[3]

2.8 Περιαγωγή

Η διαδικασία της περιαγωγής (roaming), είναι η διαδικασία με την οποία μπορεί ένας σταθμός να μεταβαίνει από ένα BSS σε ένα άλλο διατηρώντας τη σύνδεση με το δίκτυο. Η περιαγωγή στα δίκτυα 802.11 είναι παρόμοια με τη *διαδικασία μετάβασης (handover)* στις κινητές τηλεπικοινωνίες με δύο διαφορές:

Σε ένα τοπικό δίκτυο 802.11, το οποίο βασίζεται στη μετάδοση πακέτων, η μετάβαση από κελί σε κελί μπορεί να πραγματοποιηθεί **μεταξύ** μεταδόσεων, καθιστώντας τη

διαδικασία της περιαγωγής ευκολότερη απ' ότι σε ένα δίκτυο κινητής τηλεφωνίας, όπου η μετάβαση μπορεί να γίνει και κατά τη διάρκεια μιας τηλεφωνικής συνδιάλεξης.

Σε ένα δίκτυο κινητής τηλεφωνίας, μια προσωρινή διακοπή της σύνδεσης δεν επηρεάζει σημαντικά την επικοινωνία, ενώ σε ένα τοπικό δίκτυο πακέτου η διακοπή της μετάδοσης ενός πλαισίου λόγω της μετάβασης σε ένα άλλο κελί, σημαίνει ότι η αναμετάδοσή του θα πρέπει να γίνει από τα ανώτερα επίπεδα, γεγονός που υποβαθμίζει σημαντικά την απόδοση του δικτύου.

Το πρότυπο 802.11 δεν προσδιορίζει κάποια συγκεκριμένη διαδικασία περιαγωγής. Το μόνο που προσδιορίζει είναι τα βασικά εργαλεία για τη λειτουργία αυτή, τα οποία περιλαμβάνουν την ενεργητική / παθητική σάρωση και μια διαδικασία ανασυσχέτισης, με την οποία ένας σταθμός ο οποίος μεταβαίνει από ένα κελί σε ένα άλλο θα μπορεί να συσχετιστεί με το καινούργιο κελί.

2.9 Θέματα ασφάλειας

Ένα από τα πρώτα θέματα που θα πρέπει να αντιμετωπίζεται από όσους υλοποιούν ένα ασύρματο δίκτυο είναι το θέμα της ασφάλειας (security). Οι μεγαλύτερες ανησυχίες που απασχολούν τους διαχειριστές ενός ασύρματου δικτύου σχετικά με τη δράση ενός εισβολέα είναι δύο: (α) η πρόσβαση στους πόρους του τοπικού δικτύου με τη χρήση παρόμοιου ασύρματου εξοπλισμού και (β) η υποκλοπή της κυκλοφορίας του δικτύου.

Η αντιμετώπιση της παράνομης πρόσβασης στο δίκτυο γίνεται, όπως έχει ήδη αναφερθεί, με τη χρήση ενός μηχανισμού επικύρωσης, όπου ο ασύρματος σταθμός για να αποκτήσει πρόσβαση στο δίκτυο θα πρέπει να αποδείξει στο σημείο πρόσβασης ότι γνωρίζει ένα μυστικό κωδικό.

Η αντιμετώπιση της υποκλοπής της κυκλοφορίας γίνεται με τη χρήση του αλγορίθμου WEP (Wired Equivalent Privacy), ο οποίος εκτελείται σε όλους τους σταθμούς και δεν είναι τίποτε άλλο από μία γεννήτρια ψευδοτυχαίων αριθμών (Pseudo Random Number Generator), η οποία αρχικοποιείται από ένα διαμοιραζόμενο μυστικό κλειδί. Για κάθε

πακέτο που μεταδίδεται από ένα σταθμό, η γεννήτρια παράγει μια ψευδοτυχαία ακολουθία bit, της οποίας το μήκος είναι ίσο με το μεγαλύτερο δυνατό μέγεθος πακέτου και η οποία χρησιμοποιείται για την κρυπτογράφηση των bits του μηνύματος. Ο δέκτης από την πλευρά του θα πρέπει να γνωρίζει το μυστικό κλειδί αρχικοποίησης, έτσι ώστε για κάθε εισερχόμενο πακέτο να μπορεί να παράγει τη σωστή ψευδοτυχαία ακολουθία για την αποκρυπτογράφησή του.

2.10 Τύποι πλαισίων

Το πρότυπο 802.11 υποστηρίζει τρεις διαφορετικούς τύπους πλαισίων:

Πλαίσια Δεδομένων: Χρησιμοποιούνται για τη μετάδοση δεδομένων

Πλαίσια Ελέγχου: Χρησιμοποιούνται για τον έλεγχο της πρόσβασης στο μέσο (πακέτα, RTS, CTS, ACK).

Πλαίσια Διαχείρισης: Χρησιμοποιούνται για τη μετάδοση πληροφοριών διαχείρισης μεταξύ των σταθμών και είναι παρόμοια με τα πλαίσια δεδομένων με τη μόνη διαφορά ότι δεν προωθούνται στα ανώτερα επίπεδα.

Η κάθε μία από τις κατηγορίες αυτές χωρίζεται σε υπο-κατηγορίες, ανάλογα με τη συγκεκριμένη λειτουργία που εκτελεί.

2.11 Δομή πλαισίων

Όλα τα πλαίσια του προτύπου 802.11 έχουν την παρακάτω γενική μορφή(Σχήμα 2.5)

Preamble	PLCP header	MAC data	CRC

Σχήμα 2.5

Τα πεδία *Preamble* και *PLCP header*, είναι δύο πεδία ελέγχου τα οποία δε θα μας απασχολήσουν εδώ. Εμείς θα ασχοληθούμε με τα πεδία *MAC data* και *CRC*. Ειδικότερα,

MAC Data: Το πεδίο αυτό περιέχει τις πληροφορίες που αποθηκεύονται σε ένα πλαίσιο MAC. Η γενική του μορφή φαίνεται παρακάτω(Σχήμα 2.6).

2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	8 bytes	6 bytes	0 - 2312 bytes	4 bytes
Frame Control	Duration / ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	CRC Check

Σχήμα 2.6

Από τα πεδία αυτά, τα πρώτα 7 αποτελούν την *επικεφαλίδα* του πλαισίου (MAC Header), τα οποία επεξηγούνται παρακάτω. Εδώ να σημειώσουμε ότι δεν περιέχονται όλα τα πεδία σε όλα τα πλαίσια. Ο τύπος και ο αριθμός των πεδίων που περιέχονται σε κάθε πλαίσιο είναι ανάλογο του τύπου του.

Frame Control (Ελεγχος Πλαισίου): Το πεδίο αυτό έχει μήκος 16 bits και χωρίζεται στα παρακάτω υπο-πεδία:

2 bits	2 bits	4 bits	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit
Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Order

Σχήμα 2.7

Protocol Version: Έχει μέγεθος 2 bits και χρησιμοποιείται για τον προσδιορισμό της έκδοσης του πρωτοκόλλου 802.11 (π.χ. 802.11, 802.11a, 802.11b, 802.11g, κλπ).

Type & Subtype: Τα δύο αυτά πεδία χρησιμοποιούνται για τον προσδιορισμό του *κύριου* και του *δευτερεύοντος τύπου* του πλαισίου. Για παράδειγμα, στο 802.11, η τιμή 00 στο πεδίο **Type** και η τιμή 1011 στο πεδίο **Subtype**, ορίζουν ότι το πλαίσιο αυτό είναι πλαίσιο *διαχείρισης (Type: management)* και ειδικότερα περιέχει πληροφορίες που σχετίζονται με την *επικύρωση* του σταθμού *(subtype: authentication)*.

ToDS: Το πεδίο αυτό έχει τιμή 1, όταν αποστέλλεται στο Σημείο Πρόσβασης με σκοπό την **προώθησή** του στο Σύστημα Διανομής (συμπεριλαμβάνεται και η περίπτωση όπου ο σταθμός προορισμού βρίσκεται μέσα στο ίδιο BSS και το AP χρησιμοποιείται απλά ως αναμεταδότης).

FromDS: Προσδιορίζει αν το πλαίσιο αυτό προήλθε από το σύστημα διανομής (1), ή όχι (0).

More Fragments: Το πεδίο αυτό χρησιμοποιείται στην περίπτωση όπου ένα πλαίσιο (frame) έχει κατακερματιστεί σε μικρότερα τμήματα (fragments). Έχει την τιμή 1, όταν ακολουθούν και άλλα τμήματα που ανήκουν στο συγκεκριμένο πλαίσιο και την τιμή 0 όταν πρόκειται για το τελευταίο τμήμα ενός πλαισίου.

Retry: Το πεδίο αυτό χρησιμοποιείται για να σηματοδοτήσει αν το πλαίσιο αυτό (ή τμήμα του) αποτελεί την **αναμετάδοση** ενός πλαισίου (ή τμήματος). Χρησιμοποιείται από το δέκτη για να μπορεί να ξεχωρίζει τα πακέτα που λαμβάνει δύο φορές (duplicates) σε περίπτωση όπου έχει χαθεί η επιβεβαίωση λήψης.

Power Management: Το πεδίο αυτό χρησιμοποιείται για τον προσδιορισμό της κατάστασης κατανάλωσης ενέργειας στην οποία θα εισέλθει ο σταθμός μετά τη μετάδοση του τρέχοντος πλαισίου (π.χ. σε κατάσταση *χαμηλής κατανάλωσης, ή αποθήκευσης ενέργειας (power saving mode),* κλπ). Αυτό το πεδίο είναι χρήσιμο, μιας και οι σταθμοί ως ασύρματοι μπορεί να λειτουργούν με μπαταρίες.

More Data: Το πεδίο αυτό έχει σχέση με τη διαχείριση της κατανάλωσης ισχύος του σταθμού (power management) και χρησιμοποιείται από το σημείο πρόσβασης.

WEP: Το πεδίο αυτό χρησιμοποιείται, για να σηματοδοτήσει ότι το κυρίως σώμα του πλαισίου έχει κρυπτογραφηθεί χρησιμοποιώντας τον αλγόριθμο Wired Equivalent Privacy.

Order: Αυτό είναι ένα εξειδικευμένο πεδίο και χρησιμοποιείται μόνο από το πρωτόκολλο της Digital Equipment Corporation, LAT.

Duration / ID: Το πεδίο αυτό έχει παραπάνω από μία έννοιες, ανάλογα με τον **τύπο** του πλαισίου (ο οποίος προσδιορίζεται από τα πεδία Type & Subtype που είδαμε παραπάνω). Στη πιο συνηθισμένη περίπτωση, η τιμή που περιέχει χρησιμοποιείται για τον υπολογισμό του NAV (Network Allocation Vector - επεξηγήθηκε παραπάνω).

Πεδία Διευθύνσεων (Address 1,2,3,4): Τα πεδία αυτά χρησιμοποιούνται για τη διευθυνσιοδότηση των πλαισίων. Η χρήση τους ποικίλει ανάλογα με την τιμή που έχουν τα πεδία **ToDS** και **FromDS**.

Sequence Control (Ελεγχος Ακολουθίας): Χρησιμοποιείται για τον έλεγχο της σειράς των τμημάτων (fragments) που ανήκουν στο ίδιο πλαίσιο (frame). Αποτελείται από δύο υπο-πεδία:

a) **Frame Number:** Προσδιορίζει τον αριθμό του πλαισίου.

b) **Sequence Number:** Προσδιορίζει τον αριθμό του **τμήματος** του πλαισίου.

CRC Check: Αυτό το πεδίο περιέχει τον CRC - 32 έλεγχο λαθών για ολόκληρο το πλαίσιο (ή τμήμα).

2.12 Δίκτυα ειδικού σκοπού με το 802.11 (Ad hoc networks)

Σε μερικές περιπτώσεις μπορεί να χρειάζεται να υλοποιηθεί ένα ασύρματο δίκτυο που να ακολουθεί το πρότυπο 802.11, αλλά του οποίου η δομή να μην είναι απαραίτητο να είναι κυψελοειδής, ή καλύτερα να μην περιέχει *Σημεία Πρόσβασης*. Παραδείγματα αυτού του τύπου περιλαμβάνουν την ασύρματη διασύνδεση δύο προσωπικών φορητών notebooks, τη διασύνδεση δύο προσωπικών φορητών υπολογιστών (laptops), κλπ.

Το πρότυπο 802.11, αντιμετωπίζει αυτήν την ανάγκη, προσδιορίζοντας τον *Ad-Hoc τρόπο λειτουργίας (Ad-Hoc mode)*. Ένα ασύρματο δίκτυο που βρίσκεται σε Ad-Hoc τρόπο λειτουργίας, δεν περιέχει σημεία πρόσβασης και ένα τμήμα των λειτουργιών του εκτελείται από τους ίδιους τους σταθμούς, όπως είναι ο συγχρονισμός, η εκπομπή πλαισίων - φάρων, κλπ. Επίσης, κάποιες άλλες λειτουργίες δεν υποστηρίζονται, όπως η αναμετάδοση πλαισίων μεταξύ σταθμών του δικτύου που δεν έχουν τη δυνατότητα άμεσης επικοινωνίας, μιας και αυτή η λειτουργία κανονικά εκτελείται από το σημείο πρόσβασης. Αυτό σημαίνει ότι όλοι οι σταθμοί σε ένα ad-hoc δίκτυο θα πρέπει να μπορούν να επικοινωνήσουν με όλους τους υπόλοιπους.[2]

Κεφάλαιο 3 : Θέματα μετάδοσης δεδομένων πολυμέσων σε IEEE 802.11 WLAN.

3.1 Εισαγωγή

Στην μετάδοση δεδομένων πολυμεσικού περιεχομένου σε ασύρματα δίκτυα, κύριο μέλημα αποτελεί η διατήρηση της ισορροπίας ανάμεσα σε αντικρουόμενες απαιτήσεις, όπως ο χαμηλός ρυθμός μετάδοσης και η υψηλή ποιότητα (robustness) της μετάδοσης έναντι του αριθμού των λαθών στο κανάλι μετάδοσης, της χαμηλής καθυστέρησης και της διατήρησης της χαμηλής πολυπλοκότητας των αλγορίθμων.

Με την ανάπτυξη των κινούμενων κόμβων μέσα σε ένα ασύρματο δίκτυο, παρατηρείται μια σειρά από περιορισμούς που δείχνουν την παραπάνω αντίθεση ανάμεσα στις τεχνικές προϋποθέσεις σε ένα ασύρματο δίκτυο. Πιο συγκεκριμένα, είναι δυνατόν να μειωθεί ο ρυθμός μετάδοσης από τον κωδικοποιητή ώστε να διατηρείται η ισορροπία στο κανάλι μετάδοσης των δεδομένων. Αυτή η ενέργεια, όμως, θα έχει ως επακόλουθο την αύξηση της πολυπλοκότητας της υλοποίησης του κωδικοποιητή και την καθυστέρηση της διαδικασίας της κωδικοποίησης. Φυσικό επόμενο αποτελεί και η αυξανόμενη κατανάλωση ενέργειας από αφού κάθε παραγόμενο bit θα έχει σημασία.

Επιπλέον, εισάγεται η έννοια της *παγκόσμιας πρόσβασης στα πολυμέσα (Universal Multimedia Access - UMA)*, που αποτελεί σημαντική αρχή στα ασύρματα συστήματα και ακολουθεί την ιδέα της παροχής του πολυμεσικού περιεχομένου σε έναν μεγάλο αριθμό συσκευών (για παράδειγμα, PDAs ή φορητούς υπολογιστές) με διαφορετικές ικανότητες.

Γίνεται φανερό, λοιπόν, η ανάγκη για την ικανοποίηση δύο ιδιοτήτων:

1. Προσαρμογή στην ποικιλία των συνθηκών του καναλιού μετάδοσης (Bit rate scalability).
2. Προσαρμογή στην ποικιλία των διαφορετικών συσκευών (Complexity Scalability).

