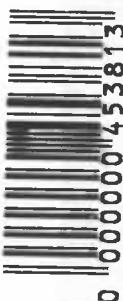


ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

**ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ (MSc)
στα ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ**

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΚΑΤΑΛΟΓΟΣ



ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

**«Μέτρηση και Στατιστική Ανάλυση Επιδόσεων
Ασύρματων Τοπικών Δικτύων IEEE 802.11»**

Οικονόμου Γιώργος

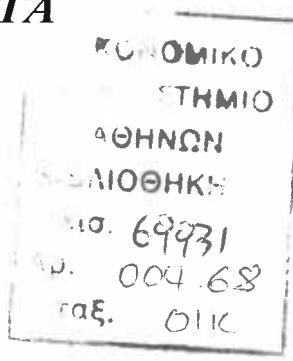
M3000009



ΑΘΗΝΑ, ΣΕΠΤΕΜΒΡΙΟΣ 2001

**ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ (MSc)
στα ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ**

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ



**«Μέτρηση και Στατιστική Ανάλυση Επιδόσεων
Ασύρματων Τοπικών Δικτύων IEEE 802.11»**

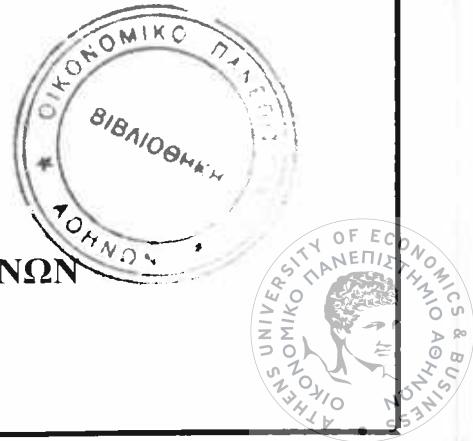
Οικονόμου Γιώργος

M3000009

**Επιβλέπων Καθηγητής: Θεόδωρος Αποστολόπουλος
Εξωτερικός Κριτής: Γεώργιος Πολύζος**

**ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ**

ΑΘΗΝΑ, ΣΕΠΤΕΜΒΡΙΟΣ 2001



EXECUTIVE SUMMARY.

Η εργασία που ακολουθεί συντάχθηκε από τον Γιώργο Οικονόμου, φοιτητή του Μεταπτυχιακού Προγράμματος Σπουδών σε Πληροφοριακά Συστήματα, του τμήματος Πληροφορικής του Οικονομικού Πανεπιστημίου Αθηνών.

Ο επιβλέπων καθηγητής ήταν ο κος Θεόδωρος Αποστολόπουλος, καθηγητής του Οικονομικού Πανεπιστημίου Αθηνών.

Τίτλος της εργασίας ήταν “Μέτρηση και στατιστική ανάλυση επιδόσεων Ασύρματων Τοπικών Δικτύων IEEE 802.11”. Όπως γίνεται φανερό και από τον τίτλο, ο σκοπός της εργασίας ήταν η μέτρηση και η εκτίμηση των επιδόσεων ενός δικτύου τεχνολογίας IEEE 802.11, με σκοπό την ανάλυση της επίδρασης που μπορούν να έχουν, στις επιδόσεις αυτές, μετατροπές σε διάφορες παραμέτρους λειτουργίας του δικτύου.

Για τον σκοπό αυτό, στο εργαστήριο Συστημάτων Υπολογιστών και Επικοινωνιών του Οικονομικού Πανεπιστημίου Αθηνών, εγκαταστάθηκε ένα infrastructure δίκτυο της τεχνολογίας αυτής.

Το δίκτυο αποτέλεσαν δύο υπολογιστές εφοδιασμένοι με κάρτες δικτύου τεχνολογίας IEEE 802.11b, ένα Access Point και ένας υπολογιστής εφοδιασμένος με Fast Ethernet κάρτα δικτύου. Οι υπολογιστές αυτοί, μέσω ενός HUB, διασυνδέθηκαν με το υπόλοιπο τοπικό δίκτυο του εργαστηρίου.

Το πρότυπο IEEE 802.11, άρχισε να αναπτύσσεται από το Institute for Electrical and Electronic Engineers, το έτος 1991 και ολοκληρώθηκε το 1997. Προδιαγράφει την λειτουργία Ασύρματων Τοπικών Δικτύων στην ζώνη συχνοτήτων των 2.4 GHz και με ταχύτητες 1Mbps και 2Mbps. Ο πλήρης τίτλος είναι “*Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*”.

Μέχρι το 1999, εκδόθηκαν δύο συμπληρωματικά πρότυπα, το IEEE 802.11b, και IEEE 802.11a που προβλέπουν ταχύτητες λειτουργίας μέχρι 11Mbps και 54Mbps αντίστοιχα.

Όπως φαίνεται και από τον τίτλο του προτύπου, το πρότυπο ασχολείται με το φυσικό επίπεδο και με το επίπεδο MAC. Καθορίζονται οι τύποι και οι δομή των πλαισίων επιπέδου MAC και των πακέτων του φυσικού επιπέδου. Επίσης καθορίζονται οι τεχνικές διαμόρφωσης σήματος, που είναι οι Frequency Hopping Spread Spectrum – FHSS, Direct Sequence Spread Spectrum – DSSS, High Rate DSSS και Orthogonal Frequency Division Multiplexing – OFDM.

Η μέθοδος πρόσβασης στο μέσο ονομάζεται Carrier Sense Medium Access / Collision Avoidance – CSMA/CA. Οι κεραίες που χρησιμοποιούνται δεν έχουν την



ικανότητα να καταλάβουν ότι συνέβη μια σύγκρουση, αν ταυτόχρονα μεταδίδουν δεδομένα. Για τον λόγο αυτό δεν μπορεί να χρησιμοποιηθεί η ανακάλυψη συγκρούσεων (Collision Detection) που χρησιμοποιείται στο πρότυπο IEEE 802.3. Έτσι, χρησιμοποιείται η αποφυγή συγκρούσεων, η οποία επιτυγχάνεται με ένα διάνυσμα (Network Allocation Vector – NAV) που διατηρούν οι σταθμοί και το οποίο τους βοηθά να γνωρίζουν πότε το μέσο είναι κατειλημμένο και πότε όχι. Με τον τρόπο αυτό τους παρέχεται η δυνατότητα να γνωρίζουν αν μπορούν να μεταδώσουν ή όχι.

Το πρότυπο καθορίζει, επίσης, τοπολογίες που μπορούν να χρησιμοποιηθούν για να εγκαταστήσουμε ένα ασύρματο τοπικό δίκτυο αυτής της τεχνολογίας. Οι τοπολογίες αυτές είναι οι Ad – Hoc και η Infrastructure.

Παρά τον καθορισμό των τοπολογιών, δεν γίνεται καμία αναφορά στο πώς ένας σταθμός μπορεί να μεταφέρεται, γεωγραφικά, και να μπορεί ταυτόχρονα να διατηρεί ανοιχτές τις ήδη εγκατεστημένες συνδέσεις που έχει. Την λύση σε αυτό δίνει το πρωτόκολλο Mobile IP και το Inter Access Point Protocol – IAPP.

Στο κείμενο που ακολουθεί γίνεται μια εκτενής επισκόπηση του προτύπου, με λεπτομερή αναφορά σε όλα όσα αναφέρθηκαν ως εδώ σε αυτή την περίληψη.

Συνεχίζοντας, περνάμε στο πρακτικό μέρος, δηλαδή στην μέτρηση και την στατιστική ανάλυση των επιδόσεων.

Αυτό που θελήσαμε να παρατηρήσουμε, ήταν κατά πόσο η μεταβολή ορισμένων παραμέτρων θα επηρέαζε την απόδοση του συστήματος. Αυτές οι παράμετροι ήταν η τοπολογία, κάποια αντικείμενα της IEEE 802.11 MIB, τα λειτουργικά συστήματα και η ύπαρξη εμποδίων.

Από τις διαθέσιμες μεθόδους, αυτή που θεωρήθηκε πιο κατάλληλη ήταν η Bulk Transfer Capacity. Για τον λόγο αυτό χρησιμοποιήσαμε τρία εργαλεία, τα TTCP, NetPerf και iPerf. Συγκεκριμένα, για το TTCP, κάναμε και μετατροπές στον κώδικα, ώστε τα αποτελέσματα να αποθηκεύονται σε Log αρχεία.

Με τα εργαλεία αυτά μεταδώσαμε 16MByte δεδομένων και μετρήσαμε την καθυστέρηση. Αυτή η μέτρηση επαναλήφθηκε 100 φορές σε κάθε πείραμα. Στο τέλος κάθε πειράματος υπολογίσαμε την μέση καθυστέρηση, την διακύμανση καθυστέρησης και την μέση ρυθμοαπόδοση. Επαναλαμβάναμε το ίδιο πείραμα, αλλάζοντας κάθε φορά μία από τις παραμέτρους που αναφέρθηκαν παραπάνω.

Έχοντας συγκεντρώσει όλα τα δεδομένα από τα έντεκα πειράματα που προέκυψαν, δημιουργήσαμε προς έλεγχο έξι στατιστικές υποθέσεις. Η καθεμία από αυτές αναφερόταν στην επίδραση μιας συγκεκριμένης παραμέτρου στις επιδόσεις του δικτύου. Ο έλεγχος των

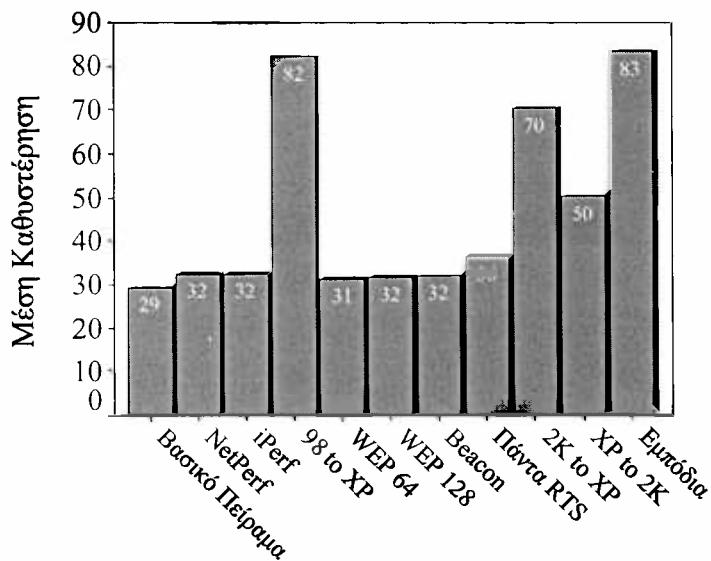


υποθέσεων αυτών έγινε με την χρήση της θεωρίας ελέγχου υποθέσεων. Συγκεκριμένα χρησιμοποιήθηκαν τα εξής test.

- Box – Plot διαγράμματα,
- test Levene για ομοιογένεια διακυμάνσεων δύο πληθυσμών,
- t – test για ισότητα μέσων δύο ανεξάρτητων πληθυσμών,
- Ανάλυση Διακύμανσης (AN.O.VA) κατά έναν παράγοντα,
- Games – Howell Post – Hoc test πολλαπλών συγκρίσεων.

Από την εκτέλεση των παραπάνω ελέγχων προέκυψαν ορισμένα πάρα πολύ χρήσιμα συμπεράσματα.

Ένα πρώτο είναι ότι η επίδοση ενός δικτύου IEEE 802.11, μειώνεται αισθητά στην περίπτωση που, στο ένα άκρο, υπάρχει υπολογιστής με Windows XP και κυρίως όταν αυτός ο υπολογιστής είναι ο παραλήπτης των δεδομένων.



Κατηγορία

Στο παραπάνω ραβδόγραμμα, τα τρία πειράματα που παρουσιάζουν μέση καθυστέρηση πάνω από 50 sec, είναι αυτά στα οποία συμμετέχει ο υπολογιστής με τα Windows XP. Επιπλέον, στο πείραμα με την μικρότερη μέση καθυστέρηση από τα τρία, ο εν λόγω υπολογιστής ήταν αποστολέας πακέτων, ενώ στα άλλα τρία ήταν παραλήπτης.

Ένα δεύτερο πολύ χρήσιμο συμπέρασμα που βγάλαμε είναι ότι η απόσταση και η ύπαρξη εμποδίων δεν επηρεάζει, στατιστικά σημαντικά, τις επιδόσεις του δικτύου.

Από τις παραμέτρους της IEEE 802.11 MIB, η τόσο η χρήση WEP, όσο και η ενεργοποίησης του RTS/CTS Handshaking για όλα τα πλαίσια, επηρεάζουν τις επιδόσεις

του δικτύου. Ωστόσο η διαφορά της μέσης καθυστέρησης στην περίπτωση WEP 64bit από την περίπτωση WEP 128bit, είναι αμελητέα.

Τα συμπεράσματα αυτά είναι πολύ ενδιαφέροντα αλλά δεν μπορεί να παραβλέψει κανείς το γεγονός ότι όλες οι μετρήσεις έγιναν σε ένα πολύ μικρό δίκτυο. Η αύξηση του μεγέθους του δικτύου θα μπορούσε να αλλάξει τις συνθήκες λειτουργίας κατά τρόπο τέτοιον που τα παραπάνω συμπεράσματα να αλλάξουν. Για παράδειγμα, η απενεργοποίηση του RTS/CTS, οδηγεί σε αισθητή μείωση της μέσης καθυστέρησης. Σε ένα δίκτυο με πολλούς κόμβους, θα μπορούσε να οδηγεί σε αύξηση του αριθμού συγκρούσεων και επαναμεταδόσεων, με τελική συνέπεια η μέση καθυστέρηση να αυξηθεί.

Επίσης, σε ένα δίκτυο μεγάλων διαστάσεων, ενδέχεται κατά την μέτρηση των επιδόσεων, κάποιοι άλλοι σταθμοί να πραγματοποιούν μεταφορές δεδομένων, χρησιμοποιώντας υπηρεσίες FTP, Web, e - mail κλπ. Οι μετρήσεις που πραγματοποιήσαμε έγιναν με τους σταθμούς αποκομμένους από το δίκτυο του εργαστηρίου. Έτσι εξασφαλίσαμε ότι δεν υπήρχε άλλος φόρτος στο δίκτυο εκτός από αυτόν που εισάγαμε με τις εφαρμογές των μετρήσεων. Θα ήταν ενδιαφέρον να εκτιμηθεί η επίδραση της επικοινωνίας μεταξύ δύο σταθμών, στην καθυστέρηση που παρουσιάζει η επικοινωνία μεταξύ δύο άλλων.

Μία τελευταία πρόταση για περαιτέρω έρευνα είναι η πραγματοποίηση παρόμοιων μετρήσεων σε δίκτυο τεχνολογίας IEEE 802.11a.

ΠΕΡΙΛΗΨΗ ΣΤΗΝ ΑΓΓΛΙΚΗ.

The following Master's thesis was composed by George Oikonomou, post graduate student of the MSc programme in Information Systems, Athens University of Economics and business.

The supervising professor was professor Theodoros Apostolopoulos, professor of the Athens University of Economics and business.

The title of this project was "Measurement and Statistical Analysis of the Performance of IEEE 802.11 Wireless Local Area Networks". The title reveals the scope of the project, which was to estimate the performance of an IEEE 802.11 compliant network, in order to analyze the impact of various parameters on the aforementioned performance.

For the reason stated in the above paragraph, we installed an infrastructure, IEEE 802.11 network, at the Communications and Computer Systems Laboratory (ccslab).

The network was comprised of an access point, two PCs with IEEE 802.11b Network Interface Cards (NICs) and a PC with an Ethernet NIC. All three PCs were connected with the rest of the lab's Local Area Network through a fast Ethernet HUB.

Works on the IEEE 802.11 standard began in 1991 by the Institute of Electrical and Electronic Engineers. The standard was completed in 1997. It specifies the functionality of Wireless Local Area Networks in the 2.4GHz band of radio frequencies, with transmit capabilities of up to 2Mbits per second. The full title is "*Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*".

In the year 1999, two supplements to the standard were published. They were IEEE 802.11b and later IEEE 802.11a. The two supplements allow transmission speeds of up to 11Mbps and 54Mbps, respectively.

The title of the standard makes it perfectly clear, that the specification deals with the two lowest layers of the protocol stack, that is to say, the MAC and physical layers. The types and structure of MAC frames and physical layer packets are well defined. Furthermore, the following modulation techniques are defined: Frequency Hopping Spread Spectrum – FHSS, Direct Sequence Spread Spectrum – DSSS, High Rate DSSS and Orthogonal Frequency Division Multiplexing – OFDM.

The function, which provides access to the medium, is called Carrier Sense Multiple Access with Collision Avoidance – CSMA/CA. The antennas used to transmit data are not capable to detect a collision while transmitting. For this reason, it is impossible to tell that a collision has taken place until, after the entire frame has been transmitted. As a result,



collision detection, as in the IEEE 802.3 standard, cannot be implemented. Therefore, there is the need to use collision avoidance.

In order to achieve that, two mechanisms are used. The first one is called physical mechanism and the second is called virtual. Using a Network Allocation Vector – NAV, the stations may know whether the medium is busy or not, at any given moment. This way, they know if they may transmit.

Apart from the MAC and physical layers, the standard defines LAN topologies. The two topologies are called Ad – Hoc and infrastructure.

However well topologies may be defined, there is absolutely no reference as to how a station may become mobile, without disrupting any ongoing connections. The solution to that is provided by the Inter Access Point Protocol, in combination with Mobile IP.

The following text describes the standard and everything else that has been mentioned, so far, in this summary.

The remainder of this report deals with the actual installation of the network and with the measurement of its performance.

What we wished to observe was, how modifying some functional parameters, would affect the performance of the system. These parameters were the topology, the Operating Systems, some objects of the IEEE 802.11 MIB and the existence of obstacles within the transmission path.

From the variety of available methods, we deemed Bulk transfer Capacity to be the most appropriate. That is the reason why we used the tools TTCP, NetPerf and iPerf. Specifically for TTCP we made a few modifications to the original source code, in order to save results in log files.

With the aforementioned tools, we transmitted 16 Mbytes of data and measured the delay. The measurement was repeated 100 times for each experiment. At the end of each experiment, we calculated the mean delay, the variance of delay and the average throughput. The same experiment was repeated, each time changing one of the aforementioned parameters. Thus, we ended with eleven experiments.

Having concentrated all the data from the experiments, we defined six statistical hypotheses. Each one of them referred to the effect of one of the parameters. In order to test them, we used the following tests.

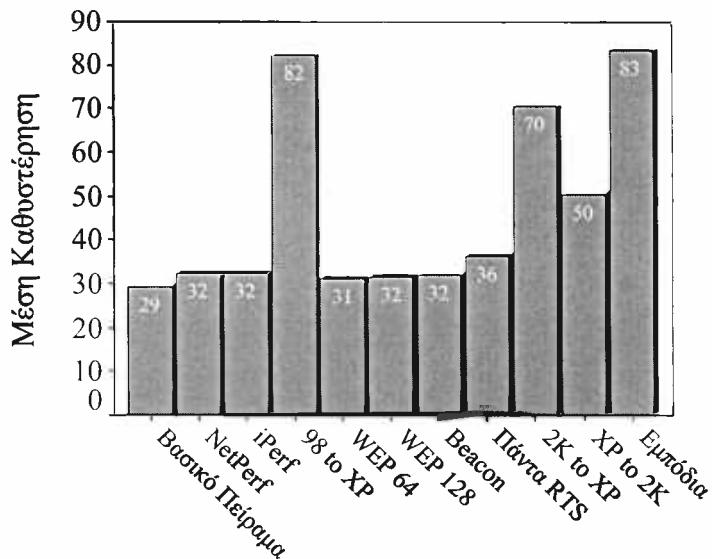
- Box – Plot diagrams,
- test Levene for homogeneity of variances,
- t – test for equality of means,
- one way Analysis of Variance (AN.O.VA),

- Games – Howell Post – Hoc test.

Many useful conclusions were drawn, after we performed the above tests.

One of them says that the performance of an IEEE 802.11 LAN is degraded when either the sender or the receiver is a Windows XP PC.

In the following bar chart, the y – axis displays the mean delay and the x – axis the experiment.



Κατηγορία

In all four experiments, where the observed mean delay was over 50 sec, the one PC was the Windows XP PC. Furthermore, in the three of them, this PC was on the server side of the measurements.

Another very useful conclusion is that obstacles only affect the strength of the signal but not the performance.

Among the MIB parameters, both using WEP and using RTS/CTS handshaking, have a negative effect on performance. However, using WEP 128 does not cause more delay than using WEP 64bit.

All of the above conclusions are indeed very important, but one cannot ignore the fact that they were all observed in a small sized LAN. Adding more stations to the network might change things radically. For example, disabling RTS/CTS handshaking leads to a decrease of delay. In a many – station network, this might lead to a larger number of collisions and, probably, to a completely different result.

Furthermore, in the case of a large network it is more than certain that there is going to be background activity. That is to say that, while two stations are performing

measurements, other stations will be exchanging data, using services such as FTP or Web. In our case, all four stations were separated from the rest of the laboratory's LAN and, therefore, it was easy to make sure that there would be no background activity. However, it would be very interesting to see, how the communication between two stations affects the delay of the communication between two others.

Last but no least, we propose that, for further research, the performance of IEEE 802.11a LANs be measured and analysed in a similar manner.



ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ.

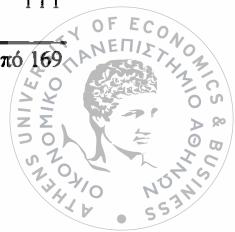
EXECUTIVE SUMMARY.	1
ΠΕΡΙΛΗΨΗ ΣΤΗΝ ΑΓΓΛΙΚΗ.	5
ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ.	9
ΕΥΡΕΤΗΡΙΟ ΠΙΝΑΚΩΝ.	15
ΕΥΡΕΤΗΡΙΟ ΣΧΗΜΑΤΩΝ.	16
ΕΥΡΕΤΗΡΙΟ ΤΥΠΩΝ.	18
ΕΙΣΑΓΩΓΗ.	19
ΕΥΧΑΡΙΣΤΙΕΣ.	21
 Μέρος 1 ^ο : Εισαγωγή στα ασύρματα τοπικά δίκτυα. και το πρότυπο IEEE 802.11.	22
1 ΑΣΥΡΜΑΤΑ ΤΟΠΙΚΑ ΔΙΚΤΥΑ (WIRELESS LAN).	22
1.1 ΠΡΟΔΙΑΓΡΑΦΕΣ ΑΣΥΡΜΑΤΩΝ ΤΟΠΙΚΩΝ ΔΙΚΤΥΩΝ.	22
1.1.1 HiperLAN.	22
1.1.2 Bluetooth.	22
1.1.3 IEEE 802.11.	23
1.2 ΙΔΙΑΙΤΕΡΟΤΗΤΕΣ ΤΩΝ ΑΣΥΡΜΑΤΩΝ ΤΟΠΙΚΩΝ ΔΙΚΤΥΩΝ.	23
1.2.1 Διασπορά πολλαπλών μονοπατιών.	23
1.2.2 Παρεμβολές.	23
1.2.3 Χρόνος ζωής μπαταρίας.	24
1.2.4 Διαλειτουργικότητα.	25
1.2.5 Ασφάλεια.	25
1.2.6 Ακαταλληλότητα TCP/IP.	25
1.2.7 Θέματα εγκατάστασης.	26
1.2.8 Θέματα υγείας.	26
1.3 ΤΕΧΝΙΚΕΣ ΔΙΑΜΟΡΦΩΣΗΣ ΣΗΜΑΤΟΣ.	27
1.3.1 Frequency Hopping Spread Spectrum – FHSS.	27
1.3.2 Direct Sequence Spread Spectrum – DSSS.	28
1.3.3 Orthogonal Frequency Division Multiplexing – OFDM.	29
1.3.4 Υπέρυθρες Ακτίνες.	29
1.4 ΤΟΠΟΛΟΓΙΕΣ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ.	30
1.4.1 Εξαρτήματα δικτύου.	30
1.4.1.1 Κάρτες δικτύου (Network Interface Card – NIC).	30
1.4.1.2 Ασύρματες γέφυρες.	30
1.4.2 Ασύρματα τοπικά δίκτυα.	31
1.4.2.1 Peer to Peer.	31
1.4.2.2 Πολλαπλών κελιών.	31
1.4.3 Ασύρματα μητροπολιτικά δίκτυα.	32
1.4.3.1 Δίκτυα Σημείου σε Σημείο (Point to Point) βασισμένα σε ραδιοκύματα.	32
1.4.3.2 Δίκτυα Σημείου σε Σημείο βασισμένα σε Laser.	33
1.4.3.3 Δίκτυα Σημείου σε Πολλαπλά Σημεία.	33
2 ΤΟ ΠΡΟΤΥΠΟ ΙΕΕΕ 802.11.	35
2.1 Η ΟΙΚΟΓΕΝΕΙΑ ΠΡΟΤΥΠΩΝ ΙΕΕΕ 802.	35
2.2 ΙΣΤΟΡΙΚΟ ΤΟΥ ΙΕΕΕ 802.11.	36
2.3 ΕΙΣΑΓΩΓΗ ΣΤΟ ΙΕΕΕ 802.11.	37
2.3.1 Ο πλήρης τίτλος.	37
2.3.2 Τα περιεχόμενα του προτύπου.	37
2.4 ΟΙ ΣΥΝΕΠΕΙΕΣ ΤΗΣ ΙΔΙΟΜΟΡΦΙΑΣ ΤΩΝ WLAN.	38



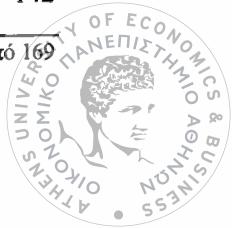
2.4.1	Διαχείριση ισχύος.	38
2.4.2	Εύρος ζώνης.	39
2.4.3	Διευθύνσεις.	39
2.4.4	Ο αντίκτυπος του μέσου στον σχεδιασμό.	39
2.4.5	Αλληλεπίδραση με τα υπόλοιπα επίπεδα IEEE 802.	40
2.5	ΤΟΠΟΛΟΓΙΕΣ ΚΑΤΑ ΤΟ IEEE 802.11.	40
2.5.1	Independent Basic Service Set (IBSS) Δίκτυο.	40
2.5.2	Extended Service Set (ESS) Δίκτυο.	40
2.5.2.1	Μεταβάσεις (Transitions).	41
2.5.2.2	Επικαλύψεις μεταξύ των συνιστωσών.	42
2.6	ΛΟΓΙΚΗ ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ IEEE 802.11.	42
2.7	ΥΠΗΡΕΣΙΕΣ.	43
2.7.1	Υπηρεσίες Σταθμού.	43
2.7.1.1	Αυθεντικοποίηση (Authentication).	43
2.7.1.2	Deauthentication.	43
2.7.1.3	Privacy.	43
2.7.2	Υπηρεσίες Συστήματος Διανομής.	44
2.7.2.1	Association.	44
2.7.2.2	Disassociation.	44
2.7.2.3	Reassociation.	44
2.7.2.4	Integration.	44
2.7.2.5	Distribution.	44
Μέρος 2 ^ο : Τα επίπεδα MAC και Φυσικό κατά το πρότυπο IEEE 802.11.		45
3	ΤΟ ΦΥΣΙΚΟ ΕΠΙΠΕΔΟ ΣΤΟ ΠΡΟΤΥΠΟ IEEE 802.11.	45
3.1	Η ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ ΦΥΣΙΚΟΥ ΕΠΙΠΕΔΟΥ.	45
3.1.1	Physical Layer Convergence Procedure – PLCP.	46
3.1.2	Physical Medium Dependent – PMD.	46
3.2	ΟΙ ΛΕΙΤΟΥΡΓΙΕΣ ΤΟΥ ΦΥΣΙΚΟΥ ΕΠΙΠΕΔΟΥ.	46
3.2.1	Carrier Sense.	46
3.2.2	Αποστολή.	47
3.2.3	Λήψη.	47
3.3	ΤΑ ΠΕΝΤΕ ΦΥΣΙΚΑ ΕΠΙΠΕΔΑ ΚΑΤΑ IEEE 802.11.	47
3.3.1	Frequency Hopping Spread Spectrum – FHSS.	48
3.3.1.1	Η Λειτουργία Frequency Hopping.	49
3.3.1.2	Λειτουργία Διαμόρφωσης Συχνότητας (Frequency Modulation Function).	50
3.3.2	Direct Sequence Spread Spectrum – DSSS, High Rate DSSS – HR DSSS.	50
3.3.2.1	Η Λειτουργία Direct Sequence.	52
3.3.2.2	Λειτουργία Διαμόρφωσης Συχνότητας (Frequency Modulation Function).	53
3.3.3	Orthogonal Frequency Division Multiplexing – OFDM.	54
3.3.3.1	Η λειτουργία του OFDM.	55
3.3.4	Infrared (IR) Physical Layer.	57
3.3.4.1	Η λειτουργία του IR.	58
4	ΤΟ ΕΠΙΠΕΔΟ MAC ΣΤΟ ΠΡΟΤΥΠΟ IEEE 802.11.	60
4.1	ΟΙ ΛΕΙΤΟΥΡΓΙΕΣ ΤΟΥ ΕΠΙΠΕΔΟΥ MAC.	60
4.1.1	Πρόσβαση στο μέσο.	60
4.1.1.1	Carrier Sense Multiple Access / Collision Avoidance – CSMA/CA.	60
4.1.1.2	Πρόσβαση Βάσει Προτεραιοτήτων (Priority Based Access).	63

4.1.2	Σύνδεση με το δίκτυο.	64
4.1.3	Authentication and Privacy.	65
4.1.3.1	Αυθεντικοποίηση Ανοικτού Συστήματος (Open System Authentication).	65
4.1.3.2	Αυθεντικοπόηση Μυστικού Κλειδιού (Shared Key Authentication).	65
4.1.3.3	Wireless Equivalent Privacy – WEP.	66
4.2	Η ΔΟΜΗ ΤΩΝ MAC ΠΛΑΙΣΙΩΝ.	67
4.2.1	Το πεδίο Frame Control.	67
4.2.1.1	Protocol Version.	68
4.2.1.2	Type.	68
4.2.1.3	Subtype.	68
4.2.1.4	To DS.	68
4.2.1.5	From DS.	69
4.2.1.6	More Frag.	69
4.2.1.7	Retry.	69
4.2.1.8	Power Management.	69
4.2.1.9	More Data.	69
4.2.1.10	WEP.	69
4.2.1.11	Order.	69
4.2.2	Duration / ID.	69
4.2.3	Address.	70
4.2.4	Sequence Control.	70
4.2.5	Frame Body.	70
4.2.6	Frame Check sequence – FCS.	70
4.3	ΤΥΠΟΙ MAC ΠΛΑΙΣΙΩΝ.	71
4.3.1	Πλαίσια Διαχείρισης.	71
4.3.2	Πλαίσια Ελέγχου.	73
4.3.2.1	Request To Send – RTS.	74
4.3.2.2	Clear To Send – CTS.	75
4.3.2.3	Acknowledgement – ACK.	75
4.3.2.4	Power Save Poll – PS Poll.	75
4.3.2.5	Contention Free End – CF End.	75
4.3.2.6	CF End + CF ACK.	76
4.3.3	Πλαίσια Δεδομένων.	76
Μέρος 3 ^ο : Ειδικά θέματα δικτύων.		77
5	ΜΕΤΑΦΕΡΣΙΜΟΤΗΤΑ ΣΤΑΘΜΩΝ.	77
5.1	MOBILE IP.	77
5.1.1	Οι Απαιτήσεις του Mobile IP.	77
5.1.2	Οι Συνιστώσεις του Mobile IP.	78
5.1.2.1	Mobile Node.	78
5.1.2.2	Home Agent.	78
5.1.2.3	Foreign Agent.	79
5.1.2.4	Tunneling..	79
5.1.3	Home Address, Home Link, Home Agent.	80
5.1.4	Care – of Address, Foreign Link, Foreign Agent.	80
5.1.4.1	Οι τύποι των Care – of διευθύνσεων.	81
5.1.5	Η λειτουργία του Mobile IP.	81
5.2	IP NEXT GENERATION – MOBILE IP VERSION 6.	82
5.2.1	IPv6.	83
5.2.1.1	Διευθύνσεις.	83

5.2.1.2	Επικεφαλίδα.	83
5.2.2	Mobile IPv6.	84
5.2.2.1	Foreign Agent. Care – of Διεύθυνση τύπου Foreign Agent.	84
5.2.2.2	Stateless Address Autoconfiguration.	85
5.2.3	Η λειτουργία του Mobile IPv6.	85
5.3	INTER ACCESS POINT PROTOCOL – IAPP.	86
5.4	Η ΝΕΑ ΓΕΝΙΑ ΤΟΥ IAPP.	86
5.4.1	Η Λειτουργία του IAPP.	87
5.4.2	Δημιουργία και Συντήρηση ενός ESS.	87
5.4.3	Μετακινήσεις Σταθμών.	88
5.5	ΣΧΟΛΙΑ ΓΙΑ ΤΟ IAPP.	88
6	ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ – ΤΟ ΠΡΩΤΟΚΟΛΛΟ SNMP.	90
6.1	ΛΕΙΤΟΥΡΓΙΚΕΣ ΠΕΡΙΟΧΕΣ ΔΙΑΧΕΙΡΙΣΗΣ.	90
6.1.1	Διαχείριση Σφαλμάτων.	90
6.1.2	Λογιστική Διαχείριση.	90
6.1.3	Διαχείριση Διάρθρωσης και Ονομάτων.	91
6.1.4	Διαχείριση Επιδόσεων.	91
6.1.5	Διαχείριση Ασφάλειας.	91
6.2	ΔΙΑΧΕΙΡΙΣΗ ΕΠΙΔΟΣΕΩΝ.	91
6.2.1	Δείκτες Επιδόσεων.	91
6.2.1.1	Διαθεσιμότητα (Availability).	92
6.2.1.2	Χρόνος Απόκρισης (Response Time).	92
6.2.1.3	Ρυθμοαπόδοση (Throughput).	92
6.2.1.4	Εκμετάλλευση – Utilization.	92
6.2.2	Λειτουργία Παρακολούθησης Επιδόσεων.	93
6.3	ΤΟ ΠΡΩΤΟΚΟΛΛΟ SNMP.	93
6.3.1	Η ιστορία και η εξέλιξη του SNMP.	94
6.3.2	Οι λογικές οντότητες του SNMP.	95
6.3.3	Τα μηνύματα στο SNMP.	95
6.3.4	Η αρχιτεκτονική του SNMP.	96
6.3.5	Η MIB στο SNMP.	97
6.4	REMOTE NETWORK MONITORING - RMON.	97
6.4.1	Έλεγχος των Remote Monitors.	99
6.4.1.1	Configuration.	99
6.4.1.2	Action Invocation.	99
6.5	RMON 2.	99
6.5.1	Παρακολούθηση Επιπέδου Δικτύου.	100
6.5.2	Παρακολούθηση Ανώτερων Επιπέδων.	100
6.6	SNMP VERSION 2.	101
6.6.1	Βελτιώσεις στο SNMPv2.	102
6.6.1.1	Δομή Πληροφοριών Διαχείρισης – SMI.	102
6.6.1.2	Λειτουργία του Πρωτοκόλλου.	103
6.7	SNMP VERSION 3.	104
6.7.1	Γενικά για το SNMPv3.	104
6.7.2	Η Αρχιτεκτονική του SNMPv3.	105
6.8	Η MIB ΤΩΝ ΔΙΚΤΥΩΝ IEEE 802.11.	107
7	ΜΕΤΡΗΣΗ ΕΠΙΔΟΣΕΩΝ ΔΙΚΤΥΟΥ.	110
7.1	ΠΡΟΤΥΠΑ ΜΕΤΡΗΣΗΣ.	110
7.1.1	IP Performance Metrics – IPPF.	110
7.1.2	Cross – Industry Working Team – XIWT.	110
7.1.2.1	Internet Performance Working Team – IPERF.	111
7.1.3	CAIDA	111



7.2	ΜΕΘΟΔΟΙ ΜΕΤΡΗΣΗΣ.	111
7.2.1	Passive Measurement.	111
7.2.2	Active Measurement.	112
Μέρος 4 ^ο : Πειραματική μέτρηση επιδόσεων ενός δικτύου IEEE 802.11b.		113
8	ΠΕΡΙΓΡΑΦΗ ΤΩΝ ΠΕΙΡΑΜΑΤΩΝ.	113
8.1	ΣΚΟΠΟΣ ΤΩΝ ΠΕΙΡΑΜΑΤΩΝ.	113
8.2	ΣΧΕΔΙΑΣΜΟΣ ΤΩΝ ΠΕΙΡΑΜΑΤΩΝ.	114
8.2.1	Παραδοχές κατά τον Σχεδιασμό.	114
8.3	Ο ΕΞΟΠΛΙΣΜΟΣ ΚΑΙ ΤΟ ΛΟΓΙΣΜΙΚΟ.	115
8.3.1	Ο Εξοπλισμός που Χρησιμοποιήθηκε.	115
8.3.2	Εργαλεία που Χρησιμοποιήθηκαν.	116
8.3.2.1	TTCP.	116
8.3.2.2	NetPerf.	119
8.3.2.3	iPerf.	120
8.3.3	Αυτοματοποίηση των Πειραμάτων.	121
8.4	ΟΙ ΠΑΡΑΜΕΤΡΟΙ ΠΟΥ ΕΠΗΡΕΑΖΟΥΝ ΤΙΣ ΕΠΙΔΟΣΕΙΣ.	122
8.4.1	Λειτουργικά Συστήματα.	122
8.4.2	Τοπολογίες.	123
8.4.2.1	Τοπολογία Wireless to Wireless (W/W).	123
8.4.2.2	Τοπολογία Wireless to Ethernet (W/E).	123
8.4.3	Ενδιαφέροντα Αντικείμενα της MIB.	124
8.4.3.1	Station Management (SMT) Attributes.	124
8.4.3.2	MAC Attributes.	124
8.4.3.3	PHY Attributes.	125
8.4.4	Εναλλαγή Αποστολέα – Παραλήπτη.	125
8.4.5	Η Απόσταση Μεταξύ των Σταθμών και η Ύπαρξη Εμποδίων.	125
9	ΣΤΑΤΙΣΤΙΚΟ ΥΠΟΒΑΘΡΟ.	126
9.1	BOXPLOTS.	126
9.2	ΚΕΝΤΡΙΚΟ ΟΡΙΑΚΟ ΘΕΩΡΗΜΑ.	127
9.3	ΕΛΕΓΧΟΣ ΣΤΑΤΙΣΤΙΚΩΝ ΥΠΟΘΕΣΕΩΝ.	127
9.3.1	Στατιστική Υπόθεση.	127
9.3.2	Έλεγχος (Test).	128
9.3.3	Σφάλματα και Επίπεδο Σημαντικότητας.	128
9.4	T – TEST.	129
9.4.1	T – test για μη κανονικούς πληθυσμούς.	130
9.5	ΑΝΑΛΥΣΗ ΔΙΑΚΥΜΑΝΣΗΣ (ANALYSIS OF VARIANCE – AN.O.V.A.).	131
9.6	ONE – WAY ΚΑΙ MULTI WAY AN.O.VA.	131
9.6.1	Ανάλυση Διακύμανσης κατά Έναν Παράγοντα.	132
9.6.2	Ομογένεια Διακυμάνσεων και Post – Hoc Έλεγχοι.	133
10	Η ΠΡΑΓΜΑΤΟΠΟΙΗΣΗ ΤΩΝ ΜΕΤΡΗΣΕΩΝ.	135
10.1	ΥΠΟΘΕΣΗ – ΠΕΙΡΑΜΑ – ΜΕΤΡΗΣΗ.	135
10.2	ΤΑ ΣΤΑΤΙΣΤΙΚΑ ΜΕΓΕΘΗ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΗΘΗΚΑΝ.	136
10.3	ΥΠΟΘΕΣΗ 1 – Η ΕΠΙΔΡΑΣΗ ΤΩΝ ΕΡΓΑΛΕΙΩΝ.	138
10.3.1	Διατύπωση της Υπόθεσης.	138
10.3.2	Εργαλεία – Εξοπλισμός – Τοπολογία.	138
10.3.3	Περιγραφική Στατιστική.	138
10.3.4	Έλεγχος της Υπόθεσης.	139
10.3.5	Σχολιασμός των Αποτελεσμάτων.	140
10.4	ΥΠΟΘΕΣΗ 2 – Η ΕΠΙΔΡΑΣΗ ΤΗΣ ΤΟΠΟΛΟΓΙΑΣ.	142
10.4.1	Διατύπωση της Υπόθεσης.	142



10.4.2	Εργαλεία – Εξοπλισμός – Τοπολογία.	142
10.4.3	Περιγραφική Στατιστική.	142
10.4.4	Έλεγχος της Υπόθεσης.	143
10.4.5	Σχολιασμός των Αποτελεσμάτων.	144
10.5	ΥΠΟΘΕΣΗ 3 – Η ΕΠΙΔΡΑΣΗ ΤΩΝ ΛΕΙΤΟΥΡΓΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ.	145
10.5.1	Διατύπωση της Υπόθεσης.	145
10.5.2	Εργαλεία – Εξοπλισμός – Τοπολογία.	145
10.5.3	Περιγραφική Στατιστική.	145
10.5.4	Έλεγχος της Υπόθεσης.	146
10.5.5	Σχολιασμός των Αποτελεσμάτων.	147
10.6	ΥΠΟΘΕΣΗ 4 – Η ΕΠΙΔΡΑΣΗ ΤΗΣ ΕΝΑΛΛΑΓΗΣ CLIENT - SERVER.	148
10.6.1	Διατύπωση της Υπόθεσης.	148
10.6.2	Εργαλεία – Εξοπλισμός – Τοπολογία.	148
10.6.3	Περιγραφική Στατιστική.	148
10.6.4	Έλεγχος της Υπόθεσης.	149
10.6.5	Σχολιασμός των Αποτελεσμάτων.	150
10.7	ΥΠΟΘΕΣΗ 5 – Η ΕΠΙΔΡΑΣΗ ΤΩΝ ΑΝΤΙΚΕΙΜΕΝΩΝ ΤΗΣ MIB.	151
10.7.1	Διατύπωση της Υπόθεσης.	151
10.7.2	Εργαλεία – Εξοπλισμός – Τοπολογία.	151
10.7.3	Περιγραφική Στατιστική.	152
10.7.4	Έλεγχος της Υπόθεσης.	153
10.7.5	Σχολιασμός των Αποτελεσμάτων.	155
10.8	ΥΠΟΘΕΣΗ 6 – Η ΕΠΙΔΡΑΣΗ ΤΩΝ ΕΜΠΟΔΙΩΝ.	156
10.8.1	Διατύπωση της Υπόθεσης.	156
10.8.2	Εργαλεία – Εξοπλισμός – Τοπολογία.	156
10.8.3	Περιγραφική Στατιστική.	157
10.8.4	Έλεγχος της Υπόθεσης.	158
10.8.5	Σχολιασμός των Αποτελεσμάτων.	158
10.9	ΣΥΝΟΠΤΙΚΟΣ ΠΙΝΑΚΑΣ ΠΕΡΙΓΡΑΦΗΣ ΤΩΝ ΠΕΙΡΑΜΑΤΩΝ.	160
11	ΤΕΛΙΚΑ ΣΥΜΠΕΡΑΣΜΑΤΑ – ΠΕΡΑΙΤΕΡΩ ΕΡΕΥΝΑ.	161
11.1	ΕΠΙΔΟΣΕΙΣ WINDOWS XP.	161
11.2	ΤΑ ΑΝΤΙΚΕΙΜΕΝΑ ΤΗΣ MIB.	163
11.3	FRAGMENTATION THRESHOLD.	163
11.4	RTS / CTS.	165
11.5	ΜΕΓΕΘΟΣ ΔΙΚΤΥΟΥ.	165
ΒΙΒΛΙΟΓΡΑΦΙΑ – ΠΗΓΕΣ.		167
11.6	ΠΑΝΕΠΙΣΤΗΜΙΑΚΕΣ ΠΑΡΑΔΟΣΕΙΣ.	167
11.7	ΠΗΓΕΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ.	167
11.8	ΑΡΘΡΑ.	167
11.9	ΠΡΟΤΥΠΑ, RFC ΚΑΙ INTERNET DRAFTS.	168



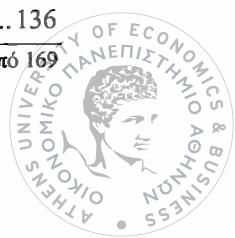
ΕΥΡΕΤΗΡΙΟ ΠΙΝΑΚΩΝ.

Πίνακας 1 - Οι Τιμές του PSF στο FHSS	48
Πίνακας 2 - Τα Κανάλια του FHSS.....	49
Πίνακας 3 - Οι Τιμές του Πεδίου Signal στο DSSS.....	51
Πίνακας 4 - Οι Συχνότητες Λειτουργίας του DSSS	53
Πίνακας 5 - Οι Διαφορές Φάσης για το DQPSK.	54
Πίνακας 6 - Οι Τιμές του Πεδίου Rate στο OFDM.....	55
Πίνακας 7 - Οι Ζώνες Συχνοτήτων Λειτουργίας του OFDM.	56
Πίνακας 8 - Τεχνικές Διαμόρφωσης του OFDM.	56
Πίνακας 9 - Το PPM 4 Επιπέδων για το IR.	59
Πίνακας 10 - Το Πεδίο Type της Επικεφαλίδας των MAC Πλαισίων.....	68
Πίνακας 11 - Το Πεδίο Subtype της Επικεφαλίδας των MAC Πλαισίων.	68
Πίνακας 12 - Συσχέτιση Τύπου Πλαισίου και Περιεχομένων.	73
Πίνακας 13 - Mobile IPv4 vs Mobile IPv6.	84
Πίνακας 14 - Παράδειγμα Αποτελεσμάτων T - test.	131
Πίνακας 15 - Παράδειγμα Ανάλυσης Διακύμανσης.	133
Πίνακας 16 - Ομογένεια Διακυμάνσεων του Levene.	134
Πίνακας 17 - Παράδειγμα test Games – Howell.	134
Πίνακας 18 - Περιγραφική Ανάλυση της Υπόθεσης 1.....	138
Πίνακας 19 - Ανάλυση Διακύμανσης για την Υπόθεση 1.....	139
Πίνακας 20 - Ομοιογένεια Διακυμάνσεων Ανάμεσα στις Ομάδες της Υπόθεσης 1.....	140
Πίνακας 21 - Games – Howell για την Υπόθεση 1.....	140
Πίνακας 22 - Περιγραφική Ανάλυση της Υπόθεσης 2.....	142
Πίνακας 23 - Τα Αποτελέσματα του t – test για την Υπόθεση 2.	143
Πίνακας 24 - Περιγραφική Ανάλυση της Υπόθεσης 3.....	145
Πίνακας 25 - Τα Αποτελέσματα του t – test για την Υπόθεση 3.	146
Πίνακας 26 - Περιγραφική Ανάλυση της Υπόθεσης 4.....	148
Πίνακας 27 - Τα Αποτελέσματα του t – test για την Υπόθεση 4.	150
Πίνακας 28 - Περιγραφική Ανάλυση της Υπόθεσης 5.....	152
Πίνακας 29 - Ανάλυση Διακύμανσης για την Υπόθεση 5.....	153
Πίνακας 30 - Ομοιογένεια Διακυμάνσεων Ανάμεσα στις Ομάδες της Υπόθεσης 5.....	153
Πίνακας 31 - Games – Howell για την Υπόθεση 5.	154
Πίνακας 32 - AN.O.V.A. Μόνο για τα Πειράματα 41, 42 και 43.....	154
Πίνακας 33 - Περιγραφική Ανάλυση της Υπόθεσης 6.....	157
Πίνακας 34 - Τα Αποτελέσματα του t – test για την Υπόθεση 6.	158
Πίνακας 35 - Η Κατηγοριοποίηση των Πειραμάτων.	160



ΕΥΡΕΤΗΡΙΟ ΣΧΗΜΑΤΩΝ.

Σχήμα 1 - Διάδοση Πολλαπλών Μονοπατιών.	23
Σχήμα 2 - Η Χρησιμότητα του Spread Spectrum.....	27
Σχήμα 3 - Frequency Hopping.	28
Σχήμα 4 - Access Point.	31
Σχήμα 5 - Peer to Peer.	31
Σχήμα 6 - Πολλαπλά Κελιά.	32
Σχήμα 7 - Σύνδεση Point to Point με Laser.	33
Σχήμα 8 - Μια Κυψέλη LMDS.	34
Σχήμα 9 - Η Συσχέτιση των Προτύπων IEEE 802.	35
Σχήμα 10 - Extended Service Set (ESS).	41
Σχήμα 11 - Η Στοίβα Πρωτοκόλλων του IEEE 802.11.....	43
Σχήμα 12 - Η Αρχιτεκτονική του Φυσικού Επιπέδου.	45
Σχήμα 13 - Η Δομή του PLCP PDU για το FHSS.	48
Σχήμα 14 - Two - Level και Four – Level GFSK.	50
Σχήμα 15 - Η Δομή του PLCP PDU για το DSSS.	51
Σχήμα 16 - Η Ακολουθία 11 - chip του Barker.	53
Σχήμα 17 - Η Δομή του PLCP PDU για το OFDM.	54
Σχήμα 18 - Το 64 - QAM για Μετάδοση 48 και 54Mbps.	57
Σχήμα 19 - Η Δομή του PLCP PDU για το IR.	57
Σχήμα 20 - Η Εκθετική Αύξηση του CW.	62
Σχήμα 21 - RTS/CTS/ACK και Ρύθμιση του NAV.	63
Σχήμα 22 - Τα Διάφορα IFS.....	63
Σχήμα 23 - Αυθεντικοποίηση Ανοικτού Συστήματος.	65
Σχήμα 24 - Αυθεντικοποίηση Μυστικού Κλειδιού.	66
Σχήμα 25 - Ο Αλγόριθμος WEP.....	66
Σχήμα 26 - Η Δομή των Πλαισίων MAC.	67
Σχήμα 27 - Η Δομή ενός MAC Πλαισίου Διαχείρισης.	71
Σχήμα 28 - Ανταλλαγή Πλαισίων RTS, CTS, ACK.	74
Σχήμα 29 - Το Πεδίο Frame Control στα Πλαίσια Ελέγχου.	74
Σχήμα 30 - Πλαίσιο RTS.	74
Σχήμα 31 - Η Δομή των Πλαισίων CTS και ACK.	75
Σχήμα 32 - Πλαίσιο Power Save Poll.	75
Σχήμα 33 - Πλαίσιο CF End.	75
Σχήμα 34 - Πώς τα Πεδία Address Επηρεάζονται από τα Υποπεδία To DS και From DS.	76
Σχήμα 35 - Οι Οντότητες του Mobile IP.	78
Σχήμα 36 - IP Encapsulation Within IP.	79
Σχήμα 37 - Η Λειτουργία του Mobile IP.	82
Σχήμα 38 - Η Αρχιτεκτονική του SNMP.	96
Σχήμα 39 - RMON.	98
Σχήμα 40 - Η Αρχιτεκτονική του SNMPv3.	106
Σχήμα 41 - Η MIB του IEEE 802.11.	108
Σχήμα 42 - Η Μορφή των Αποτελεσμάτων του TTCP.	118
Σχήμα 43 - Η Μορφή του Log File του TTCP.	118
Σχήμα 44 - Το Log File του NetPerf.	119
Σχήμα 45 - Log Αρχείο Του iPerf πριν από την Επεξεργασία.	120
Σχήμα 46 - Το ίδιο Log Αρχείο Του iPerf, μετά από την Επεξεργασία.	120
Σχήμα 47 - Τοπολογία 1, Wireless to Wireless.	123
Σχήμα 48 - Τοπολογία 2, Wireless to Ethernet.	123
Σχήμα 49 - Παράδειγμα BoxPlot.	126
Σχήμα 50 - Υπόθεση - Πείραμα - Μέτρηση.	136



Σχήμα 51 - BoxPlot για την Υπόθεση 1	139
Σχήμα 52 - BoxPlot για την Υπόθεση 2	143
Σχήμα 53 - BoxPlot για την Υπόθεση 3	146
Σχήμα 54 - BoxPlot για την Υπόθεση 4	149
Σχήμα 55 - BoxPlot για την Υπόθεση 5	152
Σχήμα 56 - Κάτοψη του 4 ^{ου} Ορόφου της Πτέρυγας Αντωνιάδου	157
Σχήμα 57 - BoxPlot για την Υπόθεση 6	158
Σχήμα 58 - Ραβδόγραμμα για την Μέση Καθυστέρηση σε κάθε Πείραμα	161
Σχήμα 59 - Ραβδόγραμμα για την Μέση Ρυθμοαπόδοση σε κάθε Πείραμα	162
Σχήμα 60 - Οι Προσθήκες Headers ανά Επίπεδο Δικτύου	165

ΕΥΡΕΤΗΡΙΟ ΤΥΠΩΝ.