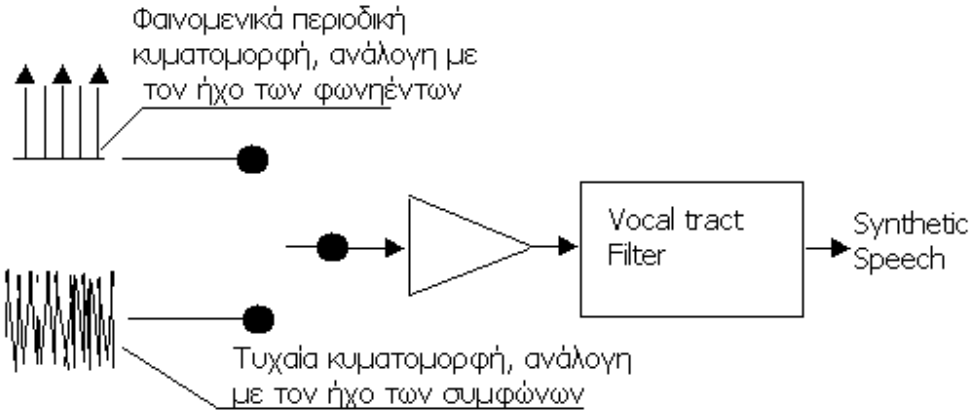
Αυτές οι δύο ιδιότητες είναι απαραίτητες για την ικανοποίηση του *Παραδείγματος των ασύρματων δικτύων* (wireless system network paradigm).
Στην συνέχεια, ακολουθεί αναφορά στην κωδικοποίηση της φωνής και του video σε ασύρματο περιβάλλον και προτάσεις που έχουν γίνει για βελτιώσεις στην ποιότητα των παρεχόμενων υπηρεσιών.[4]

3.2 Κωδικοποίηση πηγής φωνής (Speech Source Coding)

Αναδρομή

Η έρευνα για την κωδικοποίηση της φωνής έχει προχωρήσει ιδιαίτερα τα τελευταία δέκα χρόνια, με αποτέλεσμα να έχει προκύψει μια σειρά από αλγόριθμους που έχουν υιοθετηθεί από πρότυπα ασύρματων επικοινωνιών.

Οι βασικές αρχές για την δημιουργία μοντέλων αναπαραγωγής της φωνής αναπαρίστανται στο σχήμα που ακολουθεί (Σχήμα 3.1). Ο πραγματικός ήχος μοντελοποιείται από ένα ψηφιακό φίλτρο που εγείρεται από μια φαινομενικά περιοδική κυματομορφή , που δημιουργείται όταν ο λόγος εξέρχεται ως φωνή (όπως ο ήχος των φωνηέντων) από το ανθρώπινο σύστημα παραγωγής φωνής (η ακολουθία των λεκτικών συμβόλων σε συνδυασμό με τις φωνητικές χορδές) και από τυχαίες κυματομορφές, που δημιουργούνται από την παύση της φωνής (όπως ο ήχος των συμφώνων). Το φίλτρο που εφαρμόζεται για την απόδοση του συνθετικού ήχου υπολογίζεται με τη χρήση αλγορίθμων γραμμικής πρόβλεψης (Linear Prediction – LP). Αυτοί οι αλγόριθμοι αποτελούν μέρος πολλών πρότυπων κωδικοποίησης όπως το ADPCM (Adaptive Differential Pulse Code Modulation), ή το CELP (Code Excited Linear Prediction).



Εικόνα 3.1

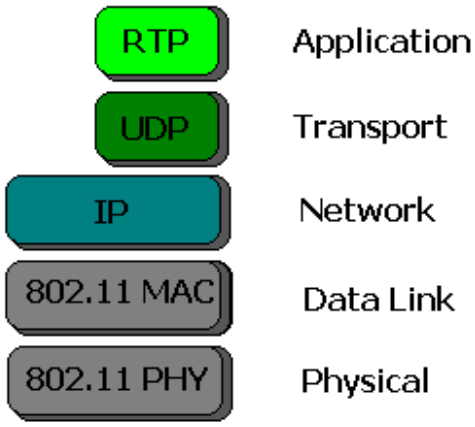
3.3Κωδικοποιητές ευρείας ζώνης (wide band codecs)

Ένα από τα προβλήματα που σχετίζονται με την κωδικοποίηση σε όλο το εύρος της συχνότητας της φωνής είναι το γεγονός ότι ο κωδικοποιητής δεν μπορεί να χειριστεί τις λιγότερο προβλέψιμες υψηλές συχνότητες. Αυτό το πρόβλημα λύθηκε από τον κωδικοποιητή ITU G.722 που χωρίζει το σήμα σε υπό-συχνότητες. Συγκεκριμένα, ο G.722 χρησιμοποιεί δύο υπό-συχνότητες, ίδιου εύρους των οποίων τα σήματα κωδικοποιούνται με χρήση ADPCM τεχνικών και μπορεί να μεταδίδει την φωνή με ρυθμούς 48, 56 και 64 Kbit/s δεσμεύοντας 16, 8 ή 0 kbit/s για την μετάδοση δεδομένων. Οι χαμηλότερες συχνότητες περιέχουν τις σημαντικότερες πληροφορίες, δεδομένου ότι οι υψηλές συχνότητες συνεισφέρουν περίπου 1% στην ποιότητα του ήχου και επομένως δεσμεύονται περισσότερα bits από ότι για τις υψηλότερες συχνότητες. Ο Quackenbush πρότεινε μια προσέγγιση που θα επέτρεπε υψηλότερη προσαρμογή όσον αφορά στον καταμερισμό των διαθέσιμων bits. Η πρότασή του, ακολούθησε αυτήν του Johnston η οποία αφορούσε ακουστικά σήματα υψηλής ευκρίνειας (high fidelity) σε δειγματοληψία στα 30 kHz και μείωσε τον ρυθμό μετάδοσης σύμφωνα με ρυθμό δειγματοληψίας στα 16kHz. Οι

Ordentlich και Shoham πρότειναν έναν κωδικοποιητή χαμηλής καθυστέρησης, βασιζόμενο σε αλγόριθμο CELP με ρυθμό μετάδοσης 32 kbit/s. Η ποιότητα της φωνής ήταν ανάλογη με αυτήν του G.728, αλλά επακόλουθη ήταν η υψηλότερη πολυπλοκότητα. Το LPC φίλτρο ήταν της τάξης των 32 αντί της τάξης 50 του G.728.

3.4 Μετάδοση φωνής στο 802.11

Η μετάδοση της φωνής σε ένα ασύρματο δίκτυο 802.11, ακολουθεί τις οδηγίες που αφορούν την υλοποίηση της ίδιας διαδικασίας σε ένα ενσύρματο δίκτυο (π.χ Ethernet). Ουσιαστικά, πρέπει να γίνει μελέτη όσον αφορά στην συνεργασία των μηχανισμών που θα αποτελούν μέρος κάθε πρωτοκόλλου στην στοίβα των πρωτοκόλλων. Έχοντας αναφερθεί στα κυριότερα κομμάτια του 802.11, πρέπει να γίνει αναφορά στον τρόπο με τον οποίο πραγματοποιείται η συνεργασία του 802.11 με τα πρωτόκολλα του ανώτερου επιπέδου, ώστε να είναι δυνατή η μετάδοση της φωνής. Η τυπική μορφή της στοίβας των πρωτοκόλλων φαίνεται στο σχήμα που ακολουθεί(Σχήμα 3.2).

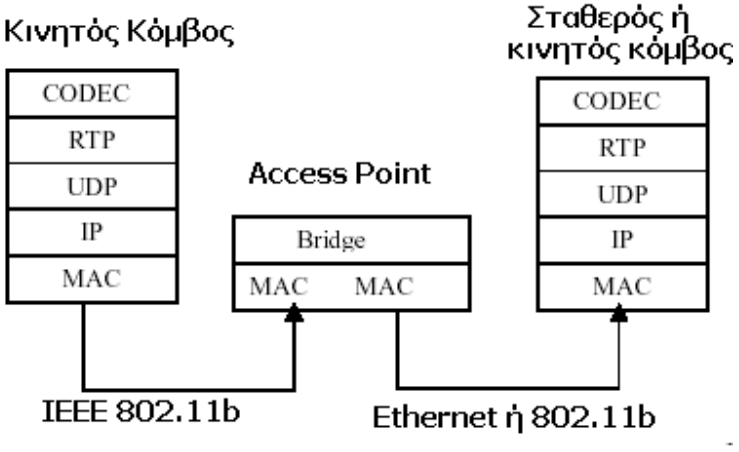


Σχήμα 3.2

Για την συνεργασία μεταξύ των διαφορετικών πρωτοκόλλων στα χαμηλότερα επίπεδα (επίπεδο MAC – επίπεδο δικτύου), πρέπει να γίνεται επιλογή, ώστε το μέγεθος του πλαισίου να είναι συμβατό από τα συναλλασσόμενα μέρη. Για παράδειγμα, ύστερα από μετρήσεις (Harvard University trace), διαπιστώθηκε ότι το 802.3 (Ethernet) χρησιμοποιεί επί το πλείστον, ως μέγιστο μέγεθος μεταδιδόμενης μονάδας (MAC PDU) τα 1500 bytes, ενώ το 802.11b καθορίζει ως μέγιστο μέγεθος τα 2.312 bytes. Επομένως, χρειάζεται προσοχή στην επιλογή των μεγεθών, ώστε να μην υπάρχει πρόβλημα στην μετάδοση της φωνής. Στο Σχήμα 3.3, απεικονίζεται μια στοίβα πρωτοκόλλων για την μετάδοση του ήχου - φωνής, που μπορεί να αλλάξει δεδομένου ότι το IP δεν είναι απαραίτητο για την μεταφορά της φωνής μέσα στο ασύρματο δίκτυο, αφού μπορεί να χρησιμοποιηθεί άλλο πρωτόκολλο μεταφοράς .

Η σύγχρονη μετάδοση της φωνής ανάμεσα σε δύο χρήστες πρέπει να ακολουθεί κάποιους κανόνες, όσον αφορά στην ποιότητα της υπηρεσίας που προσφέρεται. Η επιλογή του κωδικοποιητή θα πρέπει να γίνει με προσοχή, ώστε να μειώνονται τα λάθη που μπορεί να γίνουν κατά την διαδικασία της κωδικοποίησης και στη συνέχεια μετάδοση της φωνής. Για παράδειγμα, στο γίνεται αναφορά σε συγκεκριμένες απαιτήσεις, που καθορίστηκαν από το περιβάλλον της προσομοίωσης. Ακόμη, όσον αφορά στο πρωτόκολλο σηματοδοσίας, ειδικά για εφαρμογές τηλεφωνίας στο Διαδίκτυο (IP telephony) μπορεί να υπάρχουν συγκεκριμένες οδηγίες για τον συνδυασμό των πρωτοκόλλων. Για παράδειγμα η ITU, για την υπηρεσία της φωνής σε μια εφαρμογή, επιβάλλει τη χρήση του κωδικοποιητή G.711 όταν χρησιμοποιείται το H.323 για την σηματοδοσία .

Επομένως, στο επίπεδο της εφαρμογής (application layer), το φωνητικό σήμα κωδικοποιείται και στη συνέχεια προστίθεται σε κάθε πακέτο φωνής μια επικεφαλίδα (header) του RTP. Αυτή η επικεφαλίδα περιλαμβάνει μια σφραγίδα χρόνου (timestamp) απαραίτητη για την αναπαραγωγή. Στη συνέχεια, στο επίπεδο μεταφοράς (transport layer), το UDP χρησιμοποιείται για την πολύπλεξη διαφορετικών ροών και στο επίπεδο του δίκτυο, το IP αναλαμβάνει την διευθυνσιοδότηση και την παράδοση στο απομακρυσμένο μηχάνημα. Στη μεριά του παραλήπτη, παραλαμβάνονται τα πακέτα RTP, που αποθηκεύονται προσωρινά, ώστε να αποκωδικοποιηθούν και να αναπαραχθεί ο ήχος.



Σχήμα 3.3

Το AP, αποτελεί τον ενδιάμεσο μηχανισμό, που πραγματοποιεί την διαδικασία της γεφύρωσης ανάμεσα σε δύο διαφορετικά υπό-δίκτυα, όπως το 802.11 και το Ethernet. Επιπλέον, αποτελεί και το μέσο μετάδοσης για όλους τους κινητούς κόμβους μέσα στο πεδίο κάλυψης που παρέχει.

Ένα σημαντικό θέμα που αφορά στην υπηρεσία της μετάδοσης της φωνής σε ένα 802.11 ασύρματο δίκτυο, είναι η βελτίωση της ποιότητας της παρεχόμενης υπηρεσίας. Έχουν γίνει προτάσεις, που αφορούν επεμβάσεις είτε στο φυσικό επίπεδο , είτε στο επίπεδο MAC του 802.11, ή προτάσεις που αφορούν ανάπτυξη λογισμικού , που θα επιτρέπει τον διαχωρισμό των πακέτων σε κατηγορίες διαφορετικής προτεραιότητας.

Πιο συγκεκριμένα, όταν το AP έχει ως παράμετρο λειτουργίας την DCF, τότε όλα τα πακέτα που μεταδίδονται, μεταχειρίζονται ως ίσα, χωρίς να λαμβάνονται υπόψη, οποιεσδήποτε προτεραιότητες. Έτσι τα πακέτα της φωνής, που υπόκεινται σε χρονικούς περιορισμούς (σφραγίδα χρόνου ζωής από το RTP), συναγωνίζονται για την μετάδοση με πακέτα δεδομένων, που δεν υπόκεινται σε χρονικούς περιορισμούς (π.χ απλό κείμενο). Σε αυτήν την περίπτωση και για την βελτίωση της υπηρεσίας της φωνής, είναι απαραίτητη η ύπαρξη ενός μηχανισμού κατηγοριοποίησης, που θα επιτρέπει τον διαχωρισμό των πακέτων. Όταν χρησιμοποιούνται διαφορετικές ουρές μετάδοσης (οι οποίες πραγματοποιούν τον διαχωρισμό των πακέτων σε best effort και real time) υπάρχει διαφορά στα αποτελέσματα των μετρήσεων. Βέβαια, όπως αναφέρεται στην ίδια εργασία,

η χρήση ενός απλού μηχανισμού κατηγοριοποίησης πακέτων για την λειτουργία του 802.11 σε DCF έχει αποτελέσματα για ρυθμούς μετάδοσης μικρότερους από 24Mbps.

Επιπλέον, στο αναφέρεται ο τρόπος βελτίωσης της υπηρεσίας της φωνής με την υλοποίηση ενός μηχανισμού, που θα διαχωρίζει τα πακέτα της φωνής σε κατηγορίες σημαντικότητας. Αυτός ο μηχανισμός, αφορά μόνον τα πακέτα της φωνής και βρίσκεται στο MAC επίπεδο.

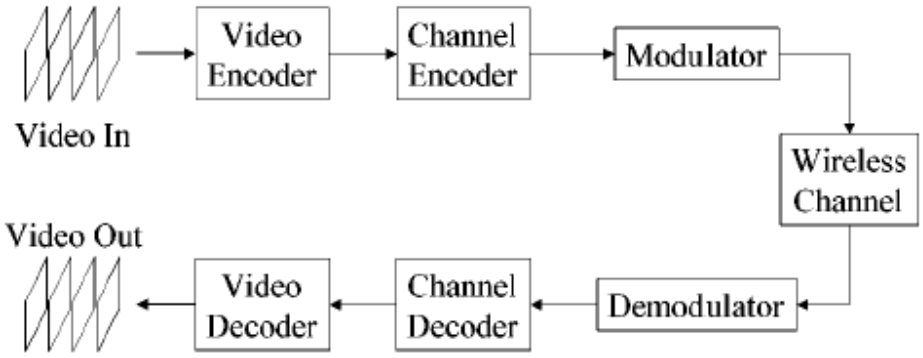
Επίσης, παρουσιάζονται συμπεράσματα που δείχνουν ότι, σε PCF τρόπο λειτουργίας του 802.11 είναι εφικτές οι εφαρμογές της τηλεφωνίας με πολύ καλύτερα αποτελέσματα από ότι σε DCF. Επιπλέον, αν αυξηθεί ο ρυθμός μετάδοσης (data rate), τότε η χρήση ενός σχήματος κεντρικού ελέγχου (όπως ο PCF) παρουσιάζει πλεονεκτήματα ακόμα και σε συνθήκες υψηλού φόρτου. Το πρόβλημα, όμως, με τον PCF τρόπο λειτουργίας είναι η δυσκολία υλοποίησης του μηχανισμού για την λίστα των σταθμών που θα μεταδώσουν πακέτα (polling list) και εξαρτάται από τον κατασκευαστή του υλικού (AP) . Επιπλέον, υπάρχει περίπτωση μερικές συσκευές να μην υποστηρίζουν αυτόν τον τρόπο λειτουργίας, με αποτέλεσμα η χρήση του DCF να καθίσταται υποχρεωτική.