Τύπος 1 - Ο Τύπος για το DPSK.	53
Τύπος 2 - Ο Υπολογισμός του Backoff.	61
Τύπος 3 - Διαθεσιμότητα..	92
Τύπος 4 - Συμβολισμός Προβλήματος Ελέγχου.	128
Τύπος 5 - Διατύπωση Στατιστικής Υπόθεσης.	129
Τύπος 6 - Ο Δειγματικός Αριθμητικός Μέσος.	129
Τύπος 7 - Η Δειγματική Διακύμανση.	129
Τύπος 8 - Μία Τυχαία Μεταβλητή που Ακολουθεί Κατανομή Student.	130
Τύπος 9 - Προϋπόθεση για την Ισότητα δύο Πληθυσμιακών Μέσων.	130
Τύπος 10 - Μια Τυχαία Μεταβλητή που Ακολουθεί Κατανομή F.	132
Τύπος 11 - Μέση Καθυστέρηση Πειράματος.	137
Τύπος 12 - Δειγματική Διακύμανση της Καθυστέρησης πειράματος.	137
Τύπος 13 - Μέση Ρυθμοαπόδοση Πειράματος.	137
Τύπος 14 - Η Στατιστική Έκφραση της Υπόθεσης 1.	138
Τύπος 15 - Η Στατιστική Έκφραση της Υπόθεσης 2.	142
Τύπος 16 - Η Στατιστική Έκφραση της Υπόθεσης 3.	145
Τύπος 17 - Η Στατιστική Έκφραση της Υπόθεσης 4.	148
Τύπος 18 - Η Στατιστική Έκφραση της Υπόθεσης 1.	151
Τύπος 19 - Η Στατιστική Έκφραση της Υπόθεσης 6.	156

ΕΙΣΑΓΩΓΗ.

Το κείμενο αυτό αποτελεί μέρος της εικπόνησης διπλωματικής εργασίας με επιβλέποντα καθηγητή τον κο. Θεόδωρο Αποστολόπουλο. Συντάχθηκε από τον Γιώργο Οικονόμου, φοιτητή στο Μεταπτυχιακό Προγράμματος Σπουδών σε Πληροφοριακά Συστήματα του Τμήματος Πληροφορικής του Οικονομικού Πανεπιστημίου Αθηνών.

Ο τίτλος της εργασίας είναι "Μέτρηση και στατιστική ανάλυση επιδόσεων Ασύρματων Τοπικών Δικτύων IEEE 802.11."

Στα πλαίσια της εργασίας, μελετήθηκε η τεχνολογία Ασύρματων Τοπικών Δικτύων και συγκεκριμένα αυτή που ακολουθεί το πρότυπο IEEE 802.11.

Στο Εργαστήριο Συστημάτων Υπολογιστών και Επικοινωνιών του Οικονομικού Πανεπιστημίου Αθηνών εγκαταστάθηκε, ένα δίκτυο τέτοιας τεχνολογίας και έγιναν πειραματικές μετρήσεις των επιδόσεών του. Σκοπός της εργασίας ήταν, με την χρήση συγκεκριμένων εργαλείων, να εκτιμηθεί, πώς οι παράμετροι της Management Information Base (MIB) των κόμβων του δικτύου επηρεάζουν τις επιδόσεις του. Η μέτρηση των επιδόσεων έγινε με τα εργαλεία "Test TCP" (TTCP), NetPerf και iPerf. Η δε στατιστική αξιολόγηση των αποτελεσμάτων έγινε με την χρήση των μεθόδων t – test και ANalysis of VAriance (AN.O.VA.).

Το κείμενο αυτό αποτελείται από τέσσερα μέρη.

Το πρώτο περιλαμβάνει τα κεφάλαια 1 και 2. Αποτελεί μια εισαγωγή στην τεχνολογία των ασύρματων τοπικών δικτύων. Περιέχει μια επισκόπηση των τεχνολογιών ασύρματων τοπικών δικτύων και του προτύπου IEEE 802.11.

Το δεύτερο, που εκτείνεται στα κεφάλαια 3 και 4, αναφέρεται στα επίπεδα της στοίβας πρωτοκόλλων των ασύρματων τοπικών δικτύων, σύμφωνα με το πρότυπο IEEE 802.11. Περιέχει μια αναλυτική περιγραφή του φυσικού επιπέδου και του επιπέδου MAC.

Στο τρίτο μέρος, ο αναγνώστης θα βρει κάποια ειδικά θέματα δικτύων που σχετίζονται με την εργασία αυτή. Συγκεκριμένα, στο κεφάλαιο 5 υπάρχουν λίγα λόγια για την ικανότητα ενός σταθμού να είναι συνδεδεμένος με το δίκτυο ενώ μετακινείται. Επίσης, μια επισκόπηση του Mobile IP για το κλασσικό IPv4 αλλά και για το IPv6. Στο κεφάλαιο 6, βρίσκεται μια επισκόπηση του τομέα της διαχείρισης δικτύων και μια ανάλυση του πρωτοκόλλου SNMP. Στο 7^ο κεφάλαιο υπάρχουν κάποια θέματα σχετικά με την μέτρηση των επιδόσεων ενός δικτύου. Αναφέρονται τα πρότυπα που σχετίζονται με αυτό το θέμα, καθώς και εργαλεία που μπορούν να χρησιμοποιηθούν για τέτοιου είδους ανάλυση.

Στο τέταρτο και τελευταίο μέρος υπάρχει η πλήρης περιγραφή των πειραμάτων που εκτελέστηκαν καθώς και η παρουσίαση και ανάλυση των αποτελεσμάτων. Συγκεκριμένα,

στο όγδοο κεφάλαιο, ο αναγνώστης μπορεί να βρει όλες τις λεπτομέρειες για τον σχεδιασμό των πειραμάτων. Στο κεφάλαιο 9 υπάρχει λίγη θεωρία στατιστικής, η οποία χρειάζεται στο κεφάλαιο 10, όπου γίνεται διεξοδική ανάλυση των αποτελεσμάτων των πειραμάτων. Το επόμενο κεφάλαιο, υπ' αριθμόν 11, περιέχει τα τελικά συμπεράσματα που προέκυψαν από την πειραματική μέτρηση των επιδόσεων και προτάσεις για περαιτέρω έρευνα.

Αθήνα, Σεπτέμβριος 2000 – Φεβρουάριος 2001.

ΕΥΧΑΡΙΣΤΙΕΣ.

Θερμά ευχαριστώ:

Τον Καθηγητή του Οικονομικού Πανεπιστημίου Αθηνών, κο **Θεόδωρο Αποστολόπουλο** για την υποστήριξή του και την καθοδήγησή του κατά την διάρκεια της εκπόνησης της παρούσας εργασίας.

Τον υπεύθυνο του Κέντρου Διαχείρισης Δικτύων του Οικονομικού Πανεπιστημίου Αθηνών κο **Αλέξιο Ζάβρα** για τις συμβουλές του.

Τον υποψήφιο διδάκτορα **Αθανάσιο Ανδρούτσο** για τις συμβουλές του στα θέματα διαχείρισης δικτύων με το πρωτόκολλο SNMP. Τους υποψήφιους διδάκτορες **Κώστα Κουμάνταρο** και **Δημήτρη Μπότη** για την βοήθεια που προσέφεραν σε τεχνικά θέματα.

Τον συμφοιτητή μου, **Παναγιώτη Μαχαίρα** για την συνεργασία του στην εγκατάσταση του εξοπλισμού και στην εκτέλεση των μετρήσεων.

Τους συμφοιτητές μου **Χρήστο Αμανατίδη** και **Σταύρο Σπανό** για τις συμβουλές τους σχετικά με την χρήση της γλώσσας προγραμματισμού C. Η βοήθειά τους ήταν καταλυτική στις μετατροπές του κώδικα της εφαρμογής TTCP.



Μέρος 1^ο:

Εισαγωγή στα ασύρματα τοπικά δίκτυα. και το πρότυπο IEEE 802.11.

1 ΑΣΥΡΜΑΤΑ ΤΟΠΙΚΑ ΔΙΚΤΥΑ (WIRELESS LAN).

Τα τελευταία χρόνια έχει παρατηρηθεί μια ραγδαία ανάπτυξη των δικτύων υπολογιστών, τα οποία πλέον, με τις κατάλληλες εφαρμογές που τα συνοδεύουν, έχουν διεισδύσει σε πολλούς τομείς της ζωής μας. Στην περίπτωση μάλιστα των τοπικών δικτύων, η μείωση των τιμών και η ραγδαία αύξηση των επιδόσεων, τα έχει κάνει τόσο χρήσιμα όσο και προσιτά ακόμα και για τον οικιακό χρήστη.

Πολύ συχνά, τελευταία, συναντάμε περιπτώσεις όπου ένας σταθμός που είναι συνδεδεμένος με ένα τοπικό δίκτυο απαιτείται να μην είναι στάσιμος, αλλά να κινείται. Για παράδειγμα, στα νοσοκομεία γιατροί και νοσοκόμοι κινούνται συνεχώς από δωμάτιο σε δωμάτιο, ενώ για να καταγραφούν τα αποτελέσματα μιας εξέτασης χρειάζεται πολύ γραφειοκρατική δουλειά. Με τη χρήση μιας συσκευής χειρός (palmtop PC), θα μπορούσε αυτή η εργασία να γίνεται εύκολα και άμεσα. Έτσι δημιουργήθηκε η ανάγκη για την ανάπτυξη ασύρματων τοπικών δικτύων.

1.1 ΠΡΟΔΙΑΓΡΑΦΕΣ ΑΣΥΡΜΑΤΩΝ ΤΟΠΙΚΩΝ ΔΙΚΤΥΩΝ.

Η ανάγκη αυτή άρχισε να βρίσκει λύση με την ανάπτυξη διάφορων προδιαγραφών ασύρματης δικτύωσης. Τέτοια είναι το Bluetooth, το HiperLAN και το πρόσφατο πρότυπο IEEE 802.11.

1.1.1 HiperLAN.

Προδιαγραφή που αναπτύχθηκε από το European Telecommunication Standards Institute (ETSI) το 1996. Λειτουργεί στη ζώνη των 5GHz και αναπτύσσει ταχύτητες ως 24Mbps μέσω ενός πρωτοκόλλου χωρίς σύνδεση. Τους τελευταίους μήνες βρίσκεται υπό ανάπτυξη το πρότυπο HiperLAN/2 το οποίο θα αναπτύσσει ταχύτητες ως 54Mbps μέσω πρωτοκόλλου με σύνδεση. Τα HiperLAN/1 και HiperLAN/2 υποστηρίζουν εγγυημένη ποιότητα υπηρεσιών (QoS) και μπορούν να μεταφέρουν Ethernet πλαίσια, ATM κελιά και IP Datagrams.

1.1.2 Bluetooth.

Είναι μια προδιαγραφή που δημοσιεύθηκε από το Bluetooth Special Interest Group (BSIG) σε συνεργασίες με μεγάλες εταιρείες όπως οι 3COM, Ericsson, IBM, Intel, Lucent Technologies, Microsoft, Motorola, Nokia... Δεν αποτελεί ακριβώς Wireless LAN, αλλά

περισσότερο Personal Area Network, που επιτρέπει την επικοινωνία φορητών συσκευών σε μικρές αποστάσεις, για παράδειγμα ένα Bluetooth κινητό τηλέφωνο μπορεί να επικοινωνήσει με ένα Personal Digital Assistant. To Bluetooth λειτουργεί στο 1Mbps.

1.1.3 IEEE 802.11.

Πρόσφατα (1999) εκδόθηκε από το IEEE το πρότυπο IEEE 802.11. Αποτελεί ένα πρότυπο για ασύρματα τοπικά δίκτυα, μέσω ραδιοκυμάτων ή υπέρυθρων ακτινών. Το IEEE έχει αποτελέσει την πηγή για τα πιο ευρέως χρησιμοποιούμενα πρότυπα για τοπικά δίκτυα και έτσι και αυτό το πρότυπο αναμένεται να επικρατήσει. Οι συσκευές που ακολουθούν το πρότυπο αυτό λειτουργούν, συνήθως, στην ζώνη συχνοτήτων των 2.4GHz.

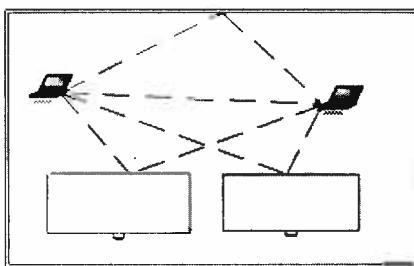
Με το πρότυπο αυτό θα ασχοληθούμε εκτενέστερα παρακάτω σε αυτό το κείμενο.

1.2 ΙΔΙΑΙΤΕΡΟΤΗΤΕΣ ΤΩΝ ΑΣΥΡΜΑΤΩΝ ΤΟΠΙΚΩΝ ΔΙΚΤΥΩΝ.

Τα ασύρματα τοπικά δίκτυα προσφέρουν μεγάλες δυνατότητες στους σχεδιαστές, τους χρήστες και τους διαχειριστές έργων. Ωστόσο η ιδιαιτερότητα του μέσου δημιουργεί ορισμένα νέα προβλήματα. Προβλήματα που δεν είναι υπαρκτά στην περίπτωση των παραδοσιακών ενσύρματων τοπικών δικτύων. Με αυτές τις ιδιαιτερότητες θα ασχοληθούμε παρακάτω και όπου σε ορισμένες περιπτώσεις θα αναφέρουμε τις λύσεις που προτείνει το πρότυπο IEEE 802.11.

1.2.1 Διασπορά πολλαπλών μονοπατιών.

Αν φανταστούμε την περίπτωση του σχήματος θα δούμε ότι όταν ένας σταθμός εκπέμπει ένα σήμα, το σήμα αυτό μπορεί να ανακλαστεί σε αντικείμενα, να συνδυαστεί με τα νέα σήματα και να ληφθεί κατεστραμμένο. Delay Spread αποκαλείται η χρονική διαφορά με την οποία λαμβάνονται τα δύο, ή παραπάνω σήματα (αρχικό και εξ αντανάκλασης). Όσο μεγαλύτερο είναι το κενό αυτό, τόσο μεγαλύτερο το πρόβλημα που δημιουργείται.



Σχήμα 1 - Λύσηση Πολλαπλών Μονοπατιών.

1.2.2 Παρεμβολές.

Η διαδικασία εναέριας διάδοσης ραδιοκυμάτων κάνει τα ασύρματα συστήματα ευάλωτα σε θόρυβο εξαιτίας της ατμόσφαιρας και άλλων ασύρματων μεταδόσεων.

Παρεμβολές μπορούν να συμβούν όταν δύο συστήματα, που λειτουργούν σε παρόμοια συχνότητα, βρίσκονται σε μικρή απόσταση μεταξύ τους. Για παράδειγμα οι φούρνοι μικροκυμάτων, που λειτουργούν στη ζώνη S των 2.4GHz, μπορεί να προκαλέσουν παρεμβολές σε ένα ασύρματο τοπικό δίκτυο.

Στην αντίστροφη περίπτωση έχουμε το ενδεχόμενο, το ασύρματο δίκτυο να προκαλέσει παρεμβολές σε κάποιο άλλο σύστημα. Αυτή, όμως η περίπτωση είναι αμελητέα, καθώς οι συσκευές των ασύρματων δικτύων δουλεύουν σε πολύ χαμηλή ισχύ (< 1watt).

Ειδικά στην περίπτωση του IEEE 802.11, χρησιμοποιούνται Spread Spectrum τεχνολογίες. Αυτό έχει σαν αποτέλεσμα να μειώνονται κατά πολύ οι παρεμβολές από άλλες συσκευές.

Ειδική μνεία πρέπει να γίνει στην περίπτωση που συνυπάρχουν δίκτυα τεχνολογίας Bluetooth και IEEE 802.11 στον ίδιο χώρο. Οι συσκευές Bluetooth, όταν λειτουργούν, αλλάζουν συχνότητα εκπομπής 600 φορές γρηγορότερα από τις συσκευές IEEE 802.11. Είναι, έτσι, πολύ πιθανόν η συσκευή Bluetooth να προκαλέσει παρεμβολή στη συσκευή 802.11. Γι' αυτό το θέμα, οι ομάδες που αναπτύσσουν τα δύο πρότυπα έχουν δημιουργήσει την ομάδα 802.15 Coexistence Task Group 2. Έχουν ήδη γίνει προκαταρκτικές αναλύσεις και έχουν γίνει προτάσεις για την επόμενη του ζητήματος. Ο στόχος είναι να μειωθεί η πιθανότητα να εκπέμψει μια συσκευή Bluetooth ταυτόχρονα με μία συσκευή 802.11.

1.2.3 Χρόνος ζωής μπαταρίας.

Οι χρήστες φορητών υπολογιστών έχουν ως πρόσθετο το πρόβλημα της διάρκειας ζωής της μπαταρίας. Η επιπλέον ενέργεια που καταναλώνει μια κάρτα δικτύου αποτελεί μείζον πρόβλημα.

Το γεγονός ότι τα ασύρματα τοπικά δίκτυα αφορούν, κυρίως, φορητές συσκευές, οδήγησε τους κατασκευαστές σε διάφορες λύσεις. Συνήθως οι κάρτες δικτύου λειτουργούν σε τρεις καταστάσεις. Πέρα από την κανονική λειτουργία, υπάρχει η επιλογή να μπαίνουν σε Sleep ή Doze Mode, καταναλώνοντας λιγότερη ενέργεια. Στην πρώτη περίπτωση οι κάρτα δεν μπορεί να λάβει και ελέγχει περιοδικά σε ένα mailbox για εισερχόμενα μηνύματα. Αυτό το σύστημα εξοικονομεί 50% ενέργεια. Στην δεύτερη περίπτωση η κάρτα δεν έχει δυνατότητα να λάβει αλλά παραμένει σε κατάσταση έτοιμη για αποστολή. Είναι, λοιπόν προφανές ότι, ανάλογα με την χρήση του δικτύου καταναλώνεται περισσότερη ή λιγότερη ενέργεια. Όταν, δε, επιθυμούμε μεγαλύτερες επιδόσεις, έχουμε σαν κόστος μεγαλύτερη κατανάλωση.

Για παράδειγμα μια κάρτα δικτύου συμβατή με IEEE 802.11b καταναλώνει:

- Αποστολή: 350mA
- Λήψη: 250mA
- Sleep: 10mA

Στο πρότυπο IEEE 802.11, όπως θα δούμε όταν το μελετήσουμε διεξοδικότερα, γίνεται ιδιαίτερη μνεία στα θέματα διαχείρισης ενέργειας.

1.2.4 Διαλειτουργικότητα.

Πέρα από το μεγάλο πρόβλημα συμβατότητας συσκευών ασύρματων τοπικών δικτύων πριν από την ανάπτυξη του προτύπου 802.11, υπάρχει πρόβλημα και μεταξύ συσκευών που ακολουθούν το πρότυπο. Αυτό συμβαίνει γιατί κάθε κατασκευαστής κάνει δικές του προσθήκες στα προϊόντα του, ώστε να προσφέρει επιπλέον λειτουργίες. Έτσι, συσκευές διαφορετικών κατασκευαστών μπορεί να επικοινωνούν αλλά χωρίς τις επιπλέον λειτουργίες που προσφέρει η καθεμία. Συνεπώς, είναι προτιμότερο να χρησιμοποιεί κανείς συσκευές από τον ίδιο κατασκευαστή.

1.2.5 Ασφάλεια.

Σε αντίθεση με τα ενσύρματα τοπικά δίκτυα, όπου υπάρχει χωρικός περιορισμός για την κάλυψη του δικτύου, στα ασύρματα τοπικά δίκτυα, τα όρια του δικτύου είναι ασαφή. Αυτό συμβαίνει γιατί τα ραδιοικύματα μπορούν να διαδόθουν μέσα από τοίχους και, γενικά, δεν έχουν φυσικά όρια. Έτσι κάποιος κακόβουλος χρήστης θα μπορούσε να συνδεθεί με ένα ασύρματο τοπικό δίκτυο ενός οργανισμού, βρισκόμενος αρκετά μέτρα μακριά από την έδρα του οργανισμού.

Αυτό το πρόβλημα έχει αντιμετωπισθεί στο πρότυπο 802.11 με την χρήση ενός αριθμού δικτύου που πρέπει να γνωρίζει ο χρήστης ώστε να συνδεθεί με ένα δίκτυο. Επίσης υπάρχει δυνατότητα για κρυπτογραφημένη μετάδοση δεδομένων.

Ειδικά για αυτό το θέμα, μια ομάδα εργασίας ιδρύθηκε από τον IEEE. Πρόκειται για το Work Group IEEE802.11e που ασχολείται, με θέματα ποιότητας υπηρεσιών (QoS) και με θέματα ασφάλειας. Συγκεκριμένα, μελετώνται βελτιώσεις των μηχανισμών του επιπέδου MAC. Η ομάδα αυτή, πρόσφατα, τον Μάιο 2001 χωρίστηκε σε δύο. Έτσι το Work Group e συνεχίζει να ασχολείται με θέματα ποιότητας υπηρεσιών ενώ τα θέματα ασφάλειας ανεξαρτητοποιήθηκαν με την δημιουργία της ομάδας IEEE 802.11i που ασχολείται αποκλειστικά με αυτά.

1.2.6 Ακαταλληλότητα TCP/IP.

Η στοίβα πρωτοκόλλων TCP/IP λειτουργεί άψογα στην περίπτωση των ενσύρματων τοπικών δικτύων. Αυτό γιατί το πρωτόκολλο TCP προσφέρει υπηρεσίες με σύνδεση, άκρως αξιόπιστες. Στην περίπτωση των ασύρματων τοπικών δικτύων, η προσωρινή

απώλεια σήματος, όταν μια συσκευή βρίσκεται οριακά εντός δικτύου και κινείται, μπορεί να οδηγήσει το TCP σε διακοπή της σύνδεσης.

Επίσης, σε επίπεδο δικτύου κατά OSI, τα υπάρχοντα πρωτόκολλα δρομολόγησης δεν καλύπτουν την περίπτωση που ένας σταθμός μετακινείται από σημείο σε σημείο. Αυτό γιατί η λογική διεύθυνση (IP διεύθυνση) έχει άμεση σχέση με την φυσική θέση της συσκευής. Έτσι, αν μια συσκευή μετακινηθεί από τον χώρο ενός IP υποδικτύου στο χώρο ενός άλλου, θα πρέπει να αλλάξει και IP διεύθυνση. Κάτι τέτοιο δεν είναι καθόλου πρακτικό. Έτσι, γίνονται προσπάθειες, με το πρωτόκολλο Mobile IP, μόνο του ή σε συνδυασμό με την νέα γενιά του IP – το IPv6 – να μπορεί ένας σταθμός να μετακινηθεί από ένα υποδίκτυο σε ένα άλλο χωρίς να αλλάξει η IP διεύθυνσή του.

1.2.7 Θέματα εγκατάστασης.

Στην περίπτωση των τοπικών δικτύων, η εγκατάσταση είναι απλή. Αρκεί να αποφασισθεί από πού θα περάσει η καλωδίωση.

Αντίθετα, όταν πρόκειται να εγκαταστήσουμε ασύρματο δίκτυο, τα πράγματα δεν είναι τόσο απλά. Η επίδραση των υλικών της κατασκευής του κτιρίου και των επίπλων που βρίσκονται μέσα σε αυτό έχουν άμεση σχέση με την διάδοση των κυμάτων. Τοίχοι, παράθυρα, ταβάνια και πόρτες μπορούν να επηρεάσουν την πορεία των κυμάτων ή και να τα παραμορφώσουν. Έτσι, για να επιτευχθεί η επιθυμητή κάλυψη, δεν αρκεί μια απλή επισκόπηση του χώρου, αλλά απαιτείται να γίνουν δοκιμές για να εξακριβωθεί που και πώς πρέπει να τοποθετηθούν οι συσκευές για την αδιάλειπτη λειτουργία του δικτύου.

Στην περίπτωση των μητροπολιτικών δικτύων, κάτι που φαίνεται ως καθαρή οπτική επαφή μεταξύ δύο κτιρίων, που απέχουν 500 μέτρα, μπορεί να κατακλύζεται από συσκευές που εκπέμπουν άλλα σήματα. Έτσι η διασύνδεση αυτών των κτιρίων μπορεί να αποβεί προβληματική.

1.2.8 Θέματα υγείας.

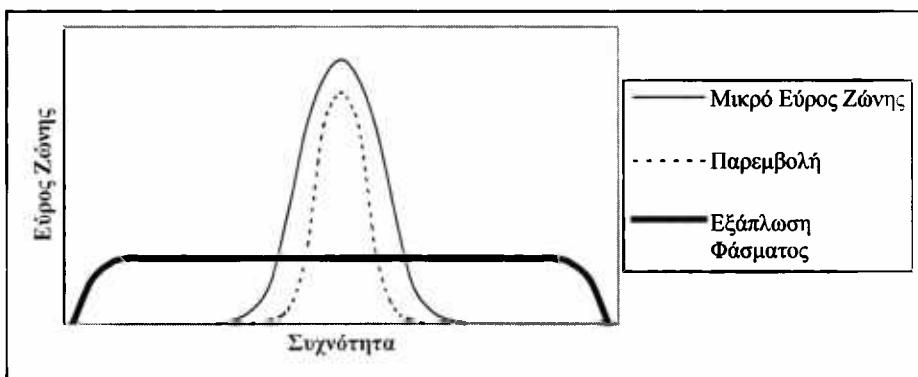
Έχουν εκφραστεί πολλές ανησυχίες για το αν οι συσκευές των ασύρματων τοπικών δικτύων αποτελούν κίνδυνο για την υγεία των χρηστών. Οι απαντήσεις είναι ασαφείς. Ωστόσο φαίνεται ότι οι συσκευές αυτές είναι πολύ πιο ακίνδυνες από τα κινητά τηλέφωνα. Στις Η.Π.Α. τα κινητά τηλέφωνα λειτουργούν στην ακριβώς χαμηλότερη ζώνη συχνοτήτων από αυτή των ασύρματων τοπικών δικτύων. Ωστόσο η ισχύς των κινητών είναι από 600 milliwatt μέχρι 3 Watt, των δε συσκευών ασύρματων τοπικών δικτύων είναι από 50 έως 100 milliwatt. Επιπλέον, αυτές οι συσκευές εκπέμπουν κάθε φορά για μικρότερο χρονικό διάστημα από αυτό που διαρκεί μια συνομιλία.

Στην περίπτωση της διασύνδεσης με Laser, οι ακτίνες είναι Κλάσης III, που σημαίνει ότι είναι επιβλαβείς για την όραση μόνο αν κάποιος κοιτάξει απευθείας την ακτίνα.

1.3 ΤΕΧΝΙΚΕΣ ΔΙΑΜΟΡΦΩΣΗΣ ΣΗΜΑΤΟΣ.

Στο φυσικό επίπεδο ενός δικτύου γίνεται η ουσιαστική μεταφορά των bits μέσα από ένα τηλεπικοινωνιακό κανάλι. Διαμόρφωση καλείται η διεργασία, κατά την οποία ο αποστολέας προετοιμάζει το σήμα για μετάδοση στο μέσο. Το μέσο μπορεί να είναι ενσύρματο (χαλκός, οπτική ίνα) ή ασύρματο (ραδιοκύματα, laser, υπέρυθρες ακτίνες).

Spread Spectrum είναι μια ομάδα τεχνικών διαμόρφωσης σήματος που μοιράζονται την ίδια φιλοσοφία. Στηρίζονται στην εξάπλωση του σήματος σε πιο ευρεία ζώνη συχνοτήτων. Έτσι θυσιάζεται εύρος ζώνης αλλά έχουμε κέρδος σε σηματοθορυβική σχέση. Μπορεί η τεχνικές αυτές να αντιτίθενται στη γενικότερη προσπάθεια εξοικονόμησης εύρους ζώνης, αλλά κάνουν το σήμα πολύ πιο ανθεκτικό στον θόρυβο απ' ότι στα παραδοσιακά συστήματα διαμόρφωσης AM, FM κλπ. Αυτό, άλλωστε φαίνεται ξεκάθαρα στο παραπάνω σχήμα. Μια άλλη μετάδοση, ή θόρυβος, τυπικά μικρού εύρους ζώνης, θα επηρεάσει μόνο ένα μικρό μέρος του Spread Spectrum σήματος, με αποτέλεσμα λιγότερα σφάλματα κατά την αποδιαμόρφωση (demodulation) από τον παραλήπτη.

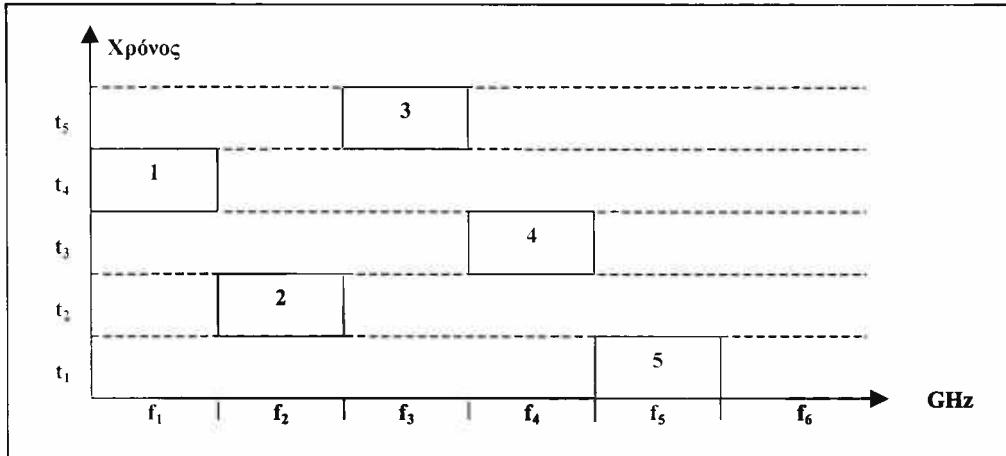


Σχήμα 2 - Η Χρησιμότητα του Spread Spectrum.

Στις παραγράφους που ακολουθούν θα αναφερθούμε, συνοπτικά, στα χαρακτηριστικά των κυριότερων τεχνικών Spread Spectrum και άλλων τεχνικών διαμόρφωσης σήματος.

1.3.1 Frequency Hopping Spread Spectrum – FHSS.

Στην περίπτωση του Frequency Hopping, το διαμορφωμένο σήμα κάνει άλματα (Hops) από συχνότητα σε συχνότητα σε μια ευρύτερη ζώνη συχνοτήτων. Για παράδειγμα στο IEEE 802.11 η συχνότητα φέροντος πραγματοποιεί τα άλματα στη ζώνη από 2.4GHz μέχρι 2.483GHz.



Σχήμα 3 - Frequency Hopping.

Για να ξέρει ο παραλήπτης σε ποια συχνότητα πρέπει να συγχρονιστεί κάθε στιγμή και για πόσο χρόνο, καθορίζεται ο Hopping Code. Αυτόν χρησιμοποιεί και ο αποστολέας για να στείλει το σήμα. Στην περίπτωση του σχήματος το Hopping Pattern είναι 5 2 4 1 3.

Σύμφωνα με την Ομοσπονδιακή Επιτροπή Τηλεπικοινωνιών (Federal Communications Committee – FCC) των Η.Π.Α, κάθε κανάλι πρέπει να χρησιμοποιεί τουλάχιστον 75 συχνότητες και ο μέγιστος χρόνος εκπομπής στην ίδια συχνότητα (Maximum Dwell Time) περιορίζεται στα 400ms. Αν ο πομπός συναντήσει παρεμβολή σε κάποια συχνότητα, ξαναμεταδίδει το μέρος αυτό του σήματος στο επόμενο άλμα.

Όπως φαίνεται από το παραπάνω σχήμα, η παρεμβολή ενός σήματος μικρού εύρους σε ένα άλλο που μεταδίδεται με Frequency Hopping, συμβαίνει μόνο όταν τα δύο σήματα συμπέσουν στην ίδια συχνότητα, την ίδια χρονική στιγμή. Το αποτέλεσμα αυτού είναι, τα σήματα Frequency Hopping, να είναι πολύ ανθεκτικά στον θόρυβο και η συνολική παρεμβολή επιφέρει πολύ λίγα έως καθόλου λάθη.

Είναι, επιπλέον, δυνατόν δύο FHSS συστήματα που λειτουργούν στην ίδια ζώνη συχνοτήτων, να χρησιμοποιούν τέτοια Hopping Patterns ώστε να μην παρεμβάλλονται ποτέ το ένα στο άλλο. Δύο Hopping Patterns που έχουν αυτή την ιδιότητα ονομάζονται ορθογώνια (orthogonal).

1.3.2 Direct Sequence Spread Spectrum – DSSS.

To Direct Sequence Spread Spectrum, για κάθε bit δεδομένων αποστέλλεται μια ακολουθία bits σήματος, με μεγαλύτερο bit rate. Η ακολουθία αυτή ονομάζεται Chipping Code ή Processing Gain. Για το πρότυπο IEEE 802.11 το Processing Gain έχει ελάχιστο μήκος 11 ψηφία. Όσο μεγαλύτερο το μήκος του, τόσο μεγαλύτερη η αντοχή σε παρεμβολές.

Για παράδειγμα:

- Bit 0: 00010011100
- Bit 1: 11101100011
- Ακολουθία Bits 011: 00010011100 11101100011 11101100011

Το πλεονέκτημα του DSSS είναι ότι μπορεί να υποστηρίξει ψηλότερους ρυθμούς μετάδοσης από το FHSS.

1.3.3 Orthogonal Frequency Division Multiplexing – OFDM.

Το OFDM διασπά το αρχικό σήμα σε πολλά υποσήματα χαμηλότερης ταχύτητας και τα μεταδίδει παράλληλα σε διαφορετικές συχνότητες.

Συγκεκριμένα, το OFDM μεταδίδει το σήμα σε 52 μέρη. Τα 4 από αυτά δρουν ως σημείο αναφοράς για τον παραλήπτη ενώ τα υπόλοιπα 48 μεταδίδουν τα δεδομένα. Το OFDM, χωρίζει τα δεδομένα σε ομάδες συνόλων των 1, 2, 4 ή 6 bits, ανάλογα με την επιθυμητή ταχύτητα.

1.3.4 Υπέρυθρες Ακτίνες.

Αντί για ραδιοκύματα, μπορούμε, εναλλακτικά, να χρησιμοποιήσουμε υπέρυθρες ακτίνες για την επικοινωνία δύο υπολογιστών.

Οι υπέρυθρες έχουν μεγαλύτερο μήκος κύματος – χαμηλότερη συχνότητα – από τα χρώματα τις ίριδας, αλλά μεγαλύτερη συχνότητα από τα ραδιοκύματα. Το υπέρυθρο φως είναι αόρατο, κάτω από τις περισσότερες συνθήκες φωτισμού, σε γυμνό μάτι. Τα προϊόντα τοπικών δικτύων, που λειτουργούν με υπέρυθρες ακτίνες, λειτουργούν συνήθως με μήκος κύματος 820nm, γιατί σε αυτό το μήκος κύματος, ο αέρας προκαλεί την χαμηλότερη εξασθένηση.

Τυπική περίπτωση επικοινωνίας με υπέρυθρες ακτίνες είναι τα τηλεχειριστήρια των τηλεοράσεων.

Συγκριτικά με τα ραδιοκύματα, οι υπέρυθρες έχουν τις ακόλουθες διαφορές:

1. Ψηλότερο βαθμό ασφάλειας.

Το υπέρυθρο φως δεν διαδίδεται, μέσα από σταθερά αντικείμενα, όπως τοίχους κλπ. Αυτό σημαίνει ότι είναι σαφή τα όρια λειτουργίας του ασύρματου τοπικού δικτύου και δεν υπάρχει ο κίνδυνος υποκλοπής του σήματος από σταθμό που βρίσκεται έξω απ' αυτά. Το σήμα παραμένει περιορισμένο μέσα στο όρια ενός γραφείου ή ενός κτιρίου.

2. Μεγαλύτερη αντοχή σε παρεμβολές.

Το υπέρυθρο φως δεν επηρεάζεται καθόλου από ηλεκτρομαγνητικά παιδία, όπως ενός φούρνου μικροκυμάτων ή άλλων συσκευών που εκπέμπουν ραδιοκύματα.

3. Ψηλότερες επιδόσεις.

Οι υπέρυθρες ακτίνες έχουν μεγάλο εύρος ζώνης. Αυτό τις κάνει κατάλληλες για μετάδοση δεδομένων σε ψηλές ταχύτητες.

4. Μικρότερη περιοχή κάλυψης.

Το γεγονός ότι η επικοινωνία με υπέρυθρες έχει μικρή περιοχή κάλυψης, τις κάνει ακατάλληλες για εφαρμογές ασύρματων δικτύων μεγάλης κλίμακας.

1.4 ΤΟΠΟΛΟΓΙΕΣ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ.

Υπάρχουν πολλοί τρόποι να διασυνδέσουμε υπολογιστές σε ένα ασύρματο δίκτυο. Η τελική μας επιλογή βασίζεται σε πολλές παραμέτρους, όπως η απόσταση μεταξύ των σταθμών, το πλήθος τους και το αν επιθυμούμε διασύνδεση με κάποιο τοπικό δίκτυο ή άλλης τεχνολογίας (CSMA/CD, Token Ring, Token Bus).

1.4.1 Εξαρτήματα δικτύου.

Τα εξαρτήματα που πρέπει να χρησιμοποιήσουμε είναι διάφορα και τα βασικότερα από αυτά θα αναφέρουμε παρακάτω.

1.4.1.1 Κάρτες δικτύου (Network Interface Card – NIC).

Είναι το εξάρτημα που προετοιμάζει τα δεδομένα για μετάδοση στο μέσο, είτε ενσύρματο είτε ασύρματο. Ουσιαστικά πραγματοποιεί την διαμόρφωση του σήματος και την ενίσχυσή του, σε μορφή κατάλληλη για διάδοση. Αποτελεί την διεπαφή μέσου – συσκευής.

Συνήθως είναι κάρτες PCI, ISA ή PCMCIA που τοποθετούνται στο εσωτερικό του υπολογιστή ή εξωτερικές συσκευές όπως τα Modems.

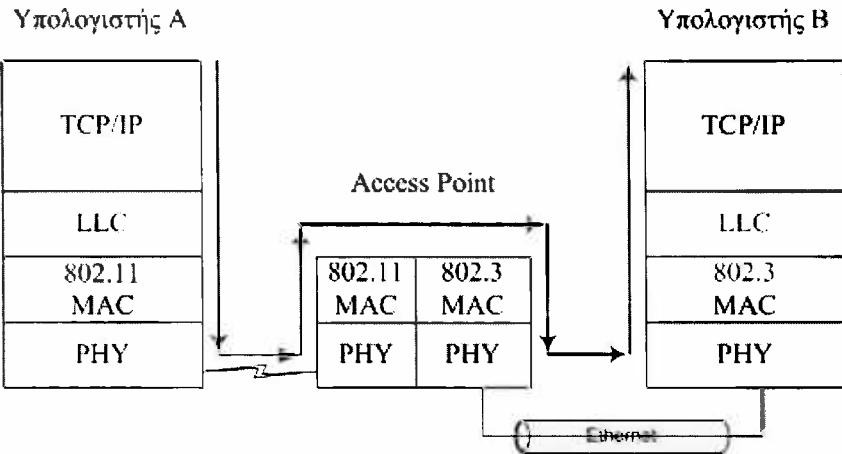
Στην περίπτωση των ασύρματων τοπικών δικτύων, οι κάρτες είναι PCMCIA ή ISA και μεταδίδουν τα δεδομένα με ραδιοκύματα, μέσω κάποιας κεραίας, ή με υπέρυθρες ακτίνες.

1.4.1.2 Ασύρματες γέφυρες.

Ένα πολύ σημαντικό εξάρτημα για κάθε τοπικό δίκτυο. Συνδέουν δύο τμήματα τοπικού δικτύου, σε επίπεδο MAC (υποεπίπεδο του επιπέδου σύνδεσης δεδομένων κατά OSI), κάνοντας δυνατή την ανταλλαγή δεδομένων ακόμα και αν τα δίκτυα είναι διαφορετικών τεχνολογιών (π.χ. Ethernet to Token Ring).

Επιπλέον, οι γέφυρες κάνουν φιλτράρισμα πακέτων. Όταν φτάσει σε αυτές ένα πακέτο από το ένα τμήμα του δικτύου και προορίζεται για υπολογιστή που ανήκει στο ίδιο τμήμα, τότε το πακέτο αυτό δεν προωθείται στο δεύτερο τμήμα. Αυτή η λειτουργία ονομάζεται segmentation και είναι πολύ σημαντική γιατί εξοικονομεί εύρος ζώνης.





Σχήμα 4 - Access Point.

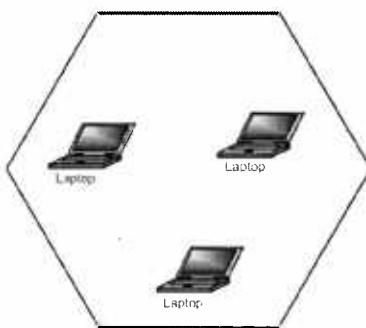
Στην περίπτωση των ασύρματων τοπικών δικτύων, οι γέφυρες ονομάζονται Σημεία Πρόσβασης (Access Points) και έχουν δύο διεπαφές. Η μία τους επιτρέπει να μεταδίνουν στο και να λαμβάνουν από το ασύρματο μέσο και η δεύτερη να συνδέονται με κάποιο τοπικό δίκτυο (π.χ. CSMA/CD).

1.4.2 Ασύρματα τοπικά δίκτυα.

1.4.2.1 Peer to Peer.

Στην περίπτωση σπιτιών και μικρών γραφείων, ενδέχεται να μην υπάρχει ανάγκη για γέφυρες και να αρκεί ένα Peer to Peer δίκτυο. Αυτό σημαίνει ότι τα δίκτυο αποτελείται μόνο από ισότιμους υπολογιστές, εφοδιασμένους με κάρτες δικτύου.

Η περιοχή – κελί – που καλύπτει ένα τέτοιο δίκτυο αποκαλείται, στο πρότυπο IEEE 802.11, Basic Service Area (BSA) και καλύπτει από 20 έως 100 μέτρα περίπου. Ενα BSA μπορεί να υποστηρίξει μέχρι 25 χρήστες με αποδεκτή καθυστέρηση.

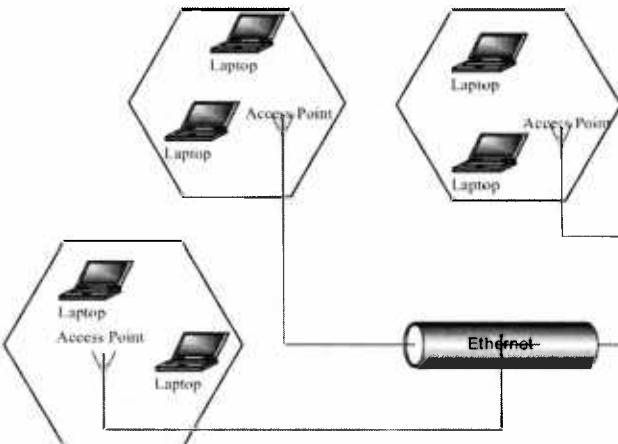


Σχήμα 5 - Peer to Peer.

1.4.2.2 Πολλαπλών κελιών.

Αν οι απαιτήσεις σε αριθμό χρηστών ή περιοχή κάλυψης, δεν καλύπτονται από ένα Peer to Peer δίκτυο, υπάρχει η λύση εγκατάστασης πολλαπλών κελιών. Τα κελιά αυτά

επικοινωνούν μεταξύ τους με κάποια “Σημεία Πρόσβασης” (Access Points) που διασυνδέονται μέσω ενός δικτύου κορμού.



Σχήμα 6 - Πολλαπλά Κελιά.

Αυτή η διάρθρωση μπορεί να επεκταθεί σε πολλούς ορόφους ενός κτιρίου. Μια συσκευή εφοδιασμένη με κάρτα δικτύου μπορεί να επικοινωνεί με το υπόλοιπο δίκτυο ανεξάρτητα από τον χώρο που βρίσκεται (και κατά συνέπεια από το ποιο είναι το πλησιέστερο Access Point).

1.4.3 Ασύρματα μητροπολιτικά δίκτυα.

Πολλές φορές, η έδρα μιας εταιρείας ή ενός οργανισμού εκτείνεται σε πολλά οικοδομικά τετράγωνα, που πρέπει να έχουν την δυνατότητα επικοινωνίας.

Η λύση που συνήθως δίνεται σε αυτό το θέμα είναι η μίσθωση τηλεπικοινωνιακών γραμμών για την διασύνδεση. Οι γραμμές αυτές χρησιμοποιούν καλώδια χαλκού ή οπτικές ίνες. Η εγκατάσταση αυτών των καλωδίων είναι συχνά δύσκολη και δαπανηρή, κυρίως όταν πρέπει να καλυφθούν μεγάλες αποστάσεις. Εξίσου δαπανηρή μπορεί να αποβεί και η συντήρηση αυτών των εγκαταστάσεων.

Μια αντιμετώπιση σε αυτά τα ζητήματα έρχονται να προτείνουν τα Ασύρματα Μητροπολιτικά Δίκτυα.

1.4.3.1 Δίκτυα Σημείου σε Σημείο (Point to Point) βασισμένα σε ραδιοκύματα.

Σε αυτή την περίπτωση μπορούμε να πετύχουμε διασύνδεση χώρων που απέχουν μεταξύ τους μερικές δεκάδες χιλιόμετρα. Οι τεχνικές που χρησιμοποιούνται είναι παρόμοιες με αυτές των τοπικών δικτύων με ραδιοκύματα. Υπάρχουν, όμως, και μερικές πολύ βασικές διαφορές.

Η κυριότερη διαφορά είναι ότι οι κεραίες που χρησιμοποιούνται δεν εκπέμπουν προς όλες τις κατευθύνσεις (omni directional) αλλά συγκεντρώνουν όλη την ισχύ του σήματος (<1Watt) σε μια λεπτή δέσμη, επιτυγχάνοντας, έτσι, την μεγαλύτερη ακτίνα δράσης. Η

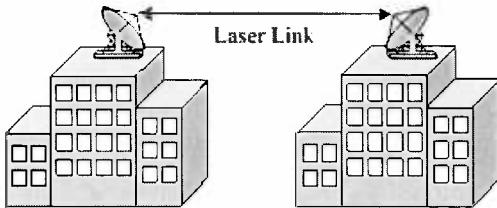
ακτίνα δράσης, με την σειρά της, επηρεάζεται από περιβαλλοντολογικά φαινόμενα, όπως η βροχή, που μπορούν να την μειώσουν.

Έτσι, μπορούν να επιτευχθούν ρυθμοί μέχρι 11Mbps, για απόσταση περίπου μέχρι 5 Km. Αυξανόμενης της απόστασης (μέχρι 50Km), οι ρυθμοί που επιτυγχάνονται είναι σημαντικά χαμηλότεροι.

1.4.3.2 Δίκτυα Σημείου σε Σημείο βασισμένα σε Laser.

Αντί για ραδιοκύματα, μπορούμε το σήμα να το διαδώσουμε με ακτίνα Laser, σε μια πολύ λεπτή δέσμη συγκεκριμένου μήκους κύματος.

Ένα Modem διαμορφώνει τα δεδομένα ως μια δέσμη φωτός, ικανή να τα μεταδώσει. Οι ρυθμοί, σε αυτή την περίπτωση μπορούν να είναι εξαιρετικά ψηλοί, μέχρι και πάνω από 20Mbps.



Σχήμα 7 - Σύνδεση Point to Point με Laser.

Για να διατηρηθεί ένα επίπεδο φυσικής ασφάλειας στη μετάδοση, η μέγιστη απόσταση είναι, συνήθως, χαμηλότερη του μιλίου (1609m) και τα προϊόντα είναι κλάσης III. Ψηλότερες τιμές για την απόσταση θα μπορούσαν να επιτευχθούν, αυξάνοντας την ισχύ του σήματος, αλλά η ακτίνα θα μπορούσε, τότε, να προκαλέσει ζημιές σε κτίρια ή ζωντανούς οργανισμούς.

Ένας πολύ βασικός παράγοντας που επηρεάζει αυτή την μορφή επικοινωνίας είναι οι καιρικές συνθήκες. Η βροχή, η υγρασία και το χιόνι προξενούν εξασθένηση του σήματος. Για παράδειγμα, η δυνατή βροχή προκαλεί περίπου 6dB εξασθένηση ανά χιλιόμετρο. Επιπλέον, το ηλιακό φως περιέχει περίπου 60% υπέρυθρη ακτινοβολία που ενδέχεται να προκαλέσει παρεμβολές. Έτσι θα πρέπει να αποφεύγεται η τοποθέτηση των πομπών – δεκτών με προσανατολισμό Ανατολικό ή Δυτικό.

Τέλος, σε θέματα υποκλοπής, οι ακτίνες Laser, είναι πολύ ασφαλείς, γιατί για να υποκλέψει κάποιος το σήμα, θα πρέπει να τοποθετήσει έναν δέκτη ακριβώς στο μονοπάτι της ακτίνας, το οποίο είναι δύσκολο. Εκτός αυτού, υπάρχει και μεγάλη πιθανότητα το σήμα να εξασθενήσει τόσο πολύ ώστε να μην φτάσει καν στον προτιθέμενο παραλήπτη, κάτι που θα αναγκάσει τον ιδιοκτήτη της σύνδεσης να ελέγξει την εγκατάστασή του.