3.4 Μετάδοση video σε ασύρματα δίκτυα.

Μερικές από τις αντικρουόμενες προδιαγραφές που πρέπει να αντιμετωπίσει ο σχεδιασμός μιας εφαρμογής που θα στηρίζεται στην μετάδοση video, είναι η ποιότητα της εικόνας, ο ρυθμός μετάδοσης, η πολυπλοκότητα της υλοποίησης, η ανοχή στα λάθη του καναλιού μετάδοσης, η καθυστέρηση στην μετάδοση κ.α. Στην εργασία των Khansari *et al* παρουσιάζονται συμπεράσματα που δείχνουν ότι η χρήση του H.261 για εφαρμογές σε ασύρματο περιβάλλον, αποτελεί μια υποσχόμενη λύση.. Ο συγκεκριμένος κωδικοποιητής χρησιμοποιεί πολύ καλές τεχνικές ελέγχου λαθών και επεξεργασίας του σήματος, ώστε να μπορεί να δώσει λύση στην ανάπτυξη μιας εφαρμογής, βασισμένης σε αυτόν τον κωδικοποιητή, σε ένα δυναμικό ασύρματο περιβάλλον . Βέβαια, ο συγκεκριμένος κωδικοποιητής μπορεί να καθορίζει ένα συγκεκριμένο συντακτικό και διαδικασία

αποκωδικοποίησης, αλλά οι περισσότερες επιλογές, όπως η δέσμευση των bits για διαφορετικά μέρη της εικόνας αφήνονται στην ευχέρεια του υλοποιητή του κωδικοποιητή.

Το βασικό σχήμα ενός συστήματος για μετάδοση video μέσω ασύρματου καναλιού, σε υψηλό επίπεδο, παρουσιάζεται στην παρακάτω Σχήμα 3.4.



Σχήμα 3.4

Ο κωδικοποιητής video λαμβάνει μια ροή video που την κωδικοποιεί. Οι βασικές αρχές που πρέπει να ακολουθεί ένας κωδικοποιητής video είναι να συμπιέζει την αρχική ροή και να καθιστά την κωδικοποιημένη ροή ανθεκτική σε λάθη. Η συμπίεση μειώνει τον αριθμό των bits εκμεταλλευόμενη τον πλεονασμό που υπάρχει μέσα στη ροή του video. Το συμπιεσμένο video θα μεταδοθεί στη συνέχεια διαμέσου του ασύρματου καναλιού, το οποίο εκ φύσεως υπόκειται σε απώλειες. Επομένως, η ροή video πρέπει να κωδικοποιηθεί με τρόπο που θα μειώνει τα αποτελέσματα των λαθών κατά την μετάδοση.

Ο κωδικοποιητής στο κανάλι (channel encoder) προσθέτει πλεονασμό στην ροή των bits μέσω κωδικοποίησης ώστε να προστατεύσει αυτή τη ροή από τα λάθη στο κανάλι μετάδοσης. Ο πλεονασμός που προστίθεται, βοηθά την ανίχνευση των λαθών και την διαδικασία διόρθωσης τους στον από-κωδικοποιητή. Ο ρυθμός κωδικοποίησης είναι το μέτρο για τον πλεονασμό που προστίθεται από τον κωδικοποιητή του καναλιού και είναι ο αριθμός των κωδικοποιημένων bits του video προς τον αριθμό των κωδικοποιημένων bits του καναλιού.

Στη συνέχεια, η κωδικοποιημένη ροή video μετασχηματίζεται ως προς την συχνότητα για να μπορεί να μεταδοθεί μέσω του καναλιού. Ο ρυθμός μετασχηματισμού (modulation rate) είναι ο αριθμός των bits που έχουν κωδικοποιηθεί από τον κωδικοποιητή του καναλιού προς τον αριθμό των bits που μεταδίδονται στο κανάλι ανά δευτερόλεπτο.

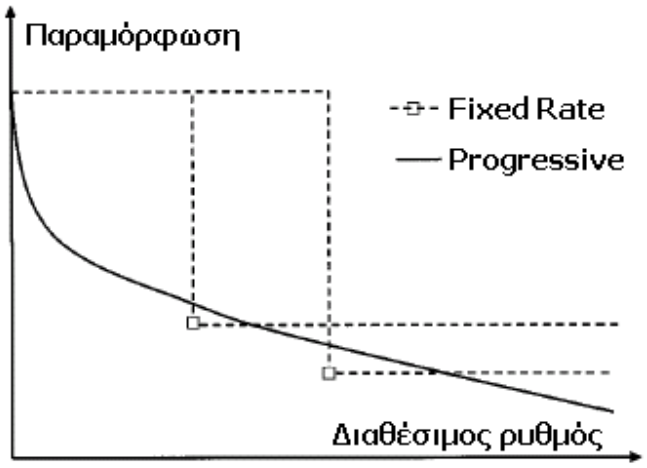
Το ασύρματο κανάλι μοντελοποιείται σαν μια διαδικασία απώλειας (fading process), που αδυνατίζει το σήμα που πρόκειται να μεταδοθεί, σε συνδυασμό με μια διαδικασία θορύβου (noise process). Η διαδικασία αλλοίωσης συλλαμβάνει τις χρονικές μεταβολές στις αποκρίσεις του καναλιού που οφείλονται στο φαινόμενο των πολλαπλών μονοπατιών ή στην απώλεια του μονοπατιού προς τον προορισμό. Η διαδικασία θορύβου μοντελοποιεί τον θερμικό θόρυβο που δημιουργείται στον λήπτη του σήματος καθώς και άλλες πηγές παρεμβολών.

Κατά την λήψη του σήματος, εφαρμόζεται η από-διαμόρφωση του σήματος και η ροή που προκύπτει επεξεργάζεται από τον από-κωδικοποιητή του καναλιού που πραγματοποιεί τον έλεγχο των λαθών. Οι πληροφορίες που περιέχουν λάθη μπορούν εισαχθούν στον από-κωδικοποιητή ή να απορριφθούν σε αυτό το σημείο. Ο από-κωδικοποιητής θα συνθέσει την ακολουθία των εικόνων για την ορθή απόδοση του video. Σε αυτό το σημείο, ο από-κωδικοποιητής πρέπει να κρύβει τις πληροφορίες που έχουν χαθεί (η απώλεια μπορεί να οφείλεται στο φαινόμενο deep-fade). Η γνώση της στρατηγικής που χρησιμοποιείται για την απόκρυψη των λαθών από τον από-κωδικοποιητή, είναι ιδιαίτερα σημαντική, αφού παίζει ιδιαίτερο ρόλο στην αποτελεσματική δέσμευση της ενέργειας που απαιτείται για την μετάδοση και τους πόρους που είναι απαραίτητοι για την κωδικοποίηση της πηγής.

3.5 Το σχήμα FGS για την ασύρματη μετάδοση video

Τα παραδοσιακά σχήματα κωδικοποίησης για video (MPEG-1,2) στόχευαν σε συμπίεση των δεδομένων σε συγκεκριμένο μέγεθος και για συγκεκριμένο εύρος ζώνης (bandwidth). Πολλές από αυτές τις τεχνικές εκμεταλλεύονται την εξάρτηση των δεδομένων μεταξύ τους, ώστε να πετύχουν μεγαλύτερους ρυθμούς συμπίεσης. Ωστόσο, η εκμετάλλευση αυτής της

ιδιότητας οδηγεί σε εξάρτηση των δεδομένων και στην κωδικοποιημένη μορφή τους. Επομένως, σε περίπτωση που υπάρχουν λάθη σε κάποια bits ή πακέτα των δεδομένων, η αποκωδικοποίηση θα φανερώσει τα λάθη σε όλη την αλυσίδα της εξάρτησης. Επιπλέον, αφού αυτά τα σχήματα κωδικοποίησης έχουν σταθερό αποτέλεσμα, δεν μπορούν να εκμεταλλευτούν τυχόν αύξηση του εύρους ζώνης (bandwidth) που μπορεί να διατεθεί σε μια εφαρμογή ή να μην έχουν εφαρμογή σε μειωμένο εύρος ζώνης. Στο σχήμα που ακολουθεί(Σχήμα 3.5) φαίνεται ότι η κωδικοποίηση που στοχεύει σε συγκεκριμένο εύρος ζώνης έχει αποτέλεσμα (ίσως βέλτιστο) μόνο σε ένα σημείο, δηλαδή στη συγκεκριμένη τιμή για την οποία επιλέχθηκε. Η ποιότητα της εικόνας παραμένει ίδια ακόμα και με την αλλαγή του ρυθμού μετάδοσης.



Σχήμα 3.5

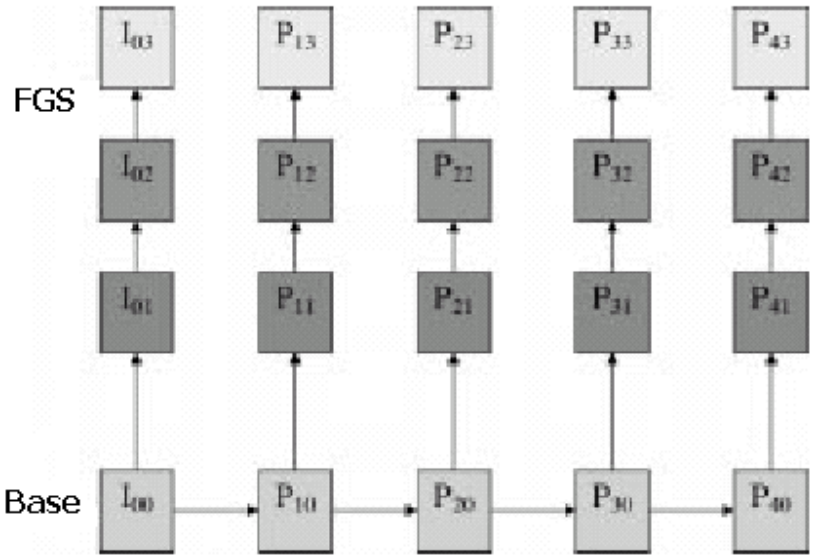
Επομένως, γίνεται ξεκάθαρο ότι αυτά τα παραδοσιακά σχήματα κωδικοποίησης video, δεν έχουν καλή εφαρμογή σε περιβάλλον ασύρματων δικτύων, στα οποία το εύρος ζώνης αλλάζει δυναμικά.

Ένα σημαντικό παράδειγμα ενός σχήματος προοδευτικής κωδικοποίησης για video, αποτελεί το **MPEG-4 FGS** (**Fine Grain Scalability**) το οποίο απεικονίζει τα δεδομένα video ως συνδυασμό δύο ροών:

1. Η **βασική ροή (base layer - stream)**, που είναι μια ροή συμβατή με το MPEG-4.
2. Τη **ροή βελτίωσης (refinement layer)**, που αποτελεί μια προοδευτικά κωδικοποιημένη ροή (progressively coded stream) και βελτιώνει την ποιότητα της βασικής ροής.

Το συγκεκριμένο σχήμα προσαρμόζεται σε πραγματικό χρόνο (κατά το χρόνο μετάδοσης) στις αλλαγές του εύρους ζώνης, που διατίθεται μέσα σε ετερογενή δίκτυα και στις ικανότητες της κάθε συσκευής.

Τα δεδομένα αναπαριστώνται σαν μια σειρά μονάδων (data units), δηλαδή πλαίσια video, πλαίσια για μετάδοση ήχου, εικόνες και κάθε κωδικοποιημένη μονάδα *l* συσχετίζεται με το μέγεθός της (σε bits) *Bl,* την παραμόρφωση που έχει υποστεί *dl,* και τον χρόνο μέχρι τον οποίο θα πρέπει να έχει αποκωδικοποιηθεί αυτή η μονάδα ώστε να είναι χρήσιμη. Οι διαφορετικές μονάδες θα πρέπει να μοντελοποιούνται σαν ένας ακυκλικός κατευθυνόμενος γράφος που τονίζει τις εξαρτήσεις ανάμεσα στις μονάδες.



Σχήμα 3.6

Στην παραπάνω εικόνα (Σχήμα 3.6), εκτός από τις εξαρτήσεις στο βασικό επίπεδο (base) που προκύπτουν από την πρόβλεψη, υπάρχουν εξαρτήσεις και στο επίπεδο FGS που προκύπτουν από την επιτυχημένη κωδικοποίηση bit-planes μέσα σε ένα πλαίσιο.

3.7 802.11 και ποιότητα Υπηρεσίας (Quality of Service)

Οι εφαρμογές που αφορούν στην επικοινωνία μεταξύ ατόμων με τη χρήση της φωνής, αναπτύσσονται διαρκώς και κερδίζουν έδαφος στην εκτίμηση των χρηστών. Όμως, αυτές οι εφαρμογές δημιουργούν μεγάλους όγκους κίνησης πακέτων UDP. Το UDP διακρίνεται για την μη φιλικότητα του προς το δίκτυο, δεδομένου ότι δεν υποχωρεί σε περίπτωση που υπάρχει συμφόρηση σε κάποιο πόρο. Επομένως, υπάρχει αντίκτυπο στην διαχείριση ενός δικτύου και λαμβάνονται μέτρα ως προς την ανάπτυξη των πολυμεσικών εφαρμογών με την χρήση μηχανισμών που επιτρέπουν τον έλεγχο στην ποιότητα της υπηρεσίας (QoS-Quality of Service).
Με την ανάπτυξη των μηχανισμών για παροχή QoS, ώστε να ελέγχονται οι επιδράσεις των streaming media εφαρμογών, μπορεί να υπάρξει εγγύηση ως προς την ποιότητα των εφαρμογών και μπορούμε να μιλήσουμε για την συγχώνευση των δικτύων (δεδομένα και πολυμέσα).

3.8 Παράμετροι QoS

Όπως αναφέρθηκε, οι διαφορετικές εφαρμογές έχουν και διαφορετικές απαιτήσεις από το δίκτυο. Αυτές οι απαιτήσεις μπορούν να συνοψιστούν ως εξής:

1. **Εύρος ζώνης (Bandwidth)**. Ο ρυθμός με τον οποίο ικανοποιείται η κίνηση που δημιουργεί μια εφαρμογή.

2. **Καθυστέρηση (latency)**. Η καθυστέρηση που μπορεί να υποστεί μια εφαρμογή ως προς την παράδοση πακέτων δεδομένων
3. **Μεταβλητότητα καθυστέρησης (Jitter).** Οι διακυμάνσεις στην καθυστέρηση.
4. **Αξιοπιστία (Reliability).** Το αριθμητικό μέγεθος των πακέτων που χάνονται από τον δρομολογητή (router).

Οι εφαρμογές που δουλεύουν σε ένα δίκτυο μπορεί να έχουν προκαθορισμένες απαιτήσεις **(ποσοτικές-quantitive)** ή οι απαιτήσεις να κυμαίνονται ανάλογα με την διαθεσιμότητα των πόρων και την δυνατότητα των εφαρμογών να δουλεύουν σε συνθήκες φόρτου εργασίας του δικτύου.(**ποιοτικές – qualitative).** Χαρακτηριστικά παραδείγματα *ποσοτικών* εφαρμογών, αποτελούν αυτές που αφορούν την μετάδοση video και η τηλεφωνία μέσω Διαδικτύου. Η μετάδοση video απαιτεί αρκετό εύρος ζώνης, ώστε να μην υπάρχουν απώλειες πακέτων που οδηγούν στην μείωση της ποιότητας της εικόνας. Η τηλεφωνία από την άλλη μεριά, είναι το κλασσικό παράδειγμα εφαρμογής που δεν είναι ανεκτική στην καθυστέρηση.

3.9 Προτάσεις για QoS σε 802.11 δίκτυα.

Έχοντας λάβει υπόψη τις βασικές αρχές για την παροχή της ποιότητας της υπηρεσίας μέσα σε ένα δίκτυο, πρέπει να γίνει επέκταση και αναφορά πως επιτυγχάνεται αυτή η ποιότητα μέσα σε 802.11 ασύρματα δίκτυα. Οι προτάσεις που έχουν γίνει μπορούν να χωριστούν σε δύο κατηγορίες :

- Προτάσεις για QoS που αφορούν στο περιβάλλον μέσα στο οποίο αναπτύσσεται μια εφαρμογή πολυμέσων. Ουσιαστικά, μιλάμε για προτάσεις που αφορούν στην υλοποίηση μιας λύσης που θα λειτουργεί ως ανεξάρτητος μηχανισμός ανάμεσα στην εφαρμογή και το 802.11 δίκτυο.
- Προτάσεις για Qos που αφορούν το ίδιο το 802.11 δίκτυο. Ουσιαστικά, μιλάμε για λύσεις που αφορούν στην υλοποίηση μηχανισμών μέσα στο πρωτόκολλο 802.11.