1.4.3.3 Δίκτυα Σημείου σε Πολλαπλά Σημεία.

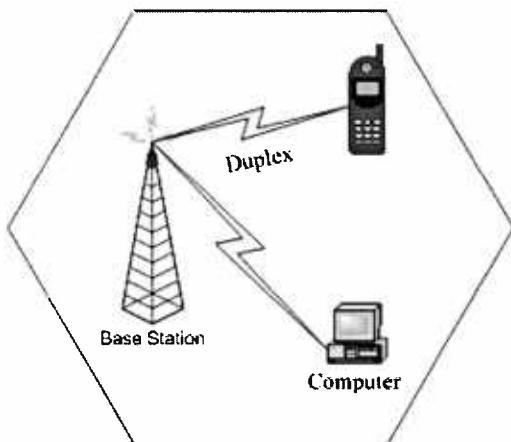
Είναι μια λύση που έχει αρχίσει πρόσφατα να κερδίζει έδαφος, μιας και έχει κερδίσει την προσοχή μεγάλων τηλεπικοινωνιακών οργανισμών. Πρόκειται για αυτό που

αποκαλείται σταθερή ασύρματη πρόσβαση (fixed wireless access), όπου μια κεραία τοποθετημένη σε κάποιο υψόμετρο, μπορεί να προσφέρει υπηρεσίες τηλεφωνίας και διαδικτύου σε πολλούς χρήστες – συνδρομητές, που διαθέτουν κατάλληλο εξοπλισμό, σε ακτίνα πολλών χιλιομέτρων.

Δυο πρωτόκολλα που έχουν αναπτυχθεί για αυτόν τον σκοπό είναι τα LMDS (Local Multipoint Distribution System) και MMDS (Multichannel Multipoint Distribution System).

Το MMDS είναι σχεδιασμένο για τις ζώνες συγχοτήτων των 2.1 έως 2.7GHz με ισχύ από 1 έως 100Watt. Δεν απαιτείται οπτική επαφή με τον δέκτη.

Το LMDS έχει ακτίνα περίπου 5Km και απαιτείται οπτική επαφή μεταξύ πομπού και δέκτη. Είναι σύστημα με κυψέλες όπου κάποιοι σταθμοί βάσης (Base Stations) συνδέονται με ένα κεντρικό σημείο ελέγχου. Κάθε σταθμός βάσης καλύπτει την περιοχή μιας κυψέλης. Το LMDS υποστηρίζει ρυθμισύς έως 155Mbps με ισχύ σήματος από 1 έως 100Watt.



Σχήμα 8 - Μια Κυψέλη LMDS.

Πρόσφατα, τον Δεκέμβριο 2000, η ελληνική ρυθμιστική αρχή σε ζητήματα τηλεπικοινωνιών, η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.), διοργάνωσε δημοπρασία στην οποία δόθηκαν άδειες για εγκατάσταση δικτύου και παροχή υπηρεσιών Σταθερής Ασύρματης Πρόσβασης. Δημοπρατήθηκαν 7 άδειες και αγοράστηκαν οι 6 από 5 εταιρείες. Το πρωτόκολλο που θα χρησιμοποιείται θα είναι το LMDS. Οι άδειες ήταν 3 στην φασματική περιοχή των 3.5GHz και 4 σε αυτή των 25GHz. Μια επιπλέον άδεια από κάθε κατηγορία, χορηγήθηκε στον Ο.Τ.Ε. μετά από το τέλος των διαδικασιών, αντί προσυμφωνημένης τιμής.

2 ΤΟ ΠΡΟΤΥΠΟ ΙΕΕΕ 802.11.

Σε αυτό το τμήμα του κειμένου θα γίνει μια σύντομη αναφορά στο πρότυπο IEEE 802.11. Συγκεκριμένα θα περιγραφεί γενικά η οικογένεια προτύπων IEEE 802, θα παρατεθούν ορισμένα ιστορικά στοιχεία και τέλος θα γίνει μια σύντομη περιγραφή του επιπέδου MAC και του φυσικού επιπέδου, όπως αυτά ορίζονται στην περίπτωση των ασύρματων τοπικών δικτύων.

2.1 Η ΟΙΚΟΓΕΝΕΙΑ ΠΡΟΤΥΠΩΝ ΙΕΕΕ 802.

Το ερευνητικό έργο IEEE 802 αποκαλείται επίσης και LMSC το οποίο σημαίνει LAN / MAN Standards Committee, δηλαδή επιτροπή προτύπων για τοπικά και μητροπολιτικά δίκτυα. Ασχολείται κυρίως με την ανάπτυξη προτύπων για τα δύο κατώτερα επίπεδα του μοντέλου OSI. Η επιτροπή αυτή συνεργάζεται στενά με άλλες διεθνείς επιτροπές και πολλά από τα πρότυπα που έχει προτείνει έχουν ήδη υιοθετηθεί από τον Διεθνή Οργανισμό Προτυποποίησης (ISO). Για παράδειγμα, το IEEE 802.11 με το οποίο θα ασχοληθούμε υιοθετήθηκε από τον ISO ως ISO/IEC 8802.11: 1999.

Η πρώτη συνεδρίαση της LMSC έγινε τον Φεβρουάριο του 1980. Προβλεπόταν η δημιουργία ενός προτύπου για τοπικά δίκτυα. Θα χωριζόταν σε Φυσικό Επίπεδο (PHY), επίπεδο MAC και διεπαφή ανώτερου επιπέδου (Higher Level Interface – HILI). Η μέθοδος πρόσβασης βασίστηκε στο Ethernet και στην τοπολογία Bus. Τελικά, τρία χρόνια αργότερα, ολοκληρώθηκαν τρία διαφορετικά MAC επίπεδα, τα CSMA/CD, Token Bus και Token Ring. Πρόκειται για τα πολύ γνωστά πρότυπα IEEE 802.3 – 4 – 5.

802.10 Security		802.2 Logical Link Control (LLC)							OSI Επίπεδο Σύνδεσης Δεδομένων
		802.1 Bridging							
802 Overview and Architecture	802.1 Management	802.3 CSMA/CD	802.4 Token Bus	802.5 Token Ring	802.6 MAN	802.9 Integrated Services LAN	802.11 WLAN	802.12 Demand Priority	
		MAC	MAC	MAC	MAC	MAC	MAC	MAC	
		802.3 PHY	802.4 PHY	802.5 PHY	802.6 PHY	802.9 PHY	802.11 PHY	802.12 PHY	
OSI Φυσικό Επίπεδο									

Σχήμα 9 - Η Συσχέτιση των Προτύπων IEEE 802.

Επίσης προτυποποιήθηκε ένα πρωτόκολλο Επιπέδου Σύνδεσης Δεδομένων (Data Link Control Layer – Επίπεδο 2 κατά OSI), το οποίο είχε σαν σκοπό την ενοποίηση όλων

των MAC επιπέδων με μια κοινή διεπαφή προς τα ανώτερα επίπεδα. Αυτό αποτέλεσε το IEEE 802.2 και ονομάστηκε LLC (Logical Link Control). Το LLC αποτελεί μια προσαρμογή του HDLC, το οποίο αναπτύχθηκε από τον ISO, κατάλληλη για τοπικά δίκτυα. Ειδικότερα, υιοθετεί από το HDLC μόνο τον ένα από τους τρεις τρόπους λειτουργία, τον ABM (Asynchronous Balanced Mode). Το υποεπίπεδο LLC, έχει μεγάλη σημασία γιατί επιτρέπει την διασύνδεση υπολογιστών ανεξαρτήτως του χρησιμοποιούμενου MAC επιπέδου. Επίσης, ως υποσύνολο του HDLC, επιτρέπει την διασύνδεση τοπικών δικτύων με δίκτυα ευρείας περιοχής (WANs).

Ο παραπάνω πίνακας περιλαμβάνει τα περισσότερα, αλλά όχι όλα τα πρότυπα της οικογένειας IEEE 802. Σκοπός του είναι να αναδείξει την γενικότερη αρχιτεκτονική του IEEE 802. Τα περιεχόμενά του αλλάζουν συνεχώς, καθώς προστίθενται νέα πρότυπα και μετονομάζονται παλαιότερα.

Είναι, επίσης, προφανές από τον πίνακα, ότι η επιτροπή του έργου δεν ασχολήθηκε καθόλου με τα ανώτερα επίπεδα δικτύων αλλά ανέπτυξε πρότυπα μόνο για τα κατώτερα επίπεδα, μέχρι το επίπεδο σύνδεσης δεδομένων (DLC). Αυτό οφείλεται στο ότι, στην περίπτωση των τοπικών δικτύων, δεν υπάρχει ανάγκη για εξειδικευμένα πρωτόκολλα δρομολόγησης, άρα ούτε για ειδικό επίπεδο δικτύου (Network Layer – επίπεδο 3 κατά OSI). Φαίνεται επίσης η διάσπαση του Επιπέδου Σύνδεσης Δεδομένων σε δύο υποεπίπεδα, τα MAC και LLC, διάσπαση που παρατηρείται στα τοπικά και στα μητροπολιτικά δίκτυα. Έτσι το ανώτερο τμήμα του επιπέδου αυτού, δηλαδή το LLC, προσφέρει μια διεπαφή με τα ανώτερα επίπεδα, ενώ το κατώτερο, δηλαδή το MAC, επικοινωνεί με το φυσικό επίπεδο.

2.2 ΙΣΤΟΡΙΚΟ ΤΟΥ IEEE 802.11.

Το 1985 η Federal Communications Committee (FCC), η ρυθμιστική αρχή των ΗΠΑ, νομιμοποίησε την δημόσια χρήση της ζώνης συχνοτήτων από τα 902MHz έως τα 5.85GHz, η οποία ονομάστηκε ISM (Industrial, Scientific and Medical). Αυτό σήμαινε, με απλά λόγια, ότι επιτρεπόταν η χρήση συσκευών, που λειτουργούν σε αυτές τις συχνότητες, χωρίς ειδική άδεια από το κράτος, αρκεί να λειτουργούν σε ισχύ χαμηλότερη του 1Watt.

Έτσι οι χρήστες ασύρματων δικτύων δεν θα χρειάζονταν άδεια από το FCC για τις εγκαταστάσεις τους, αν το δίκτυό τους λειτουργούσε σε αυτή την ζώνη συχνοτήτων. Ως αποτέλεσμα αυτού, άρχισε η ανάπτυξη συσκευών για ασύρματα τοπικά δίκτυα. Η έλλειψη προτυποποίησης, όμως, είχε σαν αποτέλεσμα την μη διαλειτουργικότητα των συσκευών διαφορετικών κατασκευαστών και το ψηλό κόστος τους.

Τον Μάιο του 1991, το ινστιτούτο IEEE (Institute for Electrical and Electronic Engineers) ξεκίνησε εργασίες για ένα πρότυπο για ασύρματα τοπικά δίκτυα.

Το πρότυπο IEEE 802.11 για ασύρματα τοπικά δίκτυα ολοκληρώθηκε τον Ιούνιο του 1997, όταν εκδόθηκε η τελική έκδοση, η οποία καθορίζει ως συχνότητα λειτουργίας την ζώνη των 2.4GHz με ρυθμούς μετάδοσης δεδομένων 1Mbps και 2Mbps.

Μέσα στο 1999 εκδόθηκαν δύο επιπλέον συμπληρώματα για το πρότυπο αυτό, τα IEEE 802.11a και IEEE 802.11b, με σκοπό την επίτευξη ψηλότερων επιδόσεων. Σύμφωνα με το 2^o από αυτά, υποστηρίζονται ρυθμοί μετάδοσης δεδομένων έως 11Mbps.

Το πρότυπο IEEE 802.11a επιφέρει μια πιο δραστική μετατροπή στο αρχικό. Με συχνότητα λειτουργίας την ζώνη των 5GHz, επιτυγχάνονται ρυθμοί μετάδοσης έως και 54Mbps. Για να είναι ένα προϊόν σύμφωνο με αυτό, πρέπει να υποστηρίζει ταχύτητα τουλάχιστον 24Mbps.

2.3 ΕΙΣΑΓΩΓΗ ΣΤΟ IEEE 802.11.

Σε αυτή την παράγραφο θα εξετασθούν ορισμένα εισαγωγικά θέματα γύρω από το πρότυπο IEEE 802.11.

2.3.1 Ο πλήρης τίτλος.

Ο πλήρης τίτλος του προτύπου είναι:

“Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”.

Επίσης έχουν εκδοθεί τα πρότυπα IEEE 802.11a και IEEE 802.11b. Οι τίτλοι τους είναι:

“Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”.

“High-speed Physical Layer in the 5 GHz Band”.

“Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification”.

“Higher-Speed Physical Layer Extension in the 2.4 GHz Band”.

2.3.2 Τα περιεχόμενα του προτύπου.

Στην εισαγωγή του επίσημου εγγράφου της IEEE για το πρότυπο 802.11 περιέχεται μια σύντομη περιγραφή για το περιεχόμενο:

“This standard defines the protocol and compatible interconnection of data communication equipment via the “air”, radio or infrared, in a local area network (LAN) using the carrier sense multiple access protocol with collision avoidance (CSMA/CA) medium sharing mechanism...”

“...The standard includes the definition of the management information base (MIB) using Abstract Syntax Notation 1 (ASN.1) and specifies the MAC

protocol in a formal way, using the Specification and Description Language (SDL)."

Σύμφωνα, λοιπόν, με τα παραπάνω, το πρότυπο ορίζει το πρωτόκολλο και την συμβατή διασύνδεση συσκευών επικοινωνίας δεδομένων μέσω αέρος, ραδιοκυμάτων ή υπέρυθρων ακτινών σε ένα τοπικό δίκτυο χρησιμοποιώντας, για το διαμερισμό του μέσου, το πρωτόκολλο Carrier Sense Multiple Access με Αποφυγή Συγκρούσεων (Collision Avoidance), CSMA/CA. Το πρότυπο συμπεριλαμβάνει τον ορισμό της Βάσης Πληροφοριών Διαχείρισης (Management Information Base – MIB) χρησιμοποιώντας Abstract Syntax Notation 1 (ASN.1) και καθορίζει το MAC πρωτόκολλο με την χρήση της Specification Description Language (SDL).

Πιο συγκεκριμένα το πρότυπο περιγράφει τα εξής:

- Τις λειτουργίες και τις υπηρεσίες που απαιτούνται από μια συσκευή συμβατή με αυτό, ώστε αυτή να λειτουργήσει εντός ενός δικτύου και κατά την μετακίνησή της μεταξύ δικτύων.
- Τις MAC διεργασίες που υποστηρίζουν την παράδοση MAC Service Data Units (MSDUs).
- Τις διάφορες τεχνικές σηματοδοσίας σε φυσικό επίπεδο.
- Τρόπους ώστε μια συσκευή να λειτουργεί σε ένα συγκεκριμένο ασύρματο τοπικό δίκτυο, ακόμα και αν αυτό συνυπάρχει με άλλα επικαλυπτόμενα.
- Τις απαιτήσεις και τις διεργασίες που παρέχουν μυστικότητα των δεδομένων που μεταφέρονται από το μέσο και υπηρεσίες αυθεντικοποίησης.
- Τρόπους για να προσφέρεται η υπηρεσία του δικτύου σε ευρύτερη περιοχή (Extended Area) μέσω ενός συστήματος διανομής, όπως Ethernet.
- Υπηρεσίες πολυμετάδοσης και πανεκπομπής (multicast και broadcast).

2.4 ΟΙ ΣΥΝΕΠΕΙΕΣ ΤΗΣ ΙΔΙΟΜΟΡΦΙΑΣ ΤΩΝ WLAN.

Η ομάδα ανάπτυξης του προτύπου δεν θα μπορούσε να μην λάβει υπ' όψιν τις τις σοβαρές ιδιαιτερότητες που παρουσιάζουν τα ασύρματα τοπικά δίκτυα. Αυτές οφείλονται, σε μεγάλο βαθμό, από τις συνέπειες που επιφέρει στον σχεδιασμό το μέσο μετάδοσης. Έτσι, στο πρότυπο, γίνεται ιδιαίτερη αναφορά στα παρακάτω θέματα.

2.4.1 Διαχείριση ισχύος.

Οι περισσότερες κάρτες που προσφέρουν διασύνδεση με ασύρματα τοπικά δίκτυα, κυκλοφορούν σε PCMCIA μορφή. Αυτό για να είναι δυνατόν να εξοπλίσει κάποιος ένα φορητό υπολογιστή με μια από αυτές. Όμως, οι υπολογιστές αυτοί βασίζονται σε μπαταρίες για να λειτουργήσουν. Η προσθήκη κάρτας δικτύου μπορεί να μειώσει

δραστικά την διάρκεια ζωής της μπαταρίας. Επιπλέον δεν μπορούμε, κατά τον σχεδιασμό, να θεωρήσουμε ότι ο δέκτης ενός υπολογιστή θα είναι πάντα σε ετοιμότητα.

Κατά το πρότυπο IEEE 802.11, η εξοικονόμηση ενέργειας επιτυγχάνεται στο επίπεδο MAC, που έχει ενσωματωμένες λειτουργίες διαχείρισης ενέργειας. Βάσει αυτών, η κάρτα μπαίνει σε τρόπο λειτουργίας “sleep”, όταν δεν έχει δεδομένα προς μετάδοση. Επιπλέον, χρησιμοποιούνται ενταμιευτές οι οποίοι αποθηκεύουν τα εισερχόμενα μηνύματα. Περιοδικά η κάρτα “ξυπνάει” και ελέγχει αυτούς τους ενταμιευτές. Έτσι αποφεύγεται η απώλεια εισερχόμενων μηνυμάτων.

2.4.2 Εύρος ζώνης.

Η ζώνη συχνοτήτων που λειτουργούν τα ασύρματα τοπικά δίκτυα δεν προσφέρει δυνατότητα για υψηλές ταχύτητες μετάδοσης. Η IEEE κάνει προσπάθειες εξοικονόμησης εύρους ζώνης με μεθόδους συμπίεσης δεδομένων.

2.4.3 Διευθύνσεις.

Σε ένα ενσύρματο δίκτυο η διεύθυνση δικτύου είναι ισοδύναμη με την φυσική διεύθυνση και αυτό εξυπακούεται κατά την σχεδίαση.

Η τοπολογία ενός ασύρματου δίκτυου είναι δυναμική. Ένας σταθμός μπορεί να μεταφερθεί από ένα χώρο σε έναν άλλο και πρέπει να συνεχίσει να έχει πρόσβαση στο δίκτυο. Για τον λόγο αυτό, η λογική διεύθυνση ενός υπολογιστή (π.χ. IP address) δεν αντιστοιχεί πάντα με την φυσική του διεύθυνση. Έτσι δημιουργείται πρόβλημα δρομολόγησης των πακέτων στον προτιθέμενο προορισμό τους. Για την αντιμετώπιση αυτού του θέματος έχει προταθεί η λύση του Mobile IP.

2.4.4 Ο αντίκτυπος του μέσου στον σχεδιασμό.

Μεγάλες ιδιαιτερότητες επιβάλλει και το μέσο μετάδοσης των δεδομένων στον σχεδιασμό. Η διάδοση μέσω αέρα, είτε με ραδιοκύματα είτε με υπέρυθρες, έχει μεγάλες διαφορές σε σχέση με την διάδοση με ενσύρματα μέσα, όπως ο χαλκός ή οι οπτικές ίνες. Αυτό συμβαίνει γιατί:

- Το μέσο είναι απροστάτευτο από ξένα σήματα.
- Δεν υπάρχουν απόλυτα ούτε άμεσα ορατά φυσικά όρια.
- Η αξιοπιστία του μέσου είναι σημαντικά χαμηλότερη.
- Δεν υπάρχει πλήρης σύνδεση μεταξύ των σταθμών. Έτσι η υπόθεση ότι όταν εκπέμπει ένας υπολογιστής, ακούν όλοι οι υπόλοιποι (πολλαπλή πρόσβαση), δεν ισχύει. Υπάρχουν περιπτώσεις που ένας σταθμός μπορεί να είναι “κρυμμένος” από έναν άλλο.



2.4.5 Αλληλεπίδραση με τα υπόλοιπα επίπεδα IEEE 802.

Είναι απαραίτητη προϋπόθεση, ένα δίκτυο σύμφωνο με το IEEE 802.11, να φαίνεται στα ανώτερα επίπεδα ως δίκτυο του κλασικού τύπου IEEE 802. Με άλλα λόγια το LLC δεν πρέπει να διαχωρίζει, ούτε να “ξέρει” αν το επίπεδο MAC είναι τύπου Ethernet ή IEEE 802.11. Έτσι, η κινητικότητα των σταθμών πρέπει να διαχειριστεί από το επίπεδο MAC. Επιπλέον, το επίπεδο LLC, είναι σχεδιασμένο κατά τέτοιο τρόπο ώστε να θεωρεί ως δεδομένη την αξιοπιστία των παρακάτω επιπέδων. Το μη αξιόπιστο του μέσου υποχρεώνει να προστεθεί στο επίπεδο MAC του IEEE 802.11, λειτουργικότητα που δεν υπάρχει στα MAC επίπεδα των υπόλοιπων προτύπων IEEE.

2.5 ΤΟΠΟΛΟΓΙΕΣ ΚΑΤΑ ΤΟ IEEE 802.11.

Το πρότυπο καθορίζει ένα σύνολο από συνιστώσες (components) που αποτελούν ένα ασύρματο τοπικό δίκτυο και που, αλληλεπιδρώντας επιτρέπουν, η μεταφορά σταθμών από το ένα σημείο σε ένα άλλο να γίνεται αδιαφανώς προς τα ανώτερα επίπεδα – ουσιαστικά προς το LLC.

Οποιοδήποτε εξάρτημα περιέχει διεπαφή τύπου IEEE 802.11 και την λειτουργικότητα του φυσικού επιπέδου και του επιπέδου MAC, καλείται σταθμός (STA).

Η βασική δομική μονάδα ενός IEEE 802.11 καλείται Βασικό Σύνολο Υπηρεσιών (Basic Service Set – BSS). Αποτελεί μια περιοχή η οποία προσφέρει δυνατότητα πλήρους επικοινωνίας μεταξύ των σταθμών που βρίσκονται σε αυτήν.

Οι τοπολογίες που υποστηρίζονται από το πρότυπο είναι οι εξής δύο:

2.5.1 Independent Basic Service Set (IBSS) Δίκτυο.

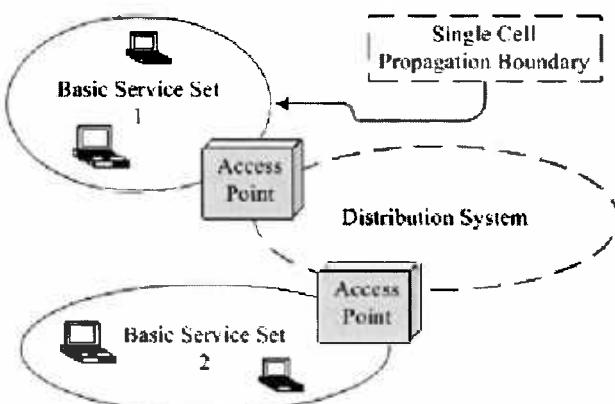
Αποτελείται από τουλάχιστον δύο σταθμούς σε ένα μοναδικό και ανεξάρτητο BSS. Είναι ο βασικότερος τύπος IEEE 802.11 δικτύου. Αποκαλείται και δίκτυο Ad Hoc διότι η εγκατάστασή του είναι άμεση και δεν χρειάζεται σχεδόν κανένα σχεδιασμό. Καλύπτει τις ανάγκες χρηστών που βρίσκονται σε έναν μικρό χώρο π.χ. ένα δωμάτιο.

Η συσχέτιση (association) ενός σταθμού με ένα BSS γίνεται δυναμικά. Όταν ένας σταθμός βγει από μια περιοχή και έρθει εντός των ορίων μιας άλλης, θα γίνει “associated”. Αυτή η υπηρεσία αναλαμβάνεται από την “Υπηρεσία Συστήματος Διανομής” (Distribution System Service – DSS)

2.5.2 Extended Service Set (ESS) Δίκτυο.

Όταν οι ανάγκες των χρηστών – για παράδειγμα η περιοχή κάλυψης – δεν καλύπτονται από ένα IBSS, τότε χρησιμοποιείται η τοπολογία ESS, που επιτρέπει την διασύνδεση πολλών σταθμών σε δίκτυο μεγάλης περιοχής κάλυψης και ψηλής πολυπλοκότητας.

Αυτό επιτυγχάνεται με την εισαγωγή μιας νέας συνιστώσας που καλείται “Σύστημα Διανομής” (Distribution System – DS). Το πρότυπο διαχωρίζει λογικά το ασύρματο μέσο (Wireless Medium – WM) από το μέσο που χρησιμοποιεί το DS. Ετσι δεν απαιτείται τα δύο μέσα να είναι ίδια ή ανόμοια. Για παράδειγμα το μέσο διανομής μπορεί να είναι ένα δίκτυο FDDI, ATM ή μια Point to Point γραμμή. Το DS προσφέρει τις λογικές υπηρεσίες που είναι απαραίτητες για την ενοποίηση απεριόριστου αριθμού από BSS. Τέτοια υπηρεσία είναι, για παράδειγμα, η αντιστοίχηση διεύθυνσης δικτύου με φυσική διεύθυνση. Έτσι εξασφαλίζεται η επικοινωνία ενός σταθμού που ανήκει στο BSS₁ και ενός άλλου που ανήκει στο BSS₂.



Σχήμα 10 - Extended Service Set (ESS).

Η διασύνδεση του BSS με το DS γίνεται με την χρήση ενός “Σημείου Πρόσβασης” (Access Point – AP). Ένα Access Point, λειτουργεί ως σταθμός και προσφέρει ταυτόχρονα και υπηρεσίες του Συστήματος Διανομής. Έχει, συνήθως, δύο διεπαφές. Η μία χρησιμεύει στην σύνδεση με το ασύρματο δίκτυο και η άλλη με το Σύστημα Διανομής. Στην περίπτωση που θέλουμε να συνδέσουμε ένα δίκτυο IEEE 802.11 με ένα άλλο τοπικό ενσύρματο δίκτυο (LAN), τότε χρησιμοποιείται ένα Portal. Όταν το Σύστημα Διανομής είναι τεχνολογίας IEEE 802.x το Portal και το Access Point είναι ένα και το αυτό. Κλασσικά Access Points που κυκλοφορούν στην αγορά έχουν μια διεπαφή σύμφωνη με το IEEE 802.11 και μία διεπαφή Ethernet.

Ένα ESS λειτουργεί με πλήρη διαφάνεια ως προς το επίπεδο LLC. Αυτό σημαίνει ότι ένας σταθμός μπορεί να βρεθεί από ένα BSS σε ένα άλλο – πάντα μέσα στο ίδιο ESS – χωρίς αυτό να χρειάζεται να γνωστοποιηθεί στο LLC.

2.5.2.1 Μεταβάσεις (Transitions).

Σχετικά με την μετακίνηση των σταθμών, το πρότυπο ορίζει τους εξής τύπους, τους οποίους αναφέρει ως μεταβάσεις (Transitions).

1. No – transition.

Οι σταθμοί μετακινούνται αλλά παραμένουν πάντα μέσα στο ίδιο BSS.

2. BSS – transition.

Οι σταθμοί μετακινούνται μεταξύ BSS αλλά δεν φεύγουν ποτέ από τα όρια του ESS.

3. ESS – transition.

Οι σταθμοί φεύγουν από ένα ESS και μπαίνουν στα όρια ενός άλλου ESS.

Το πρότυπο υποστηρίζει ξεκάθαρα τις δύο πρώτες περιπτώσεις. Η πρώτη αντιμετωπίζεται στην περίπτωση ενός IBSS και η δεύτερη στην περίπτωση ενός ESS δικτύου, όπου η μετακίνηση γίνεται δυνατή με την χρήση του Συστήματος Διανομής και των Σημείων Πρόσβασης. Ωστόσο δεν δίνεται καμία εγγύηση ότι θα συνεχίσει να υπάρχει σύνδεση στην Τρίτη περίπτωση. Μάλιστα το πρότυπο αναφέρει ότι το πιθανότερο ενδεχόμενο είναι να διακοπεί.

2.5.2.2 Επικαλύψεις μεταξύ των συνιστωσών.

Εντός του ίδιου ESS, επιτρέπονται οι ακόλουθες διαρθρώσεις για τα BSS.

1. Μερική Επικάλυψη (BSSs partially Overlap).

Αυτή η διάρθρωση μας επιτρέπει να έχουμε πλήρη κάλυψη σε μία συγκεκριμένη περιοχή. Χρησιμεύει όταν μια εφαρμογή δεν μπορεί να ανεχθεί διακοπές των υπηρεσιών του δικτύου κατά την μετακίνηση.

2. Καμία Επικάλυψη (Physically Disjointed BSSs).

Τα BSSs δεν έχουν επικαλύψεις. Να σημειωθεί ότι δεν υπάρχει όριο απόστασης μεταξύ δύο BSS. Το όριο το επιβάλει ο σχεδιασμός και η τεχνολογία του Συστήματος Διανομής.

3. Παράθεση (Physically Collocated BSSs).

Μας χρειάζεται αν επιθυμούμε αυξημένες επιδόσεις ή αξιοπιστία.

4. Ταυτόχρονη ύπαρξη ενός ή παραπάνω ESSs με ένα ή παραπάνω BSSs.

Ένα παράδειγμα είναι όταν επιθυμούμε ένα Ad Hoc δίκτυο να βρίσκεται στην ίδια περιοχή με ένα ESS αλλά να μην ανήκει – να μην έχει πρόσβαση – σε αυτό.

2.6 ΛΟΓΙΚΗ ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ IEEE 802.11.

Λέγοντας λογική αρχιτεκτονική εννοούμε την περιγραφή του τρόπου λειτουργίας ενός δικτύου. Αν παρατηρήσουμε το σχήμα παρακάτω έχουμε να πούμε ότι σε κάθε σταθμό υλοποιούνται τα τρία επίπεδα της στοίβας πρωτοκόλλων. Συγκεκριμένα υλοποιούνται τα επίπεδα MAC και LLC και ένα από τα φυσικά επίπεδα. Από αυτά, μόνο το MAC και το φυσικό επίπεδο αποτελούν μέρος του προτύπου IEEE 802.11. Το LLC αποτελεί ξεχωριστό πρότυπο (IEEE 802.2).



Logical Link Control (LLC)				
Medium Access Control (MAC)				
Frequency Hopping (FHSS) PHY (802.11)	Direct Sequence (DSSS) PHY (802.11)	Orthogonal Frequency Division Multiplexing (OFDM) PHY (802.11a)	High – Rate Direct Sequence (HR – DSSS) PHY (802.11b)	Infrared Light PHY (802.11)

Σχήμα 11 - Η Στοίβα Πρωτοκόλλων του IEEE 802.11.

2.7 ΥΠΗΡΕΣΙΕΣ.

Στο πρότυπο IEEE 802.11 ορίζεται ένα σύνολο υπηρεσιών που προσφέρουν οι σταθμοί και το Σύστημα Διανομής. Οι υπηρεσίες αυτές προσφέρονται από το επίπεδο MAC.

2.7.1 Υπηρεσίες Σταθμού.

Οι υπηρεσίες σταθμού (Station Services) προσφέρονται από όλους τους σταθμούς του δικτύου, Access Points, Laptops κλπ. Αντιμετωπίζουν κυρίως το θέμα της περιορισμένης φυσικής ασφάλειας που χαρακτηρίζει τα Wireless LANs.

2.7.1.1 Αυθεντικοποίηση (Authentication).

Όλοι οι σταθμοί, πρέπει να χρησιμοποιήσουν αυτή την υπηρεσία πριν εγκαταστήσουν σύνδεση με οποιονδήποτε άλλο σταθμό. Για να συμβεί αυτό, αποστέλλεται ένα unicast πλαίσιο διαχείρισης (Management Frame), στον αντίστοιχο σταθμό.

Η αυθεντικοποίηση μπορεί να γίνει με δύο τρόπους:

- Ανοικτού Συστήματος.
- Μυστικού Κλειδιού.

Και οι δύο τρόποι θα αναλυθούν αργότερα στην παράγραφο που αναφέρεται στο MAC.

2.7.1.2 Deauthentication.

Όταν ένας σταθμός αποσυνδεθεί στέλνει ένα Deauthentication πλαίσιο.

2.7.1.3 Privacy.

Η υπηρεσία Privacy έχει σχεδιαστεί ώστε να προσφέρει ένα επίπεδο ασφάλειας ισοδύναμο με αυτή των ενσύρματων δικτύων. Για τον λόγο αυτό αποκαλείται Wireless Equivalent Privacy – WEP. Ουσιαστικά πρόκειται για μετάδοση των πλαισίων με

κρυπτογραφημένα δεδομένα. Κρυπτογραφούνται τα πάντα εκτός από τις επικεφαλίδες του φυσικού επιπέδου, με αλγόριθμους 64bit ή 128bit.

2.7.2 Υπηρεσίες Συστήματος Διανομής.

Οι υπηρεσίες αυτές προσφέρονται κυρίως από τα Access Points.

2.7.2.1 Association.

Κάθε σταθμός γίνεται Associate με ένα Access Point πριν μπορέσει να στείλει δεδομένα που θα περάσουν μέσα από το σύστημα διανομής. Κάθε σταθμός μπορεί να είναι Associated μόνο με ένα Access Point.

2.7.2.2 Disassociation.

Αυτή η υπηρεσία χρησιμοποιείται όταν ένας σταθμός βγαίνει από το δίκτυο. Ένα Access Point κάνει Disassociate όλους τους σταθμούς όταν παύει να λειτουργεί.

2.7.2.3 Reassociation.

Αυτή η υπηρεσία καλείται όταν ένας σταθμός που είναι Associated με ένα Access Point, επιθυμεί να αλλάξει τις παραμέτρους του Association. Επίσης πρέπει να χρησιμοποιηθεί όταν ένας σταθμός αλλάζει BSS, ώστε να γίνει Associate με το νέο Access Point.

2.7.2.4 Integration.

Επιτρέπει την παράδοση MAC πλαισίων σε ένα LAN μέσω ενός Portal.

2.7.2.5 Distribution.

Καλείται όταν ένας σταθμός στέλνει πλαίσια μέσω του DS. Προσφέρει αρκετές πληροφορίες ώστε να μπορεί να προσδιοριστεί το BSS προορισμού.

Μέρος 2^ο:

Τα επίπεδα MAC και Φυσικό κατά το πρότυπο IEEE 802.11.

3 ΤΟ ΦΥΣΙΚΟ ΕΠΙΠΕΔΟ ΣΤΟ ΠΡΟΤΥΠΟ IEEE 802.11.

Σε αυτή την παράγραφο θα γίνει μια λεπτομερής περιγραφή του φυσικού επιπέδου, όπως αυτό ορίζεται στο πρότυπο IEEE 802.11, καθώς και στα συμπληρωματικά πρότυπα IEEE 802.11a και IEEE 802.11b.

Θα γίνει ιδιαίτερη αναφορά στα υποεπίπεδα του φυσικού επιπέδου, τις λειτουργίες του καθενός και τις τεχνικές Spread Spectrum.

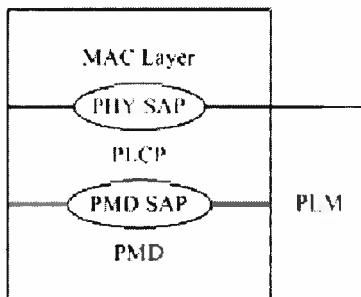
3.1 Η ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ ΦΥΣΙΚΟΥ ΕΠΙΠΕΔΟΥ.

Ο κάθε σταθμός – μέλος ενός IEEE 802.11 δικτύου, υλοποιεί τρεις συνιστώσες του φυσικού επιπέδου. Οι συνιστώσες αυτές αποτελούν το σύνολο της λειτουργικότητας του φυσικού επιπέδου.

Η πρώτη είναι η Διαχείριση Φυσικού Επιπέδου (Physical Layer Management – PLM). Λειτουργεί σε συνδυασμό με την αντίστοιχη οντότητα του επιπέδου MAC και εκτελεί λειτουργίες διαχείρισης για το επίπεδο.

Η δεύτερη είναι το άνω υποεπίπεδο του φυσικού επιπέδου και λέγεται Διαδικασία Σύγκλισης Φυσικού Επιπέδου (Physical Layer Convergence Procedure – PLCP). Η δε τρίτη είναι το κάτω υποεπίπεδο και καλείται Φυσικό Υποεπίπεδο Εξαρτώμενο από το Μέσο (Physical Medium Dependent – PMD – sublayer). Οι τρεις αυτές συνιστώσες θα περιγραφούν συνοπτικά στις δύο παραγράφους που ακολουθούν.

Αξίζει, επίσης, να σημειωθεί ότι, στο πρότυπο αναφέρεται ότι αν το PMD προσφέρει όλες τις απαιτούμενες υπηρεσίες φυσικού επιπέδου, τότε το PLCP μπορεί να έχει μηδενική λειτουργικότητα.



Σχήμα 12 - Η Αρχιτεκτονική του Φυσικού Επιπέδου.

3.1.1 Physical Layer Convergence Procedure – PLCP.

Το MAC επίπεδο επικοινωνεί με το φυσικό επίπεδο μέσω του PLCP. Συγκεκριμένα μέσω των SAP που προσφέρει το Φυσικό Επίπεδο.

Όταν το επίπεδο MAC δώσει εντολή για την μετάδοση ενός MPDU (MAC Protocol Data Unit), το PLCP προετοιμάζει τις MPDU για μετάδοση, προσθέτοντας μια επικεφαλίδα με δεδομένα αναγκαία για τους πομπούς και τους δέκτες. Το πλαίσιο, που δημιουργείται με την προσθήκη των πεδίων, αποκαλείται, στο πρότυπο IEEE 802.11, PLCP Protocol Data Unit (PPDU) και η δομή του προσφέρει το υπόβαθρο για την ασύγχρονη μεταφορά MPDUs μεταξύ δύο σταθμών.

Τέλος το PLCP αναλαμβάνει να παραδώσει τα εισερχόμενα πλαίσια στο MAC επίπεδο.

3.1.2 Physical Medium Dependent – PMD.

Το PMD, υπό την καθοδήγηση του PLCP, αναλαμβάνει την μετάδοση και λήψη των PPDUς χρησιμοποιώντας το ασύρματο μέσο μετάδοσης. Άλληλεπιδρά κατευθείαν με το μέσο και πραγματοποιεί την διαμόρφωση και αποδιαμόρφωση των σημάτων.

Η επικοινωνία PMD – PLCP γίνεται ενός SAP που καλείται PMD SAP.

3.2 ΟΙ ΛΕΙΤΟΥΡΓΙΕΣ ΤΟΥ ΦΥΣΙΚΟΥ ΕΠΙΠΕΔΟΥ.

Το PLCP εκτελεί κάποιες βασικές λειτουργίες που είναι, γενικά, ίδιες μεταξύ των διαφορετικών τύπων φυσικού επιπέδου, όπως αντοί ορίζονται στο πρότυπο.

Οι λειτουργίες είναι:

- **Carrier Sense.** Γίνεται έλεγχος για το αν το μέσο είναι κατεύλημμένο.
- **Transmit.** Αποστολή bytes δεδομένων.
- **Receive.** Παραλαβή bytes δεδομένων.

3.2.1 Carrier Sense.

Αν ο σταθμός δεν βρίσκεται σε κατάσταση αποστολή ή λήψης πλαισίου, το PLCP δίνει εντολή στο PMD να εκτελέσει την Carrier Sense λειτουργία. Ουσιαστικά γίνονται δύο υπολειτουργίες.

- Ανίχνευση Εισερχόμενου Σήματος. Το PLCP ελέγχει συνεχώς το μέσο. Αν εμφανιστεί εισερχόμενο σήμα, θα διαβαστεί το προοίμιο και η επικεφαλίδα του πλαισίου σε μια προσπάθεια του σταθμού να συγχρονιστεί.
- Εκτίμηση Ελεύθερου Καναλιού (Clear Channel Assessment – CCA). Εξακριβώνεται αν το μέσο είναι ελεύθερο ή όχι. Σε κάθε περίπτωση αποστέλλεται στο επίπεδο MAC μία PHY-CCA.ένδειξη με το πεδίο “status”

να έχει την ανάλογη τιμή. Το MAC αποφασίζει αν θα στείλει κάποιο πλαίσιο ή όχι.

Για παράδειγμα, στην περίπτωση του DSSS η λειτουργία αυτή μπορεί να γίνει με τρεις τρόπους. Το PMD μπορεί να μετράει την ένταση της ενέργειας στο μέσο ή την ύπαρξη σήματος ή και τα δύο. Ανάλογα αν η ένταση ξεπερνά ένα επίπεδο (Energy Detection – ED – threshold) ή αν υπάρχει σήμα (Carrier Sense – CS) αποστέλλεται από το PMD στο PLCP μια **PMD_ED.ένδειξη** ή μία **PMD_CS.ένδειξη**. Η επιλογή του τρόπου λειτουργίας γίνεται από παράμετρο της MIB του σταθμού.

3.2.2 Αποστολή.

Όταν το επίπεδο MAC δώσει εντολή για την αποστολή ενός πλαισίου, το PMD στέλνει ένα προοίμιο για το πλαίσιο, που αναφέρει και τον ρυθμό δεδομένων που θα χρησιμοποιηθεί. Το προοίμιο αυτό στέλνεται πάντα σε ταχύτητα 1Mbps που είναι ένας κοινός ρυθμός δεδομένων για όλους τους σταθμούς.

Στη συνέχεια ο ρυθμός δεδομένων γίνεται ίσος με αυτόν που περιγράφει το προοίμιο και αρχίζει η μετάδοση του πλαισίου.

3.2.3 Λήψη.

Όταν η εκτίμηση ελεύθερου καναλιού εκτιμήσει ότι το μέσο είναι κατεύλημμένο και ταυτόχρονα εντοπισθεί και ένα έγκυρο προοίμιο, το PLCP παρακολουθεί την επικεφαλίδα του πλαισίου. Αν αυτή είναι ελεύθερη λαθών, ενημερώνεται το επίπεδο MAC για εισερχόμενα δεδομένα μαζί με το μήκος του εισερχόμενου πλαισίου και τον ρυθμό μετάδοσης. Η ενημέρωση αυτή γίνεται με την αποστολή μιας **PHY-RXSTART.ένδειξη**.

Τα εισερχόμενα δεδομένα παραδίδονται στο MAC επίπεδο με την αποστολή από το φυσικό επίπεδο, διαδοχικών **PHY-DATA.ένδειξη**. Ταυτόχρονα υπάρχει ένας μετρητής των bytes που έχουν ληφθεί, που εξυπηρετεί στο να γνωρίζει το PLCP πότε τελειώνει το πλαίσιο. Όταν συμβεί η λήξη του πλαισίου αποστέλλεται μια **PHY-RXEND.ένδειξη**.

3.3 ΤΑ ΠΕΝΤΕ ΦΥΣΙΚΑ ΕΠΙΠΕΔΑ ΚΑΤΑ IEEE 802.11.

Σύμφωνα με το πρότυπο IEEE 802.11 και τα δύο παραρτήματα – το IEEE 802.11a και IEEE 802.11b – ορίζονται πέντε διαφορετικές μορφές για το φυσικό επίπεδο. Ουσιαστικά μιλάμε για τους διαφορετικούς τρόπους που μπορεί να υλοποιηθεί η Spread Spectrum. Έτσι, λοιπόν, ορίζονται τέσσερις τεχνολογίες (FHSS, DHSS, HR – DSSS, OFDM) και επίσης η λειτουργία του φυσικού επιπέδου στην περίπτωση που το μέσο διάδοσης είναι οι υπέρυθρες ακτίνες.

3.3.1 Frequency Hopping Spread Spectrum – FHSS.

Το FHSS λειτουργεί στην ζώνη των 2.4GHz με ρυθμούς δεδομένων 1 και 2Mbps. Είναι από τα πρώτα φυσικά επίπεδα που υλοποιήθηκαν για προϊόντα ασύρματων τοπικών δικτύων από την στιγμή που εκδόθηκε το πρότυπο.

Το υποεπίπεδο PLCP του φυσικού επιπέδου αποστέλλει τα δεδομένα που λαμβάνει από το MAC, προσθέτοντας ένα προοίμιο (PLCP Preamble), που χρησιμοποιείται για τον συγχρονισμό πομπού και δέκτη και μια επικεφαλίδα (PLCP Header), που περιέχει πληροφορίες για το πλαίσιο.

Το προοίμιο και η επικεφαλίδα στέλνονται πάντα σε ρυθμό 1Mbps. Ο ρυθμός αυξάνεται στο μέρος του Whitened PSDU, αρκεί φυσικά να υποστηρίζεται και από τους δύο σταθμούς.

Στο σχήμα που ακολουθεί, φαίνεται η δομή του PLCP PDU για το FHSS. Σημειώνονται τα όρια του προοιμίου και της επικεφαλίδας με τα αντίστοιχα μήκη σε bits.

80 bits	16 bits	12 bits	4 bits	16 bits	Μεταβλητό μήκος
SYNC	Start Frame Delimiter	PLW	PSF	Header Error Check	Whitened PSDU
PLCP προοίμιο		PLCP Επικεφαλίδα			

Σχήμα 13 - Η Δομή του PLCP PDU για το FHSS.

- **SYNC:** Διαδοχικά 0 και 1 τα οποία χρησιμοποιεί ο δέκτης για να συγχρονιστεί με τον αποστολέα.
- **Start Frame Delimiter:** Η αρχή του πλαισίου. Είναι πάντα η ακολουθία bits 0000 1100 1011 1101 με το αριστερά bit να μεταδίδεται πρώτο.
- **PLW (PSDU Length Word):** Το μήκος του Whitened PSDU σε bytes. Περνάει από το επίπεδο MAC σαν παράμετρος και παίρνει μια δεκαεξαδική τιμή από '001' μέχρι 'FFF' δηλαδή από 1 μέχρι 4095.
- **PSF (PLCP Signaling Field):** Περιέχει τον ρυθμό μετάδοσης δεδομένων με τον οποίο θα μεταδοθούν τα δεδομένα του πλαισίου. Το πρώτο bit είναι πάντα ίσο με 0 ενώ τα επόμενα παίρνουν τις τιμές που δείχνει ο πίνακας.

Bit	Παράμετρος	Τιμή
0	Δεσμευμένο	0
1 – 3	PLCP_BITRATE	000 1.0Mbps 001 1.5Mbps 010 2.0Mbps 011 2.5Mbps 100 3.0Mbps 101 3.5Mbps 110 4.0Mbps 111 4.5Mbps

Πίνακας 1 - Οι Τιμές του PSF στο FHSS.

- **Header Error Check:** Ένα Cyclic Redundancy Code (CRC) μήκους 16 bit για ανίχνευση λαθών. Βασίζεται στον αλγόριθμο ανίχνευσης λαθών CRC – 16 της CCITT. Κάνει ανίχνευση μόνο στην επικεφαλίδα και όχι στα δεδομένα. Αυτός ο έλεγχος γίνεται αργότερα, όταν τα δεδομένα παραδοθούν στο MAC επίπεδο, με την χρήση του Frame Check Sequence (FCS). Ο CRC – 16 ανιχνεύει όλα τα σφάλματα ενός ή δύο bits και γενικά εξασφαλίζει την ανίχνευση 99.998% όλων των πιθανών σφαλμάτων. Λέγεται ότι είναι επαρκής για την μετάδοση ομάδων δεδομένων μήκους μέχρι και 4KBytes.
- **Whitened PSDU:** Μια PSDU μπορεί να έχει μήκος μέχρι 4095 bytes. Πριν την μετάδοση ενός MAC πλαισίου, προστίθενται σε αυτό ειδικά σύμβολα, κάθε 4 bytes, για να αποφευχθεί η πόλωση του σήματος. Αυτή η διαδικασία καλείται Whitening και δημιουργεί μια νέα ακολουθία bits, η οποία και μεταδίδεται τελικώς.

Το PMD υποεπίπεδο του φυσικού επιπέδου, εκτελεί, ουσιαστικά, την μετάδοση και λήψη των PPDUs, σύμφωνα με τις οδηγίες του PLCP. Αυτό γίνεται με την διαμόρφωση του αρχικού σήματος, χρησιμοποιώντας την τεχνική Frequency Shift Keying (FSK), και την αποστολή του μέσω Frequency Hopping.

3.3.1.1 Η Λειτουργία Frequency Hopping.

Το πρότυπο IEEE 802.11 περιγράφει ένα σύνολο καναλιών που είναι ίσα κατανεμημένο στην περιοχή των 2.4GHz. Ο αριθμός των καναλιών εξαρτάται από την γεωγραφική περιοχή, όπως δείχνει και ο πίνακας. Τα κανάλια είναι μοιρασμένα σε μια ζώνη συχνοτήτων. Η ζώνη εξαρτάται και αυτή, από την γεωγραφική περιοχή.

Το PMD, το βασιζόμενο στο FHSS, μεταδίδει τις PDUs αλλάζοντας συνεχώς συχνότητα μετάδοσης. Η μετάβαση αυτή βασίζεται σε μια ψευδοτυχαία ακολουθία αλμάτων που μοιράζει το σήμα στην συνολική περιοχή συχνοτήτων. Η ακολουθία αυτή ρυθμίζεται σε ένα Access Point και όλοι οι σταθμοί χρησιμοποιούν την ίδια. Η συχνότητα εκπομπής πριν το άλμα και η συχνότητα μετά από αυτό πρέπει να απέχουν τουλάχιστον 6MHz σε όλες τις γεωγραφικές περιοχές εκτός της Ιαπωνίας (5MHz).

Κάτω Όριο	Άνω Όριο	Πλήθος	Εύρος	Γεωγραφική Περιοχή
2,402 GHz	2,480 GHz	79	2,4000 - 2,4835 GHz	Β. Αμερική
2,402 GHz	2,480 GHz	79	2,4000 - 2,4835 GHz	Ευρώπη *
2,473 GHz	2,495 GHz	23	2,4710 - 2,4970 GHz	Ιαπωνία
2,447 GHz	2,473 GHz	27	2,4450 - 2,4750 GHz	Ισπανία
2,448 GHz	2,482 GHz	35	2,4465 - 2,4835 GHz	Γαλλία

* εκτός Ισπανίας και Γαλλίας.

Πίνακας 2 - Τα Κανάλια του FHSS.

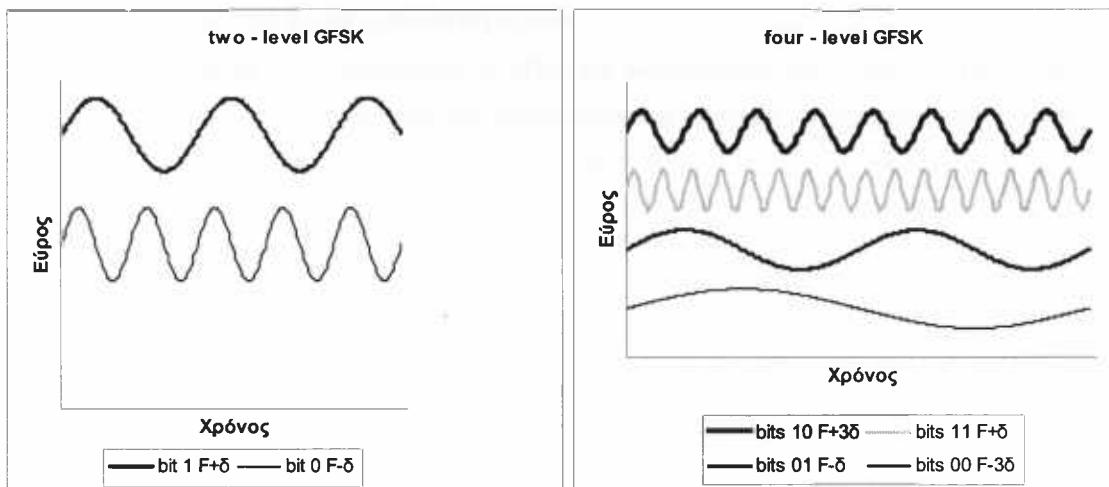
3.3.1.2 Λειτουργία Διαμόρφωσης Συχνότητας (Frequency Modulation Function).

Οι σταθμοί που λειτουργούν σύμφωνα με το FHSS μεταδίδουν τα δεδομένα με ρύθμο 1 ή 2Mbps. Χρησιμοποιείται και στις δύο περιπτώσεις διαμόρφωση συχνότητας. Συγκεκριμένα χρησιμοποιείται η Frequency Shift Keying και μάλιστα η Gaussian Frequency Shift Keying (GFSK), όπου το φέρον σήμα αλλάζει συχνότητα ανάλογα με το bit που μεταδίδεται. Η χρήση του GFSK προτιμάται γιατί ο θόρυβος επηρεάζει, συνήθως, το εύρος του σήματος και όχι την συχνότητα. Έτσι το σήμα γίνεται πιο ανθεκτικό σε παρεμβολές.

Στην περίπτωση του 1Mbps χρησιμοποιείται, συγκεκριμένα, two – level Gaussian Frequency Shift Keying, όπου κάθε bit μεταδίδεται με διαφορετική συχνότητα. Το bit 1 μεταδίδεται με συχνότητα μεγαλύτερη κατά δ από την μέση συχνότητα (F) του καναλιού και το bit 0 σε συχνότητα μικρότερη κατά δ από την μέση συχνότητα του καναλιού. Το πρότυπο περιγράφει αναλυτικά την διαδικασία υπολογισμού του δ, το οποίο πρέπει να είναι τουλάχιστον 110MHz.

Όταν, από την άλλη, το FHSS λειτουργεί στα 2Mbps, γίνεται διαχωρισμός σε 4 συχνότητες ανάλογα με το ζεύγος bit που αποστέλλεται. Χρησιμοποιείται four – level GFSK.

Στα παρακάτω σχήματα έχουμε αναπαράσταση του two – level και four – level GFSK.



Σχήμα 14 - Two - Level και Four - Level GFSK.

3.3.2 Direct Sequence Spread Spectrum – DSSS, High Rate DSSS – HR DSSS.

Όπως το FHSS, έτσι και το DSSS λειτουργεί στην ζώνη των 2.4GHz με ρυθμούς δεδομένων 1 και 2Mbps. Είναι από τα πρώτα φυσικά επίπεδα που υλοποιήθηκαν για προϊόντα ασύρματων τοπικών δικτύων από την στιγμή που εκδόθηκε το πρότυπο.

Το συμπληρωματικό IEEE 802.11b καθορίζει αυξημένους ρυθμούς μετάδοσης για το DSSS και έτσι η ταχύτητα φτάνει έως τα 5.5 και τα 11Mbps. Για την διαμόρφωση χρησιμοποιείται η Complementary Code Keying. Αποτελεί την πιο διαδεδομένη μορφή WLAN στην αγορά.

Γενικά, στο DSSS οι λειτουργίες του PLCP και του PMD είναι ίδιες με τις αντίστοιχες στην περίπτωση του FHSS και ο αναγνώστης παραπέμπεται στην προηγούμενη παράγραφο. Και σε αυτήν την περίπτωση το προοίμιο και η επικεφαλίδα αποστέλλονται σε ρυθμό 1Mbps. Οι βασικότερες διαφορές, εκτός από την διαμόρφωση του σήματος, έγκεινται στην δομή των πλαισίων (PPDUs). Η δομή αυτή φαίνεται στο σχήμα.

128 bits	16 bits	8 bits	8 bits	16 bits	16 bits	Μεταβλητό μήκος
SYNC	Start Frame Delimiter	Signal	Service	Length	Header Error Check	MAC PDU

PLCP προοίμιο | PLCP Επικεφαλίδα

Σχήμα 15 - Η Δομή του PLCP PDU για το DSSS.

- **SYNC:** Διαδοχικά 0 και 1 τα οποία χρησιμοποιεί ο δέκτης για να συγχρονιστεί με τον αποστολέα. Εναλλακτικά, το μήκος αυτού του πεδίου, στην περίπτωση του IEEE 802.11b, δηλαδή του High – Rate DSSS, μπορεί να έχει μήκος μόλις 56bits, για την βελτίωση της ρυθμοαπόδοσης.
- **Start Frame Delimiter:** Η αρχή του πλαισίου. Παίρνει την δεκαεξαδική τιμή F3A0. δηλαδή είναι πάντα η ακολουθία bits 1111 0011 1010 0000 με το αριστερά bit να μεταδίδεται πρώτο.
- **Signal:** Εδώ σημειώνεται το είδος της διαμόρφωσης που ο παραλήπτης πρέπει να χρησιμοποιήσει για να αποδιαμορφώσει το σήμα. Η τιμή του πεδίου είναι ίση με τον ρυθμό μετάδοσης δια 100. Έτσι, πριν την έκδοση του συμπληρώματος IEEE 802.11b, οι μόνες δυνατές τιμές ήταν 00001010 (1Mbps) ή 00010100 (2Mbps). Στην πρώτη περίπτωση η διαμόρφωση είναι DBPSK και στην δεύτερη DQPSK. Σύμφωνα με το IEEE 802.11b η κατάσταση διαμορφώνεται ως εξής:

Ρυθμός Μετάδοσης	Τιμή Πεδίου
1Mbps	00001010
2Mbps	00010100
5.5Mbps	00110111
11Mbps	01101110

Πίνακας 3 - Οι Τιμές του Πεδίου Signal στο DSSS.

- **Service:** Δεσμεύεται για μελλοντική χρήση. Η τιμή 00000000 σημαίνει συμβατότητα με το IEEE 802.11. με το IEEE 802.11b χρησιμοποιούνται και τα bits 2 και 7 του πεδίου.

- **Length:** Η τιμή αυτού του πεδίου είναι ένας χωρίς πρόσημο ακέραιος μήκους 16bit (κανονικά 0 – 65535 αλλά οι τιμές περιορίζονται στις μεγαλύτερες ή ίσες με 16) και αναφέρει την διάρκεια εκπομπής της PSDU (δηλαδή του MAC πλαισίου) σε microseconds.
- **Header Error Check:** Ένα Cyclic Redundancy Code (CRC) μήκους 16 bit για ανίχνευση λαθών. Βασίζεται στον αλγόριθμο ανίχνευσης λαθών CRC – 16 της CCITT. Κάνει ανίχνευση μόνο στην επικεφαλίδα και όχι στα δεδομένα. Αυτός ο έλεγχος γίνεται αργότερα, όταν τα δεδομένα παραδοθούν στο MAC επίπεδο, με την χρήση του Frame Check Sequence (FCS). Ο CRC – 16 ανιχνεύει όλα τα σφάλματα ενός ή δύο bits και γενικά εξασφαλίζει την ανίχνευση 99.998% όλων των πιθανών σφαλμάτων. Λέγεται ότι είναι επαρκής για την μετάδοση ομάδων δεδομένων μήκους μέχρι και 4KBytes.
- **PSDU:** Σε αντίθεση με το FHSS, στο DSSS δεν έχουμε την διαδικασία Whitening. Το MAC πλαίσιο προστίθεται μετά από την επικεφαλίδα, ακριβώς όπως παραλήφθηκε από το MAC επίπεδο. Μπορεί να φτάνει σε μήκος μέχρι έναν αριθμό που καταχωρείται στην MIB του σταθμού κάτω από την παράμετρο **aMPDUMaxLength**.

Το PMD υποεπίπεδο του φυσικού επιπέδου, εκτελεί, ουσιαστικά, την μετάδοση και λήψη των PPDUs, σύμφωνα με τις οδηγίες του PLCP. Αυτό γίνεται με την διαμόρφωση του αρχικού σήματος, χρησιμοποιώντας την τεχνική DBPSK ή την DQPSK (Differential Binary ή Quadrature Phase Shift Keying), και την αποστολή του μέσω Direct Sequences.

3.3.2.1 Η Λειτουργία Direct Sequence.

Σύμφωνα με το DSSS, τα δεδομένα, δηλαδή οι PPDUs, μετατρέπονται σε σήμα κατάλληλο προς μετάδοση. Αυτό συμβαίνει πολλαπλασιάζοντας το σήμα με ένα ψευδοθόρυβο (Pseudo-noise – PN). Σε ένα διάγραμμα στο πεδίο των συχνοτήτων, το νέο σήμα μοιάζει με παρεμβολές. Ωστόσο το σήμα απλώνεται σε μεγαλύτερο εύρος ζώνης και έτσι γίνεται ανθεκτικότερο σε θόρυβο.

Η λειτουργία του DSSS γίνεται στην περιοχή συχνοτήτων των 2.4GHz και καθορίζεται ένα πλήθος καναλιών λειτουργίας ανά γεωγραφική περιοχή. Τα κανάλια αυτά μπορεί να είναι μέχρι και 14, ενώ το εύρος του καθενός είναι 22 MHz. Φυσικά οι ρυθμιστικές αρχές σε κάθε περιοχή μπορούν να επέμβουν σε αυτές τις τιμές. Αυτό φαίνεται και στον παρακάτω πίνακα.

Η γενική ιδέα της λειτουργίας του DSSS είναι η εξάπλωση της PPDU και στη συνέχεια η διαμόρφωση του εξαπλωμένου συνόλου δεδομένων σε συγκεκριμένη συχνότητα.



Κανάλι	Συχνότητα (GHz)	ΗΠΑ - Καναδάς	Ευρώπη	Ισπανία	Γαλλία	Ιαπωνία
1	2.412	✓	✓			
2	2.417	✓	✓			
3	2.422	✓	✓			
4	2.427	✓	✓			
5	2.432	✓	✓			
6	2.437	✓	✓			
7	2.442	✓	✓			
8	2.447	✓	✓			
9	2.452	✓	✓			
10	2.457	✓	✓	✓	✓	
11	2.462	✓	✓	✓	✓	
12	2.467		✓		✓	
13	2.472		✓		✓	
14	2.484					✓

Πίνακας 4 - Οι Συχνότητες Λειτουργίας του DSSS

Όπως αναφέρθηκε, σε κάθε bit εφαρμόζεται ένα ψευδοθόρυβος, που συχνά αναφέρεται και σαν Chipping Code ή Spreading Sequence. Ουσιαστικά πρόκειται για μια ακολουθία θετικών και αρνητικών άσσων. Συγκεκριμένα, για το IEEE 802.11, χρησιμοποιείται η ακολουθία 11-chip του Barker.

$$+1 \quad -1 \quad +1 \quad +1 \quad -1 \quad +1 \quad +1 \quad +1 \quad -1 \quad -1 \quad -1$$

Σχήμα 16 - Η Ακολουθία 11 - chip του Barker.

Τα δεδομένα που προκύπτουν είναι ψηλότερου ρυθμού από τα αρχικά. Η αναλογία του ρυθμού του εξαπλωμένου σήματος προς τον ρυθμό του αρχικού καλείται “Processing Gain” και στο πρότυπο IEEE 802.11 έχει καθοριστεί να είναι μεγαλύτερη από 11.

Στο IEEE 802.11b εισάγεται μια νέα Spread Spectrum τεχνική η οποία καλείται CCK, ενώ για την διαμόρφωση χρησιμοποιούνται παραλλαγές της DQPSK οι οποίες επιτρέπουν την μετάδοση οχτάδων bits σε ένα από οχτώ πιθανά σύμβολα, μήκους 8 chips.

3.3.2.2 Λειτουργία Διαμόρφωσης Συχνότητας (Frequency Modulation Function).

Οι σταθμοί που χρησιμοποιούν DSSS, διαμορφώνουν το σήμα με την τεχνική της Διαφορικής PSK (Differential Phase Shift Keying). Η χρήση του DPSK προτιμάται γιατί ο θόρυβος επηρεάζει, συνήθως, το εύρος του σήματος και όχι την φάση. Έτσι το σήμα γίνεται πιο ανθεκτικό σε παρεμβολές.

$$s(t) = \begin{cases} A \cdot \cos(2 \cdot \pi \cdot f_c \cdot t + \vartheta_c) \\ A \cdot \cos(2 \cdot \pi \cdot f_c \cdot t) \end{cases}$$

Τύπος 1 - Ο Τύπος για το DPSK.

Σύμφωνα με την DPSK κάθε σύμβολο μεταδίδεται με διαφορετική φάση σχετικά με το προηγούμενό του. Για παράδειγμα αν έχουμε δύο σύμβολα προς μετάδοση, το 0 και το 1, τότε το 0 μεταδίδεται με την ίδια φάση με το προηγούμενο και το 1 με διαφορετική, σύμφωνα με τον παραπάνω τύπο.

Στην περίπτωση του 1Mbps DSSS χρησιμοποιείται η DBPSK, όπου στέλνεται ένα bit και χρησιμοποιούνται δύο σύμβολα. Ισχύουν ακριβώς τα παραπάνω με $\vartheta_c = \pi$. Η περίπτωση καλείται και Basic Access Rate.

Όταν έχουμε Enhanced Access Rate, δηλαδή 2Mbps DSSS, χρησιμοποιείται η DQPSK. Σύμφωνα με αυτήν μεταδίδονται τέσσερα πιθανά σύμβολα και το καθένα αντιπροσωπεύει ένα δυαδικό ζεύγος 0 ή 1. Το κάθε σύμβολο έχει διαφορά φάσης από το προηγούμενο, σύμφωνα με τον παρακάτω πίνακα.

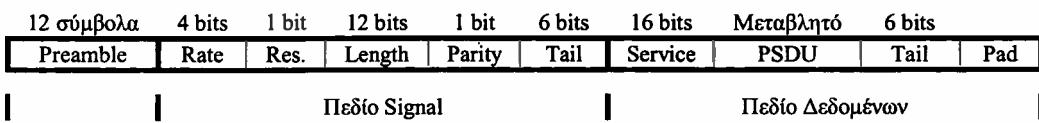
Σύμβολο	ϑ_c
00	0
01	$\pi/2$
11	π
10	$3\cdot\pi/2$

Πίνακας 5 - Οι Διαφορές Φάσης για το DQPSK.

3.3.3 Orthogonal Frequency Division Multiplexing – OFDM.

Η τελευταία προσθήκη στο πρότυπο IEEE 802.11, είναι αυτή που περιγράφεται στο συμπλήρωμα IEEE 802.11a. Μιλάει για ασύρματα τοπικά δίκτυα ταχύτητας μέχρι 54Mbps που λειτουργούν, πλέον, στην περιοχή των 5GHz. Αξίζει να σημειωθεί ότι έχουν κυκλοφορήσει ιδιοκτησιακές τεχνικές για την αύξηση του ρυθμού μετάδοσης σε ακόμα ψηλότερα επίπεδα. Το OFDM είναι παρόμοιο με το φυσικό επίπεδο που χρησιμοποιείται στο HiperLAN/2.

Με τις αλλαγές αυτές επιδιώκουμε να πετύχουμε, εκτός από την αύξηση της ταχύτητας, αντοχή σε παρεμβολές και μικρότερη παραμόρφωση του σήματος λόγω διάδοσης πολλαπλών μονοπατιών. Οι υποσυγχρότητες που φέρουν το σήμα, όπως θα δούμε παρακάτω, είναι ορθογώνιες μεταξύ τους και, θεωρητικά πάντα, απέχουν τόσο ώστε να μην παρεμβάλλονται η μία με την άλλη.



Σχήμα 17 - Η Δομή του PLCP PDU για το OFDM.

- **Preamble:** Το προοίμιο δίνει την δυνατότητα στον παραλήπτη του σήματος να συγχρονίσει τον αποδιαμορφωτή. Αποτελείται από 12 σύμβολα. Τα δέκα πρώτα καλούνται "Short Training Sequences" και έχουν διάρκεια 0.8μSec το καθένα. Τα δύο τελευταία λέγονται "Long Training Sequences" και έχουν μήκος 3.2μSec το καθένα. Μεταξύ των πρώτων και των τελευταίων μεσολαβούν δύο GI (Guard Intervals) διάρκειας 0.8μSec το καθένα. Έτσι η

συνολική διάρκεια του προοιμίου είναι: $10 \times 0.8 + 2 \times 0.8 + 2 \times 3.2 = 16 \mu\text{Sec}$. Σε αυτό το χρονικό διάστημα ο παραλήπτης “εκπαιδεύεται” για το επερχόμενο σήμα.

Μετά από το προοίμιο ακολουθεί το πεδίο Signal. Αυτό θεωρείται ως ενιαίο και έχει τα υποπεδία που αναφέρονται ακριβώς παρακάτω. Να σημειωθεί ότι αυτό το πεδίο αποτελεί ένα μοναδικό OFDM σύμβολο που αποστέλλεται με BPSK διαμόρφωση.

- **Rate:** 4 bits που περιγράφουν τον ρυθμό μετάδοσης του πεδίου δεδομένων, σύμφωνα με τον πίνακα.

Bits	Ρυθμός
1101	6Mbps
1111	9Mbps
0101	12Mbps
0111	18Mbps
1001	24Mbps
1011	36Mbps
0001	48Mbps
0011	54Mbps

Πίνακας 6 - Οι Τιμές του Πεδίου Rate στο OFDM

- **Reserved:** Έχει πάντα την τιμή 0.
- **Length:** Ο αριθμός bytes που το επίπεδο MAC επιθυμεί να μεταδώσει. Είναι ένας ακέραιος, χωρίς πρόσημο, μήκους 12bit.
- **Parity:** bit ισοτιμίας. Βασίζεται στα πρώτα 17 bits του πεδίου Signal.
- **Tail:** 6 bits, όλα ίσα με 0.
- **Service:** Με αυτό το πεδίο ξεκινάει το μέρος των δεδομένων. Αποτελείται από 16 bit που είναι όλα 0. Τα επτά πρώτα χρησιμεύουν στον συγχρονισμό του παραλήπτη και τα υπόλοιπα εννιά είναι δεσμευμένα για μελλοντική χρήση.
- **PSDU:** Τα δεδομένα από το επίπεδο MAC.
- **Tail:** 6 bits, όλα ίσα με 0.
- **Pad:** περιέχει τουλάχιστον 6 μηδενικά και χρησιμεύει στο να γεμίσει το πλαίσιο, ώστε το πεδίο των δεδομένων να έχει μήκος πολλαπλάσιο του αριθμού των bits σε ένα OFDM σύμβολο (48, 96, 192, 288).

3.3.3.1 Η λειτουργία του OFDM.

Η φιλοσοφία που κρύβεται πίσω από το OFDM είναι η διαίρεση του σήματος σε πολλά υποσήματα, χαμηλότερης ταχύτητας και η παράλληλη μετάδοσή τους σε διαφορετικές συχνότητες. Για την μετάδοση στο OFDM, ορίζονται τρεις ζώνες εύρους 100MHz η καθεμία και δώδεκα κανάλια των 20MHz το καθένα.

Ζώνη (GHz)	Κανάλι	Μέση Συχνότητα Καναλιού (MHz)
U-NII lower band (5.15–5.25)	36	5180
	40	5200
	44	5220
	48	5240
U-NII middle band (5.25–5.35)	52	5260
	56	5280
	60	5300
	64	5320
U-NII upper band (5.725–5.825)	149	5745
	153	5765
	157	5785
	161	5805

Πίνακας 7 - Οι Ζώνες Συχνοτήτων Λειτουργίας του OFDM.

Σχετικά με την διαμόρφωση, αξίζει να σημειωθεί ότι για κάθε ρυθμό μετάδοσης χρησιμοποιείται και διαφορετική τεχνική διαμόρφωσης του σήματος. Οι τεχνικές που χρησιμοποιούνται είναι οι:

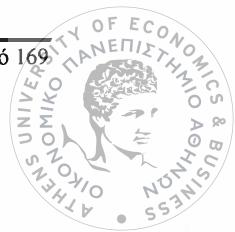
- Binary Phase Shift Keying – BPSK.
- Quadrature Phase Shift Keying – QPSK.
- Quadrature Amplitude Modulation – QAM.

Ρυθμός Δεδομένων (Mbps)	Διαμόρφωση	Κωδικοποιημένα bits ανά υποφέρουσα (N _{BPSC})	Κωδικοποιημένα bits ανά OFDM σύμβολο (N _{CBPS})	Bits δεδομένων ανά OFDM σύμβολο (N _{DBPS})
6	BPSK	1	48	24
9	BPSK	1	48	36
12	QPSK	2	96	48
18	QPSK	2	96	72
24	16-QAM	4	192	96
36	16-QAM	4	192	144
48	64-QAM	6	288	192
54	64-QAM	6	288	216

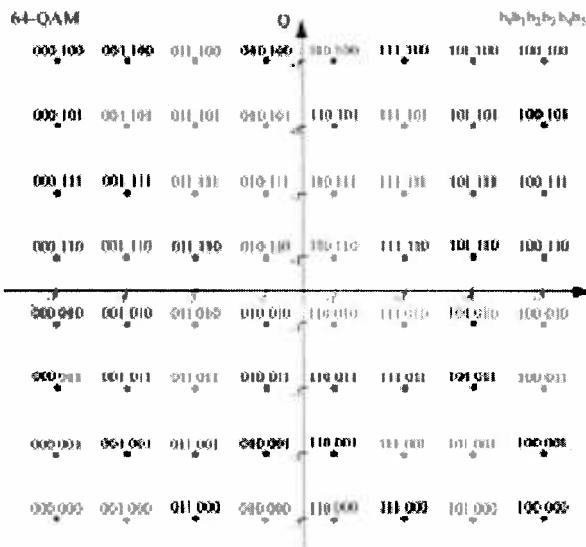
Πίνακας 8 - Τεχνικές Διαμόρφωσης του OFDM.

Το OFDM σπάει το σήμα σε 52 ξεχωριστές φέρουσες. Τέσσερις από αυτές δρουν πιλοτικά και χρησιμοποιούνται από το σύστημα σαν σημείο αναφοράς. Μέσα από αυτές στέλνεται μια ψευδοδυαδική ακολουθία για την αποφυγή δημιουργίας φασματικών γραμμών. Οι υπόλοιπες 48 αποτελούν μονοπάτια μέσα από τα οποία θα σταλούν, παράλληλα, τα δεδομένα.

Το OFDM επίσης δημιουργεί σύμβολα, που είναι ακολουθίες 1, 2, 4 ή 6 bits, ανάλογα με τον επιλεγμένο ρυθμό μετάδοσης, όπως φαίνεται και στον προηγούμενο πίνακα. Αυτά τα σύμβολα μετατρέπονται σε σύνθετους αριθμούς. Τέλος πραγματοποιείται ένας αντίστροφος μετασχηματισμός fast Fourier που συνδυάζει τις φέρουσες πριν από την αποστολή.



Πρέπει να τονισθεί και πάλι ότι το πεδίο Signal των PPDU, αντιμετωπίζεται πάντα σαν ένα και μοναδικό σύμβολο. Διαμορφώνεται κατά BPSK, ανεξαρτήτως του ρυθμού που υπαγορεύει το πεδίο Rate του PPDU. Μεταδίδεται, δε, πάντα, σε ρυθμό 6Mbps.



Σχήμα 18 - Το 64 - QAM για Μετάδοση 48 και 54Mbps.

3.3.4 Infrared (IR) Physical Layer.

Τελευταία στην αναφορά του φυσικού επιπέδου έρχεται η περίπτωση των υπέρυθρων ακτινών. Αποδίδει ταχύτητες 1 ή 2Mbps με υπέρυθρο φως. Προς το παρόν δεν έχουν κυκλοφορήσει προϊόντα που να εκμεταλλεύονται αυτή την τεχνολογία. Ωστόσο, η ύπαρξή του στο πρότυπο επιβάλλει να γίνει αναφορά σε αυτό.

Στο σχήμα που ακολουθεί βλέπουμε την δομή του πλαισίου φυσικού επιπέδου (PPDU), η οποία μοιάζει πάρα πολύ με αυτή του DSSS PPDU. Να σημειωθεί ότι, αντί για bits έχουμε την μετάδοση παλμών σε διαδοχικές χρονικές θυρίδες (Time Slots). Όπου αναφέρονται bits, το bit 1 σημαίνει ύπαρξη παλμού και το 0 απουσία αυτού.

57 – 73 θυρίδες	4 θυρίδες	3 θυρίδες	32 θυρίδες	16 θυρίδες	16 θυρίδες	Μεταβλητό μήκος
SYNC	Start Frame Delimiter	Data Rate	DC Level Adjustment	Length	Header Error Check	MAC PDU

PLCP προοίμιο | PLCP Επικεφαλίδα

Σχήμα 19 - Η Δομή του PLCP PDU για το IR.

- **SYNC:** Διαδοχική εναλλαγή ύπαρξης ακτίνας και όχι, σε διαδοχικές θυρίδες. Χρησιμεύει, ώστε ο παραλήπτης να συγχρονιστεί με το σήμα, να εκτιμήσει την σηματοθορυβική σχέση και να εκτελέσει άλλες, προαιρετικές, λειτουργίες.
- **Start Frame Delimiter:** Η αρχή του πλαισίου. Είναι πάντα η ακολουθία bits 1001.

- **Data Rate:** Εδώ σημειώνεται ο ρυθμός με τον οποίο θα μεταδοθεί το πλαίσιο, δηλαδή 000 για 1Mbps και 001 για 2Mbps. Το προοίμιο μεταδίδεται πάντα με ρυθμό 1Mbps.
- **DC Level Adjustment:** χρησιμοποιείται ώστε ο δέκτης να μπορέσει να σταθεροποιήσει το DC επίπεδο του σήματος.
- **Length:** Η τιμή αυτού του πεδίου είναι ένας ακέραιος μήκους 16bit (0 – 65535) χωρίς πρόσημο και αναφέρει τον χρόνο που θα διαρκέσει η εκπομπή της PSDU. (δηλαδή του MAC πλαισίου) σε microseconds.
- **Header Error Check:** Ένα Cyclic Redundancy Code (CRC) μήκους 16 bit για ανίχνευση λαθών. Βασίζεται στον αλγόριθμο ανίχνευσης λαθών CRC – 16 της CCITT. Κάνει ανίχνευση μόνο στην επικεφαλίδα και όχι στα δεδομένα. Αυτός ο έλεγχος γίνεται αργότερα, όταν τα δεδομένα παραδοθούν στο MAC επίπεδο, με την χρήση του Frame Check Sequence (FCS). Ο CRC – 16 ανιχνεύει όλα τα σφάλματα ενός ή δύο bits και γενικά εξασφαλίζει την ανίχνευση 99.998% όλων των πιθανών σφαλμάτων. Λέγεται ότι είναι επαρκής για την μετάδοση ομάδων δεδομένων μήκους μέχρι και 4KBytes.
- **PSDU:** 0 έως 2500 bytes δεδομένων.

3.3.4.1 Η λειτουργία του IR.

Η δυαδική μορφή των PPDUs μετατρέπεται σε υπέρυθρο σήμα κατάλληλο προς μετάδοση. Το πρότυπο αναλύει την μη κατευθυνόμενη μετάδοση που σημαίνει ότι δεν είναι αναγκαίο να υπάρχει οπτική επαφή μεταξύ πομπού και δέκτη. Χρησιμοποιείται κάποιο ταβάνι ως σημείο ανάκλασης. Αυτή η περίπτωση καλείται και “διαχεόμενες υπέρυθρες” (Diffused Infrared). Στην περίπτωση αυτή έχουμε πολλούς περιορισμούς. Περιοριζόμαστε σε χρήση σε κλειστό χώρο. Η ακτίνα δράσης είναι πολύ μικρή και, τέλος, τα παράθυρα ενδέχεται να προκαλέσουν εξασθένηση του σήματος.

Για την διαμόρφωση χρησιμοποιείται η τεχνική Διαμόρφωσης Θέσης Παλμού (Pulse Position Modulation – PPM). Η λογική είναι να μεταδίδονται διαφορετικά δυαδικά σύμβολα με την μετατόπιση της θέσης του παλμού.

Για την μετάδοση ρυθμού 1Mbps χρησιμοποιείται PPM 16 επιπέδων. Αντιστοιχίζεται μία ακολουθία υπέρυθρων παλμών (Σύμβολο), μήκους 16, σε κάθε τετράδα από bits προς μετάδοση. Για την μετάδοση ρυθμού 2Mbps χρησιμοποιείται PPM 4 επιπέδων, όπου αντιστοιχίζεται ένα Σύμβολο σε κάθε ζευγάρι από bits προς μετάδοση. Αυτά φαίνονται και στον επόμενο πίνακα.

Γενικά οι υπέρυθρες ακτίνες είναι πάρα πολύ ανθεκτικές σε θόρυβο, σε σχέση με τα ραδιοικύματα και η χρήση τους προσφέρει πολύ ψηλό βαθμό ασφάλειας. Όμως, τα

προβλήματα που αναφέραμε παραπάνω, όπως για την ακτίνα κάλυψης, και η έλλειψη προϊόντων οδηγεί αναπόφευκτα στην επιλογή μιας από τις τεχνολογίες Spread Spectrum.

Ζεύγος bits	4-PPM σύμβολο
00	0001
01	0010
11	0100
10	1000

Πίνακας 9 - Το PPM 4 Επιπέδων για το IR.

4 ΤΟ ΕΠΙΠΕΔΟ MAC ΣΤΟ ΠΡΟΤΥΠΟ IEEE 802.11.

Μετά από την ανάλυση του φυσικού επιπέδου, η περιγραφή του προτύπου θα συνεχιστεί με την διεξοδική ανάλυση του επιπέδου MAC.

Στις παρακάτω παραγράφους θα δούμε τις λειτουργίες του επιπέδου MAC, σε γενικό επίπεδο και στην συνέχεια θα περάσουμε στον τρόπο με τον οποίο το επίπεδο MAC πλαισιώνει τα LLC πακέτα, πριν τα παραδώσει στο φυσικό επίπεδο για την αποστολή.

4.1 ΟΙ ΛΕΙΤΟΥΡΓΙΕΣ ΤΟΥ ΕΠΙΠΕΔΟΥ MAC.

Όπως είναι σαφές από το όνομά του, το επίπεδο MAC εκτελεί λειτουργίες ελέγχου πρόσβασης στο μέσο. Τέτοιες λειτουργίες είναι η διευθυνσιοδότηση, ο έλεγχος της σύνδεσης και της αποσύνδεση με ένα δίκτυο και οι υπηρεσίες αυθεντικοποίησης.

4.1.1 Πρόσβαση στο μέσο.

Πριν από την αποστολή των πλαισίων, η κάρτα δικτύου πρέπει πρώτα να πάρει πρόσβαση στο μέσο. Αυτό μπορεί να γίνει με τους δύο παρακάτω τρόπους. Να σημειωθεί ότι οι δύο τρόποι μπορούν να λειτουργούν ταυτόχρονα μέσα στο ίδιο BSS.

4.1.1.1 Carrier Sense Multiple Access / Collision Avoidance – CSMA/CA.

Το CSMA/CA είναι ένα πρωτόκολλο παρόμοιο με το CSMA/CD του Ethernet. Στο πρότυπο IEEE 802.11 αναφέρεται και ως Distributed Coordination Function – DCF. Αποτελεί τον πρωτεύοντα – και υποχρεωτικό – τρόπο πρόσβασης στο μέσο.

Το πρωτόκολλο βασίζεται στην Ανίχνευση Φέροντος (Carrier Sense) και την Αποφυγή Συγκρούσεων (Collision Avoidance) για τον αυτόματο καταμερισμό του ασύρματου μέσου.

Σχετικά με την λειτουργία Ανίχνευσης Φέροντος, χρησιμοποιείται τόσο ένας φυσικός όσο και ένας ιδεατός μηχανισμός, ώστε να μπορεί το MAC επίπεδο να καταλάβει αν το μέσο χρησιμοποιείται ή όχι.

Τέλος, πρέπει να αναφερθεί ότι το πρότυπο χρησιμοποιεί το Collision Avoidance και όχι Collision Detection όπως στο Ethernet. Δεν θα μπορούσε να χρησιμοποιηθεί CD γιατί ο πομποδέκτης δεν έχει την δυνατότητά να εκπέμπει και να δέχεται δεδομένα ταυτόχρονα από το ίδιο κανάλι.

1. Φυσικός Μηχανισμός.

Ο φυσικός μηχανισμός βασίζεται στο φυσικό επίπεδο, το οποίο, ανάλογα με το είδος του (FHSS, DSSS), έχει τρόπους να εκτιμά αν το κανάλι χρησιμοποιείται ή όχι. Η πληροφορία αυτή αποστέλλεται στο MAC επίπεδο και χρησιμοποιείται στο να αποφασισθεί αν το κανάλι είναι ελεύθερο.



2. Ιδεατός Μηχανισμός.

Ο ιδεατός μηχανισμός βασίζεται στα MAC πλαίσια που κυκλοφορούν στο δίκτυο και συγκεκριμένα σε πληροφορίες που βρίσκονται στο πεδίο Duration της επικεφαλίδας. Κάθε σταθμός που εκπέμπει θέτει σε αυτό το πεδίο την διάρκεια που θα χρειαστεί η μετάδοση του πλαισίου, άρα και της επικείμενης δέσμευσης του μέσου. Το MAC επίπεδο παρακολουθεί όλα τα πλαίσια που κυκλοφορούν στο δίκτυο και καταχωρεί το Duration του τελευταίου στο Network Allocation Vector – NAV. Το NAV λειτουργεί ως χρονόμετρο και μετράει αντίστροφα. Όταν μηδενιστεί, μόνο τότε το MAC επίπεδο θα στείλει ένα πλαίσιο και μόνο αν το φυσικό επίπεδο αναφέρει ότι το μέσο είναι ελεύθερο.

Οι δύο μηχανισμοί εξασφαλίζουν αρκετή πληροφόρηση σχετικά με το αν το μέσο είναι δεσμευμένο. Για να επιτραπεί η αποστολή ενός πλαισίου πρέπει να συμφωνήσουν και οι δύο μηχανισμοί. Αν, για παράδειγμα, το φυσικό επίπεδο επιτρέψει την μετάδοση αλλά το NAV δεν έχει την τιμή 0 τότε η μετάδοση αναβάλλεται. Όταν το μέσο βρεθεί δεσμευμένο, τότε εκτελείται ένας αλγόριθμος backoff.

3. Αλγόριθμος Backoff.

Όπως είναι γνωστό, σε συστήματα πολλαπλής πρόσβασης, όταν το μέσο βρεθεί κατειλημμένο, η μεγαλύτερη πιθανότητα σύγκρουσης είναι ακριβώς μετά από το τέλος της μετάδοσης. Αυτό συμβαίνει γιατί ενδέχεται και άλλοι σταθμοί να περιμένουν να ελευθερωθεί το μέσο και να προσπαθήσουν να μεταδώσουν όλοι μαζί. Για αυτό τον λόγο η αναμετάδοση γίνεται μετά από την πάροδο ενός τυχαίου χρονικού διαστήματος. Στην MIB του σταθμού υπάρχουν οι παράμετροι aCWmin και aCWmax που αναφέρονται σε αυτό που αποκαλείται Collision Window – CW. Μετά από σύγκρουση δημιουργείται ένας ψευδοτυχαίος ακέραιος που εκλέγεται από μια ομοιόμορφη κατανομή στο διάστημα $[0, CW]$: $CW \in [aCWmin, aCWmax]$ και πολλαπλασιάζεται με μία άλλη παράμετρο της MIB, την aSlotTime. Η αναμετάδοση γίνεται μόλις περάσει το χρονικό διάστημα ίσο με το γινόμενο των δύο αριθμών.

$$\text{BackoffTime} = \text{Random} \times aSlotTime$$

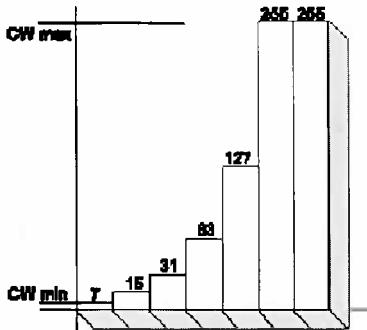
$$P(\text{Random} = r) = \frac{r}{CW} : r \in [0, CW]$$

Τύπος 2 - Ο Υπολογισμός του Backoff.

Αν συμβεί νέα σύγκρουση, το CW αυξάνει. Έτσι, τελικά ο χρόνος αναμονής μεταξύ δύο προσπαθειών αναμετάδοσης αυξάνει εκθετικά. Σε περίπτωση χαμηλής χρήσης του μέσου δεν χρειάζεται ένας σταθμός να περιμένει πολύ. Σε περίπτωση μεγάλης χρήσης αποφεύγονται οι συγκρούσεις στις αναμεταδόσεις αλλά ενδέχεται ένας σταθμός να περιμένει την σειρά του για μεγάλο χρονικό διάστημα. Το CW είναι ευνόητο ότι αυξάνει

μέχρι να φτάσει την τιμή aCWmax. Στις επόμενες – αν υπάρχουν – προσπάθειες αναμετάδοσης, η τιμή παραμένει σταθερή και ίση με αυτή την ποσότητα.

Η γενική ιδέα της εκθετικής αύξησης είναι να επιτευχθεί η μέγιστη ρυθμοαπόδοση και ο ελάχιστος αριθμός συγκρούσεων για δίκτυα τόσο υψηλού βαθμού χρησιμοποίησης όσο και χαμηλού.



Σχήμα 20 - Η Εκθετική Αύξηση του CW.

4. Μηχανισμός Ανάκαμψης από Σφάλματα (Error Recovery).

Γενικά η μετάδοση αντιμετωπίζει παρεμβολές και συγκρούσεις. Έτσι μπορούν να παρουσιαστούν σφάλματα που διαταράσσουν την σειρά των πλαισίων. Για παράδειγμα ένας σταθμός μπορεί να στείλει ένα πλαίσιο και να μην λάβει επιβεβαίωση. Για αυτούς τους λόγους χρησιμοποιείται ο μηχανισμός ανάκαμψης.

Ο μηχανισμός έγκειται ουσιαστικά στην αναμετάδοση πλαισίων μετά από μια χρονική περίοδο αν δεν έχει έρθει καμία απάντηση από τον δέκτη. Αυτή η διαδικασία είναι γνωστή ως Automatic Repeat Request – ARQ.

Ο αριθμός των επαναλήψεων ρυθμίζεται από παραμέτρους της MIB και είναι διαφορετικός για τα μικρά πακέτα από ότι για τα μεγάλα. Μικρά πακέτα θεωρούνται αυτά που δεν προηγείται Request To Send – RTS πλαίσιο πριν από την μετάδοσή τους. Το μέγεθός τους ορίζεται από την παράμετρο της MIB aRTSThreshold και οι επαναλήψεις συνεχίζουν μέχρι τον αριθμό aShortRetryLimit. Αντίστοιχα υπάρχει η παράμετρος aLongRetryLimit. Αν ο αριθμός επαναλήψεων φτάσει αυτά τα όρια αυτά, τότε το πλαίσιο απορρίπτεται.

5. Διαστήματα Πρόσβασης (Access Spacing).

Στο IEEE 802.11 καθορίζονται κάποια πρότυπα διαστήματα μεταξύ μεταδόσεων που καθυστερούν την πρόσβαση των σταθμών στο μέσο και προσφέρουν έτσι έναν τρόπο να δίνονται προτεραιότητες. Τα διαστήματα ονομάζονται Interframe Spaces – IFS.

- **Short IFS – SIFS:** Είναι το μικρότερο σε διάρκεια IFS και δίνει την μεγαλύτερη προτεραιότητα από όλα. Όταν ένας σταθμός τελειώσει την

μετάδοση, πριν μεταδώσουν περιμένουν διάρκεια ίση με ένα SIFS οι σταθμοί που έχουν για μετάδοση ένα πλαίσιο:

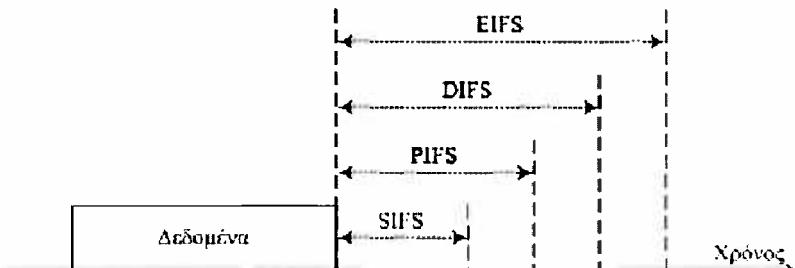
- ~ ACK (Acknowledgement),
- ~ CTS (Clear To Send),
- ~ Το επόμενο τμήμα ενός Fragment Burst.
- PCF IFS – PIFS: Κατά ένα PIFS περιμένουν οι σταθμοί που χρησιμοποιούν την πρόσβαση βάσει προτεραιοτήτων που θα δούμε στην αμέσως επόμενη παράγραφο.
- DCF IFS – DIFS: Κατά ένα PIFS περιμένουν οι σταθμοί που χρησιμοποιούν την μέθοδο πρόσβασης CSMA/CA.

Άλλως Συμμόδια:										DIFS	RIFS
NAV(RTS)					NAV(FRAGMENT1)			NAV(FRAGMENT2)		DIFS	RIFS
NAV(CTS)			NAV(ACK0)		NAV(ACK1)						
RTS	SIFS		SIFS	FRAGMENT0	SIFS	SIFS	FRAGMENT1	SIFS	SIFS	FRAGMENT2	SIFS
	CTS			ACK 0				ACK 1			ACK 2

Αποστολές:

Σχήμα 21 - RTS/CTS/ACK και Ρύθμιση των NAV.

- Extended IFS – EIFS: Όλοι οι σταθμοί που χρησιμοποιούν DFS χρησιμοποιούν το EIFS όταν η μετάδοση ενός πλαισίου έχει ως αποτέλεσμα την κακή λήψη του πλαισίου λόγω λανθασμένης τιμής Frame Check Sequence – FCS.



Σχήμα 22 - Τα Διάφορα IFS.

4.1.1.2 Πρόσβαση Βάσει Προτεραιοτήτων (Priority Based Access).

Ο δεύτερος τρόπος πρόσβασης στο μέσο είναι προαιρετικός. Αποκαλείται και Point Coordination Function – PCF.

Είναι μια μέθοδος πρόσβασης στο μέσο χωρίς ανταγωνισμό που χρησιμοποιείται όταν πρέπει να μεταδοθούν πλαίσια επείγοντος περιεχομένου.

Πρόκειται για έναν συγκεντρωτικό αλγόριθμο, όπου ένα Access Point ελέγχει την μετάδοση των πλαισίων από όλους τους σταθμούς. Οι σταθμοί ακολουθούν τις εντολές του Access Point θέτοντας το NAV στην τιμή που τους υπαγορεύει.

Έτσι η λειτουργία του δικτύου χωρίζεται σε περιόδους Contention (CSMA/CA) και Contention – Free (PCF). Στην αρχή μιας Contention – Free περιόδου ο Point Coordinator (το Access Point) έχει την ευκαιρία να πάρει τον έλεγχο του μέσου. Αυτό συμβαίνει γιατί τηρεί το διάστημα PIFS οπότε θα προλάβει το μέσο πριν από άλλους σταθμούς που θέλουν να μεταδώσουν, οι οποίοι θα περιμένουν διάστημα DIFS, που είναι μακρύτερο. Αφού ο PC πάρει τον έλεγχο του μέσου, στέλνει ένα Beacon πλαίσιο που περιέχει την ομάδα παραμέτρων CF Parameter. Οι σταθμοί θέτουν το NAV ίσο με CFPMaxDuration, δηλαδή ίσο με την διάρκεια της περιόδου Contention – Free και έτσι δεν τους επιτρέπεται να καταλάβουν το μέσο.

Ο Point Coordinator, αφού περιμένει ένα SIFS, μπορεί να στείλει ένα πλαίσιο ανάμεσα σε τέσσερα είδη:

- **Πλαίσιο Data:** Ο Point Coordinator στέλνει ένα unicast, multicast ή broadcast πλαίσιο. Στην περίπτωση του unicasting και αν δεν ληφθεί ACK πλαίσιο, μπορεί να γίνει αναμετάδοση μετά από ένα PIFS.
- **Πλαίσιο CF Poll:** Αποστέλλεται ένα πλαίσιο σε έναν σταθμό, δίνοντάς του άδεια να στείλει ένα μόνο πλαίσιο με οποιονδήποτε προορισμό. Αν ο σταθμός δεν έχει τίποτα να μεταδώσει, απαντάει με ένα κενό πλαίσιο. Αν δεν ληφθεί ACK πλαίσιο δεν υπάρχει αναμετάδοση παρά μόνο όταν ξαναδοθεί η άδεια από τον Point Coordinator.
- **Πλαίσιο Data + CF Poll:** Αποστέλλεται ένα πλαίσιο Data σε έναν μόνο προορισμό (unicasting). Το πλαίσιο παρέχει στον παραλήπτη και την άδεια να μεταδώσει.
- **Πλαίσιο CF End:** Σημαίνει το τέλος της Contention – Free περιόδου. Αποστέλλεται όταν:
 - ~ Εκπνεύσει ο χρόνος CFPDurRemaining.
 - ~ Ο Point Coordinator δεν έχει άλλα πλαίσια να μεταδώσει και δεν υπάρχουν άλλοι σταθμοί να κάνει Poll. Όταν ένας σταθμός συνδεθεί με ένα BSS έχει την επιλογή να δηλώσει πως είναι Pollable. Ο Point Coordinator τηρεί μια λίστα από αυτούς και σε κάθε Contention – Free περίοδο στέλνει τουλάχιστον ένα Poll πλαίσιο σε κάθε μέλος αυτής της λίστας.

4.1.2 Σύνδεση με το δίκτυο.

Όταν ένας σταθμός μπει σε λειτουργία, πρέπει να διαπιστώσει αν υπάρχει κάποιος άλλος σταθμός ή Access Point στην γύρω περιοχή. Αυτό μπορεί να γίνει με Active ή Passive τρόπο. Μετά από αυτήν την διαδικασία, ο σταθμός γνωρίζει τον κωδικό του ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

δικτύου (Service Set ID – SSID) και τις παραμέτρους με τις οποίες αυτό λειτουργεί, όπως για παράδειγμα το Frequency Hopping Pattern.

Στην Passive λειτουργία ο σταθμός παρακολουθεί τα κανάλια επικοινωνίας για κάποιο προκαθορισμένο χρόνο, περιμένοντας για Beacon πλαίσια με το SSID που επιθυμεί να συνδεθεί. Όταν εντοπίσει κάποιο από αυτά προχωράει σε διαδικασίες Association και Αυθεντικοποίησης.

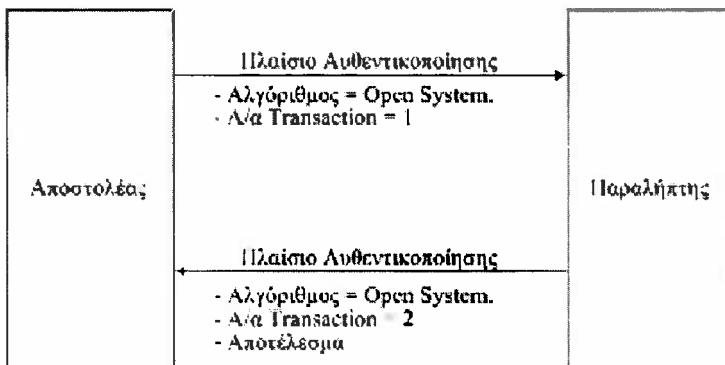
Στην Active Scanning λειτουργία, ο σταθμός στέλνει ένα Probe πλαίσιο με το SSID που επιθυμεί να συνδεθεί. Περιμένει ένα Probe Response πλαίσιο που επιβεβαιώνει την άπαρξη αυτού του BSS.

4.1.3 Authentication and Privacy.

Όπως αναφέραμε και στο κεφάλαιο 2 νωρίτερα, για να αντιμετωπιστεί η μη ασφαλής φύση του μέσου, το πρότυπο προτείνει κάποιες μεθόδους που αυξάνουν την ασφάλεια. Αυτές είναι η αυθεντικοποίηση και το WEP.

4.1.3.1 Αυθεντικοποίηση Ανοικτού Συστήματος (Open System Authentication).

Η λειτουργία αυτή περιγράφεται στο επόμενο σχήμα.



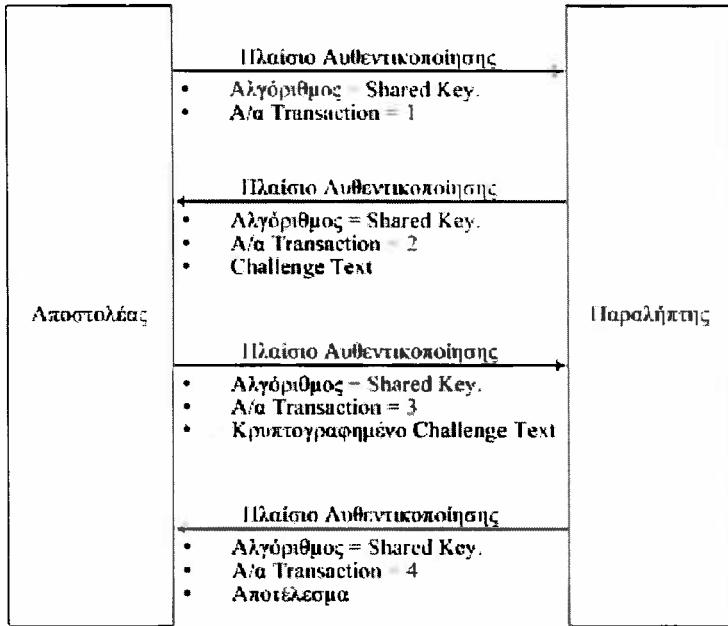
Σχήμα 23 - Αυθεντικοποίηση Ανοικτού Συστήματος.

4.1.3.2 Αυθεντικοποίηση Μυστικού Κλειδιού (Shared Key Authentication).

Αυτή η λειτουργία προσφέρει πολύ μεγαλύτερο επίπεδο ασφάλειας. Για να χρησιμοποιηθεί, πρέπει οι σταθμοί να χρησιμοποιούν WEP. Η διαδικασία φαίνεται στο σχήμα.

Πρόκειται για μια διαδικασία ανταλλαγής τεσσάρων μήνυμάτων:

- Αποστέλλεται η αίτηση αυθεντικοποίησης.
- Στο δεύτερο στάδιο ο σταθμός – παραλήπτης στέλνει ένα πλαίσιο που περιέχει ένα κείμενο μήκους 128 bytes.
- Ο πρώτος σταθμός κρυπτογραφεί αυτό το μήνυμα και το επιστρέφει.
- Με το ίδιο κλειδί, ο παραλήπτης αποκρυπτογραφεί το κείμενο και το συγκρίνει με το αρχικό. Αν ταιριάζουν, τότε η αυθεντικοποίηση είναι επιτυχής.