3.10 Ανεξάρτητοι μηχανισμοί QoS

Οι κόμβοι που βρίσκονται μέσα σε ένα ασύρματο δίκτυο, υπόκεινται σε εναλλαγές της ποιότητας της μετάδοσης και αν τα κατώτερα επίπεδα δεν ανταποκρίνονται σε αυτές τις αλλαγές, παρατηρείται μια αύξηση στην απώλεια πακέτων. Έτσι, η εφαρμογή QoS στο επίπεδο δικτύου καθίσταται δύσκολη αφού αυτό το επίπεδο έχει σχεδιαστεί ώστε να ασχολείται κυριότερα με τον έλεγχο της συμφόρησης (congestion control) και τις επιδράσεις από τα αποτελέσματα των ουρών στις συσκευές του δικτύου.

Άλλος ένας λόγος της μεταβλητότητας στο εύρος ζώνης, αποτελεί η κίνηση των κόμβων, που μεγαλώνει το πρόβλημα στο επίπεδο σύνδεσης, δεδομένου ότι οι κόμβοι επαναρυθμίζονται ανάλογα με την ποιότητα του σήματος. Επιπλέον, η τοπολογία του δικτύου αλλάζει διαρκώς με την κίνηση των κόμβων, με αποτέλεσμα οι δρομολογητές να υποχρεώνονται να προσαρμόζονται στην κίνηση των κόμβων.

Συνεπώς, μια λύση για QoS σε ένα ασύρματο περιβάλλον, πρέπει να είναι ικανή να προσαρμόζεται σε αλλαγές στο εύρος ζώνης, τόσο σε ανεξάρτητους κόμβους (αν αλλάξουν τα χαρακτηριστικά ενός μόνο κόμβου), όσο και για μια ομάδα κόμβων που δημιουργούν ένα μονοπάτι για μια από άκρη σε άκρη υπηρεσία.

Υπάρχουν διάφορες προτάσεις για παροχή QoS σε ένα δυναμικό περιβάλλον. Μια πρόταση βασίζεται στην δέσμευση πόρων με την εισαγωγή της έννοιας της περιοχής QoS (QoS range). Σε αυτήν την προσέγγιση, δημιουργείται μια επέκταση του RSVP, που αποκαλείται Dynamic RSVP (dRSVP). Σύμφωνα με την ερμηνεία της προσέγγισης, το δίκτυο θα παρέχει υπηρεσίες σε ένα σημείο, μέσα σε μια περιοχή QoS και αν μια εφαρμογή μπορεί να προσαρμόζει τον ρυθμό μετάδοσης ώστε να παραμένει μέσα σε μια περιοχή QoS, θα μπορεί να δέχεται την υπηρεσία QoS από το δίκτυο.

Η συγκεκριμένη προσέγγιση, ευνοεί την αποδέσμευση της δρομολόγησης από την παροχή QoS. Αν μια αλλαγή στην τοπολογία του δικτύου, υποχρεώνει τον δρομολογητή να υπολογίσει μια νέα διαδρομή ή αν συμβεί μια αλλαγή στην ρυθμό-απόδοση (throughput) ενός κόμβου μέσα σε μια διαδρομή, τότε είναι προτιμότερο να υπάρχει μια περιοχή από

σημεία παροχής QoS, ώστε να είναι δυνατή η συνέχιση της υπηρεσίας QoS. Αν οι πόροι που έχουν δεσμευθεί μειωθούν, τότε είναι προτιμότερο να μειώνεται η δέσμευση των πόρων μέσα σε μια περιοχή από το να αποτυγχάνει η δέσμευση.

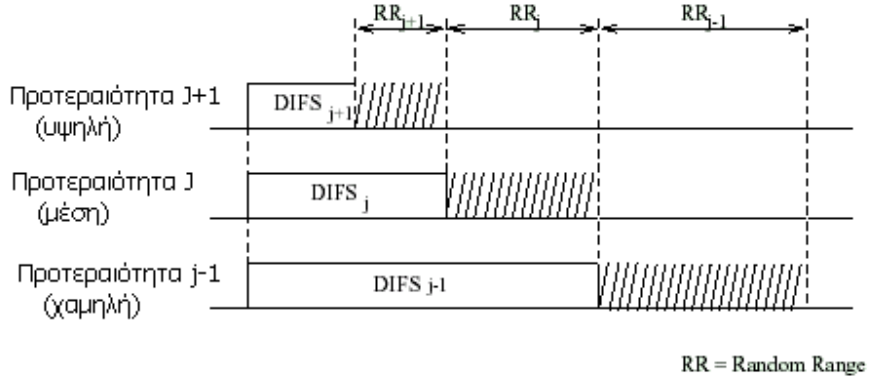
3.10 Μηχανισμοί για QoS μέσα στο 802.11

Μια προσέγγιση, για την παροχή διαφοροποιημένων υπηρεσιών βασίζεται στην υλοποίηση μηχανισμών στο επίπεδο MAC, ώστε να είναι δυνατή η παροχή QoS ανάλογα με την προτεραιότητα, που θα έχει ο κάθε σταθμός. Ειδικότερα, οι παράμετροι του 802.11 που λαμβάνονται υπόψη είναι:

- η **συνάρτηση υποχώρησης** (backoff increase function), με κάθε σταθμό να έχει διαφορετική συνάρτηση αύξησης του βήματος υποχώρησης.
- **DIFS**: Σε κάθε επίπεδο προτεραιότητας αντιστοιχεί DIFS διαφορετικού μεγέθους και μετά την πάροδό του να μεταδίδεται το πλαίσιο RTS ή πακέτο δεδομένων.
- **Μέγιστο μήκος πλαισίου**: σε κάθε επίπεδο προτεραιότητας αντιστοιχεί ένα μέγιστο μήκος πλαισίου που επιτρέπεται να μεταδοθεί κάθε φορά.

Αναφορικά με την πρώτη παράμετρο, διαπιστώθηκε σε περιβάλλον προσομοίωσης, ότι μια ροή UDP με υψηλή προτεραιότητα δεν έχει πλεονέκτημα έναντι μιας ροής TCP με χαμηλότερη προτεραιότητα και το κανάλι διαμοιράζεται εξίσου. Αντίστροφα, αν δοθεί υψηλή προτεραιότητα σε μια ροή TCP, αυτή θα έχει υψηλότερη ρυθμό-απόδοση, σε σχέση με μια ροή UDP με χαμηλή προτεραιότητα. Ουσιαστικά, η απόδοση προτεραιοτήτων με βάση την συνάρτηση υποχώρησης, ευνοεί την ρυθμό-απόδοση του TCP, αλλά δεν έχει πάντοτε εφαρμογή.

Η εξέταση της δεύτερης παραμέτρου, ως τρόπος απόδοσης προτεραιοτήτων βασίζεται στην απόδοση διαφορετικού μήκους DIFS σε κάθε σταθμό, σύμφωνα με την φιλοσοφία των πλαισίων ACK, που έχουν υψηλότερη προτεραιότητα από τα RTS πλαίσια.



Σχήμα 3.7

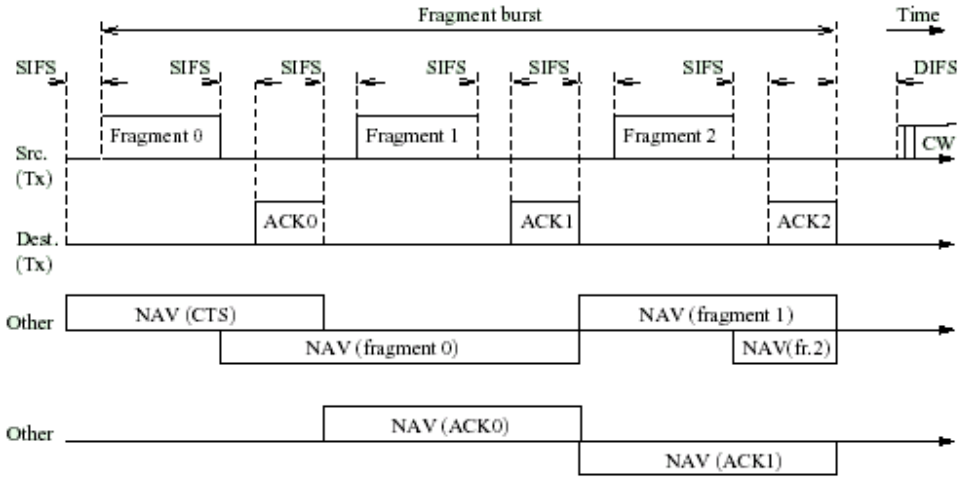
Έτσι, σε κάθε επίπεδο προτεραιότητας θα αντιστοιχεί διαφορετικό DIFS, ($DIFS_j$ με $DIFS_{j+1}$ < DIFSj) Σχήμα 3.7. Η κυκλοφορία χαμηλής προτεραιότητας, θα είναι σε χαμηλές θέσεις στην ουρά εξυπηρέτησης, όσο υπάρχουν πλαίσια με υψηλή προτεραιότητα. Αν ένα πακέτο, αποτύχει να δεσμεύσει το κανάλι για μετάδοση, θα μειωθεί η προτεραιότητα που του έχει αποδοθεί, σύμφωνα με τα DIFS και τα RR.

Τα συμπεράσματα της προσομοίωσης, έδειξαν ότι το UDP παρουσιάζει μεγαλύτερη προσαρμογή σε αυτήν την παράμετρο, όσον αφορά στην απόδοση προτεραιοτήτων, από ότι το TCP για το ίδιο $DIFS_j$. Αυτή η παράμετρος, μπορεί να χρησιμοποιηθεί για την απόδοση προτεραιότητας του UDP έναντι του TCP και αντίστροφα, με την απόδοση διαφορετικού DIFS σε καθεμία ροή. Αυτός ο μηχανισμός, μπορεί να εφαρμοστεί σε εφαρμογές πολυμέσων σε ασύρματα δίκτυα, στις οποίες σημαντικό ρόλο παίζει η καθυστέρηση. Με την απόδοση υψηλής προτεραιότητας, στα πλαίσια μιας εφαρμογής πραγματικού χρόνου (π.χ τηλεφωνία), μπορούμε να πετύχουμε την επιθυμητή διαφοροποίηση ανάμεσα στα πακέτα που μεταδίδονται.

Ο τρίτος μηχανισμός, αφορά στον περιορισμό του μήκους του πλαισίου που μπορεί να μεταδώσει ο κάθε σταθμός. Ανάλογα με το μήκος του πλαισίου διακρίνονται:

- Αν θα απορριφθούν τα πακέτα που ξεπερνούν το επιτρεπόμενο μήκος
- Αν θα γίνει τεμαχισμός (fragmentation) των πακέτων που ξεπερνούν το επιτρεπόμενο μήκος.

Αυτός ο μηχανισμός, χρησιμοποιείται ήδη από το 802.11 για την αύξηση της αξιοπιστίας της μετάδοσης, αλλά μπορεί να εφαρμοστεί για την απόδοση διαφοροποίησης ανάμεσα στους σταθμούς. Επιτρέποντας σε κάποιους σταθμούς να έχουν μεγαλύτερο μήκος πλαισίου και να επιτρέπεται η μετάδοση αυτών των πλαισίων με τον τεμαχισμό, είναι δυνατή η διαφοροποίηση ανάμεσα στους σταθμούς.



Σχήμα 3.8

Στην παραπάνω εικόνα (Σχήμα 3.8), ο σταθμός που μεταδίδει ένα τεμαχισμένο πλαίσιο θα συνεχίσει να μεταδίδει τα κομμάτια του πλαισίου, όσο θα δέχεται τα ACK. Με αυτόν τον τρόπο, κάποιοι σταθμοί θα μπορούν να έχουν διαφορετικούς (υψηλότερους) ρυθμούς μετάδοσης.

Κεφάλαιο 4: Πειραματική μελέτη

4.1 Εισαγωγή

Το Qcheck είναι ένα πρόγραμμα software το οποίο παρέχει μετρήσεις όσον αφορά την απόδοση του δικτύου. Αναπτύχθηκε έτσι ώστε οι τελικοί χρήστες να μπορούν να κάνουν εξονυχιστικούς ελέγχους στα άκρα τερματισμού (endpoints).

Δημιουργήθηκε από την εταιρεία IXIA, η οποία ιδρύθηκε το 1997 και αποτελεί μία από τις πιο σημαντικές και συνεχώς αναπτυσσόμενες εταιρείες όσον αφορά το IP Network Testing.

Γι' αυτό το λόγω άλλωστε πολλοί άλλοι κατασκευαστές δικτύου και τηλεφωνίας βασίζονται σε αυτήν όπως π.χ. η Cisco, η Hewlett Packard, η Intel, η Ericsson κλπ.

4.2 ΠΕΡΙΓΡΑΦΗ Qcheck

Αποτελείται από δύο συστατικά:

α)Μία κονσόλα με γραφικό περιβάλλον (Graphical User Interface), η οποία τρέχει σαν ένα πρόγραμμα εφαρμογής σε Windows 95, 98, 2000 και XP.(Σχήμα 4.1)

β)Από δύο software agents που ονομάζονται "Performance Endpoints" ή αλλιώς "Endpoints" (σημεία τερματισμού).


QCHECK
From Endpoint 1
xubx
To Endpoint 2
endpoint.gary.mede.com
TCP
UDP
SPX
IPX
Protocol
Response Time
Throughput
Streaming (UDP or IPX)
Traceroute (TCP or UDP)
Operation
Iterations
3
Data Size
100
bytes
Response Time Results
Minimum
34 ms
Average
36 ms
Maximum
38 ms
Run
Details
netiq

Σχήμα 4.1

Στην κονσόλα του Qcheck μπορούμε να επιλέξουμε τις διευθύνσεις των endpoints καθώς επίσης και το πρωτόκολλο που θα χρησιμοποιήσουμε, το οποίο μπορεί να είναι το TCP ή το UDP για TCP/IP δίκτυα και το IPX/SPX για Novell δίκτυα. Στη συνέχεια, επιλέγουμε μεταξύ ορισμένων test τα οποία αφορούν:

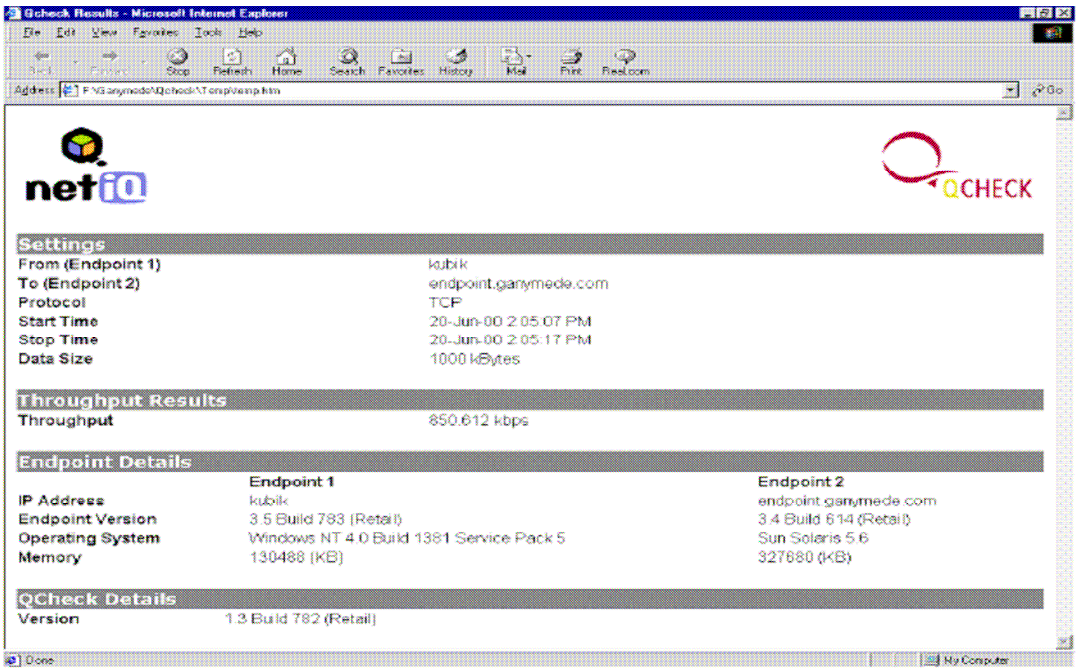
- το χρόνο απόκρισης (response time), ο οποίος επιστρέφει τον ελάχιστο , το μέγιστο και τον μέσο όρο των seconds που απαιτούνται για να γίνει η επικοινωνία.