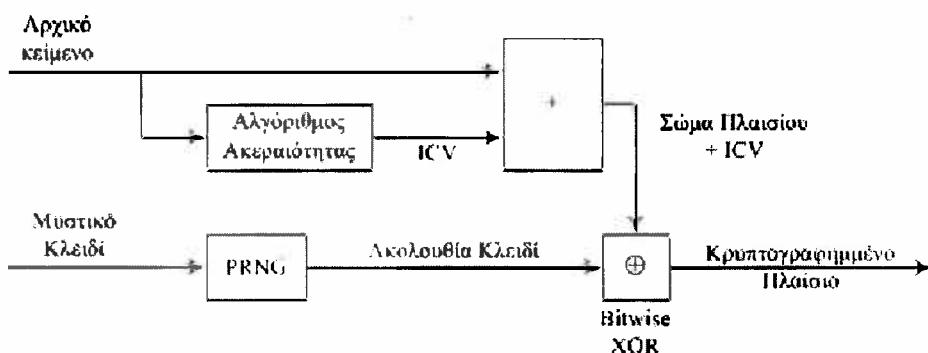


Σχήμα 24 - Αυθεντικοποίηση Μυστικού Κλειδιού.

4.1.3.3 Wireless Equivalent Privacy – WEP.

Πρόκειται για μια διαδικασία συμμετρικής κρυπτογράφησης πέντε βημάτων που “εγγυάται” την αποφυγή υποκλοπής. Έχει ως εξής:

- Αρχικά, το σώμα του πλαισίου περνά από έναν αλγόριθμο ελέγχου ακεραιότητας. Αυτός παράγει μία τιμή ελέγχου 4 bytes (Integrity Check Value – ICV) που στέλνεται μαζί με το πλαίσιο με σκοπό να προστατευτούν τα δεδομένα από αλλαγή.
- Το μυστικό κλειδί περνά από μια γεννήτρια ψευδοτυχαίων αριθμών (Pseudo Random Number Generator – PRNG) που παράγει μια ακολουθία μήκους ίσου με το μήκος των δεδομένων του πλαισίου συν το μήκος του ICV.
- Τα δεδομένα και το ICV κρυπτογραφούνται με την ακολουθία PRNG με bitwise XOR.



Σχήμα 25 - Ο Αλγόριθμος WEP.

- Στον παραλήπτη, τα δεδομένα αποκρυπτογραφούνται με την χρήση του ίδιου κλειδιού που παράγει την ίδια ακολουθία.
- Υπολογίζεται ένα ICV το οποίο πρέπει να ταυτίζεται με αυτό που έστειλε ο αποστολέας. Αυτό εγγυάται ότι τα δεδομένα δεν έχουν αλλαχτεί.

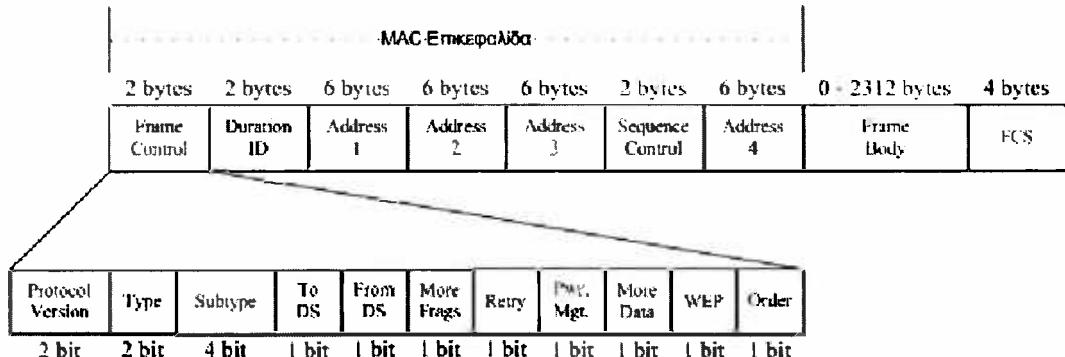
4.2 Η ΔΟΜΗ ΤΩΝ MAC ΠΛΑΙΣΙΩΝ.

Στις ακόλουθες παραγράφους θα γίνει μια αναλυτική παρουσίαση της δομής των πλαισίων MAC, όπως αυτή ορίζεται στο παράρτημα C του προτύπου IEEE 802.11.

Στο σχήμα που ακολουθεί, παρουσιάζεται η γενική δομή ενός πλαισίου MAC. Η δομή αυτή είναι κοινή για όλους τους τύπους πλαισίων (Data πλαίσια, Management πλαίσια κλπ).

Ένα πλαίσιο αποτελεί, ουσιαστικά, το κομμάτι των δεδομένων ενός πακέτου του φυσικού επιπέδου.

Κάθε πλαίσιο, όπως θα δούμε παρακάτω, αποτελείται από μία επικεφαλίδα μήκους, το πολύ, 30 bytes, το κομμάτι των δεδομένων μεταβλητού μήκους μέχρι 2.312 bytes και ένα πεδίο Frame Check Sequence μήκους 4 bytes. Έτσι το συνολικό μέγεθος ενός πλαισίου MAC είναι μικρότερο ή ίσο με 2.346 bytes.



Σχήμα 26 - Η Δομή των Πλαισίων MAC.

Στις παραγράφους που ακολουθούν θα περιγραφεί αναλυτικά η σημασία του κάθε πεδίου ξεχωριστά.

4.2.1 Το πεδίο Frame Control.

Το πεδίο αυτό είναι ουσιαστικά η περιγραφή του περιεχομένου του πλαισίου. Αποτελείται από πολλά υποπεδία, όπως φαίνεται στο σχήμα, το περιεχόμενο των οποίων ακολουθεί.

4.2.1.1 Protocol Version.

Έχει πάντα την τιμή 00. Στην περίπτωση που γίνουν σημαντικές αλλαγές στο πρότυπο, θα χρησιμοποιούνται νέες τιμές. Λέγοντας σημαντικές, εννοούμε αλλαγές που θα κάνουν την νέα έκδοση του προτύπου μη συμβατή με την παρούσα.

4.2.1.2 Type.

Περιγράφει τον τύπο του πλαισίου, σύμφωνα με τον ακόλουθο πίνακα.

Bit 2 και 3.	Τύπος πλαισίου.
00	Πλαίσιο Διαχείρισης
10	Πλαίσιο Ελέγχου
01	Πλαίσιο Δεδομένων
11	Δεσμευμένο

Πίνακας 10 - Το Πεδίο Type της Επικεφαλίδας των MAC Πλαισίων.

4.2.1.3 Subtype.

Σύμφωνα με την τιμή του πεδίου Type, το Subtype μπορεί να πάρει κάποιες τιμές, περιορισμένες. Οι δυνατοί συνδυασμοί φαίνονται στον ακόλουθο πίνακα. Τα bits στην στήλη “Τιμή Subtype” αναφέρονται με αντίστροφη σειρά.

Τιμή Type	Περιγραφή Type	Τιμή Subtype	Περιγραφή Subtype
00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	0110 – 0111	Reserved
00	Management	1000	Beacon
00	Management	1001	Announcement traffic indication message (ATIM)
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101 – 1111	Reserved
10	Control	0000 – 1001	Reserved
10	Control	1010	Power Save (PS)-Poll
10	Control	1011	Request To Send (RTS)
10	Control	1100	Clear To Send (CTS)
10	Control	1101	Acknowledgment (ACK)
10	Control	1110	Contention-Free (CF)-End
10	Control	1111	CF-End + CF-Ack
01	Data	0000	Data
01	Data	0001	Data + CF-Ack
01	Data	0010	Data + CF-Poll
01	Data	0011	Data + CF-Ack + CF-Poll
01	Data	0100	Null function (no data)
01	Data	0101	CF-Ack (no data)
01	Data	0110	CF-Poll (no data)
01	Data	0111	CF-Ack + CF-Poll (no data)
01	Data	1000 – 1111	Reserved
11	Reserved	0000 – 1111	Reserved

Πίνακας 11 - Το Πεδίο Subtype της Επικεφαλίδας των MAC Πλαισίων.

4.2.1.4 To DS.

Τίθεται ίσο με 1 όταν το πλαίσιο έχει προορισμό το Σύστημα Διανομής. Άλλιώς το πεδίο έχει την τιμή 0.

4.2.1.5 From DS.

Τίθεται ίσο με 1 όταν το πλαίσιο προέρχεται από το Σύστημα Διανομής. Άλλιώς το πεδίο έχει την τιμή 0.

Έτσι, όταν επικοινωνούν δύο Access Points, τα πεδία To DS και From DS έχουν και τα δύο, την τιμή 1.

4.2.1.6 More Frag.

Τίθεται ίσο με 1, όταν τα δεδομένα του επιπέδου LLC έχουν διασπασθεί σε πολλά MAC πλαίσια, τα οποία ακολουθούν. Δεν συμβαίνει ποτέ διάσπαση αν τα πλαίσια είναι Multicast ή Broadcast. Η διάσπαση των πλαισίων μειώνει την πιθανότητα συγκρούσεων, αλλά προσθέτει φόρτο στο δίκτυο, καθώς κάθε τμήμα απαιτεί δική του επικεφαλίδα και πλαίσια ACK, αυξάνοντας τα προς μετάδοση δεδομένα.

4.2.1.7 Retry.

Αν αναμεταδίδεται κάποιο προηγούμενο πλαίσιο λόγω αποτυχίας στην αρχική μετάδοση, το bit αυτό τίθεται ίσο με 1. Retry μπορεί να έχουμε, για παράδειγμα, αν ένα πλαίσιο ληφθεί με σφάλματα που εντοπίσθηκαν από το Frame Check Sequence, ή αν δεν ληφθεί ACK.

4.2.1.8 Power Management.

Το πεδίο αυτό παίρνει την τιμή 1, όταν ο σταθμός πρόκειται να μπει σε Sleep, μετά από την ανταλλαγή πλαισίων.

4.2.1.9 More Data.

Τίθεται ίσο με 1 όταν ο αποστολέας έχει και άλλα δεδομένα προς μετάδοση και ο παραλήπτης είναι σε Sleep.

4.2.1.10 WEP.

Τίθεται ίσο με 1, όταν το σώμα του πλαισίου έχει κρυπτογραφηθεί με WEP.

4.2.1.11 Order.

Τίθεται ίσο με 1 όταν τα πλαίσια πρέπει να τύχουν επεξεργασίας από τον παραλήπτη με την σειρά.

4.2.2 Duration / ID.

Στις πιο πολλές περιπτώσεις, σε αυτό το πεδίο περιέχεται η διάρκεια μετάδοσης του επόμενου πλαισίου. Οι σταθμοί χρησιμοποιούν αυτή την πληροφορία για να αναστείλουν τυχόν μεταδόσεις.

4.2.3 Address.

Τα τέσσερα αυτά πεδία περιέχουν διευθύνσεις διάφορων τύπων ανάλογα με τον τύπο πλαισίου. Οι διευθύνσεις μπορούν να είναι MAC διευθύνσεις (αρχικού αποστολέα, τελικού παραλήπτη, ενδιάμεσου αποστολέα ή παραλήπτη) ή κάποιο BSSID.

Οι διευθύνσεις είναι όλες μήκους 48 bit και μπορούν να είναι ατομικές (Unicast) ή ομαδικές (Multicast). Στην περίπτωση Broadcast η διεύθυνση είναι ίση με μια ακολουθία 48 άσσων. Οι MAC διευθύνσεις των σταθμών ακολουθούν τους ίδιους κανόνες με τις MAC διευθύνσεις όλων των τύπων δικτύων της οικογένειας IEEE 802.

Οι MAC διευθύνσεις μπορεί να αναφέρονται σε τέσσερις διαφορετικές λογικές οντότητες του δικτύου και ανάλογα έχουν και διαφορετικό όνομα.

- **Sender Address – SA.** Η MAC διεύθυνση του σταθμού που κατασκευάζει αρχικά το πλαίσιο. Με άλλα λόγια η πηγή του πλαισίου.
- **Destination Address – DA.** Η MAC διεύθυνση του σταθμού στον οποίο προορίζεται, τελικά, το πλαίσιο. Ο τελικός προορισμός.
- **Receiver Address – RA.** Ο επόμενος σταθμός που θα λάβει το πλαίσιο. Μπορεί να είναι ένας ενδιάμεσος σταθμός και να μην συμπίπτει με τον προορισμό.
- **Transmitter Address – TA.** Ο σταθμός που έστειλε το πλαίσιο. Μπορεί να είναι ενδιάμεσος σταθμός.

4.2.4 Sequence Control.

Το πεδίο αυτό έχει μήκος 16 bit. Τα τέσσερα πρώτα αποτελούν τον αύξοντα αριθμό του τμήματος (Fragment). Το πρώτο τμήμα έχει την τιμή 0. Η τιμή αυξάνει κατά 1 σε κάθε επόμενο τμήμα. Τα επόμενα 12 bit αποτελούν τον κωδικό του συνόλου των τμημάτων. Για κάθε σύνολο, ο αριθμός αυτός δεν αλλάζει.

4.2.5 Frame Body.

Αυτό το πεδίο έχει μεταβλητό μήκος και περιέχει τις πληροφορίες που μεταφέρει το πλαίσιο. Στην περίπτωση ενός πλαισίου δεδομένων (Data Frame), περιέχεται ένα πακέτο LLC. Στην περίπτωση πλαισίων Management, περιέχονται οι παράμετροι διαχείρισης.

4.2.6 Frame Check sequence – FCS.

Ο αποστολέας υπολογίζει ένα FCS χρησιμοποιώντας τον 32 – bit Cyclic Redundancy Code – CRC της IEEE και τοποθετεί το αποτέλεσμα σε αυτό το πεδίο. Χρησιμοποιείται για την ανίχνευση λαθών κατά την μετάδοση.

4.3 ΤΥΠΟΙ MAC ΠΛΑΙΣΙΩΝ.

Όπως έγινε σαφές από τα παραπάνω, τα πλαίσια MAC ανήκουν σε έναν από τρεις διαφορετικούς τύπους.

- Πλαίσια Διαχείρισης (Management Frames).
- Πλαίσια Ελέγχου (Control Frames).
- Πλαίσια Δεδομένων (Data Frames).

Ανάλογα με τον τύπο αλλάζει η επικεφαλίδα του πλαισίου και η σημασία των περιεχομένων του σώματός του.

Στις παραγράφους που ακολουθούν θα εξετάσουμε καθέναν από τους τύπους ξεχωριστά.

4.3.1 Πλαίσια Διαχείρισης.

Ο βασικός σκοπός των πλαισίων διαχείρισης είναι η εγκατάσταση επικοινωνίας μεταξύ σταθμών και Access Points. Για παράδειγμα, τέτοια πλαίσια χρησιμοποιούνται για να προσφερθούν υπηρεσίες Association κλπ.

Η δομή των πλαισίων διαχείρισης φαίνεται παρακάτω.

2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	0 - 2312 bytes	4 bytes
Frame Control	Duration	DA	SA	BSSID	Sequence Control	Frame Body	FCS

Σχήμα 27 - Η Δομή ενός MAC Πλαισίου Διαχείρισης.

Παρατηρούμε ότι το μήκος της επικεφαλίδας είναι μειωμένο κατά 6 bytes αφού δεν χρησιμοποιείται το πεδίο Address 4.

Το πεδίο Duration, σε περίοδο Contention – Free, έχει πάντα την τιμή 32.768 (δυαδικό 10000000 00000000). Έτσι τα πλαίσια διαχείρισης δεσμεύουν το μέσο για αρκετό χρονικό διάστημα, ώστε να εγκατασταθεί η απαραίτητη επικοινωνία.

Στην περίπτωση που έχουμε περίοδο CSMA / CA, το πεδίο Duration παίρνει διαφορετική τιμή, ανάλογα με τις παρακάτω περιπτώσεις.

- Την τιμή 0, αν το DA είναι ομαδική διεύθυνση.
- Αν το More Frag είναι 0 και το DA είναι ατομική διεύθυνση, το πεδίο παίρνει τιμή ίση με τον χρόνο που χρειάζεται για την αποστολή ενός ACK, συν την διάρκεια ενός SIFS.
- Αν το More Frag είναι 1 και το DA είναι ατομική διεύθυνση, το πεδίο παίρνει τιμή ίση με τον χρόνο που χρειάζεται για την αποστολή του επόμενου πλαισίου, συν δύο ACK, συν την διάρκεια τριών SIFS.

Ανάλογα με την υπηρεσία που περιγράφεται στο πλαίσιο, υπάρχουν αρκετοί υποτύποι:

1. Association Request.

Στέλνεται όταν ένας σταθμός επιθυμεί να γίνει associated με ένα access Point.

2. Association Response.

Η απάντηση στην προηγούμενη αίτηση.

3. Reassociation Request.

Αποστέλλεται όταν ένας σταθμός βγει από την ακτίνα ενός Access Point και επιθυμεί να συνδεθεί με ένα άλλο.

4. Reassociation Response.

Η απάντηση στην προηγούμενη αίτηση.

5. Probe Request.

Το στέλνει ένας σταθμός όταν επιθυμεί να λάβει πληροφορίες για έναν άλλο. Για παράδειγμα ένας σταθμός μπορεί να επιθυμεί αν ένα Access Point είναι διαθέσιμο.

6. Probe Response.

Η απάντηση στην προηγούμενη αίτηση. Περιέχει ένα σύνολο παραμέτρων – απαντήσεων που αφορούν τον σταθμό που παραλαμβάνει το Probe Request.

7. Beacon.

Στέλνεται περιοδικά από τα Access Points με στόχο τον συγχρονισμό των σταθμών που χρησιμοποιούν κοινό φυσικό επίπεδο.

Όταν χρησιμοποιείται PCF, ένα τέτοιο πλαίσιο στέλνεται ώστε να ανακοινωθεί η έναρξη περιόδου Contention – Free.

8. Announcement Traffic Indication Message – ATIM.

Το στέλνει ένας σταθμός που έχει ενταμιεύσει μηνύματα τα οποία προορίζονται για κάποιους άλλους. Περιέχει μια λίστα αυτών των σταθμών (Traffic Indication Map – TIM). Ακολουθεί η μετάδοση των ενταμιευμένων πλαισίων. Ένα ATIM πλαίσιο ενημερώνει τους σταθμούς που βρίσκονται σε sleep ότι υπάρχουν πλαισία. Ένας τέτοιος σταθμός ελέγχει, περιοδικά, τα Beacon πλαισία και αν βρει τον εαυτό του στο TIM “ξυπνά” για αρκετό χρονικό διάστημα ώστε να λάβει αυτά τα πλαισία.

9. Disassociation.

Το στέλνει ένας σταθμός που επιθυμεί να γίνει Disassociate από το αντίστοιχο Access Point.

10. Authentication.

Ένα σύνολο πλαισίων που στέλνονται με σκοπό την αυθεντικοποίηση ενός σταθμού από ένα Access Point. Το πλήθος των πλαισίων που ανταλλάσσονται εξαρτάται από τον αλγόριθμο αυθεντικοποίησης, Μυστικού Κλειδιού ή Ανοικτού Συστήματος, που αναλύεται σε παραπάνω παράγραφο.

11. Deauthentication.

Σημαίνει τον τερματισμό ασφαλούς επικοινωνίας.

Περιεχόμενα του Σώματος του Πλαισίου.	Association Request	Association Response	Reassociation Request	Reassociation Response	Probe Response	Probe Request	Beacon	Disassociation	Authentication	Deauthentication
Authentication Algorithm Number									✓	
Authentication Transaction Sequence Number									✓	
Beacon Interval					✓		✓			
Current AP Address		✓								
Listen Interval	✓		✓							
Reason Code								✓		✓
Association ID (AID)	✓		✓							
Status Code	✓		✓						✓	
Timestamp					✓		✓			
Service Set Identity (SSID)	✓		✓		✓	✓	✓			
Supported Rates	✓	✓	✓	✓	✓	✓	✓			
FH Parameter Set					✓		✓			
DS Parameter Set					✓		✓			
CF Parameter Set					✓		✓			
Capability Information	✓	✓	✓	✓	✓		✓			
Traffic Indication Map (TIM)							✓			
IBSS Parameter Set						✓	✓			
Challenge Text										✓

Πίνακας 12 - Συσχέτιση Τύπου Πλαισίου και Περιεχομένων.

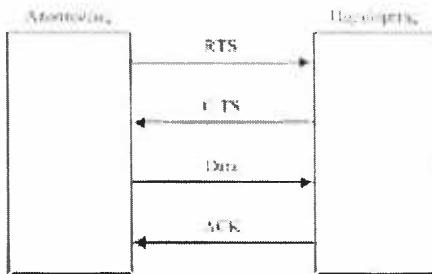
Τέλος, πρέπει να αναφέρουμε ότι ανάλογα με τον τύπο του πλαισίου διαχείρισης αλλάζουν και τα περιεχόμενα του σώματός του. Τα περιεχόμενα αυτά, σε αντίθεση με τα πλαίσια δεδομένων, είναι αυστηρώς δομημένα ανά περίπτωση, με υποπεδία σταθερού μήκους και σημασίας κλπ. Για λεπτομέρειες ο αναγνώστης παραπέμπεται στο πρότυπο IEEE 802.11, σελίδα 50 παράγραφος 7.3. Εδώ παρατίθεται ένας συνοπτικός πίνακας που περιέχει μια σύνοψη του τι είδους δεδομένα περιέχει κάθε τύπος πλαισίου διαχείρισης.

4.3.2 Πλαίσια Ελέγχου.

Για την υποστήριξη της ανταλλαγής δεδομένων μεταξύ δύο σταθμών και αφού έχει γίνει αυθεντικοποίηση και έχει εγκατασταθεί επικοινωνία, χρησιμοποιούνται τα πλαίσια ελέγχου. Τα πλαίσια αυτά δεν μεταφέρουν δεδομένα καθαυτά, αλλά διαφορετικού είδους πληροφορίες που προσθέτουν λειτουργικότητα στο δίκτυο.

Ένα κλασσικό παράδειγμα ροής πλαισίων ελέγχου είναι η RTS – CTS – ACK, η οποία χρησιμοποιείται σε κάθε ανταλλαγή δεδομένων. Μάλιστα είναι ένα παράδειγμα που συναντάμε σε δίκτυα πολλών μορφών και δεν αποτελεί καινοτομία του IEEE 802.11.





Σχήμα 28 - Ανταλλαγή Πλαισίων RTS, CTS, ACK.

Σύμφωνα με αυτό το μοντέλο, ένας σταθμός, πριν στείλει δεδομένα σε κάποιον άλλο, ενημερώνει για την πρόθεσή του αυτή, με ένα RTS (Request To Send) πλαίσιο ελέγχου. Αν ο προτιθέμενος παραλήπτης είναι έτοιμος για παραλαβή απαντά με ένα CTS (Clear To Send) πλαίσιο, δίνοντας άδεια στον πρώτο σταθμό να πραγματοποιήσει την αποστολή. Όταν αυτή ολοκληρωθεί, ο παραλήπτης επιβεβαιώνει την ορθή λήψη των δεδομένων με ένα πλαίσιο ACK (Acknowledgement).

Ένα αξιοσημείωτο χαρακτηριστικό των πλαισίων ελέγχου είναι ότι το πεδίο Frame Control, της επικεφαλίδας τους, είναι πανομοιότυπο ανεξαρτήτως περιεχομένου του πλαισίου.

Protocol Version	Control	Subtype	0	0	0	0	Par Mgt	0	0	0
------------------	---------	---------	---	---	---	---	---------	---	---	---

Σχήμα 29 - Το Πεδίο Frame Control στα Πλαίσια Ελέγχου.

Στις αμέσως επόμενες παραγράφους, θα εξετάσουμε αναλυτικά την δομή και λειτουργία αυτών των πλαισίων.

4.3.2.1 Request To Send – RTS.

Ένας σταθμός στέλνει ένα πλαίσιο RTS σε έναν συγκεκριμένο παραλήπτη, για να ενημερώσει ότι προτίθεται να στείλει ένα πλαίσιο δεδομένων. Να σημειωθεί ότι για πολύ μικρά πλαίσια η αποστολή ενός RTS δεν είναι απαραίτητη. Το όριο μεγέθους πλαισίου, πάνω από το οποίο επιβάλλεται η αποστολή RTS ορίζεται σαν παράμετρος στην MIB του σταθμού.

2 Bytes	2 Bytes	6 Bytes	6 Bytes	4 Bytes
Frame Control	Duration	RA	TA	FCS

Σχήμα 30 - Πλαίσιο RTS.

Στο παραπάνω σχήμα φαίνεται η δομή ενός RTS.

Το πεδίο Duration περιέχει, σε μSec, τον χρόνο που χρειάζεται για την αποστολή του πλαισίου, συν ένα CTS, συν ένα ACK, συν την διάρκεια τριών SIFS.

4.3.2.2 Clear To Send – CTS.

Όταν ένας σταθμός λάβει ένα RTS, επιστρέφει ένα CTS, δίνοντας άδεια στον αποστολέα να στείλει τα δεδομένα του.

2 Bytes	2 Bytes	6 Bytes	4 Bytes
Frame Control	Duration	RA	FCS

Σχήμα 31 - Η Δομή των Πλαισίων CTS και ACK.

Στο παραπάνω σχήμα φαίνεται η δομή ενός CTS.

Το πεδίο Duration περιέχει, σε μSec, τον χρόνο που περιείχε το RTS, μείον τον χρόνο που χρειάζεται για την αποστολή του CTS, μείον ένα SIFS.

4.3.2.3 Acknowledgement – ACK.

Όταν ένας σταθμός λάβει ένα πλαίσιο δεδομένων, ελεύθερο σφαλμάτων, επιστρέφει ένα πλαίσιο ACK, επιβεβαιώνοντας την ορθή λήψη.

Η δομή των πλαισίων ACK ταυτίζεται με αυτή των CTS.

Το πεδίο Duration περιέχει την τιμή 0 αν το πλαίσιο, το οποίο επιβεβαιώνεται από το ACK, είχε την τιμή 0 στο πεδίο More Frag. Αν η τιμή του More Frag ήταν 1, η τιμή του Duration περιέχει, σε μSec, την διάρκεια του εν λόγω πλαισίου διαχείρισης ή δεδομένων, μείον τον χρόνο που χρειάζεται η αποστολή του ACK, μείον ένα SIFS.

4.3.2.4 Power Save Poll – PS Poll.

Παρατηρούμε ότι ένα PS Poll πλαίσιο δεν περιέχει το πεδίο Duration.

2 Bytes	2 Bytes	6 Bytes	6 Bytes	4 Bytes
Frame Control	AID	BSSID	TA	FCS

Σχήμα 32 - Πλαίσιο Power Save Poll.

Αντίθετα περιέχει το AID, δηλαδή τον κωδικό αριθμό του Association μεταξύ του Access Point και του σταθμού. Τον κωδικό αυτό απέστειλε το Access Point με το Association Response πλαίσιο διαχείρισης όταν ο σταθμός έγινε αρχικά associated.

4.3.2.5 Contention Free End – CF End.

Όταν το δίκτυο βρίσκεται σε περίοδο λειτουργίας Contention – Free, και ο Point Coordinator επιθυμεί να σημάνει την επιστροφή σε λειτουργία CSMA / CA, στέλνει ένα CF End πλαίσιο ελέγχου. Το πλαίσιο αυτό έχει στο Duration την τιμή 0 και στην διεύθυνση προορισμού την Broadcast διεύθυνση.

2 Bytes	2 Bytes	6 Bytes	6 Bytes	4 Bytes
Frame Control	Duration	RA	BSSID	FCS

Σχήμα 33 - Πλαίσιο CF End.

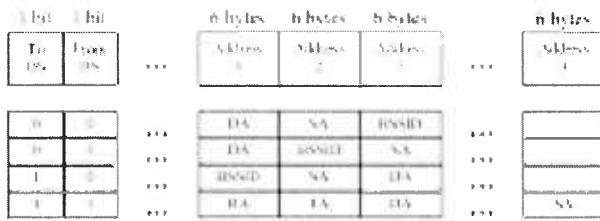


4.3.2.6 CF End + CF ACK.

Το πλαίσιο αυτό ανακοινώνει την αναγνώριση τέλους της περιόδου CF. Η δομή του είναι ίδια με την δομή του CF End.

4.3.3 Πλαίσια Δεδομένων.

Είναι τα πλαίσια που μεταφέρουν τα δεδομένα του επιπέδου LLC, από μια οντότητα του δικτύου σε μία άλλη.



Σχήμα 34 - Πώς τα Πεδία Address Επηρεάζονται από τα Υποπεδία To DS και From DS.

Το μόνο αξιοσημείωτο είναι να δούμε τον τρόπο με τον οποίο τα πεδία Address της επικεφαλίδας αλλάζουν σημασία ανάλογα με τις τιμές των υποπεδίων To DS και From DS του πεδίου Frame Control.

Συγκεκριμένα, το πεδίο Address 4 χρησιμοποιείται μόνο στην περίπτωση που τα To DS και From DS έχουν τις τιμές 1 και 1. Επιπλέον, το πεδίο Address 1 περιέχει πάντα την διεύθυνση του επόμενου προορισμού, είτε ενδιάμεσου είτε τελικού και το Address 2 την διεύθυνση του αποστολέα, επίσης είτε ενδιάμεσου είτε τελικού.

Μέρος 3^ο:

Ειδικά θέματα δικτύων.

5 ΜΕΤΑΦΕΡΣΙΜΟΤΗΤΑ ΣΤΑΘΜΩΝ.

Το γεγονός ότι η λογική IP διεύθυνση ενός υπολογιστή συνδέεται με την φυσική του θέση, έχει σαν αποτέλεσμα, ο υπολογιστής αυτός, να τίθεται εκτός δικτύου όταν μετακινείται πέρα από κάποια φυσικά όρια.

Το πρότυπο IEEE 802.11 προσφέρει μια λύση στο πρόβλημα αυτό σε επίπεδο σύνδεσης δεδομένων. Ωστόσο αυτή η λύση δεν έχει γενική ισχύ, αλλά λειτουργεί σε περιορισμένο χώρο.

Λύσεις σε αυτό το πρόβλημα έρχεται να δώσει το πρωτόκολλο Mobile IP, τόσο στην έκδοση 4, όσο και στην έκδοση 6, που συνδυάζεται με το πρωτόκολλο IPv6.

Ειδικά στον χώρο των ασύρματων τοπικών δικτύων, λύσεις προσπαθούν να δώσουν και οι ίδιοι οι κατασκευαστές εξοπλισμού, δημιουργώντας το Inter Access Point Protocol – IAPP.

5.1 MOBILE IP.

Το Mobile IP είναι ένα πρωτόκολλο επιπέδου δικτύου το οποίο φιλοδοξεί να επιτρέψει αυτό που καλείται “Station Mobility”. Με άλλα λόγια, επιδιώκεται να επιλυθεί το πρόβλημα που προκύπτει όταν ένας σταθμός μετακινηθεί από ένα χώρο σε κάποιον άλλο.

Η λύση που προσφέρει το Mobile IP έχει σαν σκοπό να είναι γενική, εύκολα κλιμακώσιμη και να προσφέρει ψηλό επίπεδο ασφάλειας. Συγκεκριμένα, το Mobile IP, επιτρέπει σε έναν κόμβο να αλλάζει τοποθεσία διατηρώντας την IP διεύθυνσή του και χωρίς να διακοπούν οι σύνοδοι που έχει ήδη εγκαταστήσει.

Σε πολύ γενικές γραμμές, ο τρόπος με τον οποίο το Mobile IP επιτυγχάνει τα παραπάνω είναι με το να κάνει τις κατάλληλες μετατροπές στους πίνακες δρομολόγησης κατάλληλων ενδιάμεσων κόμβων, ώστε τα ήδη υπάρχοντα πρωτόκολλα δρομολόγησης, RIP, BGP, OSPF, να μπορούν να παραδώσουν τα IP datagrams στον προορισμό τους.

Από αυτή την σκοπιά, το Mobile IP μπορεί να θεωρηθεί πρωτόκολλο δρομολόγησης ειδικού σκοπού.

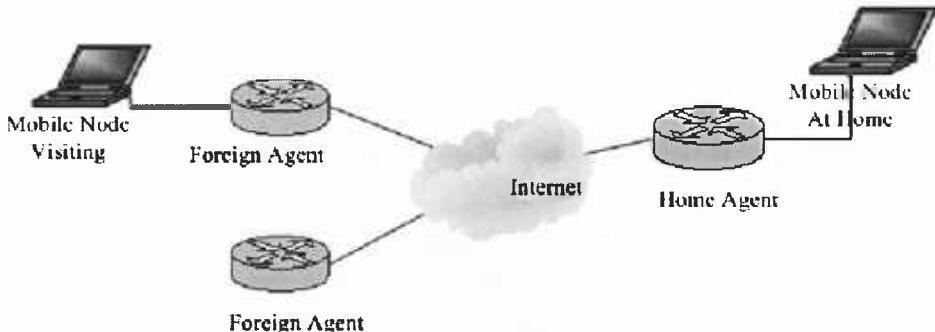
5.1.1 Οι Απαιτήσεις του Mobile IP.

Ο σχεδιασμός του Mobile IP καθοδηγήθηκε με κριτήριο κάποιες αρχικές απαιτήσεις. Οι απαιτήσεις αυτές ήταν:

- Ένας σταθμός θα πρέπει να διατηρήσει την ικανότητά του να επικοινωνεί, ανεξαρτήτως του σημείου μέσω του οποίου έχει φυσική πρόσβαση στο διαδίκτυο.
- Το παραπάνω πρέπει να επιτυγχάνεται χωρίς μεταβολή της IP διεύθυνσης του σταθμού.
- Πρέπει να είναι δυνατή η επικοινωνία με υπολογιστές που δεν υλοποιούν το πρωτόκολλο αυτό.
- Ένας κόμβος δεν πρέπει να εκτεθεί σε νέους κινδύνους σε σχέση με τους μη κινούμενους κόμβους.

5.1.2 Οι Συνιστώσες του Mobile IP.

Για να επιτευχθούν οι στόχοι που τίθενται, το πρωτόκολλο πρέπει να υλοποιηθεί, πέρα από τον μετακινούμενο κόμβο και σε κάποιους άλλους ενδιάμεσους. Σε αυτές ακριβώς τις ενδιάμεσες οντότητες θα αναφερθούμε παρακάτω, ορίζοντας τις και περιγράφοντας την λειτουργικότητά τους.



Σχήμα 35 - Οι Οντότητες του Mobile IP.

5.1.2.1 Mobile Node.

Είναι ένας κόμβος που μπορεί να αλλάζει, περιοδικά, το σημείο μέσω του οποίου συνδέεται στο διαδίκτυο. Θα πρέπει, κατά την διαδικασία αυτής της μετάβασης από σημείο σε σημείο, να διατηρεί σταθερή IP διεύθυνση και να μπορεί να συνεχίσει όλες του τις επικοινωνίες χωρίς διακοπή.

5.1.2.2 Home Agent.

Είναι ένας δρομολογητής, με μια διεπαφή με το δίκτυο στο οποίο ανήκει κανονικά ο κόμβος. Το εν λόγω σημείο είναι, ουσιαστικά, το υποδίκτυο από το οποίο ο κόμβος έχει πάρει την αρχική του IP διεύθυνση.

- Ο κόμβος που κινείται ενημερώνει τον Home Agent για την θέση του, στέλνοντάς του την Care – of διεύθυνσή του.

- Ο Home Agent "διαφημίζει" την σύνδεσή του με το υποδίκτυο στο οποίο ανήκει ο κόμβος.
- Ο Home Agent παρεμβάλλεται στα πακέτα που προορίζονται για τον κόμβο, αν ο κόμβος έχει μεταφερθεί σε κάποιο άλλο σημείο, τότε ο Home Agent δεν δρομολογεί τα πακέτα σύμφωνα με τον γνωστό τρόπο. αντίθετα, δημιουργεί ένα Tunnel, μέσω του οποίου στέλνει τα πακέτα στην care – of διεύθυνση του κόμβου.

5.1.2.3 Foreign Agent.

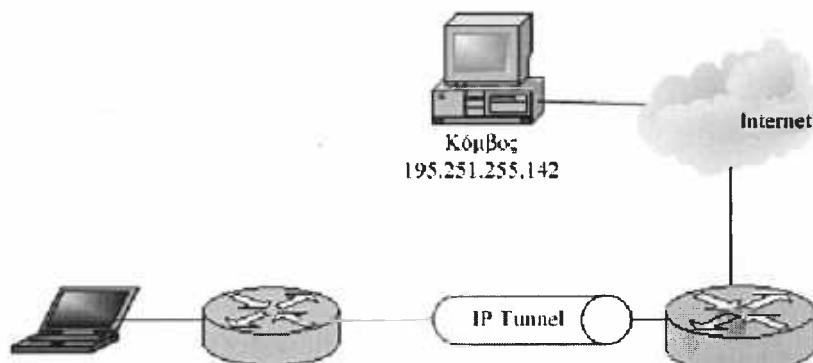
Είναι ένας δρομολογητής, με μια διεπαφή με το δίκτυο στο οποίο βρίσκεται προσωρινά ο κόμβος. Ο Foreign Agent συμβάλει ώστε ο κόμβος που κινείται να μπορεί να ενημερώσει τον Home Agent για την θέση του. Λειτουργεί ως παραδοσιακός δρομολογητής για τα πακέτα που αποστέλλει ο κόμβος.

5.1.2.4 Tunneling.

Εν συντομίᾳ, ένα Tunnel, πρόκειται για μια διαδρομή που ακολουθεί ένα πακέτο εκθυλακωμένο στο τμήμα δεδομένων ενός άλλου πακέτου του ιδίου πρωτοκόλλου. Για παράδειγμα ένα Tunnel δημιουργείται όταν ένα IP datagram "ταξιδεύει" στο τμήμα δεδομένων ενός άλλου IP Datagram. Αυτή είναι και η περίπτωση που παρατηρείται στο Mobile IP και αποκαλείται IP Encapsulation Within IP. Ωστόσο πρέπει να σημειωθεί ότι δεν είναι και η μοναδική.

Header		Data
Source Address	= 195.251.255.142	
Destination Address	= 195.251.252.72	

Αρχικό IP Datagram



Laptop
195.251.252.72

Foreign Agent
50.0.0.1

Home Agent
195.251.255.142

Header		Data:
Source Address	= 195.251.252.126	Αρχικό IP Datagram
Destination Address	= 50.0.0.1	

Φέρον IP Datagram

Σχήμα 36 - IP Encapsulation Within IP.

5.1.3 Home Address, Home Link, Home Agent.

Ως Home Address, ορίζουμε την IP διεύθυνση που αντιστοιχεί μόνιμα σε έναν κόμβο που μεταφέρεται. Η μονιμότητα αυτής της διεύθυνσης καθώς ο κόμβος μετακινείται, αποτελεί βασική προϋπόθεση στο Mobile IP. Εξυπακούεται πως η διεύθυνση αυτή μπορεί να αλλάξει για τους ίδιους λόγους που αλλάζει η διεύθυνση οποιουδήποτε κόμβου. Αυτό μπορεί να συμβεί για παράδειγμα αν αλλάξει η διεύθυνση του δικτύου στο οποίο ανήκει ο κόμβος.

Ως Home Link ορίζουμε την διεύθυνση του δικτύου στο οποίο ανήκει ο κόμβος, κατά συνέπεια, δεν πρόκειται για τίποτε άλλο από το Network Prefix της IP διεύθυνσης του κόμβου. για παράδειγμα ένας κόμβος με IP διεύθυνση την 195.251.252.72/26 θα έχει ως διεύθυνση δικτύου την 195.251.252.192.

Η διεύθυνση αυτή χρησιμοποιείται σχεδόν πάντα στα πεδία Source Address και Destination Address των πακέτων που στέλνει ή λαμβάνει, αντίστοιχα, ο κόμβος.

Ως Home Agent ορίζουμε έναν δρομολογητή που έχει τουλάχιστον μια διεπαφή με το δίκτυο που αναφέραμε παραπάνω.

5.1.4 Care – of Address, Foreign Link, Foreign Agent.

Ως Foreign Agent ορίζουμε έναν δρομολογητή που έχει τουλάχιστον μια διεπαφή με το δίκτυο που τυγχάνει να βρεθεί ο κόμβος που μετακινείται.

Εξ ορισμού, care – of διεύθυνση είναι μια IP διεύθυνση συσχετισμένη με έναν κινούμενο κόμβο, ο οποίος επισκέπτεται ένα Foreign Link.

Για να διαλευκανθεί κάπως ο ορισμός αυτός, θα παραθέσουμε ορισμένες ιδιότητες μιας Care – of διεύθυνσης.

- Η διεύθυνση αυτή αλλάζει, όταν αλλάζει ο Foreign Link τον οποίο επισκέπτεται ο κόμβος.
- Η διεύθυνση αυτή, αναφορικά στη δρομολόγηση, δεν διαφέρει καθόλου από τις κλασσικές IP διευθύνσεις. Ένα πακέτο μπορεί να παραδοθεί σε αυτή με την χρήση τυπικών μεθόδων δρομολόγησης (RIP, OSPF, BGP).
- Η διεύθυνση αυτή αποτελεί την έξοδο των Tunnels από τον Home Agent προς τον κόμβο.
- Η διεύθυνση αυτή δεν χρησιμοποιείται σχεδόν ποτέ στο πεδίο Source Address της επικεφαλίδας των IP Datagrams που αποστέλλει ο σταθμός. Επίσης δεν χρησιμοποιείται στο πεδίο Destination Address των datagrams που προορίζονται για τον σταθμό. Ένα ερώτημα σε Domain Name Server δεν θα επιστρέψει ποτέ την Care – of διεύθυνση του σταθμού.



5.1.4.1 Οι τύποι των Care – of διευθύνσεων.

Μια Care – of διεύθυνση μπορεί να είναι δύο τύπων. Ο τύπος της δεν καθορίζει ποιος θα είναι ο τελικός παραλήπτης ενός πακέτου, αλλά σε ποιο σημείο θα είναι η έξοδος του Tunnel προς τον μετακινούμενο κόμβο. Συγκεκριμένα:

1. Foreign Agent Care – of Address.

Είναι οποιαδήποτε διεύθυνση του Foreign Agent. Κατά συνέπεια το Network Prefix αυτής της διεύθυνσης δεν ταυτίζεται απαραίτητα με την διεύθυνση του δικτύου στο οποίο τυγχάνει να βρίσκεται ο σταθμός. Σε αυτή την περίπτωση, πολλοί μετακινούμενοι σταθμοί μπορούν να χρησιμοποιούν την ίδια Care – of διεύθυνση ταυτόχρονα. Όταν ένας σταθμός αποκτήσει Care – of Address αυτού του τύπου, τότε η έξοδος των Tunnels είναι ο Foreign Agent.

2. Collocated Care – of Address.

Είναι μια IP διεύθυνση η οποία ανατίθεται προσωρινά σε έναν σταθμό που έχει μετακινηθεί. Το Network Prefix αυτής ταυτίζεται με την διεύθυνση του δικτύου στο οποίο αυτός βρίσκεται. Δεν είναι δυνατή η χρησιμοποίηση της ίδιας διεύθυνσης από πολλούς σταθμούς ταυτόχρονα. Όταν ένας σταθμός αποκτήσει Care – of Address αυτού του τύπου, τότε τα Tunnels καταλήγουν κατευθείαν σε αυτόν. Σε αυτή την περίπτωση δεν έχει νόημα η ύπαρξη του Foreign Agent.

Συνοψίζοντας, μπορούμε να αναφέρουμε ότι η Care – of διεύθυνση είναι μια διεύθυνση, το πολύ ένα βήμα (Hop) μακριά από τον Foreign Agent. Δηλαδή όταν φτάσει σε αυτόν ένα πακέτο με Destination Address αυτή την διεύθυνση, τότε αυτό μπορεί να παραδοθεί άμεσα.

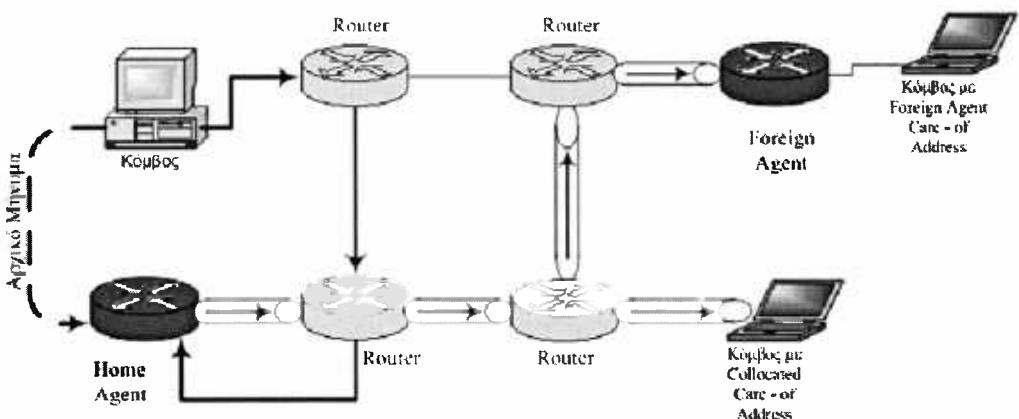
5.1.5 Η λειτουργία του Mobile IP.

Σε αυτή την παράγραφο θα περιγράψουμε με λίγα λόγια την λειτουργία του πρωτοκόλλου Mobile IP.

- Οι Home και Foreign Agents ανακοινώνουν την ύπαρξή τους με περιοδικά Broadcast ή multicast μηνύματα που καλούνται “Agent Advertisements”.
- Οι κόμβοι που έχουν ενεργοποιημένο το Mobile IP, από αυτά το μηνύματα διαπιστώνουν αν είναι συνδεδεμένοι με το δίκτυο στο οποίο ανήκουν ή αν έχουν μετακινηθεί. Αν ισχύει το δεύτερο διαπιστώνουν επίσης αν βρίσκονται στο ξένο δίκτυο που βρίσκονταν και προηγουμένως ή αν έχουν μεταφερθεί σε νέο Foreign Link.
- Στην περίπτωση που ο σταθμός έχει μεταφερθεί, προσπαθεί να αποκτήσει μια Care – of διεύθυνση. Αυτή την αποκτά χρησιμοποιώντας την διεύθυνση του αποστολέα του Agent Advertisement, οπότε είναι Foreign Agent διεύθυνση.

Επίσης μπορεί να την αποκτήσει μέσω DHCP ή χειροκίνητα, οπότε είναι Collocated διεύθυνση.

- Ο κόμβος καταχωρεί την νέα του διεύθυνση στον Home Agent.
- Ο Home Agent λαμβάνει όλα τα μηνύματα, που προορίζονται για τον κόμβο και του τα προωθεί μέσω ενός IP Tunnel με έξοδο την Care – of διεύθυνση.
- Στην έξοδο του Tunnel το αρχικό πακέτο ανακτάται από αυτό που το ενθυλακώνει και παραδίδεται στον κόμβο που έχει μεταφερθεί.
- Στην περίπτωση που στέλνει πακέτα αυτός ο κόμβος, δεν συμβαίνει τίποτα διαφορετικό, ανεξάρτητα από το πού αυτός βρίσκεται. Τα πακέτα του δρομολογούνται σύμφωνα με τους γνωστούς μηχανισμούς.



Σχήμα 37 - Η Λειτουργία του Mobile IP.

5.2 IP NEXT GENERATION – MOBILE IP VERSION 6.

Στις Προηγούμενες παραγράφους μελετήσαμε την έκδοση 4 του πρωτοκόλλου Mobile IP. Με την ανάπτυξη του IPv6, δημιουργήθηκε η ανάγκη για εύρεση νέων τρόπων για να υποστηριχθεί η μετακίνηση των κόμβων. Έτσι βρίσκεται υπό ανάπτυξη από τον IETF, η νέα έκδοση του Mobile IP, η έκδοση 6. Το πρωτόκολλο βρίσκεται ακόμα σε επίπεδο Internet Draft από την ομάδα εργασίας “IP Routing for Wireless/Mobile Hosts (mobileip)”. Έτσι, όλα όσα θα αναφερθούν εδώ δεν αποτελούν την τελική μορφή του πρωτοκόλλου. Βασιζόμαστε στην έκδοση 15 του αντίστοιχου κειμένου. “draft-ietf-mobileip-ipv6-15.txt”

Το γεγονός, πάντως, είναι ότι το IPv6 δίνει την δυνατότητα ευκολότερης υλοποίησης του Mobile IP. Επίσης, οι διαφορές του από το γνωστό σε όλους IP, αξίζει να αναφερθούν, ώστε να γίνει ομαλά η κατανόηση της δουλειάς που έχει γίνει για το Mobile IPv6.

Συνεπώς, στις παρακάτω σελίδες θα γίνει μια περιγραφή αυτών των αλλαγών και στην συνέχει θα μπούμε στην ουσία, που δεν είναι άλλη από την περιγραφή της νέας έκδοσης του Mobile IP.

5.2.1 IPv6.

Οι διαφορές του IPv6 από το IP είναι πολλές και αρκετά σημαντικές. Ονομαστικά θα αναφέρουμε την διαφορά στις διευθύνσεις και στις επικεφαλίδες των πακέτων. Αυτές, μάλιστα, είναι και οι διαφορές που παίζουν και τον σημαντικότερο ρόλο στην ανάπτυξη του Mobile IPv6.

5.2.1.1 Διευθύνσεις.

Το γνωστό εδώ και καιρό πρόβλημα ότι οι διευθύνσεις μήκους 32 bit έχουν αρχίσει να εξαντλούνται, αντιμετωπίζει το σύστημα διευθυνσιοδότησης στο IPv6.

Οι διευθύνσεις είναι πλέον μήκους 128 bit. Έτσι το πλήθος των διαθέσιμων διευθύνσεων αυξάνει σημαντικά. Οι $4.294.967.296$ γίνονται πλέον $3,4028 \times 10^{38}$. Να σημειωθεί ότι 10^{38} είναι ίσο με ένα τρισεκατομμύριο. Η αλλιώς οι διαθέσιμες διευθύνσεις είναι πλέον 2^{96} φορές περισσότερες. Με άλλα λόγια είναι σχεδόν απίθανο να εξαντληθούν. Επίσης αντιμετωπίζεται το πρόβλημα της εκρηκτικής αύξησης των πινάκων δρομολόγησης, αφού πολλές διευθύνσεις δικτύου μπορούν να συνοψίζονται με μία μεγαλύτερου μήκους. Τέλος, δίνεται η δυνατότητα χρησιμοποίησης του μηχανισμού Stateless Address Autoconfiguration που θα δούμε μιλώντας για το Mobile IPv6.

Κλείνοντας, θα αναφέρουμε ότι εκτός από τις Unicast και Multicast διευθύνσεις, το IPv6 ορίζει και τις Anycast, όπου ένα πακέτο παραδίδεται σε οποιονδήποτε, ακριβώς έναν, υπολογιστή που ανήκει στην ομάδα που περιγράφεται από την διεύθυνση προορισμού. Δεν υπάρχουν Broadcast διευθύνσεις.