- το throughput, το οποίο επιστρέφει τον αριθμό των δεδομένων ανά second, τα οποία έχουν σταλεί επιτυχώς μεταξύ των δύο endpoints.

- Το streaming, το οποίο επιστρέφει το ρυθμό με τον οποίο έχουν ληφθεί τα streaming data από το δεύτερο endpoint και τον αριθμό των πακέτων που έχουν χαθεί.

- το traceroute, το οποίο μας επιστρέφει τον αριθμό των hops, τον μέσο όρο των επιτυχών αποστολών καθώς επίσης τις διευθύνσεις και τα ονόματα των host σε κάθε hop.

Μόλις ολοκληρωθεί κάποιο από τα παραπάνω test εμφανίζονται τα αποτελέσματα στο παράθυρο της κονσόλας του Qcheck, ενώ μια πιο λεπτομερής αναφορά μπορεί να προβληθεί σαν αποτέλεσμα σε μορφή ιστοσελίδας μέσω ενός Web Browser.(Σχήμα 4.2)



Σχήμα 4.2

Εκτός από την κονσόλα του Qcheck υπάρχουν και τα endpoints τα οποία όπως ήδη έχουμε προαναφέρει είναι software agents και μπορούν να χρησιμοποιηθούν σε πάνω από 20 Λειτουργικά Συστήματα π.χ. Windows, Unix, Linux, Macintosh κλπ.

Επιπλέον, μπορούν να εγκατασταθούν σε mainframes, workstations, personal computers.

Τρέχουν σαν υπηρεσία ή σαν μία διαδικασία στο παρασκήνιο ενώ όταν βρίσκονται σε αδράνεια καταναλώνουν μηδαμινούς πόρους συστήματος.

Πριν ξεκινήσει κάποιο test το λογισμικό των endpoints θα πρέπει να εγκατασταθεί είτε στα mainframes είτε στα workstations είτε στα personal computers.

Τα test γίνονται μεταξύ των endpoints που ονομάζονται endpoint 1 και endpoint 2.

Υπάρχουν δύο μορφές αποστολής δεδομένων.

Στην πρώτη περίπτωση τα δύο endpoints συμπεριφέρονται σαν peer υπολογιστές και η όλη διαδικασία ξεκινάει από το endpoint 1.

Αντίθετα, στην δεύτερη περίπτωση σε εφαρμογές client/server το endpoint 1 υποδύεται τον client και το endpoint 2 τον server.

Ειδικότερα, όσον αφορά τα streaming test το endpoint 1 υποδύεται έναν streaming server ενώ το endpoint 2 υποδύεται τον client ή τον παραλήπτη των δεδομένων καθώς επίσης και αμφίδρομα.

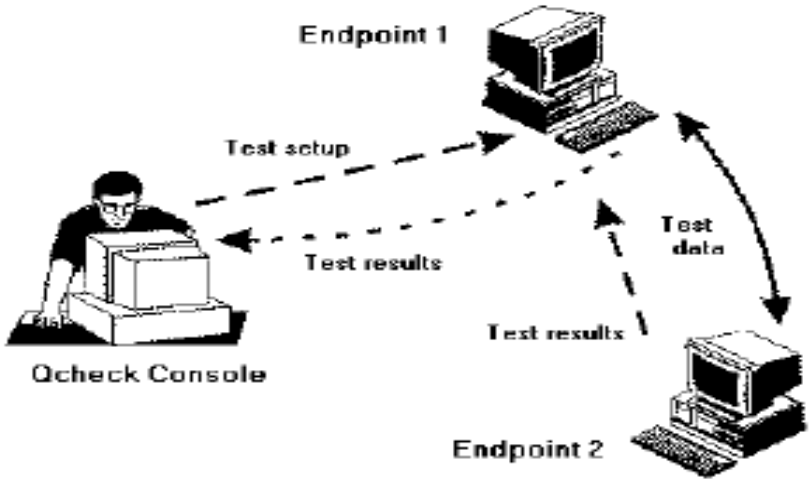
Ένα endpoint μπορεί να λειτουργήσει και στις δύο παραπάνω περιπτώσεις είτε σαν endpoint 1 είτε σαν endpoint 2, καθώς επίσης δεν είναι αναγκαία η εγκατάσταση ξεχωριστού λογισμικού, διότι λειτουργεί στα endpoints υπό τη μορφή client/server.

Στη συνέχεια περιγράφονται τα βήματα που ακολουθούμε για να πραγματοποιήσουμε ένα test με τη βοήθεια του Qcheck.

Για να τρέξει ένα test πρώτα εισάγουμε τη διεύθυνση δικτύου για το endpoint 1 και το endpoint 2 στα κατάλληλα πεδία της κονσόλας του Qcheck.

Έπειτα επιλέγουμε το κατάλληλο πρωτόκολλο και το είδος του test που θέλουμε να πραγματοποιήσουμε και πατάμε το κουμπί RUN.

Μόλις πατήσουμε το κουμπί RUN η κονσόλα στέλνει τις εντολές (διεύθυνση, πρωτόκολλο κλπ.) στο endpoint 1 το οποίο, κρατάει τις εντολές που είναι για εκείνο και προωθεί όλα τα υπόλοιπα στο endpoint 2. (Σχήμα 4.3)



Σχήμα 4.3

Στη συνέχεια, ξεκινάει η διαδικασία της ανταλλαγής των δεδομένων και επιστρέφονται τα αποτελέσματα στην κονσόλα του Qcheck.
Στην περίπτωση ενός streaming test το endpoint 2 συλλέγει τα αποτελέσματα και τα στέλνει πίσω στην κονσόλα μέσω του endpoint 1

.

4.2.1 ΕΛΕΓΧΟΣ ΧΡΟΝΟΥ ΑΠΟΚΡΙΣΗΣ (RESPONSE TIME)

Ο χρόνος απόκρισης (response time) μας προσδιορίζει το χρονικό διάστημα που χρειάζεται για να στείλουμε ένα αίτημα (request) και να λάβουμε μια απάντηση στο δίκτυο και είναι σημαντικό για πολλές συναλλαγές δικτύων.

Για παράδειγμα, ένας browser στέλνει ένα αίτημα και έπειτα περιμένει μια απάντηση προκειμένου να "φορτώσει" μια ιστοσελίδα .

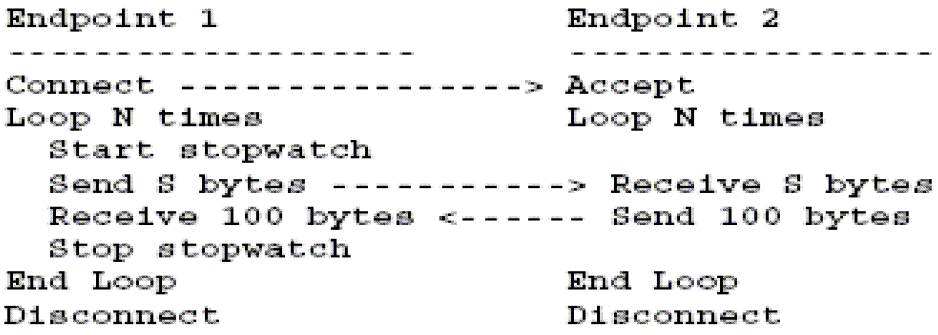
Στην συνέχεια περιγράφεται ο έλεγχος του χρόνου απόκρισης μέσω του Qcheck.

Το endpoint 1 στέλνει ένα πακέτο δεδομένων (ρυθμιζόμενο από 1 έως 32.000 bytes) στο endpoint 2. Αφότου τα δεδομένα έχουν σταλεί, το endpoint 1 περιμένει να λάβει μια απάντηση από το endpoint 2.

Στην ουσία ο χρόνος απόκρισης (response time) είναι ο χρόνος μιας πλήρους περιφοράς (round-trip-delay). Δηλαδή, είναι ο χρόνος εκείνος που απαιτείται για το εκάστοτε πακέτο δεδομένων για να πάει και να επιστρέψει στον αποστολέα του.

Ο χρόνος που απαιτείται για να γίνει η παραπάνω συναλλαγή είναι συνήθως milliseconds ή seconds.

Ο υπολογισμός του χρόνου απόκρισης (response time), γίνεται μέσω ενός αριθμού επαναλήψεων , οι οποίοι καθορίζονται από το χρήστη και κυμαίνονται από ένα έως δέκα. Όσο μεγαλύτερος είναι ο αριθμός των επαναλήψεων τόσο ακριβέστερος θα είναι και ο έλεγχος.



Σχήμα 4.4

Η συναλλαγή μεταξύ δύο endpoints (Σχήμα 4.4) σε ένα test απόκρισης χρόνου του QCHECK. **S** είναι το μέγεθος του data block που αποστέλλεται, το οποίο κυμαίνεται από 1 έως 32.000 bytes.

Ωστόσο σε μερικές περιπτώσεις είναι χρήσιμο να γνωρίζουμε και το χρόνο απόκρισης (response time) που χρειάζεται για μια απλή μετάβαση.
Ο τύπος που χρησιμοποιούμε για να υπολογίσουμε το μέσο όρο του χρόνου απόκρισης είναι:

$$\mathbf{RT = (m_1 + ... + m_N) / N}$$

όπου:

RT = ο μέσος όρος του χρόνου απόκρισης, σε seconds.
N = ο αριθμός των επαναλήψεων.
m = απαιτούμενος χρόνος της διαδρομής από το endpoint 1 έως το endpoint 2 ($t_2 - t_1$).
m_1 = η πρώτη επανάληψη.
m_N = η νιοστή επανάληψη.

Αυτό είναι πολύ χρήσιμο σε εφαρμογές πραγματικού χρόνου και ο υπολογισμός του χρόνου απόκρισης απλής μετάβασης γίνεται εάν πολύ απλά, διαιρέσουμε το αποτέλεσμα στα δύο.
Ωστόσο, ο υπολογισμός αυτός είναι μερικές φορές ανακριβής γιατί οι διαδρομές από και προς τα endpoints μπορεί να είναι διαφορετικές.

4.2.2 ΕΛΕΓΧΟΣ THROUGHPUT

Όπως έχουμε προαναφέρει το throughput μας επιστρέφει τον αριθμό των δεδομένων ανά second τα οποία έχουν σταλεί επιτυχώς μεταξύ των δύο endpoints. Μας δείχνει δηλαδή την χωρητικότητα του δικτύου, η οποία μετριέται σε bytes ή bits per second (bps).
Το Qcheck μετρά το throughput ελέγχοντας το πόσο γρήγορα μπορεί να σταλεί ή να παραληφθεί ένα πακέτο δεδομένων. Το μέγεθος του πακέτου μπορεί να οριστεί από 1.000 έως 1.000.000 Bytes.
Έπειτα, καθοδηγεί το endpoint 1 να στείλει τα δεδομένα και περιμένει για μια απάντηση ανά byte (όσα byte στείλει τόσες απαντήσεις θα λάβει).(Σχήμα 4.5)
Ο τύπος που χρησιμοποιούμε για να υπολογίσουμε το throughput είναι:

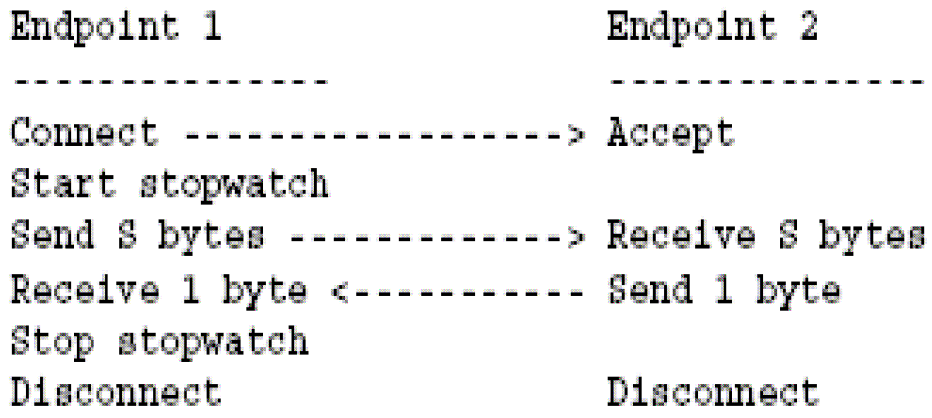
T = (S + R) / m

όπου:
T = ρυθμός μετάδοσης σε bytes/sec.
S = bytes σταλθέντα από το endpoint 1.
R = bytes ληφθέντα από το endpoint 2 (πάντα 1 byte).

m = απαιτούμενος χρόνος της διαδρομής από το endpoint 1 έως το endpoint 2 ($t_2 - t_1$).

Τα αποτελέσματα που εμφανίζονται στην κονσόλα του Qcheck μετά από ένα test throughput μας δείχνουν το μέσο όρο του throughput.

Παρόλα αυτά, σε δίκτυα με υψηλή ταχύτητα τα αποτελέσματα του throughput μπορεί να είναι μικρότερα από το συνολικά διαθέσιμο bandwidth. Αυτό συμβαίνει γιατί το Qcheck έχει σχεδιαστεί έτσι ώστε η ροή που στέλνονται τα δεδομένα να είναι μικρή και σύντομη και επίσης περιορίζεται σε μια σύνδεση και δεν στέλνει όπως έχουμε ήδη προαναφέρει πάνω από 1.000.000 Bytes δεδομένων.



Σχήμα 4.5

4.2.3 ΕΛΕΓΧΟΣ STREAMING PERFORMANCE

Κάτι επίσης πολύ σημαντικό για μερικές εφαρμογές είναι το μέγεθος των πακέτων που χάνονται. Όπως ήδη γνωρίζουμε μερικές εφαρμογές που χρησιμοποιούν το TCP -εάν πρόκειται για TCP/IP δίκτυα- ή το SPX -εάν πρόκειται για Novell δίκτυα-, τα οποία είναι connection-oriented πρωτόκολλα, δεν ανέχονται την απώλεια των δεδομένων. Έτσι εάν μία TCP εφαρμογή στείλει κάποια δεδομένα, το ίδιο το πρωτόκολλο, δηλαδή στην προκειμένη περίπτωση το TCP, είναι εκείνο που εγγυάται ότι τα δεδομένα θα φτάσουν στον παραλήπτη.

Αντίθετα, όταν πρόκειται για τα πρωτόκολλα UDP και IPX τα οποία είναι connectionless και δεν εγγυούνται ότι τα δεδομένα θα φτάσουν στον παραλήπτη, την ποιότητα της αξιοπιστίας την αναλαμβάνουν οι ίδιες οι εφαρμογές είτε στο επίπεδο μεταφοράς είτε στο επίπεδο εφαρμογής.

Ωστόσο όμως, υπάρχουν και μερικές εφαρμογές multimedia, όπως η φωνή και το video, στις οποίες δεν έχει πολύ μεγάλη σημασία η απώλεια μερικών datagram.

Γιατί είναι όμως σημαντικό να γνωρίζουμε το μέγεθος των πακέτων που χάνονται; Για παράδειγμα, σε μια εφαρμογή video η απώλεια δεδομένων σημαίνει απώλεια κάποιον σκηνών ενώ το ίδιο μπορεί να συμβεί και σε ένα απλό τηλεφώνημα.

Πως μπορούμε να καθορίσουμε από ποιο σημείο και έπειτα θα θεωρούνται "πολλά" τα δεδομένα που έχουμε χάσει;

Αυτό εξαρτάται από την ίδια την εφαρμογή. Υπάρχουν ορισμένες εφαρμογές πραγματικού χρόνου που ανέχονται την απώλεια δεδομένων, συγκεκριμένου μεγέθους, ενώ κάποιες άλλες όχι.