5.2.1.2 Επικεφαλίδα.

Μια άλλη καινοτομία του πρωτοκόλλου είναι η δομή της επικεφαλίδας. Η προσπάθεια ήταν να μην συμπεριλαμβάνονται πάντα όλα τα πεδία που μπορεί να είναι περιττά σε ορισμένες περιπτώσεις.

Ο τρόπος που επινοήθηκε ήταν να χρησιμοποιείται μια βασική επικεφαλίδα (Base Header) και τα υπόλοιπα στοιχεία συμπεριλαμβάνονται, μόνο όταν χρειάζονται, σε επικεφαλίδες επέκτασης (Extension Headers). Ένα IP πακέτο μπορεί να περιέχει απεριόριστο αριθμό τέτοιων επικεφαλίδων και καθεμία από αυτές περιέχει ένα πεδίο που περιγράφει τι τύπου είναι η επόμενη. Η τελευταία από αυτές, ή η βασική αν δεν υπάρχουν συμπληρωματικές, περιέχει σε αυτό το πεδίο τον κωδικό του πρωτοκόλλου ανώτερου επιπέδου που έχει αναλάβει να μεταφέρει το πακέτο (π.χ. TCP, UDP κλπ).



Έτσι, η βασική επικεφαλίδα περιέχει τις διευθύνσεις αποστολέα και παραλήπτη, καθώς και κάποιες άλλες χρήσιμες πληροφορίες, όπως η έκδοση του πρωτοκόλλου. Πληροφορίες κατακερματισμού και Type of Service συμπεριλαμβάνονται προαιρετικά σε συμπληρωματικές επικεφαλίδες.

5.2.2 Mobile IPv6.

Παρακάτω, θα δούμε σε πολύ γενικές γραμμές, την λειτουργία του πρωτοκόλλου Mobile IPv6 σε αντιπαράθεση με το Mobile IPv4.

Mobile IPv4	Mobile IPv6
Κόμβος Home Link Home Address Foreign Link	Παραμένουν Τίτλος
Foreign Agent	Δεν Χρησιμοποιείται
Foreign Agent Care – of Διεύθυνση Collocated Care – of Διεύθυνση	Collocated Care – of Διεύθυνση
Μέθοδος Απόκτησης Care – of Διεύθυνσης	Τίτλος + Stateless Address Autoconfiguration
Ανακάλυψη Agent	Ανακάλυψη Δρομολογητή
Καταχώρηση με τον Home Agent	Καταχώρηση με τον Home Agent και άλλους Correspondents
Tunneling	Tunneling και Δρομολόγηση Πηγής
Δεν Χρησιμοποιείται	Route Optimization

Πίνακας 13 - Mobile IPv4 vs Mobile IPv6.

Ο πίνακας περιέχει την αντιστοιχία των οντοτήτων που χρησιμοποιούνται στα δύο πρωτόκολλα. Μελετώντας τον τρόπο λειτουργίας του Mobile IPv6, θα σταθούμε σε 5 σημεία.

- Απαλοιφή του Foreign Agent.
- Απαλοιφή της Care – of Διεύθυνσης τύπου Foreign Agent.
- Stateless Address Autoconfiguration.
- Correspondents.
- Δρομολόγηση Πηγής.

5.2.2.1 Foreign Agent. Care – of Διεύθυνση τύπου Foreign Agent.

Ο χώρος διευθύνσεων στο IPv6 είναι θεωρητικά επαρκής. Έτσι δεν συντρέχει λόγος οι κόμβοι να μοιράζονται την ίδια διεύθυνση. Είναι ακίνδυνο ο κάθε κόμβος να έχει την δική του Care – of διεύθυνση και μάλιστα επιτρέπεται να έχει και εναλλακτικές. Έτσι λοιπόν, κρίθηκε σκόπιμο, το Mobile IPv6 να χρησιμοποιεί μόνο Collocated Care – of διευθύνσεις και να καταργηθεί η Διεύθυνση τύπου Foreign Agent.

Στο Mobile IPv4 την χρήση του Foreign Agent την παρατηρούσαμε μόνο στην περίπτωση της Foreign Agent Care – of διεύθυνσης, όπου ο δρομολογητής αυτός

αποτελούσε και την έξοδο ενός Tunnel από τον Home Agent προς τον κόμβο. Στην περίπτωση της Collocated Care – of διεύθυνσης, δρουόσε ως ένας κοινός δρομολογητής.

Είναι προφανής, λοιπόν, από τα παραπάνω ο λόγος για τον οποίο ο Foreign Agent παύει να υφίσταται ως ξεχωριστή οντότητα. Η ύπαρξη μόνο Collocated Care – of διευθύνσεων έχει σαν συνέπεια η έξοδος του Tunnel να είναι πάντα ο μετακινούμενος κόμβος. Ο δρομολογητής που θα έπαιξε τον ρόλο του Foreign Agent, χάνει αυτήν την ιδιότητα και υποβιβάζεται σε απλό δρομολογητή.

5.2.2.2 Stateless Address Autoconfiguration.

Εκτός από την ανάθεση Care – of διεύθυνσης μέσω DHCP ή χειροκίνητα, ένας σταθμός μπορεί να την αποκτήσει και αυτόματα, μέσω της μεθόδου Stateless Address Autoconfiguration.

Σύμφωνα με αυτή την μέθοδο η διαδικασία έχει τέσσερα στάδια:

- Ο κόμβος δημιουργεί ένα κουπόνι διεπαφής. Συνήθως πρόκειται για την διεύθυνση επιπέδου σύνδεσης δεδομένων του σταθμού αλλά αυτή δεν είναι η μόνη περίπτωση. Για παράδειγμα στα τοπικά δίκτυα Ethernet ή IEEE 802.11 μπορεί να χρησιμοποιηθεί η MAC διεύθυνση, μήκους 48bit και μοναδική για κάθε κάρτα δικτύου.
- Ο κόμβος παρατηρεί τα πακέτα που στέλνουν οι γύρω δρομολογητές για να βρει την διεύθυνση δικτύου για το δίκτυο στο οποίο βρίσκεται.
- Ο κόμβος δημιουργεί μία Care – of διεύθυνση δημιουργώντας μια ακολουθία bit που αρχίζει με την διεύθυνση δικτύου και καταλήγει με τα bits του κουπονιού.
- Ο κόμβος, τέλος, ελέγχει αν αυτή η διεύθυνση χρησιμοποιείται ήδη από κάποιον άλλο κόμβο. Για αυτή την περίπτωση, υπάρχουν μηχανισμοί που βοηθούν τον κόμβο να αποκτήσει μοναδική διεύθυνση.

5.2.3 Η λειτουργία του Mobile IPv6.

Το Mobile IPv6 λειτουργεί με τον τρόπο που περιγράφουμε παρακάτω.

- Ένας κόμβος ελέγχει αν βρίσκεται σε κάποιο ξένο δίκτυο παρακολουθώντας τα πακέτα που αποστέλλουν οι γύρω δρομολογητές.
- Αν συμβαίνει κάτι τέτοιο, αποκτά μία Collocated Care – of διεύθυνση μέσω DHCP, Stateless Address Autoconfiguration κλπ.
- Ενημερώνει τον Home Agent του για την διεύθυνση αυτή.
- Ενημερώνει για την διεύθυνση αυτή και επιλεγμένους ανταποκριτές (Correspondents).

- Τα πακέτα που αποστέλλονται προς τον κόμβο από κάποιον ανταποκριτή που έχει ενημερωθεί, σύμφωνα με το προηγούμενο στάδιο, παραδίδονται με δρομολόγηση πηγής. Για τον σκοπό αυτό χρησιμοποιείται μια IPv6 επικεφαλίδα δρομολόγησης (IPv6 Routing Header), που αποτελεί έναν από τους τύπους επικεφαλίδας επέκτασης.
- Τα πακέτα που αποστέλλονται από κάποιον μη ενημερωμένο ανταποκριτή, παραδίδονται όπως στο Mobile IPv4, δηλαδή φτάνουν μέχρι τον Home Agent, ο οποίος τα τοποθετεί σε ένα Tunnel με προορισμό τον κόμβο.
- Στην περίπτωση που ο κόμβος αποστέλλει πακέτα, συνήθως αυτά δρομολογούνται με τους γνωστούς μηχανισμούς. Πολλές φορές, ωστόσο, συντρέχουν λόγοι που τα εξερχόμενα πακέτα δεν μπορούν να φτάσουν στον προορισμό τους με τους συνηθισμένους μηχανισμούς. Αυτοί επιβάλλουν στον κόμβο να τα τοποθετήσει σε Tunnel προς τον Home Agent του.

5.3 INTER ACCESS POINT PROTOCOL – IAPP.

Όπως είδαμε σε προηγούμενο κεφάλαιο, το πρότυπο IEEE 802.11, δεν καθόριζε κάποιον τρόπο για μεταφορά σταθμών από ένα ESS σε ένα άλλο. Έτσι, η λειτουργία γνωστή ως roaming δεν υποστηριζόταν άμεσα.

Το 1996, οι εταιρείες Lucent Technologies, Aironet Corporation και Digital Ocean αποφάσισαν να καθορίσουν ένα πρωτόκολλο που θα επέτρεπε στους σταθμούς να μετακινούνται ελεύθερα μεταξύ Access Points. Το πρωτόκολλο αυτό έγινε γνωστό ως Inter – Access Point Protocol (IAPP).

Το πρωτόκολλο αυτό λειτουργεί πάνω από UDP και IP και έχει δύο βασικές λειτουργίες. Αυτές είναι η Announce και η Handover.

Η λειτουργία Announce χρησιμεύει σε δύο λειτουργίες: η πρώτη είναι η ενημέρωση των Access Points για ένα νέο Access Point. Η δεύτερη είναι η ενημέρωση των Access Points σχετικά με πληροφορίες για την διάρθρωση του δικτύου.

Η λειτουργία Handover χρησιμοποιείται για να ενημερωθεί ένα Access Point ότι ένας σταθμός του έγινε associate με κάποιο άλλο Access Point. Το παλιό Access Point αρχίζει να προωθεί τα πλαίσια που προορίζονται για τον σταθμό, στο νέο Access Point. Έτσι εγγυάται η σωστή λειτουργία του Bridging.

5.4 Η ΝΕΑ ΓΕΝΙΑ ΤΟΥ IAPP.

Το 1999 δημιουργήθηκε το group IEEE 802.11f. το group αυτό ανέλαβε να αναπτύξει Recommended Practice, για ένα IAPP που θα επιτρέπει την συνεργασία Access

Points διαφορετικών κατασκευαστών που λειτουργούν ως μέλη του ίδιου Συστήματος Διανομής.

Τον Μάρτιο 2001 εκδόθηκε από το παραπάνω Task Group, το πρώτο Draft για το IAPP. Το δεύτερο Draft εκδόθηκε τον Ιούλιο του ιδίου έτους.

5.4.1 Η Λειτουργία του IAPP.

Σύμφωνα, λοιπόν, με το δεύτερο Draft, τα Access Points λειτουργούν σαν IEEE 802.1D γέφυρες. Εκτελούν τις ακόλουθες λειτουργίες. Οι δύο πρώτες από αυτές είναι λειτουργίες μιας κλασική γέφυρας, οι υπόλοιπες είναι λειτουργίες που προσθέτει το IAPP.

- Προσφέρουν υπηρεσίες Συστήματος Διανομής, σύμφωνα με το IEEE 802.11.
- Address Mapping.
- Υποστηρίζουν την δημιουργία και συντήρηση ενός Συστήματος Διανομής.
- Επιβάλλουν τον περιορισμό που τίθεται από το IEEE 802.11, ότι ένας σταθμός θα έχει Association μόνο με ένα Access Point σε κάθε χρονική στιγμή.
- Υποστηρίζουν την Αυθεντικοποίηση και το Privacy του IEEE 802.11.
- Υποστηρίζουν ρύθμιση από απόσταση (Remote Configuration).
- Λειτουργούν σε λογικό επίπεδο ασφάλειας.

Βασικός στόχος του IAPP είναι να επιτρέψει τον μετακίνηση των σταθμών από ένα BSS σε ένα άλλο, διαφανώς προς τα ανώτερα επίπεδα και χωρίς να διαταραχθούν οι ήδη τρέχουσες συνδέσεις. Να σημειωθεί ότι το IAPP υλοποιείται μόνο στα Access Points. Το IAPP συνεχίζει να λειτουργεί πάνω από πρωτόκολλο UDP.

5.4.2 Δημιουργία και Συντήρηση ενός ESS.

Η δημιουργία και η συντήρηση ενός ESS, γίνεται με την βοήθεια μιας υπηρεσίας καταχωρήσεων (Registration Service). Η υπηρεσία αυτή διατηρεί έναν πίνακα με τις IP διευθύνσεις των Access Points και τα αντίστοιχα BSSID.

Ένα Access Point μπορεί να στείλει μία **IAPP-INITIATE.αίτηση**, μαζί με την IP διεύθυνσή του, το BSSID (MAC διεύθυνση) και το UDP Port του IAPP και να καταχωρηθεί σε αυτόν τον πίνακα. Με αυτό τον τρόπο το Access Point γίνεται μέρος του ESS.

Αντίστροφα, όταν ένας σταθμός επιθυμεί να διαγραφεί από τον πίνακα, στέλνει μία **IAPP-TERMINATE.αίτηση** και ταυτόχρονα παύει να είναι μέλος του ESS. Όταν από ένα ESS διαγραφεί και το τελευταίο μέλος, τότε παύει να υπάρχει και το ίδιο το ESS.

Να σημειωθεί ότι, μια υπηρεσία καταχωρήσεων μπορεί να διαχειρίζεται πολλά ESS. Κάθε ESS, όμως, αντιστοιχεί σε ακριβώς μία τέτοια υπηρεσία.

Σχετικά με τις ενημερώσεις των εγγραφών, δεν υπάρχει κάποια υπηρεσία που να κάνει Update. Όταν ένα Access Point επιθυμεί να αλλάξει κάποια στοιχεία του στον πίνακα με τις καταχωρήσεις, πρέπει να διαγραφεί και μετά να επανεγγραφεί με τα νέα δεδομένα.

Για να εγγυηθεί ότι όλα τα καταχωρημένα Access Points είναι ενεργά, πρέπει να ανανεώνουν την εγγραφή τους κάθε πέντε λεπτά. Αν δεν υπάρξει ανανέωση καταχώρησης από κάποιο Access Point για δεκαπέντε λεπτά, το Access Point αυτό θεωρείται ανενεργό και διαγράφεται από την υπηρεσία.

5.4.3 Μετακινήσεις Σταθμών.

Όταν ένας σταθμός γίνει για πρώτη φορά Associate με ένα Access Point, τότε το Access Point καλεί την υπηρεσία **IAPP-ADD.αίτηση**. Όλοι οι Bridging πίνακες των Access Points ενημερώνονται με την τοποθεσία του σταθμού και προωθούν τα πακέτα του καταλλήλως.

Αν ένας σταθμός γίνει Re – associate, η υπηρεσία που επιτυγχάνει το ίδιο αποτέλεσμα είναι η **IAPP-MOVE**.

Όταν ένα Access Point λάβει μια **IAPP-ADD.αίτηση** ή μία **IAPP-MOVE.αίτηση** ελέγχει αν ο εν λόγω σταθμός του ανήκε και αν η απάντηση είναι καταφατική, τότε το Access Point καλεί την υπηρεσία **IAPP-REMOVE**

Πάνω στα παραπάνω υπάρχουν διάφοροι προβληματισμοί. Πώς μπορεί να εγγυηθεί ότι θα ενημερωθούν όλα τα Access Points αν αυτά βρίσκονται σε διάσπαρτα Subnets είναι ένα από τα ερωτήματα που προκύπτουν.

5.5 ΣΧΟΛΙΑ ΓΙΑ ΤΟ IAPP.

Το IAPP είναι ένα φιλόδοξο πρωτόκολλο που επιχειρεί να λύσει ένα πολύ βασικό πρόβλημα της τεχνολογίας IEEE 802.11.

Το γεγονός ότι βρίσκεται ακόμα σε επίπεδο DRAFT, σημαίνει ότι τα πράγματα δεν είναι ακόμη ξεκάθαρα και ότι η προτυποποίησή του δεν πρέπει να αναμένεται άμεσα. Στον ίδιο λόγο οφείλονται και τα κενά που υπάρχουν ακόμα και στην ασάφεια όλων των λεπτομερειών της λειτουργίας του.

Ένα τελευταίο θέμα που πρέπει να επισημάνουμε είναι ότι το IAPP, αντίθετα με το MobileIP, δεν είναι πρωτόκολλο δρομολόγησης. Το IAPP επεμβαίνει σε επίπεδο MAC και στις λειτουργίες γεφύρωσης. Έτσι, όλα τα παραπάνω προϋποθέτουν ότι οι σταθμοί έχουν τρόπο να λαμβάνουν τα πακέτα τους από την σκοπιά της δρομολόγησης σε επίπεδο δικτύου. Με άλλα λόγια προϋποτίθεται ότι οι σταθμοί έχουν έγκυρη IP διεύθυνση για το IP subnet στο οποίο βρίσκονται σε κάθε δεδομένη χρονική στιγμή. Δεν εξετάζεται, δε,

ούτε στον μικρότερο βαθμό το πώς θα αποκτήσει ένας σταθμός αυτή την διεύθυνση (DHCP, χειροκίνητα κλπ).

Για να κατανοήσουμε το παραπάνω ας δούμε το εξής παράδειγμα. Έστω ένας οργανισμός που εδρεύει σε ένα κτίριο δύο ορόφων. Έστω επίσης ότι και οι δύο όροφοι ανήκουν στο ίδιο IP υποδίκτυο και σε κάθε όροφο υπάρχει ένα Access Point και ένα BSS αντίστοιχα. Οι δύο όροφοι επικοινωνούν μέσω ενός Ethernet. Αν ένας σταθμός χρειαστεί να μετακινηθεί από τον ένα όροφο στον άλλο, θα πρέπει να γίνει Associate με το νέο Access Point. Ωστόσο δεν χρειάζεται να αλλάξει η IP διεύθυνση του. Αυτή η μετακίνηση μπορεί να υποστηριχθεί από το IAPP.

Αν, όμως, τα δύο BSS ανήκουν σε δύο διαφορετικά υποδίκτυα που επικοινωνούν μέσω δύο δρομολογητών (ένας σε κάθε όροφο), πιθανή μετακίνηση απαιτεί και αλλαγή στην IP διεύθυνση του σταθμού. Αυτή την περίπτωση δεν την καλύπτει το IAPP, από μόνο του. Χρειάζεται η ανάθεση νέας IP διεύθυνσης, είτε μέσω DHCP είτε μέσω MobileIP. Να σημειωθεί, ωστόσο ότι και σε αυτή την περίπτωση είναι απαραίτητη η χρήση του IAPP. Αν δεν υπήρχε αυτό, τότε τα πακέτα θα δρομολογούνταν σωστά στο νέο υποδίκτυο αλλά δεν θα έφταναν ποτέ στον σταθμό γιατί το Access Point δεν θα γνώριζε την ύπαρξή του.



6 ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ – ΤΟ ΠΡΩΤΟΚΟΛΛΟ SNMP.

Η ραγδαία εξέλιξη σε μέγεθος, αλλά ταυτόχρονα σε πολυπλοκότητα, των δικτύων υπολογιστών κατά τις τελευταίες δεκαετίες είχε σαν αποτέλεσμα οι δικτυακοί πόροι να γίνουν υψηλής σημασίας και συνάμα να αυξάνεται η πιθανότητα εμφάνισης σφαλμάτων.

Είναι πρακτικά αδύνατον ένα άνθρωπος να διαχειριστεί ένα ολόκληρο δίκτυο από μόνος του. Είναι επιβεβλημένη η χρήση αυτοματοποιημένων εργαλείων, η ανάπτυξη και χρήση των οποίων δυσχεραίνεται από το γεγονός ότι ο δικτυακός εξοπλισμός προέρχεται από μια μεγάλη ποικιλία κατασκευαστών.

6.1 ΛΕΙΤΟΥΡΓΙΚΕΣ ΠΕΡΙΟΧΕΣ ΔΙΑΧΕΙΡΙΣΗΣ.

Ο διεθνής οργανισμός προτυποποίησης, ISO, παρουσίασε μία κατηγοριοποίηση των στοιχείων ενός δικτύου που χρίζουν διαχείρισης. Συγκεκριμένα, χώρισε τα στοιχεία αυτά σε πέντε λειτουργικές περιοχές (Functional Areas).

Η κατηγοριοποίηση αυτή έγινε με βάση το μοντέλο OSI. Παρά το γεγονός αυτό, η ομαδοποίηση αυτή έγινε ευρέως αποδεκτή από τους κατασκευαστές συστημάτων διαχείρισης.

Πολύ συνοπτικά οι περιοχές αυτές είναι:

- Διαχείριση Σφαλμάτων (Fault Management).
- Λογιστική Διαχείριση (Accounting Management).
- Διαχείριση Διάρθρωσης και Ονομάτων (Configuration and Name Management).
- Διαχείριση Επιδόσεων (Performance Management).
- Διαχείριση Ασφάλειας (Security Management).

6.1.1 Διαχείριση Σφαλμάτων.

Εξαιτίας της αυξημένης πολυπλοκότητας των σημερινών δικτύων, είναι πιθανότατο να προκύψουν σφάλματα λειτουργίας. Είναι σκόπιμο να γνωρίζουμε άμεσα ότι έχει παρουσιαστεί ένα σφάλμα και το σημείο στο οποίο έχει παρουσιαστεί, ώστε να το επιλύσουμε και λάβουμε τα απαραίτητα μέτρα για την, στη συνέχεια, πρόληψή του.

6.1.2 Λογιστική Διαχείριση.

Σε πολλά εταιρικά δίκτυα, προβλέπονται διαδικασίες που χρεώνουν τους χρήστες για την δέσμευση και χρήση πόρων. Η χρήση αυτή μπορεί να μην αναφέρεται αναγκαστικά σε κάποιου είδους πληρωμή, αλλά να αποτελεί έναν τρόπο για τους διαχειριστές του δικτύου να αποκτήσουν πληροφόρηση σχετικά με τον τρόπο χρήσης των πόρων. Έτσι μπορούμε να γνωρίζουμε ποιοι χρήστες καταχρώνται πόρους σε βάρος άλλων

χρηστών, ποιοι χρήστες κάνουν αποδοτική ή μη αποδοτική χρήση του δικτύου. Αυτά μπορούν να βοηθήσουν στον καλύτερο σχεδιασμό και συντήρηση της εγκατάστασης.

6.1.3 Διαχείριση Διάρθρωσης και Ονομάτων.

Βασικός σκοπός της διαχείρισης αυτής της ομάδας είναι η εκκίνηση ή ο τερματισμός τμημάτων ενός δικτύου, η συντήρησή τους και η προσθήκη συσχετισμών μεταξύ τους. Επίσης δίνεται η δυνατότητα μετατροπής των ιδιοτήτων ενός συστατικού του δικτύου.

6.1.4 Διαχείριση Επιδόσεων.

Με την διαχείριση επιδόσεων μπορούμε να καθορίσουμε μετρικές συγκεκριμένων παραμέτρων, σε συγκεκριμένα σημεία του δικτύου. Αυτές, μετά από επεξεργασία μπορούν να μας δώσουν ενδείξεις για πιθανά προβλήματα επιδόσεων.

Η διαχείριση επιδόσεων έχει έντονη συσχέτιση με την παρούσα εργασία και για τον λόγο αυτό θα γίνει εκτενέστερη αναφορά σε παρακάτω παράγραφο.

6.1.5 Διαχείριση Ασφάλειας.

Στην πέμπτη και τελευταία λειτουργική περιοχή, μας δίνεται η δυνατότητα ελέγχου παραμέτρων ασφάλειας. Η δημιουργία και το μοίρασμα κρυπτογραφικών κλειδιών και η μετατροπή του ελέγχου πρόσβασης σε πόρους αποτελούν ενδεικτικά μέρη αυτής της λειτουργικής περιοχής. Μας δίνεται επίσης η δυνατότητα να ανακαλύψουμε πιθανές απόπειρες εισβολής.

6.2 ΔΙΑΧΕΙΡΙΣΗ ΕΠΙΔΟΣΕΩΝ.

Η διαχείριση επιδόσεων μπορεί να διαιρεθεί σε δύο επιπλέον κατηγορίες.

Η πρώτη κατηγορία είναι η παρακολούθηση, όπου μιλάμε για την πρόσβαση σε πληροφορίες σχετικά με την κίνηση του δικτύου, το επίπεδο χρησιμοποίησης, τους χρόνους καθυστέρησης ή την ενδεχόμενη ύπαρξη στενωπών.

Η δεύτερη είναι ο έλεγχος, όπου μας δίνεται η δυνατότητα να κάνουμε μετατροπές σε στοιχεία του δικτύου με σκοπό την βελτίωση των επιδόσεών του.

6.2.1 Δείκτες Επιδόσεων.

Βασικότατο πρόβλημα για την ομάδα διαχείρισης αποτελεί η επιλογή των σημείων και των παραμέτρων που θα ακολουθούνται. Αυτό γιατί ο αριθμός των επιλογών που έχουμε στη διάθεσή μας είναι πολύ μεγάλος και πολλές από τις επιλογές αυτές δεν είναι πλήρως κατανοητές.

Στη συνέχεια θα παρουσιάσουμε ορισμένες παραμέτρους που θα μπορούσαμε να επιλέξουμε προς παρακολούθηση. Οι παράμετροι αυτοί μπορούν να κατηγοριοποιηθούν

σε δύο ομάδες. Η πρώτη σχετίζεται με τις υπηρεσίες (Service – Oriented) και η δεύτερη με την αποτελεσματικότητα (Efficiency – Oriented).

6.2.1.1 Διαθεσιμότητα (Availability).

Η διαθεσιμότητα μπορεί να εκφραστεί ως το ποσοστό του χρόνου που μια υπηρεσία είναι διαθέσιμη στον χρήστη προς το συνολικό χρόνο. Γενικώς, και ανάλογα με την υπηρεσία, η διαθεσιμότητα μπορεί να είναι πολύ σημαντική, οικονομικά ή όχι.

Η διαθεσιμότητα βασίζεται στην αξιοπιστία μιας συνιστώσας. Λέγοντας αξιοπιστία εννοούμε την πιθανότητα η συνιστώσα να λειτουργεί για χρονικό διάστημα τ ή περισσότερο από την στιγμή που θα τεθεί σε λειτουργία.

Αν ορίσουμε τον μέσο χρόνο μεταξύ σφαλμάτων (Mean Time Between Failures – *MTBF*) και τον μέσο χρόνο επισκευής (Mean Time To Repair – *MTTR*) τότε η διαθεσιμότητα ορίζεται ως:

$$A = \frac{MTBF}{MTBF + MTTR}$$

Τύπος 3 - Διαθεσιμότητα..

Η συνολική αξιοπιστία ενός συστήματος εξαρτάται από δύο παράγοντες:

- Την αξιοπιστία των επιμέρους συνιστωσών.
- Την τοπολογία διασύνδεσής τους (συνδυασμοί από συνδέσεις Σε Σειρά και Παράλληλες).

Έτσι για μεγάλο αριθμό συνιστωσών με περίπλοκες τοπολογίες, ο υπολογισμός της συνολικής αξιοπιστίας του συστήματος μπορεί να γίνει πολύ δύσκολός.

6.2.1.2 Χρόνος Απόκρισης (Response Time).

Ο χρόνος απόκρισης είναι ο χρόνος ο οποίος μεσολαβεί από μια εντολή του χρήστη μέχρι την εμφάνιση του αποτελέσματος το σύστημα. Είναι γενικά επιθυμητό ο χρόνος απόκρισης να είναι μικρός. Όμως ο χρόνος απόκρισης είναι αντιστρόφως συσχετισμένος με το κόστος του συστήματος.

Γενικά ο χρόνος απόκρισης είναι πολύ σημαντικός και σχετικά εύκολο να μετρηθεί.

6.2.1.3 Ρυθμοαπόδοση (Throughput).

Η ρυθμοαπόδοση είναι ο λόγος του πλήθους μίας ποσότητας προς τον χρόνο. Για παράδειγμα ρυθμοαπόδοση είναι το μέγεθος του δεδομένων που πέρασαν από ένα δίκτυο στην μονάδα του χρόνου.

6.2.1.4 Εκμετάλλευση – Utilization.

Εκφράζει το ποσοστό του χρόνου που ένας πόρος χρησιμοποιείται.

Βοηθάει στην ανεύρεση σημείων συνωστισμού (Bottlenecks) και στο να γίνουν ρυθμίσεις που θα βελτιώσουν την συνολική απόδοση του δικτύου.

6.2.2 Λειτουργία Παρακολούθησης Επιδόσεων.

Ουσιαστικά πρόκειται για μεθόδους συλλογής και ανάλυσης δεδομένων σχετικών με τις επιδόσεις.

Η συλλογή μπορεί γίνεται από μονάδες που καλούνται agents και βρίσκονται εγκατεστημένοι στους κόμβους ενός δικτύου (Υπολογιστές, Δρομολογητές, Access Points). Οι agents συλλέγουν πληροφορίες σχετικές με την κίνηση (αριθμό συνδέσεως, εισερχόμενα και εξερχόμενα πακέτα κλπ) και της αναφέρουν σε σταθμούς διαχείρισης.

Στα τοπικά δίκτυα είναι δυνατόν να αναθέσουμε σε έναν σταθμό την παρακολούθηση της κίνησης σε όλο το δίκτυο. Αυτό επιτυγχάνεται μέσω του RMON και RMON 2 που θα δούμε στην συνέχεια του κεφαλαίου.

Έτσι μπορούμε να πάρουμε πληροφορίες σχετικά με την κατανομή του μεγέθους των πακέτων, τις καθυστερήσεις στο δίκτυο, την ρυθμοαπόδοση των καναλιών και πολλά άλλα.

Επίσης, στην περίπτωση της παρακολούθησης του δικτύου στο σύνολό του, μπορούμε, αντί να καταχωρούμε όλα τα δεδομένα, να κάνουμε δειγματοληπτική καταχώριση.

Αυτό μπορεί να είναι πολύ εξυπηρετικό όταν το δίκτυο είναι πολύ φορτωμένο και ο σταθμός που παρακολουθεί δεν μπορεί να αντεπεξέλθει στην παρακολούθηση όλων των πακέτων. Μπορεί επίσης να γίνει όταν επιθυμούμε να εξοικονομήσουμε πόρους.

6.3 ΤΟ ΠΡΩΤΟΚΟΛΛΟ SNMP.

Όπως αναφέραμε και στην εισαγωγή του κεφαλαίου, στον χώρο των δικτύων υπολογιστών παρατηρείται μεγάλος αριθμός κατασκευαστών δικτυακού εξοπλισμού. Ο τρόπος με τον οποίο αντιμετωπίζεται πολύ συχνά η ποικιλία αυτή, είναι η ανάπτυξη προτύπων. Η περίπτωση της διαχείρισης δικτύων δεν αποτελεί εξαίρεση. Έτσι, για τους παραπάνω λόγους αναπτύχθηκε, από την IETF, το SNMP – Simple Network Management Protocol, ένα απλό πρωτόκολλο διαχείρισης δικτύων, όπως δηλώνει και το όνομά του.

Το SNMP είναι, στην ουσία, ένα σύνολο προτύπων που καθορίζουν τα εξής:

- Ένα πρωτόκολλο επικοινωνίας,
- Την προδιαγραφή ενός σχήματος βάσης δεδομένων,
- Ένα σύνολο από αντικείμενα δεδομένων.

Το SNMP υιοθετήθηκε ως το πρωτόκολλο διαχείρισης των TCP/IP δικτύων το 1987, ενώ μέχρι σήμερα έχει εξελιχθεί μέχρι την έκδοση 3, η οποία έχει πολύ σημαντικές διαφορές με την αρχική.

6.3.1 Η ιστορία και η εξέλιξη του SNMP.

Το 1970 δεν υπήρχαν εργαλεία διαχείρισης με την σημερινή λειτουργικότητα. Το μόνο διαθέσιμο ήταν το πρωτόκολλο ICMP – Internet Control Message Protocol και τα αντίστοιχα μηνύματα Echo Request / Echo Reply με τα οποία ήταν δυνατόν να διαπιστωθεί η ύπαρξη επικοινωνίας μεταξύ δύο υπολογιστών και να μετρηθεί ο χρόνος για ένα Round Trip. Πρόκειται για το πολύ γνωστό σε όλους Ping.

Στο τέλος της δεκαετίας του 1980, όταν η αύξηση μεγέθους του διαδικτύου έγινε εκθετική, αυξήθηκε το πλήθος και η περιπλοκότητα των υποδικτύων που έπρεπε να διαχειρισθούμε. Το πρωτόκολλο ICMP δεν ήταν πια επαρκές. Ήταν σαφής η ανάγκη ανάπτυξης ισχυρότερων μεθόδων διαχείρισης. Χρειαζόταν ένα πρωτόκολλο, με πολύ περισσότερες δυνατότητες από το Ping, προσανατολισμένο στην διαχείριση δικτύων. Τότε άρχισαν οι προσπάθειες προτυποποίησης.

Το 1987 έγινε η πρώτη απόπειρα, με το SGMP – Simple Gateway Monitoring Protocol.

Από τις επόμενες προτάσεις, τρεις ήταν αυτές που ξεχώρισαν:

HEMS – High Level Entity Management System.

CMOT – CMIP over TCP/IP: Μια απόπειρα συνδυασμού του πρωτοκόλλου Common Management Information Protocol, που είχε αναπτύξει ο ISO, και των αντίστοιχων υπηρεσιών.

SNMP: Αποτελούσε μια επέκταση του SGMP.

Το 1988 η IAB – Internet Architecture Board, έκρινε πως το SNMP θα έπρεπε να χρησιμοποιηθεί ως προσωρινή λύση μέχρι την πλήρη μετάβαση σε δίκτυα OSI, όταν και θα γινόταν μετάβαση στην χρήση του CMOT. Επιπλέον τα δύο πρωτόκολλα θα έπρεπε να χρησιμοποιούν την ίδια βάση πληροφοριών, για λόγους αμεσότερης μετάβασης.

Ωστόσο, πολύ σύντομα έγινε ξεκάθαρο ότι ο συνδυασμός αυτού του τύπου ήταν πολύ δύσκολο να υλοποιηθεί. Τα αντικείμενα που διαχειριζόταν το CMIP ήταν πολύ εξειδικευμένα με μεθόδους και ιδιότητες. Αντίθετα το SNMP, λόγω απλότητας, δεν ακολουθούσε τον αντικειμενοστρεφή τρόπο σκέψης. Έτσι, τα δύο πρωτόκολλα ακολούθησαν ξεχωριστή πορεία.

Η χαλάρωση των περιορισμών είχε ως αποτέλεσμα την ραγδαία ανάπτυξη του SNMP και την γρήγορη υιοθέτησή του από τους κατασκευαστές και τους χρήστες. Η αρχική έκδοση του SNMP χρησιμοποιείται πλέον από όλους τους κατασκευαστές. Έχουν ήδη κυκλοφορήσει νέες εκδόσεις ενώ γίνονται προσπάθειες ανάπτυξης εκδόσεων που θα δουλεύουν πάνω από άλλα περιβάλλοντα συμπεριλαμβανομένου και του OSI. Μία αξιοσημείωτη τέτοια προσπάθεια είναι το RMON και RMON 2 που ουσιαστικά

αποτελούν επεκτάσεις της MIB του SNMP ώστε να μπορούμε να διαχειριστούμε ένα τοπικό δίκτυο στο σύνολό του, επιπλέον από κάθε κόμβο ξεχωριστά.

Για να αντιμετωπισθούν ορισμένες ελλείψεις του SNMP, έχουν κυκλοφορήσει οι νεώτερες εκδόσεις SNMPv2 και SNMPv3.

6.3.2 Οι λογικές οντότητες του SNMP.

Το μοντέλο διαχείρισης που προτείνει το SNMP συμπεριλαμβάνει τις ακόλουθες οντότητες:

- Σταθμός Διαχείρισης (Management Station).
- Αντιπρόσωπος Διαχείρισης (Management Agent).
- Βάση Πληροφοριών Διαχείρισης (Management Information Base – MIB).
- Πρωτόκολλο Διαχείρισης Δικτύου.

Ο σταθμός διαχείρισης είναι συνήθως ένας υπολογιστής που παρέχει την διεπαφή ανθρώπου – συστήματος διαχείρισης. Η αρχιτεκτονική του SNMP μπορεί να θεωρηθεί Client – Server και στην περίπτωση αυτή ο σταθμός διαχείρισης είναι ο Client.

Ο Server, αντίστοιχα, είναι ο αντιπρόσωπος. Ένας αντιπρόσωπος βρίσκεται ενσωματωμένος στον κόμβο υπό διαχείριση. Αναλαμβάνει να παρέχει πληροφορίες στον σταθμό διαχείρισης, όποτε αυτό του ζητηθεί. Επίσης υπάρχει η δυνατότητα να αποστείλει πληροφορίες ασύγχρονα. Δηλαδή, για παράδειγμα, αν ένα interface ενός δρομολογητή σταματήσει να λειτουργεί, ο αντιπρόσωπος θα ενημερώσει τον σταθμό διαχείρισης, χωρίς να περιμένει να του ζητηθεί η πληροφορία. Τέλος, αναλαμβάνει να αλλάζει τις παραμέτρους λειτουργίας του κόμβου, σύμφωνα με τις εντολές του σταθμού διαχείρισης.

Οι παράμετροι που μπορούν να ελεγχθούν ή να αλλαχθούν αποτελούν αντικείμενα. Η συλλογή αυτών των αντικειμένων αποτελεί την βάση πληροφοριών διαχείρισης (MIB). Αυτή η συλλογή αντικειμένων είναι προτυποποιημένη. Έτσι ο κάθε δρομολογητής για την κάθε διεπαφή του θα χρησιμοποιεί τα ίδια αντικείμενα. Ο σταθμός διαχείρισης, γνωρίζοντας το σύνολο των αντικειμένων της MIB μπορεί να ζητήσει από τον αντιπρόσωπο λειτουργίες πάνω σε αυτά.

Το πρωτόκολλο επικοινωνίας, επιπέδου εφαρμογής, που χρησιμοποιείται για τις συναλλαγές αντιπροσώπου – σταθμού διαχείρισης είναι το SNMP.

6.3.3 Τα μηνύματα στο SNMP.

Τα μηνύματα που ανταλλάσσονται είναι τα εξής πέντε.

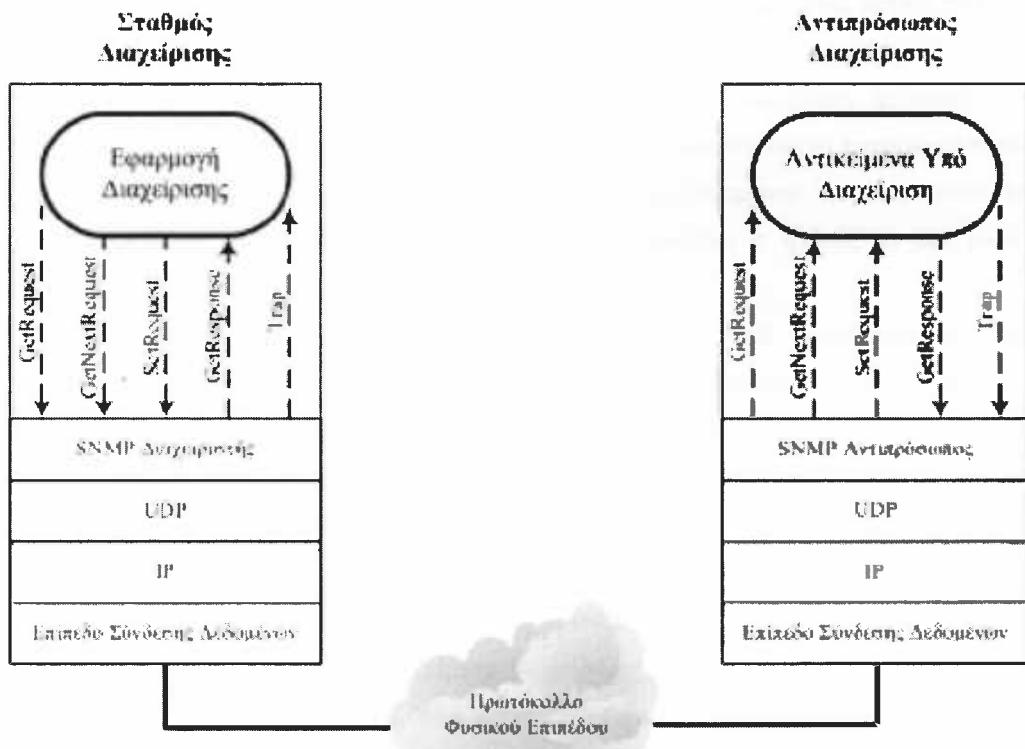
- **GetRequest:** Αυτό το μήνυμα χρησιμοποιεί ο σταθμός διαχείρισης για να ζητήσει μια πληροφορία.

- **GetNextRequest:** Αυτό το μήνυμα είναι το ίδιο με το προηγούμενο με μόνη διαφορά ότι επιστρέφεται η τιμή του επόμενου, σε λεξικογραφική σειρά, αντικειμένου από αυτό που περιέχει η παράμετρος του μηνύματος.
- **SetRequest:** Αυτό το μήνυμα χρησιμοποιεί ο σταθμός διαχείρισης για να ζητήσει την αλλαγή της τιμής ενός αντικειμένου της MIB.
- **GetResponse:** Αυτό το μήνυμα στέλνει ως απάντηση στα τρία προηγούμενα ο Agent.
- **Trap:** Αυτό το μήνυμα χρησιμοποιεί ο αντιπρόσωπος για να ενημερώσει τον σταθμό διαχείρισης για την τιμή ενός αντικειμένου, χωρίς να του έχει ζητηθεί.

6.3.4 Η αρχιτεκτονική του SNMP.

Το SNMP λειτουργεί πάνω από UDP και η υπηρεσία SNMP χρησιμοποιεί το port 51. Από τα παραπάνω προκύπτει άμεσα ότι, τόσο ο σταθμός διαχείρισης όσο και ο αντιπρόσωπος, πρέπει να υλοποιούν τα πρωτόκολλα SNMP, UDP, IP.

Στο σχήμα φαίνεται η αρχιτεκτονική του πρωτοκόλλου.



Σχήμα 38 - Η Αρχιτεκτονική του SNMP.

6.3.5 Η MIB στο SNMP.

Όπως αναφέραμε και προηγουμένως, όλες οι πληροφορίες για τα αντικείμενα που διαχειρίζομαστε, βρίσκονται αποθηκευμένες σε μια βάση δεδομένων. Στα περιβάλλοντα TCP/IP και OSI αυτή η βάση δεδομένων καλείται Βάση Πληροφοριών Διαχείρισης (Management Information Base – MIB).

Στην περίπτωση του SNMP, η MIB είναι μια βάση δεδομένων μορφής δένδρου. Κάθε κόμβος, είτε είναι υπολογιστής, είτε είναι γέφυρα, δρομολογητής, Access Point κλπ, διατηρεί μια MIB στην οποία αποθηκεύεται η κατάσταση των πόρων υπό διαχείριση. Ο σταθμός διαχείρισης μπορεί, διαβάζοντας ή γράφοντας στην MIB ενός κόμβου, να επιβλέψει ή να μετατρέψει τις παραμέτρους λειτουργίας του.

Μια MIB πρέπει να πληροί τις εξής προϋποθέσεις:

- Τα αντικείμενα πρέπει να είναι τα ίδια σε κάθε σύστημα.
- Η αναπαράσταση των αντικειμένων πρέπει να γίνεται με την χρήση ενός κοινού σχήματος βάσης.

Δηλαδή, με άλλα λόγια, τόσο τα αντικείμενα, όσο και η δομή τους, πρέπει να είναι κοινά σε όλα τα συστήματα.

Η δομή των πληροφοριών διαχείρισης (Structure of Management Information – SMI) καθορίζει ένα πλαίσιο μέσα στο οποίο μπορούν να οριστούν και να κατασκευαστούν οι MIB. Για παράδειγμα, καθορίζονται οι τύποι αντικειμένων που μπορούν να χρησιμοποιηθούν (ακέραιος, IP διεύθυνση κλπ) και ορίζεται ο τρόπος με τον οποίο ονοματίζονται τα αντικείμενα.

Είναι σαφές ότι, όταν αναφερόμαστε στη δομή της MIB, αναφερόμαστε στην περιγραφή μιας γενικής δομής δεδομένων, η οποία είναι ανεξάρτητη από τις τεχνικές κωδικοποίησης που χρησιμοποιούνται για την αναπαράσταση αυτών. Δηλαδή, πρόκειται για μια Abstract Syntax. Για τον καθορισμό των Abstract Syntax, όπως συνήθως, έτσι και στο SNMP, χρησιμοποιούμε την Abstract Syntax Notation One – ASN.1.

Η σημαντικότερη, ίσως, MIB που έχει οριστεί είναι η MIB – II. Περιέχει τον ορισμό πολλών και πολύ βασικών αντικειμένων διαχείρισης. Μια άλλη σημαντική MIB είναι η Ethernet MIB η οποία ορίζει αντικείμενα διαχείρισης των δικτύων τύπου IEEE 802.3. είναι μια Interface Specific MIB. Μια τρίτη Interface Specific MIB είναι η MIB των ασύρματων τοπικών δικτύων που θα επισκεφτούμε αργότερα στο κεφάλαιο αυτό.

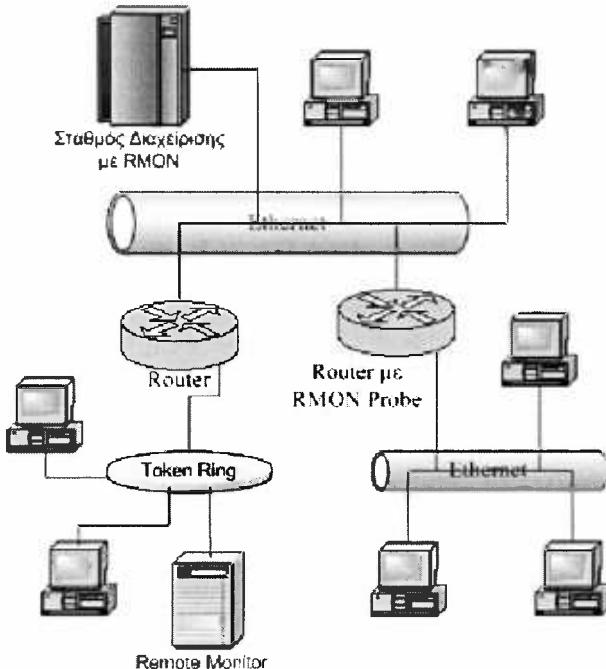
6.4 REMOTE NETWORK MONITORING - RMON.

To RMON δεν είναι τίποτα άλλο από τον καθορισμό μιας MIB. Αυτή έρχεται να συμπληρώσει την MIB – II, προσθέτοντας, ταυτόχρονα, λειτουργικότητα στο SNMP. Το

εντυπωσιακό είναι ότι αυτή η νέα λειτουργικότητα είναι εντυπωσιακά μεγάλη, ενώ δεν επήλθε καμία αλλαγή στο ίδιο το πρωτόκολλο.

Με την MIB – II, ένας διαχειριστής δικτύου μπορούσε πολύ εύκολα να δει τον αριθμό των εισερχόμενων και των εξερχόμενων πακέτων για έναν υπολογιστή. Δεν μπορούσε όμως να έχει εύκολα, εικόνα για το δίκτυο στο σύνολό του.

Για να επιτευχθεί αυτή η λειτουργικότητα υπάρχει μια οντότητα που λέγεται Network Monitor ή Network Probe ή Remote Monitor ή Remote Probe. Αυτή η οντότητα μελετάει όλα τα πακέτα που κυκλοφορούν στο δίκτυο και βγάζει περιληπτικά στοιχεία κίνησης. Μπορούμε, έτσι, να δούμε τον συνολικό αριθμό πακέτων, των συγκρούσεων κλπ. Ένα Remote Monitor μπορεί να είναι μια συσκευή που κάνει μόνο αυτή την δουλειά ή μπορεί να είναι λειτουργία που εκτελεί κάποια άλλη συσκευή.



Σχήμα 39 - RMON.

Κάθε Remote Monitor διαθέτει έναν SNMP Agent. Έτσι, ένας σταθμός διαχείρισης, μέσω των τυπικών μηνυμάτων **GetRequest** και **GetNextRequest**, μπορεί να διαβάσει τα στατιστικά κίνησης του δικτύου που βρίσκονται αποθηκευμένα στην MIB του Remote Monitor. Η ύπαρξη Agent στον Remote Monitor έχει ως αποτέλεσμα, αυτή η οντότητα συχνά να αποκαλείται και Remote Agent.

Επιπλέον ο σταθμός διαχείρισης μπορεί, με την χρήση του μηνύματος **SetRequest**, να κάνεις ρυθμίσεις και να ελέγξει τον Remote Monitor.

6.4.1 Έλεγχος των Remote Monitors.

Ο έλεγχος των Remote Monitors γίνεται, όπως αναφέραμε, με την αποστολή μηνυμάτων SetRequest. Υπάρχουν δύο τρόποι να ελεγχθεί ένας Remote Monitor. Ο πρώτος λέγεται Configuration και ο δεύτερος Action Invocation.

6.4.1.1 Configuration.

Στην περίπτωση του Configuration, ρυθμίζουμε τον σταθμό σχετικά με το ποια στοιχεία πρέπει να συλλέγει.

Όπως είπαμε νωρίτερα, μια MIB είναι χωρισμένη σε ομάδες λειτουργιών. Κάθε τέτοια ομάδα έχει έναν πίνακα δεδομένων, που είναι μόνο για ανάγνωση, και έναν πίνακα ελέγχου, στον οποίο επιτρέπεται και η εγγραφή.

Ο πίνακας ελέγχου περιέχει εγγραφές που περιγράφουν τα δεδομένα που πρέπει να συλλεχθούν, με ποια συχνότητα και άλλες τέτοιες λεπτομέρειες. Έτσι ο σταθμός διαχείρισης, γράφοντας σε αυτόν τον πίνακα ελέγχει τι δεδομένα θα συλλέγει ο Remote Agent.

Τα δεδομένα αυτά που συλλέγονται αποθηκεύονται στον πίνακα δεδομένων. Από εκεί, ο σταθμός διαχείρισης μπορεί να διαβάσει τα στατιστικά στοιχεία που έχουν συλλεχθεί. Τα περιεχόμενα του πίνακα αυτού μεταβάλλονται ανάλογα με τον πίνακα ελέγχου. Έτσι χρησιμοποιείται ο ίδιος πίνακας, ανεξαρτήτως του ποια αντικείμενα παρακολουθούνται.

6.4.1.2 Action Invocation.

Είναι γνωστό ότι το SNMP δεν προβλέπει τρόπους ώστε ένας σταθμός να δώσει εντολή σε έναν Agent, ώστε αυτός να εκτελέσει μια λειτουργία.

Αυτό επιτυγχάνεται έμμεσα με την μέθοδο του Action Invocation.

Η ιδέα είναι ότι, στην MIB υπάρχουν αντικείμενα τα οποία αντιπροσωπεύουν λειτουργίες. Ένας σταθμός διαχείρισης μπορεί, κάνοντας Set, αυτά τα αντικείμενα να προκαλέσει την εκτέλεση μιας λειτουργίας στον Agent. Τα αντικείμενα αυτά συνήθως περιγράφουν καταστάσεις (States) και η αλλαγή της τιμής τους βάζει τον Agent σε διαφορετικό State. Το αποτέλεσμα είναι η εκτέλεση μιας λειτουργίας.

6.5 RMON 2.

Τα αντικείμενα που παρακολουθούνται από έναν RMON Monitor, αναφέρονται στα κατώτερα επίπεδα των τοπικών δικτύων, δηλαδή το MAC και το Φυσικό.

Το 1994, άρχισε η ανάπτυξη μιας επέκτασης του RMON για παρακολούθηση και των ανώτερων επιπέδων. Το αποτέλεσμα αυτής της προσπάθειας ήρθε το 1997 και ονομάστηκε RMON 2.

Τα αποτελέσματα της παρακολούθησης των ανώτερων επιπέδων είναι δύο:

- Το RMON 2 παρακολουθεί το επίπεδο δικτύου. Συνεπώς, δίνεται η δυνατότητα να παρακολουθείται ξεχωριστά η κίνηση που έρχεται στο υποδίκτυο μέσω δρομολογητών, καθώς και η κίνηση που βγαίνει από το υποδίκτυο με τον ίδιο τρόπο.
- Το RMON 2 παρακολουθεί το επίπεδο εφαρμογής. Άρα μπορούμε να έχουμε πληροφόρηση σχετικά με το ποιες εφαρμογές προκαλούν την κίνηση. Μπορούμε να ξεχωρίσουμε τα πακέτα HTTP από τα πακέτα FTP και E – Mail.

6.5.1 Παρακολούθηση Επιπέδου Δικτύου.

Με την αρχική έκδοση του RMON παρακολουθούνται όλα τα πακέτα που κυκλοφορούν στο δίκτυο. Όμως δεν υπάρχει τρόπος να ξεχωρίσουμε αν κάποια από αυτά προέρχονται από υπολογιστή εκτός δικτύου, απευθύνονται σε υπολογιστή εκτός δικτύου ή και τα δύο.

Η δυνατότητα να παρακολουθούμε το επίπεδο δικτύου, κυρίως το πρωτόκολλο IP, μας επιτρέπει, από τις επικεφαλίδες των Datagrams, να συμπεράνουμε ποιος είναι ο αρχικός και τελικός προορισμός τους.

Έτσι μπορούμε να ξεχωρίσουμε τα πακέτα σε τέσσερις κατηγορίες:

- Πακέτα που προέρχονται από εντός του δικτύου και προορίζονται για υπολογιστή εντός του δικτύου. Δηλαδή πακέτα τοπικής κίνησης.
- Πακέτα που προέρχονται από κάποιον κόμβο εκτός δικτύου και εισέρχονται μέσω δρομολογητή. Δηλαδή εισερχόμενη κίνηση.
- Πακέτα που προέρχονται από κάποιον κόμβο εντός δικτύου και εξέρχονται μέσω δρομολογητή. Δηλαδή εξερχόμενη κίνηση.
- Πακέτα διερχόμενης κίνησης. Δηλαδή πακέτα που προέρχονται από υπολογιστή εκτός δικτύου και διέρχονται από το δίκτυο με προορισμό κάποιον άλλον υπολογιστή εκτός δικτύου.

Με αυτά τα δεδομένα μπορούμε να ελέγξουμε ποιοι ακριβώς υπολογιστές προκαλούν κίνηση και να κάνουμε τις απαραίτητες ρυθμίσεις.

6.5.2 Παρακολούθηση Ανώτερων Επιπέδων.

Εκτός από την κίνηση επιπέδου δικτύου, μπορούμε να παρακολουθήσουμε και την κίνηση των επιπέδων μεταφοράς και εφαρμογής. Έτσι μπορούμε να έχουμε γραφήματα που παρουσιάζουν την κίνηση ανά εφαρμογή ή πρωτόκολλο ανωτέρων επιπέδων. Ήα μπορούσαμε, για παράδειγμα, να διαχωρίσουμε την κίνηση TCP από την κίνηση UDP.



6.6 SNMP VERSION 2.

Για να αντιμετωπισθούν οι ατέλειες και οι ελλείψεις του SNMP εκδόθηκε μία νέα έκδοση, το SNMPv2. Το SNMPv2 επεκτείνει κατά πολύ το αρχικό πρωτόκολλο, προσθέτοντας νέες λειτουργίες και συμπεριλαμβάνοντας και δυνατότητα διαχείρισης δικτύων OSI.

Η ανάγκη για το SNMPv2 πρωτοφάνηκε όταν έγινε σαφές πως το SNMP ήταν ανεπαρκές για δίκτυα μεγάλης κλίμακας. Έτσι οι διαχειριστές είχαν να διαλέξουν ανάμεσα σε μία ανεπαρκή λύση και την λύση της διαχείρισης βασισμένης στο μοντέλο OSI, που δεν ήταν ακόμα διαθέσιμη. Ως εκ τούτου έγιναν προσπάθειες έτσι ώστε να διορθωθεί και να επεκταθεί το SNMP, με σκοπό την συνέχιση της χρήσης του.

Ένα από τα βασικότερα μειονεκτήματα του SNMP ήταν η παντελής έλλειψη ασφάλειας. Η ύπαρξη του, μη κρυπτογραφημένου, Community String στην επικεφαλίδα των μηνυμάτων ήταν περιττή, αφού ήταν πολύ εύκολο να παρακολουθήσει κάποιος την κίνηση σε ένα δίκτυο και να το μάθει. Έτσι, το SNMP ήταν ευάλωτο σε επιθέσεις που μπορούσαν να τροποποιήσουν παραμέτρους συσκευών και να θέσουν το δίκτυο εκτός λειτουργίας. Για να αντιμετωπιστεί αυτό το πρόβλημα, το 1992 προτάθηκε η λύση του Secure SNMP ή πιο σύντομα S – SNMP.

Ωστόσο, η ασφάλεια, ή η έλλειψή της, ήταν μόνο ένα από τα μειονεκτήματα του SNMP. Το Secure SNMP δεν αντιμετώπιζε άλλα προβλήματα, κυρίως λειτουργικότητας και επιδόσεων. Τέσσερις ιδιώτες, που είχαν συμμετάσχει στην ανάπτυξη του SNMP, ανέπτυξαν το Simple Management Protocol – SMP. Η πρότασή τους εκδόθηκε το 1992, όχι ως πρότυπο, αλλά σαν μία σύσταση προς την κοινότητα του διαδικτύου. Οι βελτιώσεις είχαν να κάνουν με τις εξής συνιστώσες:

- **Πεδίο Δράσης:** Το SMP δεν θα περιοριζόταν σε διαχείριση δικτύων αλλά θα μπορούσε να χρησιμοποιηθεί και στην διαχείριση εφαρμογών. Επίσης θα επέτρεπε την επικοινωνία μεταξύ δύο σταθμών διαχείρισης.
- **Ταχύτητα και Αποδοτικότητα:** Το SMP θα παρέμενε απλό. Ωστόσο θα επιτρεπόταν η ανταλλαγή μεγάλου όγκου δεδομένων με λίγα μηνύματα.
- **Ασφάλεια:** Το SMP χρησιμοποιεί τις βελτιώσεις που πρότεινε το Secure SNMP.
- **Συμβατότητα:** Το SMP θα λειτουργούσε πάνω από την στοίβα πρωτοκόλλων TCP/IP, αλλά και OSI. Επίσης, ένα υποσύνολο του SMP θα ήταν συμβατό με το SNMPv1.

Το γεγονός ότι και οι δύο προτάσεις εκδόθηκαν το 1992, ήταν ένα πολύ καλό κίνητρο για να αναπτυχθεί ένα μοναδικό πρωτόκολλο, που θα τις συνδύαζε. Έτσι, τον



Οκτώβριο του 1992, άρχισαν και επισήμως οι εργασίες για την ανάπτυξη του SNMPv2. τα αποτελέσματα έγιναν διαθέσιμα τον μήνα Μάρτιο του 1993.

Όμως ο τρόπος που είχε υλοποιηθεί η ασφάλεια στο SNMPv2 είχε προκαλέσει προβληματισμό στους κατασκευαστές. Έτσι, το 1996, αποφασίστηκε μια επανεξέταση του πρωτοκόλλου, για να γίνουν διορθώσεις. Οι εργασίες που ξεκίνησαν είχαν σαν σκοπό να γίνουν ορισμένες διορθώσεις στο τμήμα της ασφάλειας. Υπήρχε η ελπίδα ότι λίγες μόνο αλλαγές θα ήταν αρκετές. Το χρονοδιάγραμμα της ομάδας ήταν αρκετά σφιχτό, ώστε οι κατασκευαστές να μπορέσουν να συνεχίσουν με τα προϊόντα τους. Δυστυχώς, λίγο πριν την ολοκλήρωση των εργασιών, ένας κατασκευαστής εξέφρασε την άποψη ότι το σύστημα ασφάλειας είχε σοβαρότατα ελαττώματα, άποψη που βρήκε σύμφωνο μεγάλο μέρος της ομάδας ανάπτυξης. Για αυτόν τον λόγο δόθηκε μια παράταση, ώστε να μπορέσει να επέλθει συμφωνία στον καθορισμό του συστήματος ασφάλειας. Αυτή η συμφωνία δεν επήλθε ποτέ. Για να μην συνεχιστεί αόριστα η καθυστέρηση και για να μην χαθούν όλες οι υπόλοιπες βελτιώσεις, αποφασίστηκε να αφαιρεθεί εντελώς η ασφάλεια από το SNMPv2. Το αποτέλεσμα ήταν το Community Based SNMPv2 ή SNMPv2C που χρησιμοποιεί τα Community Names με τον ίδιο ακριβώς τρόπο όπως το SNMPv1.

6.6.1 Βελτιώσεις στο SNMPv2.

Στο SNMPv2 παρατηρείται μια πολύ βασική αλλαγή της γενικής λειτουργικότητας και φιλοσοφίας. Συγκεκριμένα, με τις τροποποιήσεις που έχουν γίνει, υποστηρίζεται κατανεμημένη προσέγγιση στην διαχείριση του δικτύου, εκτός από συγκεντρωτική. Αυτό σημαίνει ότι ορισμένοι κόμβοι λειτουργούν τόσο ως σταθμοί διαχείρισης, όσο και ως αντιπρόσωποι. Στο ρόλο του σταθμού διαχείρισης, ο κόμβος διαχειρίζεται το τμήμα του δικτύου που του έχει ανατεθεί. Συλλέγει πληροφορίες για αυτό και κάνει τις απαραίτητες ρυθμίσεις. Στο ρόλο του αντιπροσώπου, ο κόμβος αναφέρει σε κάποιον, ανώτερό του, σταθμό διαχείρισης και δέχεται εντολές από αυτόν.

Οι βελτιώσεις στο SNMPv2 έρχονται σε τρεις λειτουργικές περιοχές:

- Στην δομή των πληροφοριών διαχείρισης.
- Στην δυνατότητα επικοινωνίας σταθμού διαχείρισης με σταθμό διαχείρισης.
- Στις λειτουργίες και τα μηνύματα του πρωτοκόλλου.

Κάθε μία από αυτές τις βελτιώσεις θα εξετάσουμε, συνοπτικά, παρακάτω.

6.6.1.1 Δομή Πληροφοριών Διαχείρισης – SMI.

Η δομή των πληροφοριών διαχείρισης (Structure of Management Information – SMI), όπως έχει ήδη αναφερθεί, ορίζει το πλαίσιο μέσα στο οποίο μπορούμε να ορίσουμε μια MIB. Η SNMPv2 SMI επεκτείνεται με διάφορους τρόπους. ένας βασικός είναι ότι

υποστηρίζονται νέοι τύποι δεδομένων, όπως Unsigned32. Πρόκειται για έναν θετικό ακέραιο μήκους 32bit, δηλαδή που παίρνει τιμές από 0 μέχρι $2^{32} - 1$.

Επιπλέον, σύμφωνα με την αρχή που έκανε το RMON, υποστηρίζονται τρόποι να προστίθενται και να διαγράφονται εγγραφές από τους πίνακες της MIB. Οι μέθοδοι αυτές είναι πιο εξελιγμένες από αυτές που χρησιμοποιούσε το RMON.

6.6.1.2 Λειτουργία του Πρωτοκόλλου.

Αναφέρθηκε και πιο πριν ότι το πρωτόκολλο SNMPv2 προσφέρει την δυνατότητα και για άλλες μορφές επικοινωνίας. Αναλυτικά, οι τρόποι πρόσβασης στην πληροφορία διαχείρισης είναι:

- **Manager – Agent Request – Response:** Η κλασσική επικοινωνία όπως στο SNMPv1. Ο σταθμός διαχείρισης ζητάει πληροφορίες από τον αντιπρόσωπο και αυτός απαντάει με ένα άλλο μήνυμα. Επίσης μπορεί ο σταθμός διαχείρισης να μετατρέψει κάποια παράμετρο λειτουργίας. Και σε αυτή την περίπτωση ο αντιπρόσωπος επιβεβαιώνει.
- **Manager – Manager Request – Response:** Η περίπτωση που αποτελεί καινοτομία στο SNMPv2. Ένας σταθμός διαχείρισης στέλνει μια αίτηση σε έναν άλλο σταθμό διαχείρισης ο οποίος απαντάει ανάλογα.
- **Agent – Manager Unconfirmed:** Ένας αντιπρόσωπος στέλνει ένα μήνυμα Trap σε έναν σταθμό διαχείρισης. Χρησιμεύει για να ενημερωθεί ο σταθμός διαχείρισης για κάποιο αναπάντεχο συμβάν, όπως την πτώση μιας διεπαφής ενός δρομολογητή.

Από τις παραπάνω περιπτώσεις, η πρώτη και η τρίτη συναντώνται και στην αρχική έκδοση του SNMP.

Επιπλέον, στο SNMPv2, ορίζονται και δύο νέοι τύποι μηνυμάτων:

- **GetBulkRequest:** Χρησιμοποιείται στην περίπτωση που πρέπει να μεταφερθεί μεγάλος όγκος δεδομένων. Ο λόγος της δημιουργίας του είναι, η μεταφορά αυτή, να γίνεται με όσο το δυνατόν μικρότερη επιβάρυνση στο δίκτυο και στους κόμβους, όσο αφορά στο πλήθος των μηνυμάτων. Έτσι υπάρχει η δυνατότητα με ένα μοναδικό μήνυμα να μεταφερθεί μια ολόκληρη σειρά ενός πίνακα ή στηλών. Στο SNMPv1 αυτή η λειτουργία θα έπρεπε να γίνει με η διαφορετικά GetRequest μηνύματα.
- **InformRequest:** Αυτό το μήνυμα στέλνει ένας σταθμός διαχείρισης σε έναν άλλον σταθμό διαχείρισης για να τον εφοδιάσει με πληροφορίες διαχείρισης.

6.7 SNMP VERSION 3.

Για να συνεχίσουμε την αναδρομή στην ιστορία του SNMP, πρέπει να αναφέρουμε, για μια ακόμη φορά, ότι το SNMPv2, στην τελική του μορφή, δεν συμπεριλάμβανε μηχανισμούς ασφαλείας. Στην συνέχεια θα δούμε πώς συμπεριλήφθηκαν αυτοί οι μηχανισμοί ασφαλείας και θα κλείσουμε την αναδρομή με το πώς φτάσαμε στην έκδοση 3 του SNMP.

Μετά από το έτος 1996, όταν αφαιρέθηκαν οι διαδικασίες ασφάλειας από το SNMPv2, διάφορες ανεξάρτητες ομάδες εργασίας ανέπτυξαν και πρότειναν βελτιώσεις στον τομέα αυτόν. Το αποτέλεσμα ήταν το SNMPv2u και το SNMPv2*. Αυτές οι προτάσεις ήταν η βάση από την οποία ξεκίνησαν, τον Μάρτιο του 1997, οι νέες εργασίες της IETF. Τον Ιανουάριο του 1998 η ομάδα αυτή της IETF κατέληξε σε κάποια προτεινόμενα πρότυπα (Proposed Standards).

Ουσιαστικά, αυτή η ομάδα από προτάσεις, καθορίζει το SNMP. Όμως, δεν καθορίζονται νέοι τύποι μηνυμάτων, παρά μόνο μια γενικότερη αρχιτεκτονική και διαδικασίες ασφάλειας. Έτσι το SNMPv3 βασίζεται στην λειτουργικότητα του SNMPv2. Αυτό φαίνεται ξεκάθαρα και από την πρώτη παράγραφο του προτύπου:

“SNMPv3 is SNMPv2 plus security and administration.”

6.7.1 Γενικά για το SNMPv3.

Κατά τον σχεδιασμό του πρωτοκόλλου τέθηκαν ορισμένοι στόχοι – περιορισμοί οι οποίοι θα έπρεπε να τηρηθούν:

- Να χρησιμοποιηθεί, όσο είναι δυνατό, η ήδη υπάρχουσα δουλειά, για την οποία υπάρχουν υλοποιήσεις και αρκετή εμπειρία.
- Να βρεθεί τρόπος για ασφαλή αποστολή μηνυμάτων **SetRequest** και έτσι, να λυθεί το βασικό πρόβλημα του SNMPv1 και SNMPv2.
- Να αναπτυχθεί μία αρχιτεκτονική που:
 - Θα επιτρέπει, ανάλογα με την περίπτωση, στοιχειώδεις και οικονομικές υλοποιήσεις, σε περιορισμένου μεγέθους περιβάλλοντα και πλήρεις υλοποιήσεις σε μεγάλα περιβάλλοντα.
 - Θα δίνει την δυνατότητα να υπάρχει πρόοδος σε κάποια τμήματα, ακόμα και αν τα υπόλοιπα παραμένουν στάσιμα.
 - Θα διευκολύνει την χρησιμοποίηση εναλλακτικών μηχανισμών ασφάλειας.
- Το πρωτόκολλο να παραμείνει απλό.

Με βάση τα παραπάνω λήφθηκαν κάποιες αποφάσεις σχετικά με την δομή του πρωτοκόλλου:



- **Αρχιτεκτονική:** Το SNMPv3 θα έπρεπε να αποτελείται από ανεξάρτητες λειτουργικές μονάδες, η καθεμία από τις οποίες πρέπει να εκτελεί τον δικό της ρόλο.
- **Αυτάρκη Κείμενα:** Τα κείμενα που περιγράφουν το πρωτόκολλο, αποφασίστηκε να είναι αυτάρκη. Δηλαδή, ένα τμήμα του πλαισίου εργασίας του SNMPv3, η αντίστοιχη MIB και ότι άλλο σχετικό υπάρχει, θα πρέπει να περιγράφονται στο ίδιο κείμενο και με όσο το δυνατόν λιγότερες εξωτερικές αναφορές. Έτσι, για παράδειγμα, θα μπορούν να γίνονται αναθεωρήσεις του μηχανισμού ασφάλειας, χωρίς να επηρεάζεται η υπόλοιπη λειτουργικότητα του πρωτοκόλλου.
- **Απομακρυσμένες Ρυθμίσεις:** Οι παράμετροι λειτουργίας του SNMP (του ίδιου του πρωτοκόλλου και όχι του δικτύου υπό διαχείριση) θα πρέπει να ρυθμίζονται απομακρυσμένα.
- **Ελεγχόμενη Πολυπλοκότητα:** Κάθε υλοποίηση θα μπορεί να συμπεριλαμβάνει όσες λειτουργικές μονάδες επιθυμεί, ώστε να έχει και την επιθυμητή πολυπλοκότητα.
- **Απειλές:** Οι διαδικασίες ασφάλειας θα πρέπει να προστατεύουν από μετατροπή πληροφοριών, μετατροπή ροής μηνυμάτων, αποκάλυψη πληροφοριών (Disclosure), προσποίηση ταυτότητας (Masquerade). Το SNMPv3 δεν προστατεύει από επιθέσεις Denial of Service και από Traffic Analysis.

6.7.2 Η Αρχιτεκτονική του SNMPv3.

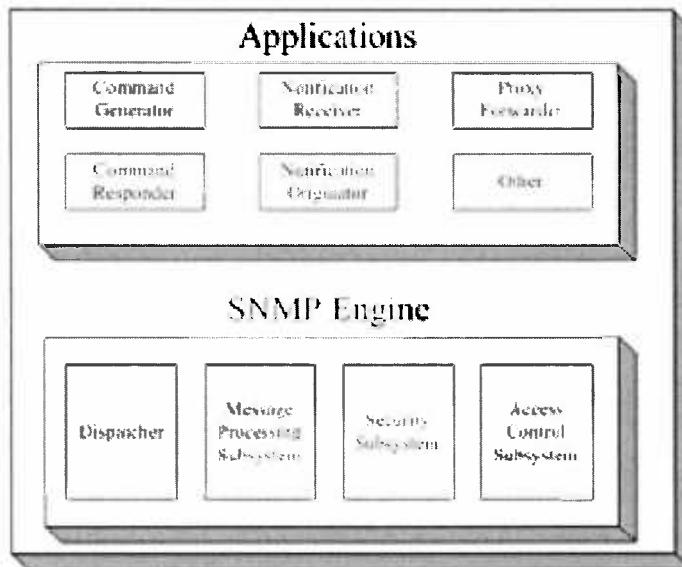
Η αρχιτεκτονική αποτελείται από μια συλλογή αλληλεπιδρώντων οντοτήτων. Κάθε οντότητα μπορεί να είναι διαχειριστής, αντιπρόσωπος ή και τα δύο. Αποτελείται από μονάδες. Κάθε μονάδα υλοποιεί ένα μέρος της λειτουργίας του πρωτοκόλλου, όπως η αποστολή μηνυμάτων.

Οι μονάδες αυτές χωρίζονται σε Εφαρμογές (Applications) και SNMP Engine και όπως είπαμε είναι ξεχωριστές. Έτσι, ο ρόλος μιας οντότητας, δηλαδή αν θα είναι σταθμός διαχείρισης ή αντιπρόσωπος, καθορίζεται από το ποιες από τις μονάδες υλοποιούνται.

Οι βασικές μονάδες είναι οι εξής:

- **Dispatcher:** Αναλαμβάνει την ταυτόχρονη υποστήριξη και των τριών εκδόσεων του SNMP. Δέχεται PDU από τις εφαρμογές και τα προωθεί στο Message Processing για να προετοιμαστούν τα μηνύματα. Επίσης, προωθεί τα εισερχόμενα PDU στις εφαρμογές.

- **Message Processing Subsystem:** Είναι υπεύθυνο για την προετοιμασία των μηνυμάτων προς αποστολή και για την ανάκτηση των δεδομένων από τα εισερχόμενα συστήματα.
- **Security Subsystem:** Παρέχει υπηρεσίες ασφάλειας, όπως αυθεντικοποίηση και Privacy. Περιέχει, ενδεχομένως, πολλαπλά μοντέλα ασφάλειας.
- **Access Control Subsystem:** Παρέχει ένα σύνολο υπηρεσιών ελέγχου δικαιωμάτων προσπέλασης.



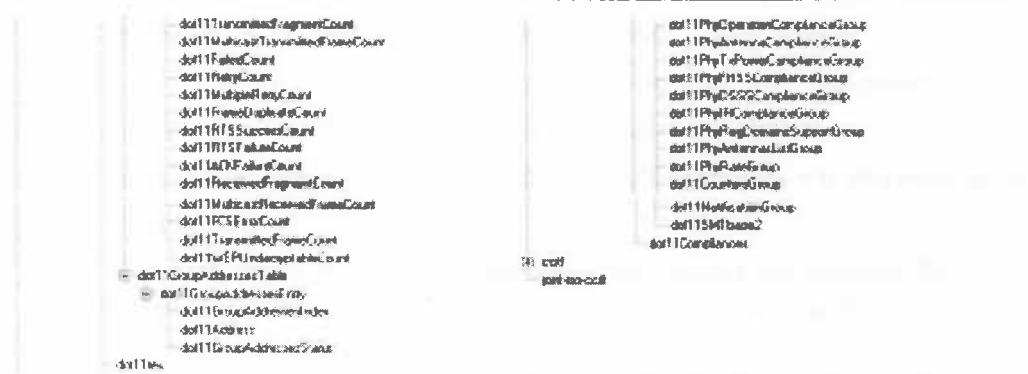
Σχήμα 40 - Η Αρχιτεκτονική του SNMPv3.

- **Command Generator:** Προετοιμάζει τις εντολές **GetRequest**, **GetNextRequest**, **GetBulkRequest** και **SetRequest**. Λαμβάνει τις απαντήσεις στα μηνύματα αυτά.
- **Command Responder:** Λαμβάνει τις ίδιες εντολές από σταθμούς διαχείρισης και απαντά αφού πρώτα πραγματοποιήσει τις ενέργειες που ζητήθηκαν. Είναι προφανές ότι ένας αντιπρόσωπος θα έχει μόνο Command Responder, ενώ ένας σταθμός διαχείρισης θα έχει μόνο Generator.
- **Notification Originator:** Αναλαμβάνει την δημιουργία των μηνυμάτων **Trap** και **InformRequest**.
- **Notification Receiver:** Ακούει για μηνύματα **Notification** και απαντά στην περίπτωση άφιξης ενός **InformRequest**.
- **Proxy Forwarder:** Αναλαμβάνει την προώθηση SNMP μηνυμάτων.

6.8 Η MIB ΤΩΝ ΔΙΚΤΥΩΝ IEEE 802.11.

Ο IEEE, σχεδιάζοντας το πρότυπο για τα ασύρματα τοπικά δίκτυα, σχεδίασε και την αντίστοιχη MIB που θα χρησιμοποιείται για την διαχείριση των κόμβων. Ορισμένα από τα στοιχεία της MIB χαρακτηρίζονται ως υποχρεωτικά και άλλα ως προαιρετικά. Το σχήμα που ακολουθεί είναι ένα δενδροειδές διάγραμμα που περιγράφει την MIB.





Σχήμα 41 - Η MIB του IEEE 802.11.

Ακολουθεί μια σύντομη περιγραφή της MIB των δικτύων IEEE 802.11, όπως αυτή ορίζεται από την IEEE. Περιέχεται μια αναφορά στις ομάδες αντικειμένων. Ωστόσο δεν γίνεται λεπτομερής περιγραφή του κάθε αντικειμένου ξεχωριστά. Κάτι τέτοιο ξεφεύγει από τον σκοπό της εργασίας αυτής.

Ο κωδικός του MIB Module είναι:

iso.member-body.us.ieee802dot11 = { 1.2.840.10036 }

Όπως μπορούμε να δούμε και στο παραπάνω σχήμα, τα αντικείμενα της MIB χωρίζονται σε τρεις ομάδες.

Η πρώτη ομάδα ονομάζεται Station Management (SMT) Attributes (ieee802dot11.1) και σύμφωνα με το επίσημο κείμενο:

"...The SMT object class provides the necessary support at the station to manage the processes in the station such that the station may work cooperatively as a part of an IEEE 802.11 network."

Περιέχονται όλα τα αντικείμενα που έχουν να κάνουν με τους αλγόριθμους αυθεντικοποίησης και τα μυστικά κλειδιά που χρησιμοποιεί το WEP. Επίσης περιέχει παραμέτρους λειτουργίας του συστήματος, όπως το αν θα χρησιμοποιείται Power Management και το χρόνο μεταξύ δύο διαδοχικών αποστολών Beacon πλαισίων.

Η δεύτερη ομάδα (ieee802dot11.2) ονομάζεται MAC Attributes και σύμφωνα με το επίσημο κείμενο:

"...The MAC object class provides the necessary support for the access control, generation, and verification of frame check sequences, and proper delivery of valid data to upper layers."

Σε αυτή την ομάδα περιέχονται όλες οι λεπτομέρειες διαχείρισης που σχετίζονται με το επίπεδο MAC. Αυτές οι λεπτομέρειες είναι η MAC διεύθυνση της διεπαφής (ή των διεπαφών αν υπάρχουν πολλές) και το μέγιστο μέγεθος πλαισίου που μπορεί να παραδοθεί στο φυσικό επίπεδο χωρίς να υποστεί κατακερματισμό (Fragmentation). Επίσης περιέχεται το οριακό μέγεθος πλαισίου, κάτω από το οποίο δεν θα πραγματοποιείται RTS/CTS.

Στην ομάδα MAC attributes διατηρείται, επίσης, ένας πίνακας που περιέχει μετρητές. Οι μετρήσεις αυτές αναφέρονται στον αριθμό των εισερχόμενων και εξερχόμενων πλαισίων και τον αριθμό εμφάνισης διαφόρων σφαλμάτων.

Η τρίτη ομάδα (ieee802dot11.4) ονομάζεται PHY Attributes και σύμφωνα με το επίσημο κείμενο:

"...The PHY object class provides the necessary support for required PHY operational information that may vary from PHY to PHY and from STA to STA to be communicated to upper layers."

Σε αυτή την ομάδα περιέχονται όλες οι λεπτομέρειες διαχείρισης που σχετίζονται με το φυσικό επίπεδο. Για παράδειγμα αναφέρουμε τα διαφορετικά επίπεδα έντασης που μπορεί να λειτουργήσει η κεραία της συσκευής.

Τελευταία αναφέρουμε την ομάδα Resource Type ID (ieee802dot11.3).

7 ΜΕΤΡΗΣΗ ΕΠΙΔΟΣΕΩΝ ΔΙΚΤΥΟΥ.

Ένα πολύ σημαντικό κομμάτι της εργασίας αυτής αναφέρεται στην μέτρηση επιδόσεων ενός δικτύου. Ως εκ τούτου, δεν θα μπορούσε να μην γίνει εκτενής αναφορά στις υπάρχουσες μεθόδους, πρότυπα και τεχνολογίες που μας βοηθάν ακριβώς σε αυτόν τον τομέα.

Στα τρία παραπάνω σημεία θα επεκταθούμε στο παρόν κεφάλαιο, ελπίζοντας να δώσουμε στον αναγνώστη μια σφαιρική αντίληψη της κατάστασης, όπως αυτή επικρατεί στις μέρες μας.

Η ουσία, πάντως, του θέματος των επιδόσεων είναι ότι βασίζονται σε τόσο πολλές παραμέτρους που για να τις βελτιστοποιήσουμε χρειάζονται γνώσεις σε πολύ μεγάλο βάθος. Έρευνες έδειξαν ότι, το έτος 1998, οι γνώστες των δικτύων υπολογιστών μπορούσαν να αυξήσουν τις επιδόσεις του TCP μέχρι και 300 φορές σε σχέση με τις τυπικές ρυθμίσεις. Αυτό γιατί το TCP και οι μηχανισμοί αποφυγής συμφορήσεων είχαν βελτιστοποιηθεί για αργά δίκτυα, κατά τρόπο τέτοιον που δεν έδιναν την δυνατότητα να εκμεταλλευτούμε πλήρως το διαθέσιμο εύρος ζώνης των δικτύων υψηλών ταχυτήων. Το γεγονός ότι οι επιδόσεις επηρεάζονται και από παραμέτρους, που δεν έχουν να κάνουν με το δίκτυο και τα πρωτόκολλα δικτύου, όπως το υλικό των υπολογιστών και το λειτουργικό σύστημα, περιπλέκει την κατάσταση ακόμη περισσότερο.

7.1 ΠΡΟΤΥΠΑ ΜΕΤΡΗΣΗΣ.

Στο θέμα των επιδόσεων δικτύου, δύο είναι οι ομάδες που έχουν αφοσιωθεί στην ανάπτυξη προτύπων. Η πρώτη είναι η IETF με το IP Performance Metrics – IPPM και η δεύτερη είναι η Cross Industry Working Group – XIWT.

7.1.1 IP Performance Metrics – IPPF.

Πρόκειται για ένα Work Group της IEEE, το οποίο σαν σκοπό έχει την ανάπτυξη ενός συνόλου μετρικών επιδόσεων δικτύων. Οι μετρικές αυτές, σύμφωνα με την ίδια την IEEE, θα μπορούν να χρησιμοποιηθούν από διαχειριστές αλλά και από απλούς χρήστες.

Θα είναι ποσοτικές, ακριβείς, επαρκώς τεκμηριωμένες και θα χαρακτηρίζονται από συνέπεια.

7.1.2 Cross – Industry Working Team – XIWT.

Η XIWT είναι μια επιτροπή που δημιουργήθηκε από την συνεργασία πολλών εταιρειών. Μερικά έλη της είναι οι:

- AT&T
- Cisco Systems, Inc.

- Compaq Computer Corporation
- EarthLink Network, Inc.
- Ericsson
- Hewlett-Packard Company
- IBM Corporation
- Intel Corporation
- National Institute for Standards and Technology

Ο σκοπός της είναι η έρευνα και το information – sharing μεταξύ της βιομηχανίας, του ακαδημαϊκού κόσμου και της κυβέρνησης.

Σχετικά με επιδόσεις δικτύων έχουν την ομάδα εργασίας Internet Performance Working Team.

7.1.2.1 Internet Performance Working Team – IPERF.

Το IPERF είναι μια προσπάθεια δημιουργίας ενός κοινού συνόλου μετρικών και μίας κοινής μεθοδολογίας μετρήσεων. Αυτά μπορούν να χρησιμεύσουν στην παρακολούθηση, την εκτίμηση και τον έλεγχο συμμόρφωσης της ποιότητας υπηρεσιών στο διαδίκτυο.

Έχει ήδη ξεκινήσει μια πρωτοβουλία συλλογής δεδομένων. Τα δεδομένα αυτά αναλύονται και μελετώνται ήδη με σκοπό να εξαχθούν συμπεράσματα για ανωμαλίες και τάσεις.

7.1.3 CAIDA

H Cooperative Association for Internet Data Analysis - CAIDA, σχεδιάζει εργαλεία και μεθόδους μέτρησης επιδόσεων δικτύων.

7.2 ΜΕΘΟΔΟΙ ΜΕΤΡΗΣΗΣ.

Οι μέθοδοι μέτρησης των επιδόσεων ενός δικτύου χωρίζονται, βασικά, σε δύο κατηγορίες. Η πρώτη είναι η παθητική μέτρηση (Passive Measurement) και η δεύτερη η ενεργητική (Active).

7.2.1 Passive Measurement.

Ο παθητικός τρόπος μέτρησης βασίζεται στην παρακολούθηση της κυκλοφορίας του δικτύου και την καταχώρισή της για μελλοντική επεξεργασία. Διάφορα εργαλεία μέτρησης μπορούν να ζητήσουν πληροφορίες από μία συσκευή, όπως αριθμός λαθών.

Παρόλο που δεν είναι καθόλου πρακτικό να αποθηκεύουμε κάθε πακέτο που κυκλοφορεί στο δίκτυο, μπορούμε να παγιδεύουμε όλα τα πακέτα και να αποθηκεύουμε κάποια από αυτά με τυχαία δειγματοληψία, παίρνοντας έτσι ένα αμερόληπτο δείγμα.

7.2.2 Active Measurement.

Σε αυτή την περίπτωση, κάποια εφαρμογή, συνήθως αρχιτεκτονικής Client – Server, βάζει κίνηση στο δίκτυο και μετράει την από άκρο σε άκρο απόδοση. Πολύ συχνά μάλιστα υπάρχει και κάποια μέθοδος αποθήκευσης των αποτελεσμάτων που μπορεί με περαιτέρω επεξεργασία να μας δώσει πληροφορίες για μέσες τιμές, μακροχρόνιες τάσεις, περιοδικότητα και άλλα. Αυτή η προσέγγιση έχει το πλεονέκτημα ότι μας δίνει μια εικόνα παρόμοια με αυτή που έχει ο χρήστης του δικτύου.

Το κακό είναι ότι η επίδοση ενός μονοπατιού, μπορεί να απέχει πάρα πολύ από την απόδοση του δικτύου στο σύνολό του.

Μέρος 4^ο:

Πειραματική μέτρηση επιδόσεων ενός δικτύου IEEE 802.11b.

8 ΠΕΡΙΓΡΑΦΗ ΤΩΝ ΠΕΙΡΑΜΑΤΩΝ.

Τα πειράματα πραγματοποιήθηκαν στον χώρο του Εργαστηρίου Συστημάτων Υπολογιστών και Επικοινωνιών, που βρίσκεται στον 4^ο όροφο της πτέρυγας Αντωνιάδου, του Οικονομικού Πανεπιστημίου Αθηνών.

Το Εργαστήριο υπάγεται στο τμήμα Πληροφορικής του Πανεπιστημίου και συγκεκριμένα στο Μεταπτυχιακό Πρόγραμμα Σπουδών σε Πληροφοριακά Συστήματα. Διευθυντής του είναι ο κος Θεόδωρος Αποστολόπουλος, Καθηγητής του Οικονομικού Πανεπιστημίου Αθηνών.

Για την διεκπεραίωση των πειραμάτων δημιουργήθηκε μια μικρογραφία εργαστηρίου για Ασύρματα Τοπικά Δίκτυα. Σε αυτόν τον χώρο έγιναν όλες οι μετρήσεις με την χρήση του εξοπλισμού που αναφέρεται παρακάτω.

8.1 ΣΚΟΠΟΣ ΤΩΝ ΠΕΙΡΑΜΑΤΩΝ.

Ο σκοπός των πειραμάτων ήταν πολλαπλός.

Βασική επιθυμία μας ήταν να εκτιμήσουμε τις επιδόσεις ενός δικτύου, σύμφωνο με το πρότυπο IEEE 802.11b και τη συμπεριφορά του κάτω από συνθήκες ψηλού φόρτου. Επιπλέον εξετάσαμε τις επιδόσεις της επικοινωνίας μεταξύ ενός σταθμού συνδεδεμένου σε ενσύρματο δίκτυο (IEEE 802.3) και ενός συνδεδεμένου ασύρματα.

Τέλος, προσπαθήσαμε να εξετάσουμε την επίδραση ορισμένων παραγόντων στις επιδόσεις αυτές. Οι παράγοντες αυτοί ήταν:

- Οι διαφορές μεταξύ των διαφορετικών λειτουργικών συστημάτων στην υποστήριξη ασύρματου τοπικού δικτύου και στην εκμετάλλευση του διαθέσιμου εύρους ζώνης. Δεν θα μπορούσε, άλλωστε, να αγνοηθεί το ότι οι οδηγοί των καρτών δικτύου δεν έχουν τελειοποιηθεί ακόμα, καθώς η τεχνολογία των ασύρματων τοπικών δικτύων είναι πολύ νέα.
- Ο αντίκτυπος που μπορεί να έχει η τοπολογία στις επιδόσεις ενός ασύρματου τοπικού δικτύου.
- Πώς οι παράμετροι της MIB ενός σταθμού μπορούν να επηρεάσουν τις επιδόσεις. Οι παράμετροι εκλέχθηκαν ανάμεσα από τα αντικείμενα διαχείρισης,

που περιγράφονται στο πρότυπο IEEE 802.11. Εξετάστηκαν αντικείμενα διαχείρισης τόσο του επιπέδου MAC όσο και του Φυσικού επιπέδου.

- Σε τι βαθμό τα εμπόδια, όπως τοίχοι, επηρεάζουν τον αριθμό των σφαλμάτων μετάδοσης.

Σε καμία περίπτωση δεν θα έπρεπε να παραληφθεί το γεγονός ότι, πολλές φορές, δύο εργαλεία μέτρησης του ιδίου αντικειμένου, δίνουν άλλα αποτελέσματα. Έτσι ελέγχθηκε το ενδεχόμενο τα δύο εργαλεία, σε ίδιες περιπτώσεις, να δίνουν αποτελέσματα με στατιστικώς σημαντική διαφορά.

8.2 ΣΧΕΔΙΑΣΜΟΣ ΤΩΝ ΠΕΙΡΑΜΑΤΩΝ.

Όπως αναφέραμε παραπάνω, τα πειράματα έγιναν με σκοπό να ελεγχθούν κάποιες υποθέσεις. Με γνώμονα αυτές τις υποθέσεις έγινε και ο σχεδιασμός τους. Εδώ παραθέτουμε, σύντομα, τι άλλες παραμέτρους λάβαμε υπ' όψιν μας και τι συμβιβασμούς κάναμε.

Έτσι, εγκαταστάθηκαν δύο διαφορετικές τοπολογίες και μετρήθηκε το διαθέσιμο εύρος ζώνης. Για κάθε τοπολογία έγιναν διαφορετικές μετρήσεις, κατά τις οποίες αλλάζαμε συνεχώς μια από τις παραμέτρους του συστήματος. Τέτοιες αλλαγές ήταν η χρήση διαφορετικών λειτουργικών συστημάτων, αλλαγές στις τιμές αντικειμένων της MIB, εναλλαγή αποστολέα – παραλήπτη.

Σε κάθε περίπτωση έγιναν 100 μετρήσεις και υπολογίστηκε η μέση τιμή και η διακύμανση της καθυστέρησης καθώς και η μέση Ρυθμοαπόδοση.

Κατά την διάρκεια των μετρήσεων, τόσο στους δύο υπολογιστές που μετείχαν, όσο και στο υπόλοιπο δίκτυο, δεν υπήρχε καθόλου κίνηση προκαλούμενη από χρήστη. Η μόνη κίνηση ήταν αυτή που χρησιμοποιήθηκε για τις μετυρήσεις.

8.2.1 Παραδοχές κατά τον Σχεδιασμό.

Η λειτουργία ενός δικτύου επηρεάζεται πάντα και από εξωγενείς παράγοντες. Για παράδειγμα, η ταχύτητα επικοινωνίας δύο υπολογιστών, που ανήκουν σε ένα δίκτυο πολλαπλής πρόσβασης, μπορεί να υποβαθμιστεί σημαντικά αν δύο άλλοι υπολογιστές – μέλη του ιδίου δικτύου αρχίσουν να ανταλλάσσουν μεγάλο όγκο δεδομένων. Αν κατά τις μετρήσεις μας, δύο άλλοι υπολογιστές, άρχιζαν να μετακινούν κάποια μεγάλα αρχεία μέσω FTP, τα αποτελέσματα των μετρήσεων θα ήταν αναξιόπιστα. Για να διατηρηθούν οι ίδιες συνθήκες σε όλους τους ελέγχους, προτιμήσαμε να τους εκτελέσουμε σε όχι κανονικές συνθήκες λειτουργίας. Για τον λόγο αυτό οι τοπολογίες ήταν απομονωμένες από το υπόλοιπο δίκτυο.



Στις περιπτώσεις που χρησιμοποιήσαμε το TTCP, υπήρχε άλλη μια μικρή λεπτομέρεια που έπρεπε να προσεχτεί. Ο τρόπος γραφής του κώδικα έχει σαν αποτέλεσμα ο πελάτης να θεωρεί ότι το πείραμα έχει τελειώσει όταν αποστείλει το τελευταίο πακέτο, πριν αυτό φτάσει στον προορισμό του. Αντίθετα ο εξυπηρετητής, θεωρεί ως λήξη του πειράματος την στιγμή της παραλαβής του τελευταίου πακέτου, όπως είναι και λογικό. Υπάρχει λοιπόν μια ανεπαίσθητη διαφορά στην αντίληψη των δύο κόμβων για την διάρκεια του πειράματος (ο πελάτης την θεωρεί μικρότερη). Αυτή η διαφορά, στις περισσότερες περιπτώσεις είναι της τάξης των μSec αλλά ενδέχεται, σπάνια, να είναι σημαντική, ώστε οι δύο σταθμοί να δώσουν διαφορετικά αποτελέσματα. Η διαφορά είναι ακόμα μεγαλύτερη, όταν μεταξύ των σταθμών παρεμβάλλονται πολλοί ενδιάμεσοι κόμβοι (Hops). Ωστόσο οι μετρήσεις πραγματοποιούνται και από τις δύο οντότητες και τα αποτελέσματα έρχονται στην ίδια μορφή. Έτσι χρησιμοποιήσαμε για την ανάλυση τις μετρήσεις του εξυπηρετητή.

8.3 Ο ΕΞΟΠΛΙΣΜΟΣ ΚΑΙ ΤΟ ΛΟΓΙΣΜΙΚΟ.

Στις παραγράφους που ακολουθούν, παρατίθεται μια αναλυτική περιγραφή του εξοπλισμού και των εργαλείων λογισμικού που χρησιμοποιήθηκε.

8.3.1 Ο Εξοπλισμός που Χρησιμοποιήθηκε.

Για τα πειράματα προμηθευτήκαμε εξοπλισμό συμβατό με το πρότυπο IEEE 802.11b. Συγκεκριμένα, χρησιμοποιήθηκε ένα Access Point της εταιρείας D – Link και δύο PCMCIA κάρτες δικτύου της ίδιας εταιρείας.

Συγκεκριμένα χρησιμοποιήθηκαν:

- Ένα 8 – port Ethernet HUB 10/100 Mbps Planet EH – 801,
- Ένα Access Point DWL 1000AP της εταιρείας D – Link με
 - Έκδοση Firmware την 3.2.28 #483 (23 Αυγούστου 2001),
 - Μια διεπαφή IEEE 802.3.
- Ένας φορητός υπολογιστής Toshiba Satellite 1640 με
 - Επεξεργαστή AMD K3 στα 475MHz,
 - 192MByte RAM,
 - 6GByte HDD
 - Λειτουργικό σύστημα Windows XP Professional,
 - Λειτουργικό σύστημα LINUX. Διανομή Debian 3.0, πυρήνα 2.2 και όλα τα packages ενημερωμένα με τις τελευταίες εκδόσεις που υπήρχαν κατά την πραγματοποίηση των πειραμάτων,
 - PCMCIA Κάρτα IEEE 802.11b, D – Link 650 στα 11Mbps.



- Ένας προσωπικός υπολογιστής με,
 - Επεξεργαστή PII 233 MHz,
 - 128 Mb RAM,
 - Gb σκληρό δίσκο,
 - Λειτουργικό Σύστημα Windows 2000 Professional Service Pack 2,
 - PCMCIA Κάρτα IEEE 802.11b, D – Link 650 στα 11Mbps.
- Ένας προσωπικός υπολογιστής με,
 - Επεξεργαστή Intel Pentium στα 120 MHz,
 - 64 Mb RAM,
 - Gb σκληρό δίσκο,
 - Λειτουργικό Σύστημα Windows 98 Release 2,
 - ISA Κάρτα IEEE 802.3, Intel EtherExpress Pro+ στα 10Mbps.

8.3.2 Εργαλεία που Χρησιμοποιήθηκαν.

Για την εκτέλεση των πειραμάτων, ανάμεσα στις επιλογές που είχαμε, καταλήξαμε στην μέθοδο Bulk Transfer Capacity. Στο διαδίκτυο διατίθενται, ελεύθερα, πάρα πολλά εργαλεία που ανήκουν στην κατηγορία αυτή. Τα κριτήρια της επιλογής μας ήταν:

- Η διαθεσιμότητα του πηγαίου κώδικα του εργαλείου,
- Η ποικιλία επιλογών που προσέφερε το καθένα,
- Το πόσο ευρέως διαδεδομένο ήταν το καθένα.

Ανεξαρτήτως από το πρόγραμμα που χρησιμοποιήθηκε για να κάνουμε τις μετρήσεις, προσπαθήσαμε τα πειράματα να έχουν τις ίδιες παραμέτρους. Έτσι, για παράδειγμα, σε όλα τα πειράματα ο όγκος των δεδομένων που μεταφερόταν ήταν ο ίδιος (16MBytes). Χρησιμοποιήσαμε το πρωτόκολλο TCP και ζητούσαμε τα αποτελέσματα σε Kbps ή KBytes ανά δευτερόλεπτο.

8.3.2.1 TTCP.

Λόγω της διαθεσιμότητας του πηγαίου κώδικα και της ευρείας διάδοσής του, το πρώτο εργαλείο που επιλέχθηκε ήταν το TTCP.

- **Ιστορικό – Έκδοση.**

Το TTCP ξεκίνησε ως ένα πρόγραμμα που θα χρησίμευε στην μετακίνηση αρχείων. Στη συνέχεια έγινε ένα πολύ δημοφιλές εργαλείο εκτίμησης επιδόσεων δικτύου. Η ονομασία του σημαίνει Test TCP. Η έκδοση που χρησιμοποιήθηκε ήταν η v1.00.00.02. της 11^{ης} Ιανουαρίου 2001.

Ο κώδικας του είναι ελεύθερα διαθέσιμος στο διαδικτύου. Εκεί βρήκαμε και μια έκδοση του προγράμματος, που είχε ξαναγραφτεί για Windows Πλατφόρμες. Αυτήν

χρησιμοποιήσαμε στα πειράματα. Οι αλλαγές σε σχέση με την αρχική έκδοση για UNIX, ήταν στις κλήσεις των sockets και στις συναρτήσεις χρονομέτρησης. Το αποτέλεσμα ήταν, το πρόγραμμα να μην έχει την ακρίβεια της έκδοσης για UNIX (mSec αντί για μSec).

Η έκδοση του TTCP που χρησιμοποιήσαμε, ήταν μια μεταφορά από UNIX σε Windows από την εταιρεία PCAUSA – Printing Communications Associates. Πρόκειται για μια εταιρεία παραγωγής λογισμικού που εξειδικεύεται στα εργαλεία ανάπτυξης λογισμικού δικτύων.

Να σημειωθεί, επίσης, ότι το TTCP υπάρχει ενσωματωμένο στους δρομολογητές της εταιρείας CISCO που έχουν λειτουργικό σύστημα Cisco IOS, έκδοση από 11.2 και πάνω.

- **Τρόπος Λειτουργίας.**

Πρόκειται για μια εφαρμογή πελάτη – εξυπηρετητή, που λειτουργεί τόσο πάνω από πρωτόκολλο TCP όσο και UDP. Ο Server ξεκινάει στο port 5001 και περιμένει τις αιτήσεις των πελατών. Ο πελάτης αποστέλλει ένα σύνολο δεδομένων που καθορίζεται από τον χρήστη και μετριέται η ρυθμοαπόδοση σε bits ανά δευτερόλεπτο. Για να μην προκαλείται καθυστέρηση από τον σκληρό δίσκο των υπολογιστών, αρχικά γεμίζονται κάποιοι ενταμιευτές με δεδομένα και μετά ξεκινάει η αποστολή τους. Το σύνολο των δεδομένων είναι ίσο με $l \times n$ όπου l το μήκος των ενταμιευτών και n το πλήθος τους. Αυτές οι τιμές καθορίζονται από την γραμμή εντολών, από την οποία καλεί το πρόγραμμα ο χρήστης.

- **Κλήση από την Γραμμή Εντολών (Command Line).**

Το TTCP το καλούνσαμε με την εξής γραμμή εντολής:

```
PCATTCP -fK -n2048 -18192 -r
PCATTCP -fK -n2048 -18192 -t 195.251.252.72
```

Δηλαδή:

- Server (-r) ή Client (-t),
- Output σε KBytes (-fK),
- 2048 ενταμιευτές προς μετάδοση (-n2048),
- μεγέθους 8192Bytes (-18192) σύνολο 16MBytes.

- **Επεμβάσεις στον πηγαίο κώδικα.**

Η εφαρμογή εμφανίζει τα αποτελέσματα των μετρήσεων στην οθόνη του χρήστη σε μορφή ευανάγνωστη και ευνόητη, αλλά εντελώς ακατάλληλη για μαζική επεξεργασία.