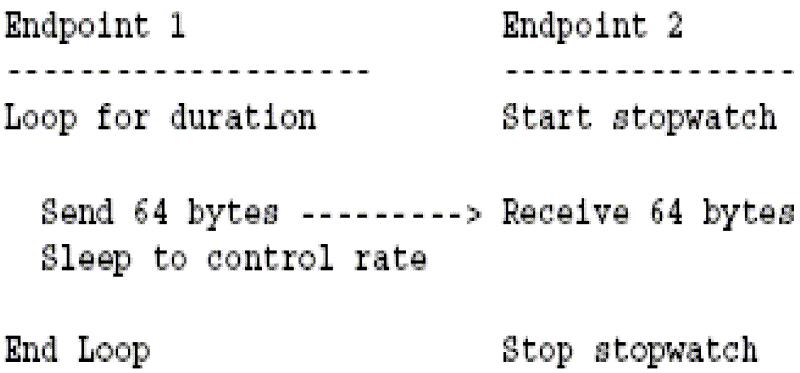
Ουσιαστικά τα δεδομένα που χάνονται εκφράζονται σε bytes ή σε ποσοστό bytes.

Το Qcheck αναπαριστά τα δεδομένα που χάνονται καθοδηγώντας το endpoint 1 να στείλει τα δεδομένα με ένα συγκεκριμένο ρυθμό μετάδοσης σε ένα σύντομο χρονικό διάστημα(Σχήμα 4.6). Σαν δεδομένα που χάνονται θεωρούνται αυτά που δεν παραλαμβάνονται από το endpoint 1. Αυτά τα δεδομένα μπορεί να βρίσκονται κάπου στο δίκτυο ή σε κάποιον router. Αξιοσημείωτο είναι, ότι ακόμα και αν φτάσουν σε λάθος σειρά, θεωρούνται σαν δεδομένα που έχουν χαθεί.

Ο τύπος που χρησιμοποιείται για τον υπολογισμό του ποσοστού των χαμένων δεδομένων είναι:

$$L = [(S - R) / S] * 100 \text{ σε } \%$$

όπου:
L = το ποσοστό των δεδομένων που έχουν χαθεί.
S = το σύνολο των bytes που έχουν σταλεί από το endpoint 1.
R = το σύνολο των bytes που έχουν ληφθεί από το endpoint 2.



Σχήμα 4.6

4.2.4 ΈΛΕΓΧΟΣ TRACEROUTE

Ένα test traceroute μας δείχνει όπως ήδη γνωρίζουμε πληροφορίες για τη διαδρομή που θα ακολουθήσει ένα πακέτο μέσα στο δίκτυο.

Επιπλέον, μας δείχνει τον αριθμό των hops, όλους τους ενδιάμεσους κόμβους ή routers από τους οποίους θα περάσει ένα πακέτο και τα ονόματά τους καθώς επίσης και τον round-trip χρόνο μεταξύ της πηγής και του κάθε ενδιάμεσου κόμβου. Ο μέγιστος αριθμός των αναπηδήσεων ορίζεται στα 30 hops και ο χρόνος Time To Live του πακέτου στα 3 seconds ανά hop.

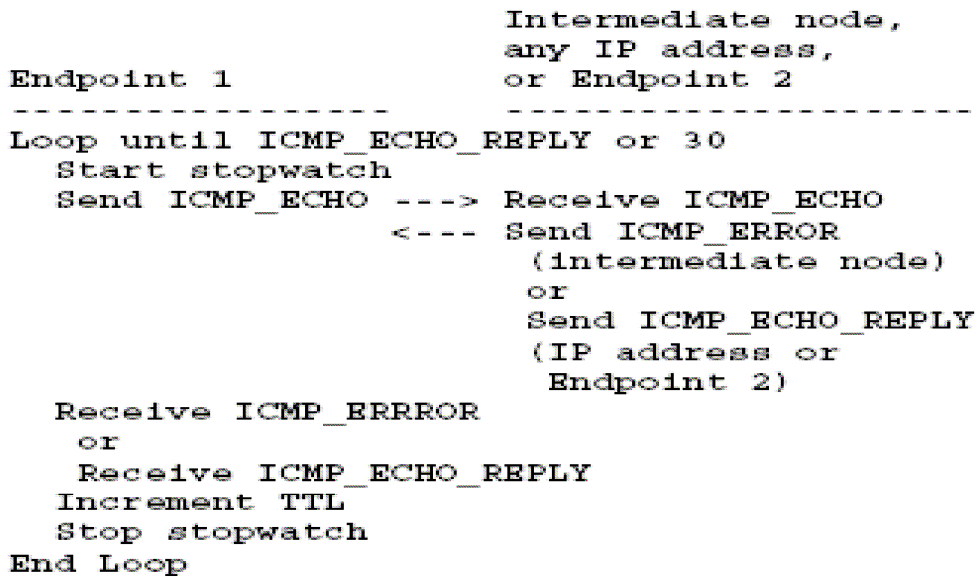
Σχήμα 4.7

Το παραπάνω test traceroute (Σχήμα 4.7) μας δείχνει 16 hops από το endpoint 1 έως την αναγραφόμενη ιστοσελίδα. Η μεσαία στήλη μας δείχνει τον round-trip χρόνο σε milliseconds σε κάθε hop. Οι αστερίσκοι υποδηλώνουν ότι δεν έχει ληφθεί καμιά απάντηση στο συγκεκριμένο hop μέσα στο χρονικό όριο των 3 seconds.

Στην πλειοψηφία τους τα endpoints όσον αφορά ένα traceroute test, χρησιμοποιούν το πρωτόκολλο ICMP για να στείλουν ένα echo μήνυμα (echo message) ενώ πολύ λίγες είναι εκείνες οι εφαρμογές που προτιμούν να στέλνουν ένα UDP echo message.
Με τη χρήση του echo μηνύματος βλέπουν κατά πόσο ένας router είναι τόσο σε λειτουργία όσο και προσιτός.
Το Qcheck συγκεντρώνει τις πληροφορίες όσον αφορά το traceroute καθοδηγώντας το endpoint 1 να στείλει ICMP echo packets και να ελέγξει τις απαντήσεις.
Η διεύθυνση που αναγράφεται στο πεδίο για το endpoint 1 θα πρέπει να είναι ένας υπολογιστής στον οποίο θα είναι ενεργοποιημένο το λογισμικό του endpoint ενώ η

διεύθυνση για το endpoint 2 μπορεί να είναι οποιαδήποτε διαθέσιμη IP διεύθυνση χωρίς να κρίνεται αναγκαία η εγκατάσταση του λογισμικού του endpoint.

Το endpoint 1 στέλνει πολλαπλά ICMP echo packets με μία ποικιλία τιμών TTL (Time To Live). Καθώς ένα πακέτο βρίσκεται μέσα στο δίκτυο ο κάθε κόμβος από τον οποίο περνάει το πακέτο μειώνει την τιμή TTL κατά ένα. Όταν ο χρόνος Time To Live φτάσει στο 0 τότε ο router στέλνει ένα μήνυμα λάθους το οποίο αναφέρει ότι ο χρόνος TTL έχει λήξει. Η διαδικασία που ακολουθείται σε ένα test tracerout περιγράφεται στο παρακάτω σχήμα (Σχήμα 4.8)



Σχήμα 4.8

4.2.5 ΣΥΓΚΡΙΣΗ ΜΕ PING

Ας δούμε λοιπόν μετά την αναλυτική περιγραφή του προγράμματος Qcheck μερικές από τις επιπρόσθετες λειτουργίες του εν συγκρίσει με τις λειτουργίες του ping.

	QCHECK	PING
Εξέταση της κίνησης του χρόνου απόκρισης (response time) στα δίκτυα.	✓	✓
Εξομοίωση της ροής των πραγματικών εφαρμογών διαμέσου του δικτύου για την εξέταση της συνδεσιμότητας και της απόδοσης.	✓	
Εξέταση του throughput του δικτύου.	✓	
Εξέταση του δικτύου για υποστήριξη εφαρμογών.	✓	
Εξέταση των γραμμών του δικτύου χρησιμοποιώντας τη ροή των εφαρμογών που δημιουργείται από εφαρμογές multimedia.	✓	
Καθορισμός του streaming ρυθμού κίνησης που λαμβάνεται και της απώλειας πακέτων.	✓	
Εξέταση της συνδεσιμότητας μεταξύ του δικού μας υπολογιστή και ενός άλλου.	✓	✓
Υποστήριξη πληθώρας πρωτοκόλλων και εξέταση της απόδοσης του δικτύου χρησιμοποιώντας TCP, UDP, IPX, SPX δίκτυα.	✓	
Εξέταση της φυσικής μνήμης ενός σταθμού εργασίας και της λειτουργικότητας του Λειτουργικού Συστήματος και της CPU.	✓	
Εκτέλεση του traceroute μεταξύ δυο οποιονδήποτε σταθμών εργασίας ανεξαρτήτως της τοποθεσίας τους.	✓	

4.2.6 ΠΡΟΒΛΗΜΑΤΑ – ΛΥΣΕΙΣ

Παρακάτω ακολουθούν μερικά παραδείγματα προβλημάτων και οι αντίστοιχες λύσεις για κάθε ένα από τα test που μπορούμε να πραγματοποιήσουμε χρησιμοποιώντας το Qcheck.

- *Παράδειγμα 1 για response time(χρόνος απόκρισης).*

Πρόβλημα: κάποιος από το λογιστήριο μιας εταιρείας καλεί τη γραμματεία λέγοντας ότι δεν έχει πρόσβαση στον server της βάσης δεδομένων.

Λύση: ένα test απόκρισης χρόνου (response time) του Qcheck καθορίζει εάν είναι πρόβλημα συνδεσιμότητας δικτύου ή όχι. Επιπλέον, καθορίζει εάν είναι πρόβλημα που το αντιμετωπίζει ένας χρήστης, ένα τμήμα ή πολλοί εργαζόμενοι.

- *Παράδειγμα 2 για throughput.*

Πρόβλημα: έχουμε πολλούς απομακρυσμένους χρήστες-εργαζόμενους οι οποίοι συνδέονται στο δίκτυο μέσω 56 Kbps dial-up modems. Αναρωτιόμαστε τι είδους throughput βλέπουν.

Λύση: ένα test throughput του Qcheck μας δείχνει πόσο γρήγορα ένας υπολογιστής μπορεί να μεταδώσει τα δεδομένα κατά μήκος ενός οποιουδήποτε δικτύου. Από το γραφείο μας μπορούμε να "οδηγήσουμε" tests του Qcheck ανάμεσα σε οποιουσδήποτε υπολογιστές του δικτύου.

- *Παράδειγμα 3 για streaming performance.*

Πρόβλημα: η λήψη από το σύστημα τηλε-συνδιάσκεψης (video-conferencing) της εταιρείας παρουσιάζει προβλήματα.

Λύση: ένα test streaming αξιολογεί την δυνατότητα του δικτύου για την υποστήριξη multimedia, ενημερώνοντας παράλληλα για τον ρυθμό με τον οποίο λαμβάνονται τα πακέτα καθώς επίσης και για τον αριθμό αυτών που χάνονται.

- *Παράδειγμα 4 για traceroute.*

Πρόβλημα: η σύνδεση μεταξύ δύο υποκαταστημάτων μιας εταιρείας τα οποία βρίσκονται το πρώτο στην Αθήνα και το δεύτερο στη Σέρρες είναι αρκετά αργή, και εμείς παράλληλα βρισκόμαστε στα Χανιά. Τι μπορούμε να κάνουμε για να λύσουμε το πρόβλημα;

Λύση: ένα test traceroute του Qcheck μπορεί να πραγματοποιηθεί μεταξύ οποιονδήποτε δύο σταθμών εργασίας του δικτύου ανεξαρτήτως της τοποθεσίας τους.

Με βάση λοιπόν όλα τα παραπάνω, πραγματοποιήσαμε κάποια test για να δούμε τα αποτελέσματα τα οποία μας εμφανίζει το Qcheck.
Τα test αυτά πραγματοποιήθηκαν στο Τ.Ε.Ι. Κρήτης Παράρτημα Χανίων.

4.3.1 Test για Response Time (Χρόνος Απόκρισης).

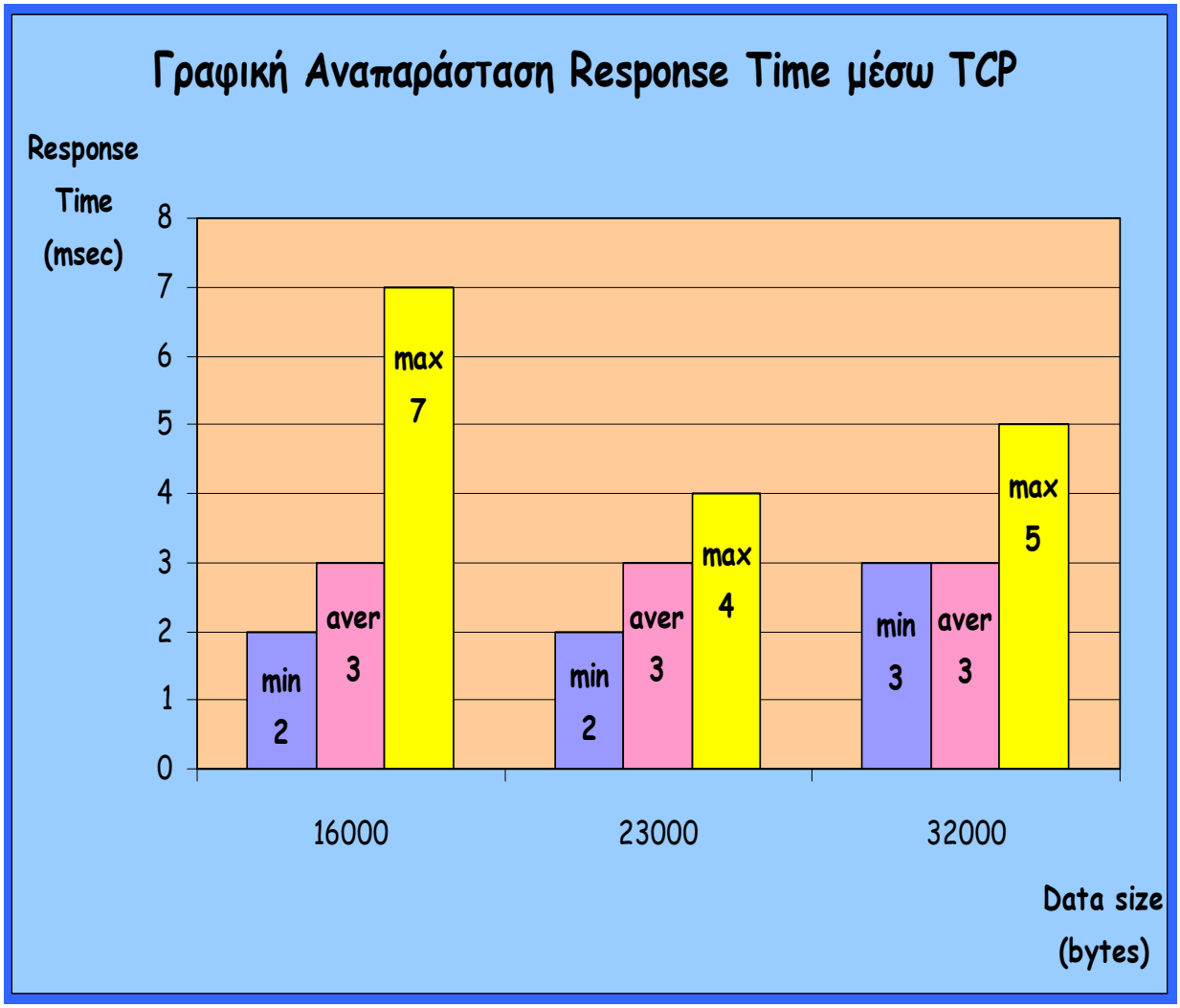
Εισάγουμε τις IP διευθύνσεις στα κατάλληλα πεδία της κονσόλας του Qcheck, τόσο για το endpoint 1 όσο και για το endpoint 2.
Οι IP διευθύνσεις που χρησιμοποιήσαμε για όλα τα test σε ενσύρματο δικτυακό περιβάλλον είναι **194.177.198.246** για το endpoint 1 και **194.177.198.11** για το endpoint 2.

Επιλέγουμε το πρωτόκολλο π.χ. TCP ή UDP και στη συνέχεια το test που στην προκειμένη περίπτωση είναι για το χρόνο απόκρισης.
Ορίζουμε το πεδίο " iterations " από 1 έως 10 και το " data size " από 1 έως 32000 bytes και τέλος πατάμε το κουμπί RUN.(Σχήμα 4.9)

Σχήμα 4.9

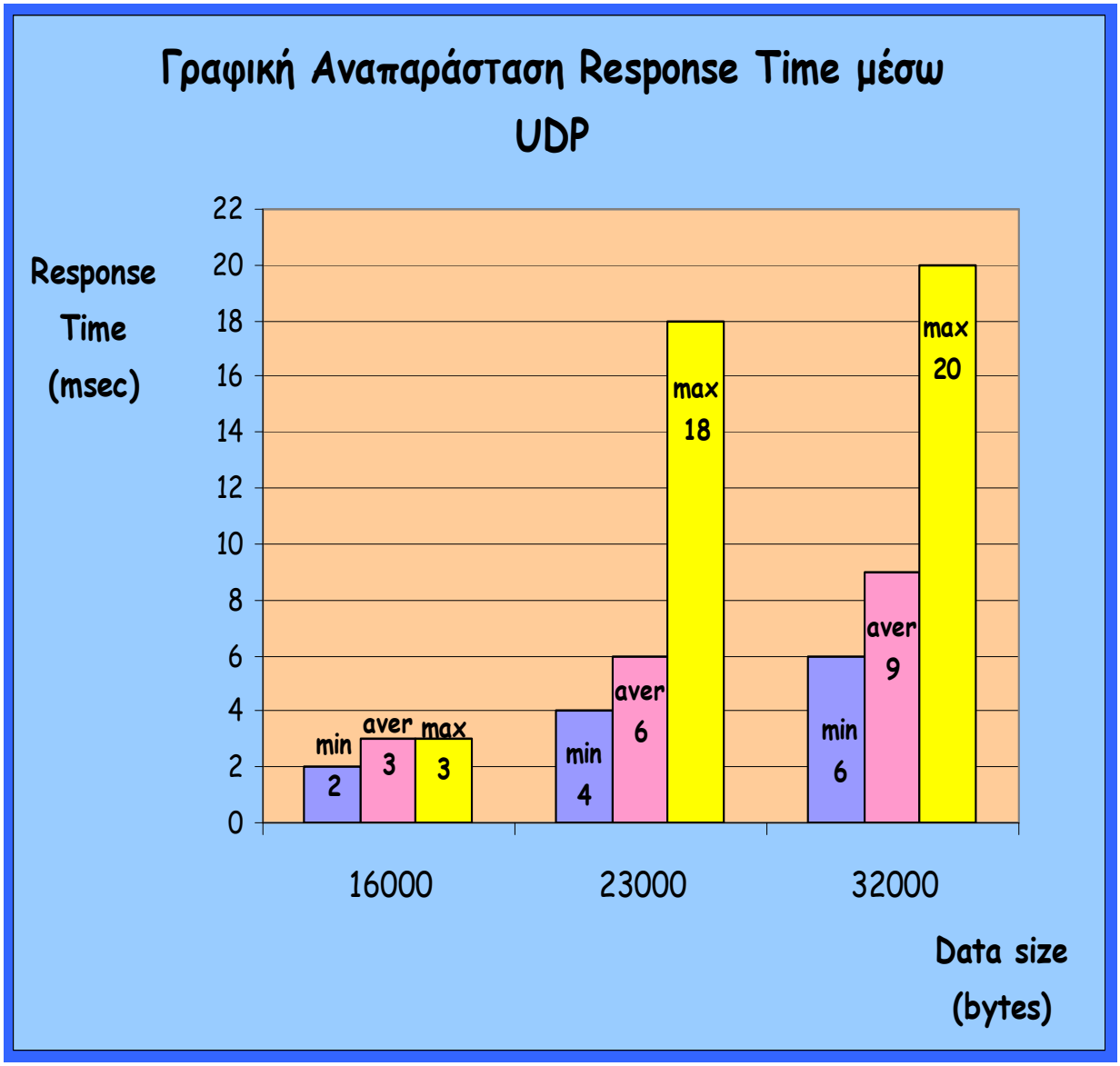
Παρακάτω ακολουθεί γραφική αναπαράσταση των test που πραγματοποιήσαμε, εισάγοντας διαφορετικές τιμές μεγέθους πλαισίου δεδομένων για κάθε πρωτόκολλο (TCP ή UDP) ξεχωριστά(Σχήμα 4.10 και 4.11).

Διάγραμμα Α



Σχήμα 4.10

Διάγραμμα Β



Σχήμα 4.11

4.3.2 Test Throughput.

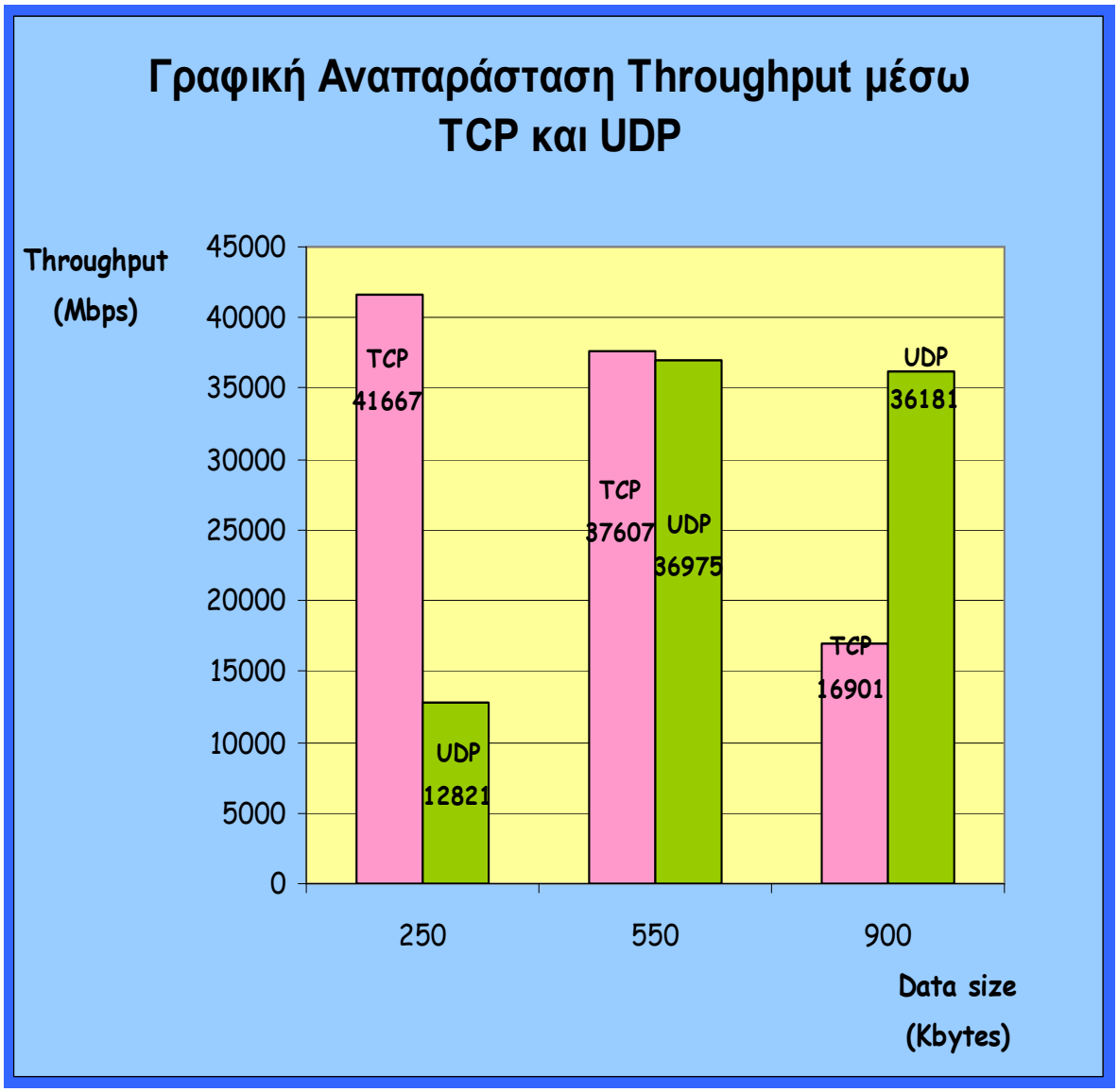
Ακολουθούμε ακριβώς την ίδια διαδικασία.

Αρχικά εισάγουμε τις IP διευθύνσεις και επιλέγουμε το πρωτόκολλο. Έπειτα ορίζουμε το πεδίο " data size " το οποίο εδώ κυμαίνεται από 1 έως 1000 Kbytes, έπειτα επιλέγουμε το κουμπί που είναι για το test throughput και τέλος πατάμε το κουμπί RUN. Σχήμα 4.12

Σχήμα 4.12

Πειραματιστήκαμε εισάγοντας διαφορετικές τιμές μεγέθους πλαισίου δεδομένων στο πεδίο “ data size “ χρησιμοποιώντας και τα δύο πρωτόκολλα (TCP ή UDP). Οι μετρήσεις που πήραμε ακολουθούν στο παρακάτω διάγραμμα.(Σχήμα 13)

Διάγραμμα Γ



Σχήμα 4.13

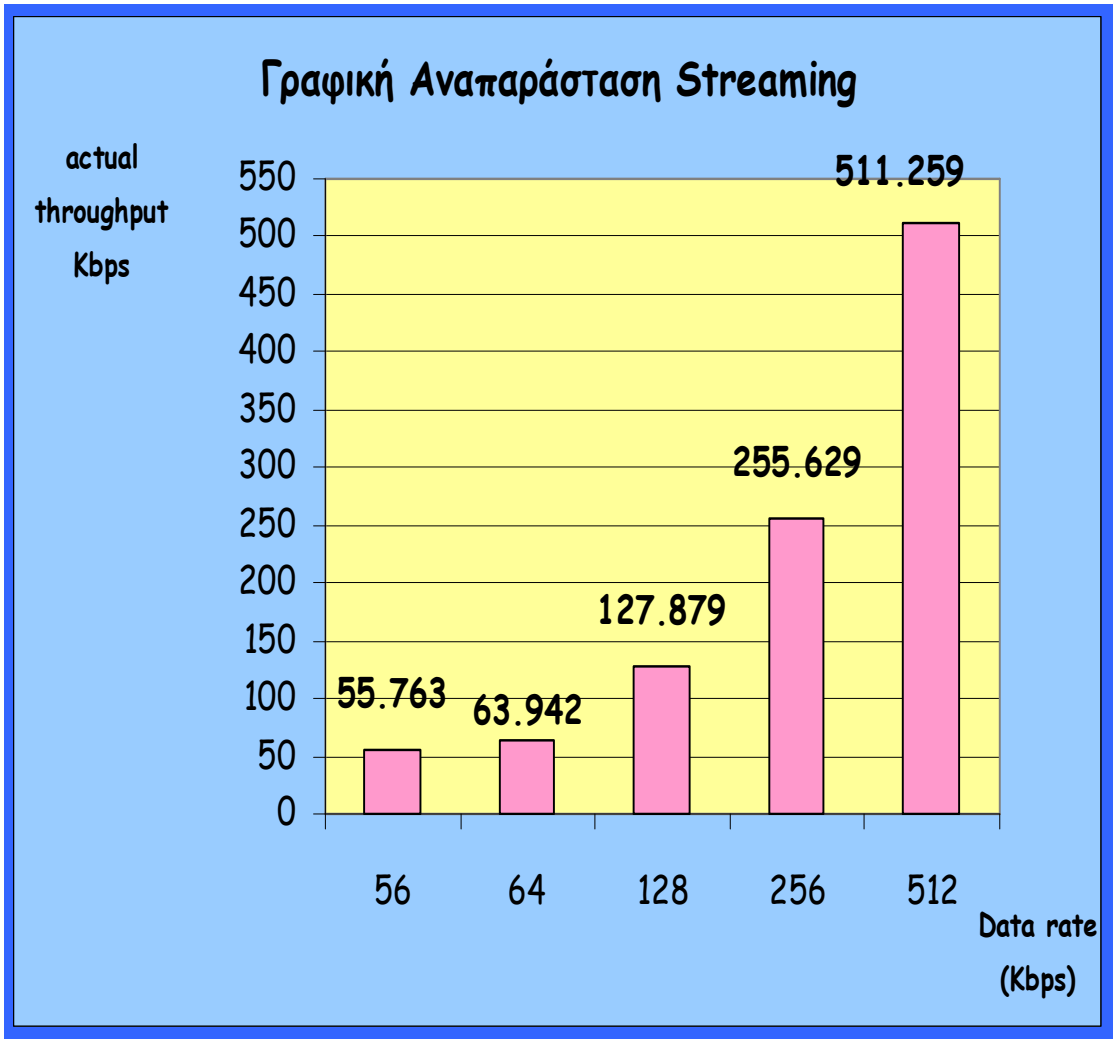
4.3.3 Test streaming performance.

Ακολουθούμε την ίδια πάγια διαδικασία. Εισάγουμε τις IP διευθύνσεις, επιλέγουμε το πρωτόκολλο, στο οποίο έχουμε κάποιο περιορισμό, καθώς μπορούμε να επιλέξουμε μόνο το UDP ή το IPX, έπειτα επιλέγουμε το κουμπί που είναι για το test streaming και τέλος πατάμε το κουμπί RUN.Σχήμα 4.14

Σχήμα 4.14

Χρησιμοποιήσαμε ενδεικτικά κάποιες από τις ταχύτητες τις οποίες έχει σήμερα ένα modem (από 56 έως και 128 Kbps), DSL (από 256 και πάνω) για να αξιολογήσουμε τη δυνατότητα του δικτύου για υποστήριξη multimedia, μιας και η ταχύτητα είναι κάτι που είναι πολύ σημαντικό, καθώς όλο και περισσότεροι χρήστες σήμερα χρησιμοποιούν ISDN ή ακόμα και DSL συνδέσεις για να επιτύχουν την καλύτερη δυνατή ταχύτητα. Τα αποτελέσματα που πήραμε απεικονίζονται στο παρακάτω διάγραμμα. Σχήμα 4.15

Διάγραμμα Δ



Σχήμα 4.15

4.3.4 Test traceroute.

Εφαρμόζουμε την ίδια διαδικασία με τη διαφορά ότι μπορούμε να επιλέξουμε μόνο το πρωτόκολλο TCP ή UDP, πατάμε το κουμπί που είναι για το test traceroute και τέλος το κουμπί RUN.Σχήμα 4.16

Σχήμα 4.16

.

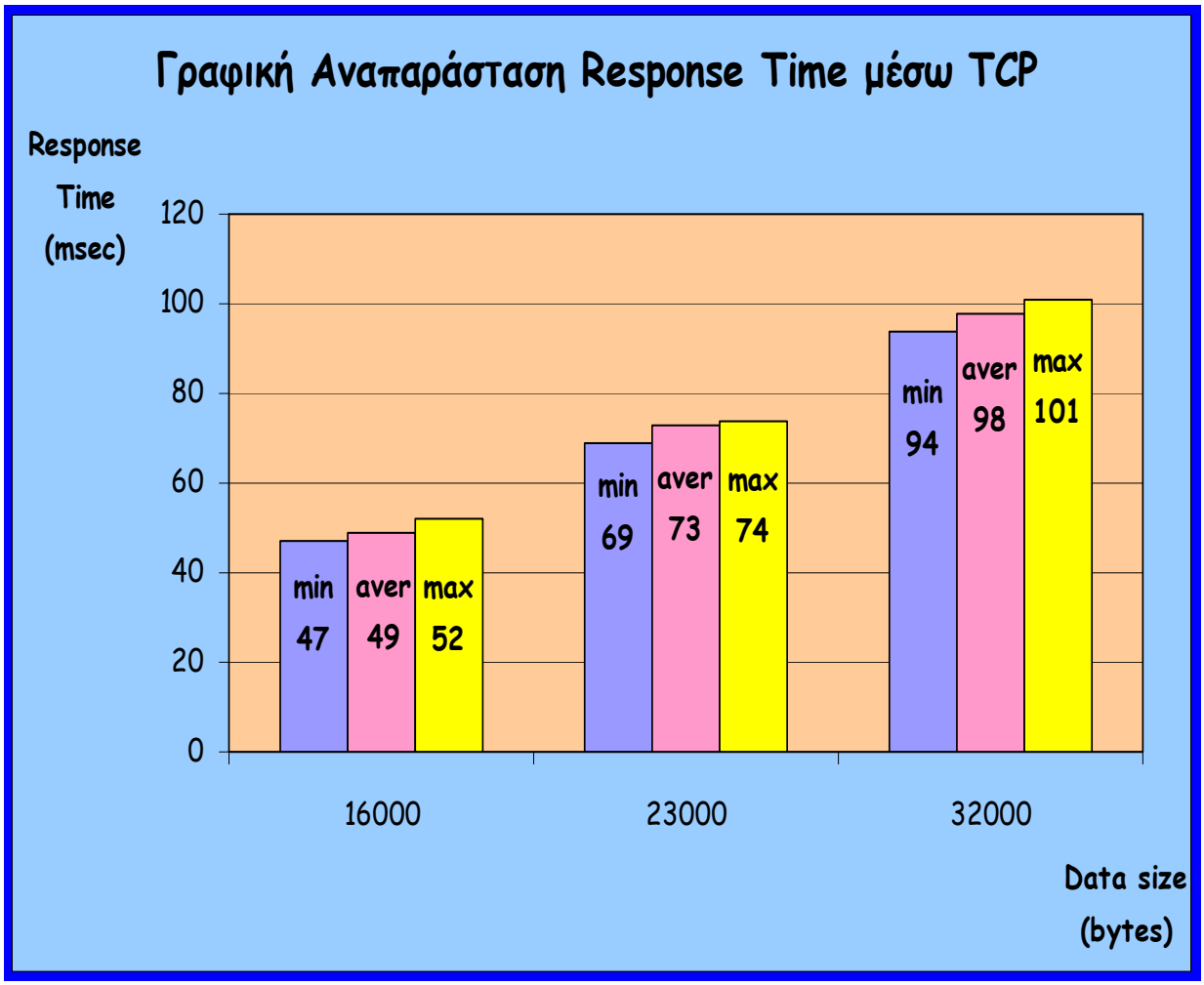
Παρατηρούμε ότι στην κονσόλα του Qcheck εμφανίστηκε το όνομα ενός υπολογιστή με το όνομα " afroditi " . Ο υπολογιστής αυτός δεν είναι άλλος από τον υπολογιστή με IP διεύθυνση 194.177.198.11, καθώς οι δύο υπολογιστές που πραγματοποιήσαμε το test συνδέονται στο ίδιο switch και γι' αυτό το λόγω εμφανίστηκε ένα hop (αναπήδηση).

4.4 **ΕΦΑΡΜΟΓΗ ΣΕ ΑΣΥΡΜΑΤΟ ΔΙΚΤΥΑΚΟ ΠΕΡΙΒΑΛΛΟΝ.**

Εφαρμόσαμε τις ίδιες τιμές μεγέθους πλαισίου δεδομένων που χρησιμοποιήσαμε στο ενσύρματο δικτυακό περιβάλλον, σε ασύρματο δικτυακό περιβάλλον.
Οι IP διευθύνσεις που χρησιμοποιήσαμε είναι για το endpoint 1 194.177.198.84 και 194.177.198.86 για το endpoint 2. Τα test πραγματοποιήθηκαν ξανά στο Τ.Ε.Ι. Κρήτης Παράρτημα Χανίων.
Τα αποτελέσματα των μετρήσεων που πήραμε ακολουθούν στα παρακάτω διαγράμματα.(Σχήμα 4.17 έως 4.20)

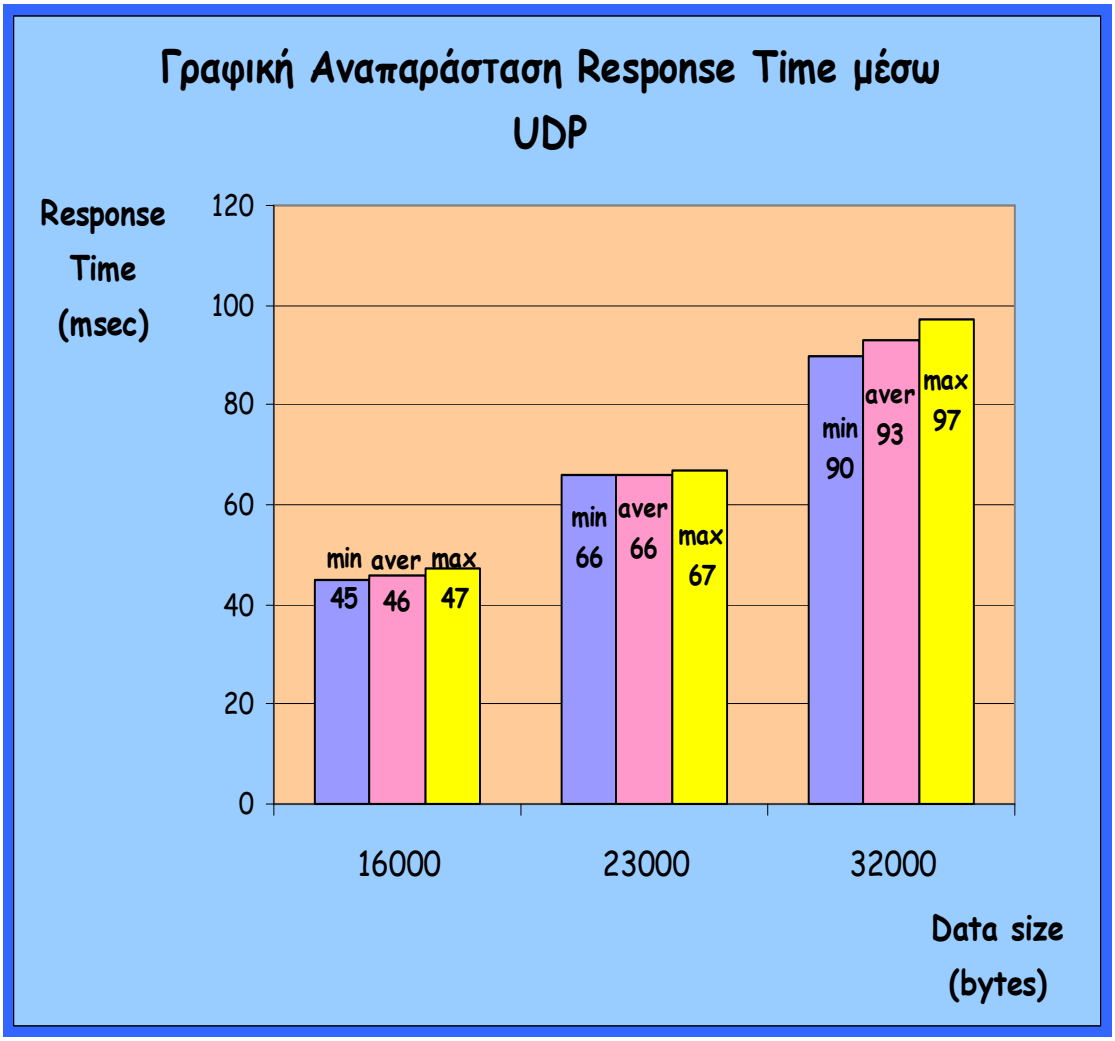
4.4.1 Test για Response Time (Χρόνος Απόκρισης).

Διάγραμμα Α'



Σχήμα 4.17

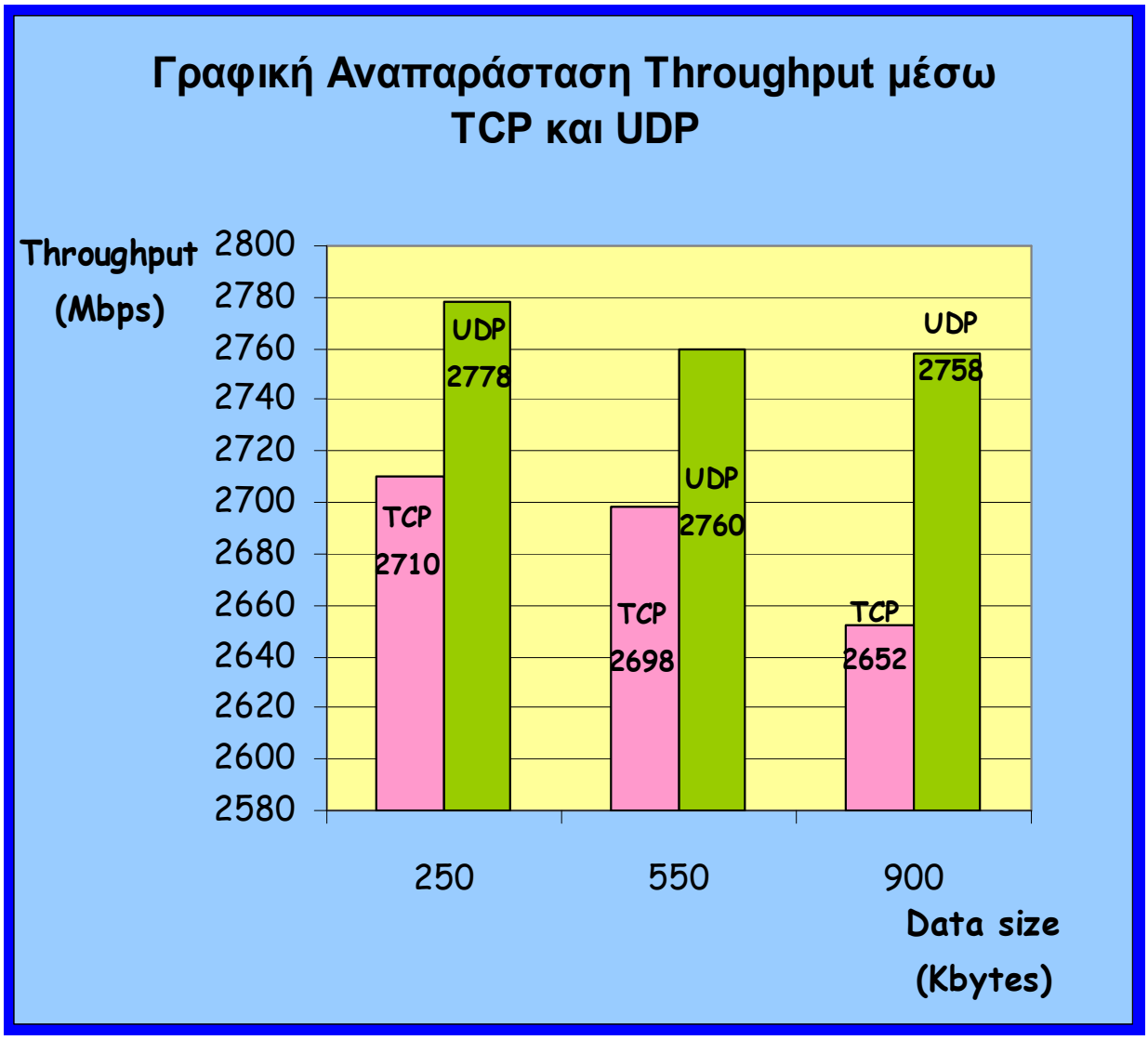
Διάγραμμα Β'



Σχήμα 4.18

4.4.2 Test Throughput.

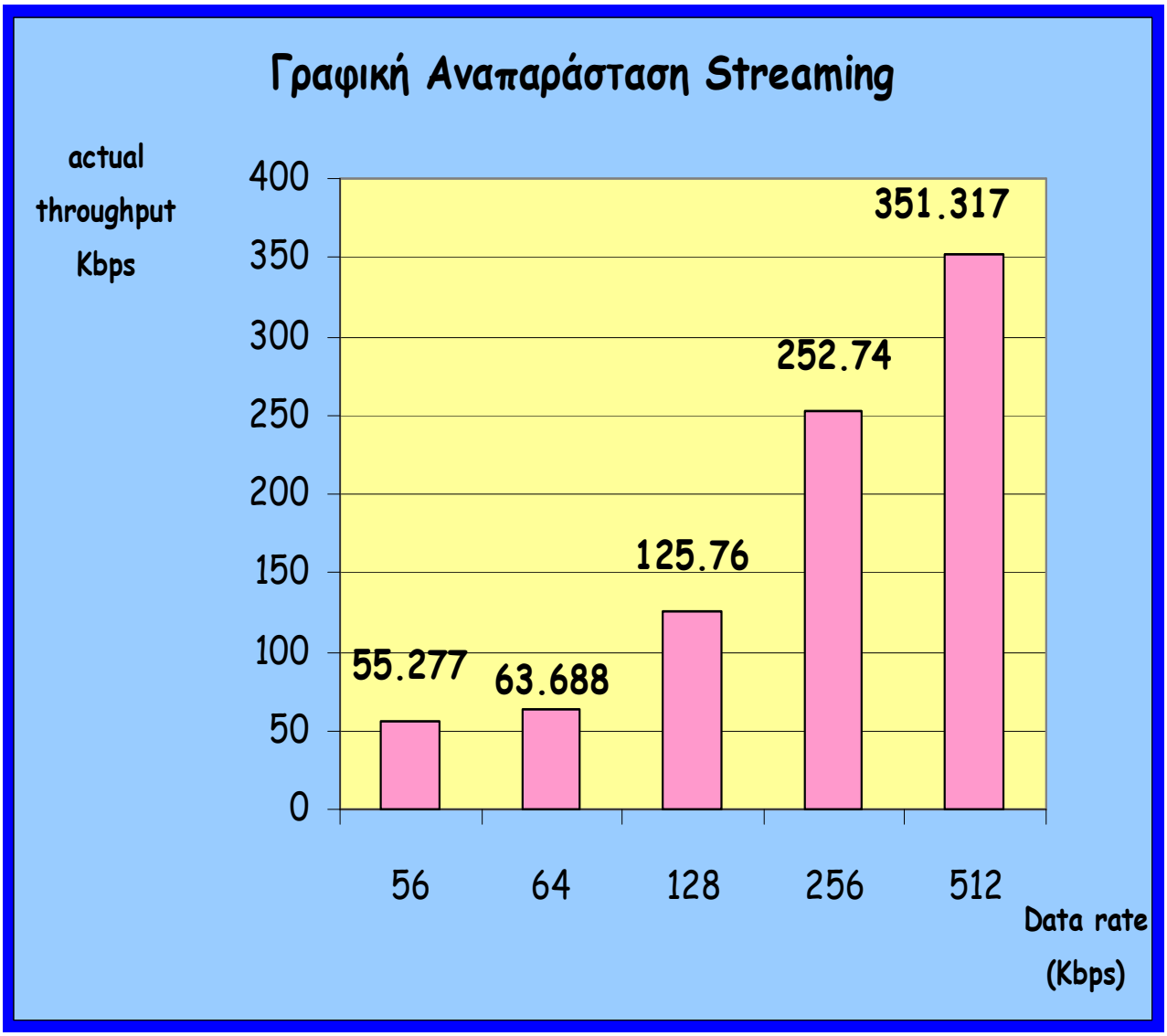
Διάγραμμα Γ'



Σχήμα 4.19

4.4.3Test streaming performance.

Διάγραμμα Δ'



Σχήμα 4.20

4.4.4 Test traceroute

Σχήμα 4.21

Παρατηρούμε στο σχήμα 4.21 ότι επειδή τα δύο endpoints συνδέονται στο ίδιο switch εμφανίζεται ένα hop και το όνομα του υπολογιστή που εμφανίζεται στην κονσόλα του Qcheck είναι του endpoint 2 με IP διεύθυνση 194.177.198.86.

Βιβλιογραφία

- [1]Εισαγωγή στα 'Ασύρματα Δίκτυα', Δρ. Ε. Μ. ΠΑΛΛΗΣ

- [2] Εθνική επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων ΕΕΤΤ, κείμενο δημόσιας διαβούλευσης για τα ασύρματα τοπικά δίκτυα WLAN,Αύγουστος 2006

- [3] Γαζάκη Θ. , Κοντούλη Β. , Τσιλιμίγκρα Κ. (2001) Τμήμα Μηχανικών Η/Υ & Πληροφορικής, Πολυτεχνική Σχολή Πανεπιστήμιο Πατρών

- [4] http://grouper.ieee.org/groups/802/11/index.html

- [5] http://www.wlana.com/

- [6] http://news.wirelessdesignonline.com/wlan-beat/