Για αυτόν τον λόγο έγινε μια προσαρμογή του κώδικα. Έτσι, πλέον το πρόγραμμα χρησιμοποιεί ένα αρχείο για να αποθηκεύει τα αποτελέσματα. Το αρχείο αυτό έχει στήλες



– πεδία σταθερού πλάτους και σε κάθε μία αποθηκεύεται συγκεκριμένη τιμή των αποτελεσμάτων. Για παράδειγμα, ο χρόνος ολοκλήρωσης της μεταφοράς αποθηκεύεται στην τρίτη. Κάθε γραμμή αντιστοιχεί και σε ξεχωριστή μέτρηση. Η μορφή είναι τέτοια ώστε τα δεδομένα να μπορούν να μεταφερθούν και να υποστούν επεξεργασία από εφαρμογές λογιστικών φύλλων, στατιστικής κλπ.

```
C:\>pcattcp -t 127.0.0.1
PCATTCP Test TCP Utility v1.00.00.02

TTCP Transmit Test
Protocol : TCP
Port      : 5001
addr     : 127.0.0.1
buflen   : 8192
nbuf     : 2048
align    : 16384/0
tcp      -> 127.0.0.1

Progress of Test
...Socket
...Binding
...nodelay DISABLED (0)
...Connecting to Server
End of Test

16777216 bytes in 37.20 real seconds - 440.395 KB/sec +++
numCalls: 2048; msec/call: 18.60; calls/sec: 55.05

C:\>
```

Σχήμα 42 - Η Μορφή των Αποτελεσμάτων του TTCP.

Στην παρακάτω εικόνα φαίνεται η μορφή του Log File που δημιουργεί το TTCP μετά τις μετατροπές.

Rcv	16384.000	26.818	610.933 KB	2178	12.609	81.21
Rcv	16384.000	26.298	623.013 KB	2277	11.827	86.58
Rcv	16384.000	26.287	623.274 KB	2142	12.567	81.49
Rcv	16384.000	25.687	637.832 KB	2138	12.303	83.23
Rcv	16384.000	25.627	639.326 KB	2135	12.291	83.31
Rcv	16384.000	26.988	607.085 KB	2129	12.981	78.89
Rcv	16384.000	28.101	583.040 KB	2115	13.605	75.26
Rcv	16384.000	27.230	601.689 KB	2128	13.103	78.15
Rcv	16384.000	28.001	585.122 KB	2113	13.570	75.46
Rcv	16384.000	26.348	621.831 KB	2117	12.745	80.35
Rcv	16384.000	28.481	575.261 KB	2108	13.835	74.01

Σχήμα 43 - Η Μορφή του Log File του TTCP.

- Η πρώτη στήλη αναγράφει Rcv ή Snd ανάλογα αν το αρχείο δημιουργείται από τον Client ή τον Server.
- Η δεύτερη αναγράφει το μέγεθος των δεδομένων σε KBytes.
- Η τρίτη τον χρόνο σε δευτερόλεπτα που χρειάστηκε για την ολοκλήρωση της μεταφοράς των δεδομένων.

- Η τέταρτη την ρυθμοαπόδοση σε KBytes ανά δευτερόλεπτο.
- Οι τρεις τελευταίες κάποια στοιχεία σχετικά με τον αριθμό των κλήσεων του συστήματος που χρειάστηκαν για την ολοκλήρωση.

8.3.2.2 NetPerf.

Το δεύτερο πρόγραμμα που χρησιμοποιήθηκε ήταν το NetPerf της Hewlett Packard.

- Έκδοση – Τρόπος Λειτουργίας.

Παρόμοιο με το TTCP, μετράει τις επιδόσεις δικτύων με την χρήση της διεπαφής των Berkeley Sockets. Επίσης υποστηρίζει την μέτρηση και άλλων τεχνολογιών δικτύων, όπως ATM.

Το NetPerf είναι αρκετά πιο εξελιγμένο από το TTCP. Ακολουθεί και αυτό το μοντέλο πελάτη – εξυπηρετητή και υποστηρίζει τα πρωτόκολλα TCP και UDP.

Τα αποτελέσματα εμφανίζονται στην οθόνη του χρήστη. Για την συλλογή όγκου αποτελεσμάτων το NetPerf εκτελέσθηκε με ανακατεύθυνση του stdOut σε ένα text αρχείο. Το αρχείο αυτό υπέστη προετοιμασία, ώστε να μπορούν να εισαχθούν τα δεδομένα από την εφαρμογή που θα έκανε την επεξεργασία.

Netperf_Log_NETvsTTCP.txt - Σημειωματάριο				
Άρχειο	Επεξεργασία	Αναζήτηση	Βοήθεια	
8192	8192	8192	33.00	4067.12
8192	8192	8192	31.00	4329.60
8192	8192	8192	32.00	4194.26
8192	8192	8192	32.00	4194.22
8192	8192	8192	31.00	4329.55
8192	8192	8192	32.00	4194.24
8192	8192	8192	31.00	4329.59
8192	8192	8192	33.00	4067.28
8192	8192	8192	31.00	4329.60
8192	8192	8192	33.00	4067.20
8192	8192	8192	31.00	4329.58
8192	8192	8192	32.00	4194.22

Σχήμα 44 - Το Log File του NetPerf.

Δυστυχώς, στην περίπτωση αυτού του προγράμματος, δεν βρέθηκε ο πηγαίος κώδικας για πλατφόρμες Windows. Η έκδοση του NetPerf που χρησιμοποιήθηκε ήταν μια ήδη μεταγλωττισμένη έκδοση, που βρήκαμε στο διαδίκτυο.

- Κλήση από την Γραμμή Εντολών (Command Line).

Για το NetPerf χρησιμοποιήσαμε τις εξής εντολές:

Netserver

```
Netperf -fk -l116777216 -P0 -tTCP_STREAM -H195.251.252.72 >>
NetPerf_Log.txt
```

Δηλαδή:

- Output σε Kbits (-fk),
- 16777216 Bytes προς μετάδοση (16MBytes) (-l16777216),
- Τύπος του test (-tTCP_STREAM),
- Αποτελέσματα χωρίς επικεφαλίδες (αλλά μόνο του αριθμούς) -P0,
- To StdOut να γίνεται append σε αρχείο >> NetPerf_Log.txt.

8.3.2.3 iPerf.

Το τελευταίο εργαλείο που χρησιμοποιήσαμε ήταν το iPerf v1.1.1.

- **Ιστορικό – Έκδοση.**

Αναπτύχθηκε από το πανεπιστήμιο του Illinois, για να ξεπεράσει τις ατέλειες παλιότερων εργαλείων. Έτσι έχει επλογές για έλεγχο πολυμετάδοσης, μέτρηση Jitter και υποστηρίζει πολλαπλές συνδέσεις τόσο για τον Client όσο και για τον Server.

Η αλήθεια είναι πως το συγκεκριμένο εργαλείο είναι σαφώς πιο εξελιγμένο από τα δύο προηγούμενα.

- **Log Αρχεία.**

Τα αποτελέσματα του iPerf ήταν τα πιο δύσκολα από την πλευρά της επεξεργασίας. Χρειάστηκε πολύς χρόνος για να καθαρίσουμε τα Log αρχεία από το περιττό κείμενο, ώστε να έρθουν σε χρήσιμη μορφή. Οι δύο εικόνες που ακολουθούν είναι από ένα τέτοιο αρχείο πριν και μετά από την επεξεργασία.

```
iPerf_Rcv_Log.txt - Σημειωματάριο
Άρχισα Επεξεργασία Αναζήτηση Βοήθεια
-----
Server listening on TCP port 5001
TCP window size: 8.0 KByte (default)
-----
[112] local 195.251.252.72 port 5001 connected with 195.251.252.67 port 1033
[ ID] Interval Transfer Bandwidth
[112] 0.0-33.1 sec 16384 KBytes 3955 Kbits/sec
[112] local 195.251.252.72 port 5001 connected with 195.251.252.67 port 1034
[ ID] Interval Transfer Bandwidth
[112] 0.0-31.8 sec 16384 KBytes 4120 Kbits/sec
[112] local 195.251.252.72 port 5001 connected with 195.251.252.67 port 1035
[ ID] Interval Transfer Bandwidth
[112] 0.0-33.0 sec 16384 KBytes 3970 Kbits/sec
[112] local 195.251.252.72 port 5001 connected with 195.251.252.67 port 1036
[ ID] Interval Transfer Bandwidth
[112] 0.0-32.7 sec 16384 KBytes 4005 Kbits/sec
[112]
```

Σχήμα 45 - Log Αρχείο Του iPerf πριν από την Επεξεργασία.

Duration in Sec	Transfer Kbytes	Bandwidth Kbps
33.1 sec	16384 KBytes	3955 Kbits/sec
31.8 sec	16384 KBytes	4120 Kbits/sec
33.0 sec	16384 KBytes	3970 Kbits/sec
32.7 sec	16384 KBytes	4005 Kbits/sec
32.2 sec	16384 KBytes	3952 Kbits/sec
32.3 sec	16384 KBytes	4058 Kbits/sec
33.3 sec	16384 KBytes	3932 Kbits/sec
31.9 sec	16384 KBytes	4104 Kbits/sec
32.7 sec	16384 KBytes	4004 Kbits/sec
31.6 sec	16384 KBytes	4142 Kbits/sec
32.1 sec	16384 KBytes	4000 Kbits/sec
31.3 sec	16384 KBytes	4184 Kbits/sec
32.3 sec	16384 KBytes	4057 Kbits/sec

Σχήμα 46 - Το ίδιο Log Αρχείο Του iPerf, μετά από την Επεξεργασία.

- **Κλήση από την Γραμμή Εντολών (Command Line).**

Για το iPerf χρησιμοποιήσαμε τις εντολές:

```
Iperf -s >> iPerf_Rcv_Log.txt
Iperf -c195.251.252.72 -fk -n16M >> iPerf_Snd_Log.txt
```

Δηλαδή:

- Output σε Kbits (-fk),
- 16MBytes προς μετάδοση (-n16M),
- To StdOut να γίνεται append σε αρχείο >> iPerf_Rcv_Log.txt.

8.3.3 Αυτοματοποίηση των Πειραμάτων.

Όπως έχουμε ήδη αναφέρει, σε κάθε πείραμα παίρναμε 100 μετρήσεις. Αντί να καλούμε τον Client και τον Server από 100 φορές, διαδικασία που θα προκαλούσε καθυστέρηση, δημιουργήσαμε δύο Batch αρχεία. Με τα αρχεία αυτά, απλά βάζαμε την εκτέλεση σε μια επαναληπτική διαδικασία. Έτσι, με το τέλος μιας μέτρησης άρχιζε αμέσως η επόμενη.

Τα αρχεία αυτά ήταν, ουσιαστικά, δύο. Κάθε φορά που καλούσαμε διαφορετικό εργαλείο, απλά αλλάζαμε μια γραμμή στο batch αρχείο.

Το πρώτο ήταν το Rcv_NT.bat ή Snd_NT.bat και το χρησιμοποιήσαμε στα Windows 2000 και XP.

Σε αυτό υπήρχε η εντολή:

```
for /L %%i in (1, 1, %1) do Call_Tool
```

Επεξήγηση της εντολής:

- **for /L:** Η παράμετρος /L χρειάζεται ώστε η εντολή for να έχει την λειτουργία που έχει στις γλώσσες προγραμματισμού. Χωρίς αυτή την παράμετρο η for αυτή κάνει κάτι το εντελώς διαφορετικό,
- **%%i:** Ο μετρητής της for,
- **(1, 1, %1):** Αρχή – Βήμα – Λήξη της for,
- **%1:** Η πρώτη αριθμητική παράμετρος της γραμμής εντολών. Έτσι, γράφοντας Rcv_NT 100, η επανάληψη εκτελείται 100 φορές.
- **Call_Tool:** Εδώ έμπαινε η εντολή που καλεί το πρόγραμμα που επιθυμούμε, π.χ. PCATTCP -r.

Αυτό το Batch αρχείο θα ήταν υπεραρκετό για την δουλειά που το θέλαμε. Δυστυχώς, η παράμετρος /L της for, είναι διαθέσιμη σε αυτό που καλείται Windows NT Command Extensions. Με άλλα λόγια, σε περιβάλλοντα Windows 9x, η παράμετρος αυτή δεν είναι διαθέσιμη. Έτσι καταφύγαμε στην λύση του Send.bat.



Το αρχείο αυτό κάνει, ουσιαστικά την ίδια δουλειά, απλά δεν δέχεται παράμετρο που να καθορίζει το πλήθος των επαναλήψεων. Έτσι, όταν ο αριθμός των μετρήσεων ξεπέρναγε τις 100, απλά διακόπταμε την εκτέλεσή του.

Η λειτουργία του είναι πάρα πολύ απλή. Αρχικά εκτελείται το εργαλείο μέτρησης και μετά το πρόγραμμα συνεχίζει από την γραμμή :Loop, που είναι ένα απλό Label. Αυτή η επανάληψη δεν τελειώνει ποτέ.

```
Call_Tool
goto Loop
:Loop
Call_Tool
goto Loop
```

8.4 ΟΙ ΠΑΡΑΜΕΤΡΟΙ ΠΟΥ ΕΠΗΡΕΑΖΟΥΝ ΤΙΣ ΕΠΙΔΟΣΕΙΣ.

Όπως αναφέραμε και νωρίτερα στο κείμενο, εξετάσαμε την επίδραση που έχουν ορισμένες παράμετροι λειτουργίας, στις επιδόσεις του δικτύου.

Οι παράμετροι που ελέγχαμε μπορούν να χωριστούν σε πέντε κατηγορίες. Αυτές είναι:

- Τα Λειτουργικά Συστήματα.
- Οι Τοπολογίες.
- Τα Αντικείμενα της MIB.
- Η εναλλαγή Αποστολέα – Παραλήπτη.
- Η απόσταση μεταξύ των σταθμών και η ύπαρξη εμποδίων.

8.4.1 Λειτουργικά Συστήματα.

Όπως έχουμε αναφέρει, η τεχνολογία των ασύρματων τοπικών δικτύων είναι ακόμα πολύ νέα. Για αυτό τον λόγο δεν έχουν τελειοποιηθεί οι οδηγοί των καρτών δικτύου. Για τον λόγο αυτόν πιστέψαμε ότι σε κάποια λειτουργικά συστήματα οι επιδόσεις μπορεί να είναι καλύτερες ή χειρότερες. Αυτό προσπαθήσαμε να το ελέγχουμε με μια σειρά πειραμάτων.

Τα λειτουργικά συστήματα που ελέγχθηκαν ήταν:

- Microsoft Windows 98 Release 2.
- Microsoft Windows XP Professional.
- Microsoft Windows 2000 Professional.
- LINUX. Διανομή Debian 3.0, με πυρήνα 2.2 και όλα τα packages ενημερωμένα με τις τελευταίες εκδόσεις που υπήρχαν κατά την πραγματοποίηση των πειραμάτων.

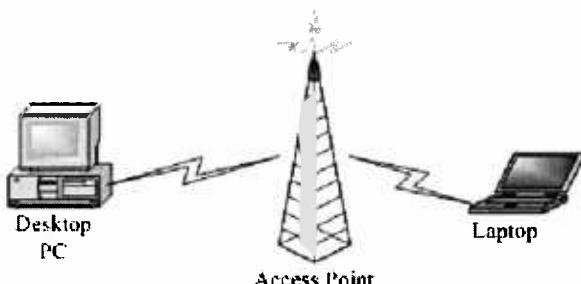
8.4.2 Τοπολογίες.

Μία άλλη σημαντική παράμετρος λειτουργίας είναι η τοπολογία, δηλαδή ο τρόπος με τον οποίο διασυνδέονται οι συσκευές. Θεωρήσαμε ότι διαφορετικές τοπολογίες θα είχαν σαν αποτέλεσμα διαφορετικές επιδόσεις.

Για να εξεταστεί η υπόθεση αυτή χρησιμοποιήθηκαν δύο διαφορετικές τοπολογίες.

8.4.2.1 Τοπολογία Wireless to Wireless (W/W).

Αυτή ήταν και η απλούστερη τοπολογία. Ελέγχθηκε ένα δίκτυο με δύο υπολογιστές εφοδιασμένους με ασύρματες κάρτες δικτύου. Οι υπολογιστές ήταν μέλη ενός Infrastructure Network και επικοινωνούσαν μέσω ενός Access Point



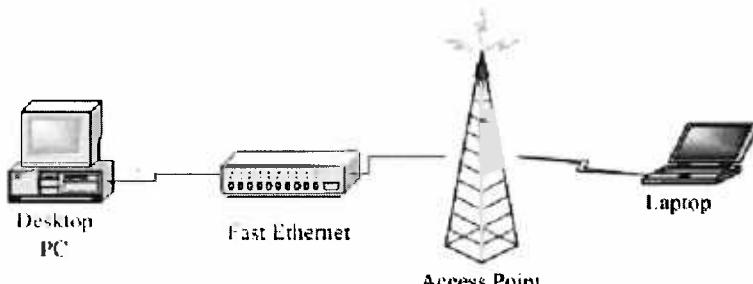
Σχήμα 47 - Τοπολογία 1, Wireless to Wireless.

8.4.2.2 Τοπολογία Wireless to Ethernet (W/E).

Στην δεύτερη τοπολογία, μετρήσαμε τις επιδόσεις στην επικοινωνία μεταξύ ενός σταθμού εφοδιασμένου με κάρτα ασύρματου δικτύου και ενός που ήταν μέλος ενός δικτύου τεχνολογίας Fast Ethernet.

Για να επιτευχθεί η επικοινωνία, το Access Point συνδέθηκε με το 802.3 δίκτυο μέσω του HUB και αποτέλεσε την γέφυρα μεταξύ των δύο υπολογιστών.

Οι δύο σταθμοί ανήκαν στο ίδιο IP υποδίκτυο.



Σχήμα 48 - Τοπολογία 2, Wireless to Ethernet.

Σε αυτή την περίπτωση έγιναν και τα περισσότερα πειράματα..

8.4.3 Ενδιαφέροντα Αντικείμενα της MIB.

Μία τρίτη παράμετρος, που θεωρήθηκε ότι θα μπορούσε να επηρεάσει τις επιδόσεις, αποτέλεσαν τα αντικείμενα της MIB των συσκευών IEEE 802.11. Πρόκειται, μάλιστα, για μια πολύ σημαντική παράμετρο, στην οποία δόθηκε ιδιαίτερη προσοχή.

Στο κείμενο που ακολουθεί αναφέρουμε τις παραμέτρους της MIB που θεωρήσαμε ως πιο ενδιαφέρουσες. Είναι κατηγοριοποιημένες, όπως και στο πρότυπο σε SMT, MAC και PHY ιδιότητες.

Αυτές ήταν και οι παράμετροι που μεταβάλλαμε κατά την διάρκεια του πειράματος. Κάποιες από αυτές δεν εξετάσθηκαν για λόγους που αναφέρονται μαζί με την επεξήγησή τους.

8.4.3.1 Station Management (SMT) Attributes.

- **dot11MediumOccupancyLimit {1.2.840.10036.1.1.1.2}.**

Ο μέγιστος αριθμός μονάδων χρόνου που ένας σταθμός μπορεί να ελέγχει το μέσο, όταν το δίκτυο βρίσκεται σε λειτουργία PCF. Δεν ελέγχθηκε γιατί ο εξοπλισμός δεν υποστήριζε Point Coordinator Function λειτουργικότητα.

- **dot11PrivacyOptionImplemented {1.2.840.10036.1.1.1.7}.**

Αν θα χρησιμοποιείται WEP 64, WEP 128 ή καθόλου WEP.

- **dot11BeaconPeriod {1.2.840.10036.1.1.1.12}.**

Καθορίζει την περίοδο σε (μονάδες χρόνου) η οποία μεσολαβεί ανάμεσα σε δύο διαδοχικές αποστολές Beacon μηνυμάτων.

8.4.3.2 MAC Attributes.

- **dot11RTSThreshold {1.2.840.10036.2.1.1.2}.**

Όταν αποστέλλεται ένα MAC protocol data unit μεγέθους κάτω από ένα όριο x, δεν γίνεται RTS/CTS handshake. Εδώ καθορίζεται ο αριθμός x. Αν αυτός τεθεί ίσος με 0, ενεργοποιείται το RTS/CTS handshake για όλα τα πακέτα τύπου DATA.

- **dot11FragmentationThreshold {1.2.840.10036.2.1.1.5}.**

Το μέγιστο μέγεθος MAC PDU που το επίπεδο MAC μπορεί να παραδώσει στο PHY επίπεδο. Αν το μέγεθος ξεπερνά αυτόν τον αριθμό, τότε το πλαίσιο κατακερματίζεται. Ο αριθμός αυτός σε καμία περίπτωση δεν μπορεί να είναι μικρότερος από 256, ούτε μεγαλύτερος από 2346. επίσης, δεν μπορεί να είναι μεγαλύτερος από την τιμή του αντικειμένου aMPDUMaxLength, που καθορίζει το μέγιστο μέγεθος MAC πλαισίου που μπορεί να παραδοθεί στο φυσικό επίπεδο. Κατά την εκτέλεση των πειραμάτων, θέσαμε αυτή την τιμή ίση με 256. Η διάρκεια μιας επανάληψης του πειράματος ήταν περίπου 30 δευτερόλεπτα. Μετά από αυτή την αλλαγή η μέση διάρκεια ανέβηκε στα 5

λεπτά. Θεωρήσαμε ότι με την εκτέλεση αυτού του πειράματος δεν θα είχαμε να αποδείξουμε τίποτα εκτός από το προφανές.

8.4.3.3 PHY Attributes.

- **dot11CurrentTxPowerLevel {1.2.840.10036.4.3.1.10}.**

Η ισχύς λειτουργίας της κεραίας. Στην MIB υπάρχουν μέχρι οχτώ αντικείμενα που αντιστοιχούν ένα σε κάθε επίπεδο ισχύος της κεραίας. Εδώ αποθηκεύεται ποιο επίπεδο ισχύος θα χρησιμοποιείται. Το Access Point έχει μόνο ένα επίπεδο έντασης στο οποίο εκπέμπει η κεραία. Έτσι δεν μπορούσαμε να επέμβουμε στην παράμετρο αυτή.

- **dot11CurrentCCAMode {1.2.840.10036.4.5.1.3}.**

Ελέγχει αν χρησιμοποιείται Energy Detect ή Carrier Sense ή και τα δύο (DSSS). Ο εξοπλισμός που είχαμε είχε μόνο την επιλογή να χρησιμοποιούνται και οι δύο τρόποι λειτουργίας.

8.4.4 Εναλλαγή Αποστολέα – Παραλήπτη.

Θελήσαμε να διαπιστώσουμε αν έχει σημασία ποιος από τους δύο σταθμούς αποστέλλει και ποιος λαμβάνει τα δεδομένα.

Πιστέψαμε πως αν μετά το τέλος ενός πειράματος, το επαναλαμβάναμε, απλά εναλλάσσοντας τον ρόλο των δύο μηχανημάτων, έτσι ώστε ο αποστολέας να γίνει παραλήπτης, τα αποτελέσματα θα ήταν διαφορετικά.

Αυτή ήταν και η πέμπτη παράμετρος που εξετάστηκε.

8.4.5 Η Απόσταση Μεταξύ των Σταθμών και η Ύπαρξη Εμποδίων.

Ήταν και η τελευταία παράμετρος που εξετάστηκε. Θελήσαμε να μάθουμε αν η καθυστέρηση είναι ανάλογη με την απόσταση που χωρίζει τους δύο υπολογιστές.

Για τον λόγο αυτό πήραμε μια ομάδα μετρήσεων και, στην συνέχεια, απομακρύναμε τους δύο υπολογιστές και επαναλάβαμε τις μετρήσεις.

9 ΣΤΑΤΙΣΤΙΚΟ ΥΠΟΒΑΘΡΟ.

Για την ανάλυση των μετρήσεων που πήραμε από τα πειράματα, χρησιμοποιήσαμε, όπως αναφέρεται και στην εισαγωγή, δύο ευρέως διαδεδομένες στατιστικές μεθόδους. Η πρώτη ήταν το t – test και η δεύτερη η Ανάλυση Διακύμανσης (Analysis Of Variance – AN.O.VA.)

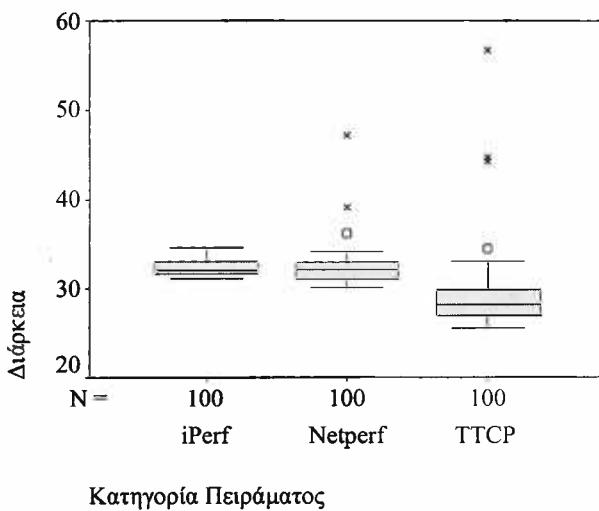
Στο κεφάλαιο αυτά θα κάνουμε μια σύντομη αναφορά στην θεωρία του ελέγχου στατιστικών υποθέσεων. Στην συνέχεια θα περιγράψουμε τις δύο αυτές μεθόδους. Θα επικεντρώσουμε το ενδιαφέρον μας, κυρίως, στο τι κάνουν αυτές οι μέθοδοι και τι συμπεράσματα μπορούμε να βγάλουμε από αυτές. Αυτό γιατί κατά την διάρκεια της στατιστικής επεξεργασίας των αποτελεσμάτων, οι δύο αυτές μέθοδοι χρησιμοποιήθηκαν κατά κόρον. Επίσης, θα αναφερθούμε σύντομα σε έναν τύπο διαγράμματος που ονομάζεται BoxPlot και που θα μας φανεί πολύ χρήσιμος στην συνέχεια.

9.1 BOXPLOTS.

Ένα διάγραμμα που χρησιμοποιείται πολύ συχνά είναι το BoxPlot.

Ένα BoxPlot έχει την πολύ χρήσιμη ιδιότητα, ότι μπορεί να μας περιγράψει, συνοπτικά, τον μέσο μιας μεταβλητής, την διασπορά της γύρω από τον μέσο και να μας αναδείξει διαταρακτικές και ακραίες τιμές.

Παρακάτω έχουμε ένα παράδειγμα BoxPlot. Ουσιαστικά πρόκειται για τρία διαγράμματα, ένα για κάθε υποκατηγορία της μεταβλητής που μελετάμε.



Κατηγορία Πειράματος

Σχήμα 49 - Παράδειγμα BoxPlot.

Για κάθε κατηγορία, στο γκρι ορθογώνιο, βρίσκεται το μεσαίο 50% των μετρήσεων, δηλαδή το Ενδοτεταρτημοριακό Εύρος (Interquartile Range – IR).

Η ενδιάμεση μαύρη ευθεία αντιπροσωπεύει την διάμεσο των τιμών (Median).

Οι δύο παράλληλες ευθείες αντιπροσωπεύουν την μέγιστη και ελάχιστη τιμή, που δεν είναι διαταρακτική (Outlier) ή ακραία (Extreme), της μεταβλητής.

Αν η απόσταση μιας τιμής, από την μέγιστη του IR, προς τα πάνω, είναι μεγαλύτερη από 1.5 φορές το IR, τότε, αυτή η τιμή, θεωρείται Outlier. Αν η απόσταση είναι μεγαλύτερη από 3 φορές το IR, η τιμή θεωρείται ακραία. Αντίστοιχα ισχύουν και για τις τιμές που είναι μικρότερες από το ελάχιστο του IR.

9.2 ΚΕΝΤΡΙΚΟ ΟΡΙΑΚΟ ΘΕΩΡΗΜΑ.

Έστω ότι έχουμε n τυχαίες μεταβλητές X_1, X_2, \dots, X_n που ακολουθούν την ίδια κατανομή και είναι και ανεξάρτητες ανά δύο.

Η κατανομή της τυχαίας μεταβλητής $\frac{\bar{X} - \mu}{\sigma/\sqrt{n}}$ ακολουθεί τυποποιημένη κανονική

κατανομή όταν $n \rightarrow +\infty$.

Αυτό το θεώρημα θα χρειαστεί στην συνέχεια, όταν χρειαστεί να μελετήσουμε την συμπεριφορά μη κανονικών πληθυσμάν.

9.3 ΕΛΕΓΧΟΣ ΣΤΑΤΙΣΤΙΚΩΝ ΥΠΟΘΕΣΕΩΝ.

Έστω ότι έχουμε έναν πληθυσμό και μια τυχαία μεταβλητή X η οποία εκφράζει μια παράμετρο του πληθυσμού αυτού. Παίρνοντας ένα τυχαίο δείγμα από αυτόν τον πληθυσμό, θέλουμε να ελέγξουμε αν ευσταθεί μια υπόθεση για την τιμή τις παραμέτρου του πληθυσμού.

Για παράδειγμα αναφέρουμε τον πληθυσμό των Ελλήνων που φοιτούν στο τμήμα πληροφορικής του Οικονομικού Πανεπιστημίου Αθηνών. Με βάση ένα δείγμα από αυτούς, θέλουμε να ελέγξουμε αν ο μέσος όρος της διάρκειας φοίτησης είναι 5 χρόνια ή όχι. Σε αυτή την περίπτωση, ο πληθυσμός είναι όλοι οι φοιτητές του εν λόγω τμήματος και η παράμετρος – τυχαία μεταβλητή – είναι η διάρκεια φοίτησης. Η υπόθεση που κάνουμε είναι ότι η μέση διάρκεια φοίτησης είναι 5 έτη.

9.3.1 Στατιστική Υπόθεση.

Το σύνολο των δυνατών τιμών που μπορεί να πάρει η παράμετρος ονομάζεται Παραμετρικός Χώρος και τον συμβολίζουμε με Θ . Έστω δύο υποσύνολα Θ_0 και Θ_1 του παραμετρικού χώρου, ξένα μεταξύ τους και, κατά κανόνα, συμπληρωματικά. Μια στατιστική υπόθεση δεν είναι τίποτε άλλο από μια παραδοχή ότι η παράμετρος Θ ανήκει στο Θ_0 και όχι στο Θ_1 . Η παραδοχή αυτή καλείται υπόθεση μηδέν ή μηδενική υπόθεση και

συμβολίζεται με H_0 , ενώ η αντίθετη προς αυτήν καλείται εναλλακτική και συμβολίζεται με H_1 . Έτσι λοιπόν, ένα πρόβλημα ελέγχου το συμβολίζουμε ως εξής:

$$H_0 : \Theta \in \Theta_0$$

vs

$$H_1 : \Theta \in \Theta_1$$

Τύπος 4 - Συμβολισμός Προβλήματος Ελέγχου.

9.3.2 Έλεγχος (Test).

Ένας έλεγχος είναι μια διαδικασία η οποία, με βάση ένα δείγμα μας επιτρέπει να απορρίψουμε ή να μην απορρίψουμε την H_0 εναντίον της εναλλακτικής H_1 .

Ουσιαστικά, αυτό που κάνουμε είναι να υπολογίσουμε την αντίστοιχη παράμετρο του δείγματος. Η παράμετρος αυτή ονομάζεται δειγματική παράμετρος και μπορεί να πάρει διάφορες τιμές. Για αυτό τον λόγο είναι μια τυχαία μεταβλητή, σε αντίθεση με την πληθυσμιακή παράμετρο η οποία είναι μια σταθερά αλλά άγνωστη. Ανάλογα με την τιμή της δειγματικής παραμέτρου, αποφασίζουμε αν δεχόμαστε την υπόθεση που έχουμε κάνει για την πληθυσμιακή.

Πιο συγκεκριμένα, καλούμε δειγματικό χώρο το σύνολο των πιθανών τιμών της δειγματικής παραμέτρου. Επίσης καλούμε κρίσιμη περιοχή, ένα υποσύνολο του δειγματικού χώρου. Αν η δειγματική παράμετρος πάρει μια τιμή που ανήκει στην κρίσιμη περιοχή τότε δεν απορρίπτουμε την μηδενική υπόθεση. Αν η δειγματική παράμετρος παρατηρηθεί εκτός της κρίσιμης περιοχής, τότε απορρίπτουμε την μηδενική έναντι της εναλλακτικής υπόθεσης.

Έτσι, ουσιαστικά, για να κάνουμε ένα Test, το πρόβλημα ανάγεται στον διαχωρισμό του δειγματικού χώρου σε κρίσιμη περιοχή και περιοχή απόρριψης. Μετά, το αποτέλεσμα είναι αυτόματο, αφού αρκεί να υπολογίσουμε την δειγματική τιμή της παραμέτρου και να την δούμε σε ποια από τις δύο περιοχές ανήκει.

9.3.3 Σφάλματα και Επίπεδο Σημαντικότητας.

Όπως και να διαχωρίσουμε τον δειγματικό χώρο σε κρίσιμη περιοχή και περιοχή απόρριψης, υπάρχει το ενδεχόμενο να διαπράξουμε δύο ειδών σφάλματα.

1. Σφάλμα Τύπου I.

Να απορρίψουμε την μηδενική υπόθεση ενώ αυτή είναι ορθή.

2. Σφάλμα Τύπου II.

Να μην απορρίψουμε την μηδενική υπόθεση ενώ αυτή είναι εσφαλμένη.

Επειδή είναι αδύνατον να μηδενίσουμε την πιθανότητα να διαπράξουμε κάποιο σφάλμα και επειδή, στην πράξη, η μείωση της πιθανότητας να διαπράξουμε σφάλμα του

ενός τύπου ισοδυναμεί με την αύξηση της πιθανότητας να διαπράξουμε σφάλμα του άλλου τύπου κάνουμε το εξής: Ωέτουμε ως περιορισμό η πιθανότητα να διαπράξουμε σφάλμα τύπου I να είναι μικρότερη ή ίση με έναν αριθμό α . Με αυτόν τον περιορισμό επιλέγουμε τον διαχωρισμό του δειγματικού χώρου κατά τέτοιον τρόπο ώστε να ελαχιστοποιείται η πιθανότητα σφάλματος τύπου II.

Ο αριθμός α , δηλαδή η πιθανότητα να διαπράξουμε σφάλμα τύπου I ονομάζεται επίπεδο σημαντικότητας.

9.4 T – TEST.

Το T – test είναι ένας έλεγχος που μας βοηθάει στην περίπτωση που έχουμε να ελέγξουμε υποθέσεις σχετικά με την διαφορά των μέσων δύο κανονικών πληθυσμών, όταν οι διακυμάνσεις των πληθυσμών αυτών είναι άγνωστες.

Συγκεκριμένα έχουμε τους πληθυσμούς $N_1(\mu_1, \sigma_1^2)$ και $N_2(\mu_2, \sigma_2^2)$, δηλαδή δύο πληθυσμούς που ακολουθούν κανονική κατανομή με μέσο μ και διακύμανση σ^2 .

Θέλουμε να ελέγξουμε την υπόθεση H_0 εναντίον της εναλλακτικής H_1 , όπου:

$$H_0 : \mu_1 - \mu_2 = 0$$

vs

$$H_1 : \mu_1 - \mu_2 \neq 0$$

Τύπος 5 - Διατύπωση Στατιστικής Υπόθεσης.

Για να το πετύχουμε, αρχικά παίρνουμε δύο τυχαία δείγματα, μεγέθους n_1 και n_2 , από τους πληθυσμούς και υπολογίζουμε για το καθένα το δειγματικό μέσο. Για το δείγμα από τον πρώτο πληθυσμό αυτός είναι:

$$\bar{X}_1 = \frac{1}{n_1} \cdot \sum_{i=1}^{n_1} x_i$$

Τύπος 6 - Ο Δειγματικός Αριθμητικός Μέσος.

και αντίστοιχα για τον δεύτερο.

Το γεγονός ότι οι διακυμάνσεις μας είναι άγνωστες, μας αναγκάζει να χρησιμοποιήσουμε τις εκτιμήσεις τους, S_1^2 και S_2^2 ως εξής:

$$S_1^2 = \frac{1}{n_1 - 1} \cdot \sum_{i=1}^{n_1} (x_i - \bar{X}_1)^2$$

Τύπος 7 - Η Δειγματική Διακύμανση.

Η συνάρτηση:

$$\frac{(\bar{X}_1 - \bar{X}_2) - (\mu_1 - \mu_2)}{\sqrt{\frac{S_1^2}{n_1} + \frac{S_2^2}{n_2}}}$$

Τύπος 8 - Μία Τυχαία Μεταβλητή που Ακολουθεί Κατανομή Student.

ακολουθεί κατανομή του Student με $n_1 + n_2 - 2$ βαθμούς ελευθερίας.

Έτσι, υπό την υπόθεση H_0 , η ποσότητα:

$$t' = \frac{\bar{X}_1 - \bar{X}_2}{\sqrt{\frac{S_1^2}{n_1} + \frac{S_2^2}{n_2}}}$$

ακολουθεί και αυτή κατανομή του Student με $n_1 + n_2 - 2$ βαθμούς ελευθερίας.

Έχοντας υπολογίσει ήδη τις απαραίτητες ποσότητες, μπορούμε να υπολογίσουμε την τιμή του t' .

Επίσης, από τους πίνακες της κατανομής Student με $n_1 + n_2 - 2$ βαθμούς ελευθερίας υπολογίζουμε τον αριθμό t_a τέτοιον ώστε $P(t \geq t_a) = \alpha/2$.

Το τελικό συμπέρασμα που βγάζουμε από το test είναι ότι:

- Αν $|t'| \geq |t_a|$ τότε απορρίπτουμε την H_0 .
- Αν $|t'| \leq |t_a|$ τότε δεν απορρίπτουμε την H_0 .

Κατά πλήρη αντιστοιχία με τα παραπάνω, δεν απορρίπτουμε την υπόθεση H_0 αν και μόνο αν ισχύει:

$$(\bar{X}_1 - \bar{X}_2) - t_a \cdot \sqrt{\frac{S_1^2}{n_1} + \frac{S_2^2}{n_2}} \leq 0 \leq (\bar{X}_1 - \bar{X}_2) + t_a \cdot \sqrt{\frac{S_1^2}{n_1} + \frac{S_2^2}{n_2}}$$

Τύπος 9 - Προϋπόθεση για την Ισότητα δύο Πληθυσμιακών Μέσων.

9.4.1 T – test για μη κανονικούς πληθυσμούς.

Όλα τα παραπάνω ισχύουν για την περίπτωση που μελετάμε δύο κανονικούς πληθυσμούς.

Στην περίπτωση μη κανονικών πληθυσμών, η ίδια ποσότητα t' προσεγγίζει ικανοποιητικά την κατανομή Student, αρκεί να έχουμε μεγάλα μεγέθη δείγματος. Αυτό γιατί ισχύει το κεντρικό οριακό θεώρημα. Επιπλέον, αν τα μεγέθη των δύο δειγμάτων, πέρα από μεγάλα, είναι και ίσα, δηλαδή αν $n_1 = n_2$, η προσέγγιση στην κατανομή Student είναι σχεδόν άριστη.

Πρακτικά όταν οι βαθμοί ελευθερίας είναι περισσότεροι από 30, δηλαδή όταν $n_1 + n_2 \geq 32$, ακολουθούμε ακριβώς την παραπάνω διαδικασία, χωρίς καμία μεταβολή.

Για να δούμε τα παραπάνω στην πράξη θα καταφύγουμε σε ένα παράδειγμα. Παραθέτουμε έναν πίνακα με αποτελέσματα ενός t – test.

Διάρκεια	Independent Samples Test									
	Levene's Test		t-test for Equality of Means						95% Confidence Interval of the Difference	
	F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper	
Equal variances	137.030	.000	30.428	198	.000	20.29104	.66686	18.97598	21.60610	
UnEqual variances			30.428	101.362	.000	20.29104	.66686	18.96822	21.61386	

Πίνακας 14 - Παράδειγμα Αποτελεσμάτων T - test.

Το πρώτο που παρατηρούμε είναι ότι πριν γίνει το test εκτελείται ένα test Levene, ομοιογένειας διακυμάνσεων. Το test αυτό επεξηγείται παρακάτω σε αυτό το κεφάλαιο. Ανάλογα με το αποτέλεσμά του, κοιτάμε την πρώτη ή την δεύτερη γραμμή αποτελεσμάτων του t – test.

Σε οποιαδήποτε περίπτωση, η μηδενική υπόθεση είναι απορριπτέα, αν το 95% διάστημα εμπιστοσύνης για την διαφορά των μέσων, δεν περιέχει την τιμή 0. Το ίδιο ισχύει αν η τιμή του πεδίου Sig. είναι μικρότερη από 0.05.

Συνεπώς, στην συγκεκριμένη περίπτωση, είτε θεωρήσουμε ίσες διακυμάνσεις στις δύο κατηγορίες, είτε όχι, η μηδενική υπόθεση την οποία ελέγχουμε πρέπει να απορριφθεί.

9.5 ΑΝΑΛΥΣΗ ΔΙΑΚΥΜΑΝΣΗΣ (ANALYSIS OF VARIANCE – AN.O.V.A.).

Η μέθοδος αυτή είναι μια στατιστική μέθοδος που, όπως και το T – test, μας βοηθά να ελέγξουμε την στατιστική υπόθεση ότι οι μέσοι κάποιων πληθυσμών είναι ίσοι. Η διαφορά της από το t – test είναι ότι, ενώ το πρώτο αναφέρεται αυστηρώς σε δύο πληθυσμούς, η AN.O.VA. αναφέρεται σε κ διαφορετικούς πληθυσμούς.

9.6 ONE – WAY KAI MULTI WAY AN.O.VA.

Οι πληθυσμοί αυτοί μπορεί να προέρχονται από έναν αρχικό πληθυσμό, χωρισμένο σε κ μέρη, με βάση η διαφορετικές ομάδες ενός χαρακτηριστικού. Για παράδειγμα, έχουμε έναν πληθυσμό χοιριδίων που χωρίζεται σε τρία μέρη και το καθένα εκτρέφεται με διαφορετική τροφή. Στην παραπάνω περίπτωση, ο πληθυσμός είναι τα χοιρίδια και χωρίζεται σε τρεις υπό – πληθυσμούς, έναν για κάθε είδος τροφής. Μετά από κάποιο χρονικό διάστημα μετράμε την αύξηση του βάρους 10 χοιριδίων από κάθε ομάδα. Με AN.O.VA. μπορούμε να συμπεράνουμε αν η αύξηση του βάρους επηρεάζεται ή όχι από το είδος τροφής.

Οι πληθυσμοί μπορεί και να προέρχονται από διαχωρισμό με βάση περισσοτέρων του ενός χαρακτηριστικών. Και αυτή η περίπτωση αντιμετωπίζεται με Ανάλυση Διακύμανσης αρκεί να μην μας ενδιαφέρει η επίδραση του κάθε παράγοντα ξεχωριστά.

Η περίπτωση που αναφέρεται στις προηγούμενες παραγράφους ονομάζεται Ανάλυση Διακύμανσης κατά έναν Παράγοντα (One – Way AN.O.VA.). Αν ο διαχωρισμός των πληθυσμών γίνει με βάση περισσότερα χαρακτηριστικά και μας ενδιαφέρει ξεχωριστά η επίδραση του καθενός από αυτά τότε μιλάμε για Multi – Way AN.O.VA. ή M.AN.O.VA.

Ειδική περίπτωση της M.AN.O.VA. είναι η Ανάλυση Διακύμανσης κατά δύο Παράγοντες (Two – Way AN.O.VA.). Αν, για παράδειγμα, τα παραπάνω χοιρίδια, εκτός από τις 3 διαφορετικές κατηγορίες τροφής, εκτρέφονταν και σε 5 διαφορετικές γεωγραφικές περιοχές, τότε θα είχαμε $3 \times 5 = 15$ διαφορετικούς πληθυσμούς. Αν θέλαμε να εκτιμήσουμε την επίδραση, στην μέση ανέηση βάρους, ξεχωριστά του είδους τροφής και ξεχωριστά της γεωγραφικής περιοχής, θα μπορούσαμε να χρησιμοποιήσουμε Ανάλυση Διακύμανσης κατά δύο Παράγοντες.

Γενικά, η AN.O.VA. είναι μια επώδυνη, υπολογιστικά, διαδικασία. Αυτή η δυσκολία αυξάνεται γεωμετρικά, όσο αυξάνει ο αριθμός των παραγόντων. Εμείς, για τους σκοπούς της παρούσας εργασίας, καλυπτόμαστε από την απλή περίπτωση κατά έναν παράγοντα την οποία θα περιγράψουμε παρακάτω.

9.6.1 Ανάλυση Διακύμανσης κατά Έναν Παράγοντα.

Έστω ότι έχουμε k πληθυσμούς και θέλουμε να ελέγξουμε την στατιστική υπόθεση

$$H_0 : \mu_1 = \mu_2 = \dots = \mu_k.$$

Δηλαδή επιθυμούμε να ελέγξουμε την υπόθεση ότι οι μέσοι των k κ πληθυσμών δεν διαφέρουν, στατιστικώς σημαντικά, μεταξύ τους.

Για να πραγματοποιήσουμε τον έλεγχο κάνουμε τα εξής.

Παίρνουμε k δείγματα μεγέθους $n_1, n_2, \dots, n_k : n_1 + n_2 + \dots + n_k = n$.

Επιλέγουμε ένα επίπεδο σημαντικότητας α .

Η ποσότητα

$$F' = \frac{\left(R_i^2 - R_o^2 \right) / k - 1}{R_o^2 / n - k}$$

Τύπος 10 - Μια Τυχαία Μεταβλητή που Ακολουθεί Κατανομή F.

ακολουθεί κατανομή F του Snedecor με ζεύγος βαθμών ελευθερίας $(k - 1, n - k)$.

Οι παράγοντες R_0^2 και R_I^2 μπορούν να υπολογιστούν πολύ εύκολα από τα δειγματικά δεδομένα που έχουμε μετρήσει. Έτσι η ποσότητα αυτή είναι υπολογίσιμη.

Στην συνέχεια, από τους πίνακες της κατανομής F, με ζεύγος βαθμών ελευθερίας $(k - I, n - k)$, υπολογίζουμε τον αριθμό f_a τέτοιον ώστε $P(F \geq f_a) = a$.

Απορρίπτουμε την H_0 αν και μόνο αν $F > f_a$. Σε αντίθετη περίπτωση δεν την απορρίπτουμε.

Κατά πλήρη αναλογία απορρίπτουμε την μηδενική υπόθεση αν και μόνο αν για το επίπεδο σημαντικότητας του test ισχύει $a' < a$, όπου η a' εκλέγεται από τους ίδιους πίνακες και είναι τέτοια ώστε $P(F > F') = a'$.

Αν θέλουμε να δούμε ένα παράδειγμα, μπορούμε να αναφέρουμε την υπόθεση 1 που θα αναλυθεί παρακάτω. Ο πίνακας περιέχει τα αποτελέσματα της μεθόδου.

AN.O.V.A.					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	696.679	2	348.339	49.849	0.000
Within Groups	2075.396	297	6.988		
Total	2772.075	299			

Πίνακας 15 - Παράδειγμα Ανάλυσης Διακύμανσης.

Η τιμή στο πεδίο Sig είναι η τιμή a' , δηλαδή το επίπεδο σημαντικότητας του test. Αν κάνουμε AN.O.VA. με επίπεδο σημαντικότητας 5%, η τιμή αυτή είναι μικρότερη και η μηδενική υπόθεση απορρίπτεται.

9.6.2 Ομογένεια Διακυμάνσεων και Post – Hoc Έλεγχοι.

Αν απορρίψουμε την μηδενική υπόθεση, δυστυχώς, δεν μπορούμε να ξέρουμε ποια από τις ισότητες δεν ισχύει. Για παράδειγμα αν $\mu_3 \neq \mu_7$, η στατιστική μέθοδος απλά θα μας οδηγήσει σε απόρριψη της H_0 , χωρίς να μας αποκαλύψει την λεπτομέρεια αυτή. Για να αποκτήσουμε αυτή την πληροφορία, πρέπει να εκτελέσουμε κάποια Post – Hoc ανάλυση, όπως το test των Games – Howell. Το test αυτό, χρησιμοποιεί τα αποτελέσματα της AN.O.V.A. και μας απαντάει στην ερώτηση “Ποια ζεύγη μέσων διαφέρουν στατιστικά σημαντικά;”.

Υπάρχει μεγάλη ποικιλία Post – Hoc test. Καθένα από αυτά ανήκει σε μία από δύο κατηγορίες. Αν οι διακυμάνσεις των ομάδων της AN.O.VA. μπορούν να θεωρηθούν ίσες, επιλέγουμε Post – Hoc test από την πρώτη κατηγορία. Ένα τέτοιο test είναι το test Turkey's Honestly Significant Difference. Αν οι διακυμάνσεις δεν μπορούν να θεωρηθούν ίσες μεταξύ των ομάδων, τότε επιλέγουμε κάποιο test από την δεύτερη κατηγορία. Ένα τέτοιο είναι το test των Games – Howell, που αναφέραμε.

Για να διαπιστώσουμε την ισχύ της ισότητας των διακυμάνσεων, εκτελούμε ένα test που ονομάζεται Homogeneity of Variances του Levene.

Test of Homogeneity of Variances			
Levene Statistic	df1	df2	Sig.
13.824	2	297	.001

Πίνακας 16 - Ομογένεια Διακυμάνσεων του Levene.

Αν η τιμή Sig. είναι μικρότερη από 0.05, τότε θεωρούμε διαφορετικές διακυμάνσεις. Άλλιως μπορούμε να τις θεωρήσουμε ίσες.

Στη συνέχεια, στην περίπτωση των διαφορετικών διακυμάνσεων εκτελούμε Games – Howell.

Multiple Comparisons						
Games-Howell		Mean	Std. Error	Sig.	95% Confidence Interval	
(I) Κατηγορία	(J) Κατηγορία	Πειράματος	Πειράματος	Difference (I-J)	Lower Bound	Upper Bound
iPerf	Netperf		-.027	.3738	.991	-.5271
	TTCP		3,219 *	.3738	.000	2.2373
Netperf	iPerf		,027	.3738	.991	-.4731
	TTCP		3,246 *	.3738		2.1898
TTCP	iPerf		-3,219 *	.3738	.000	-4.2009
	Netperf		-3,246 *	.3738		-4.3023

* The mean difference is significant at the .05 level.

Πίνακας 17 - Παράδειγμα test Games – Howell.

Για κάθε ζεύγος κατηγοριών, θεωρούμε ότι ισχύει η ισότητα των μέσων, αν και μόνο αν το 95% διάστημα εμπιστοσύνης, που αναγράφεται στον πίνακα περιέχει την τιμή 0. έτσι μπορούμε να καταλήξουμε σε συμπέρασμα σχετικά με το ποιών κατηγοριών οι μέσοι μπορούν να θεωρηθούν ίσοι και ποιών όχι. Σε αντίστοιχα συμπεράσματα και με αντίστοιχο τρόπο καταλήγουμε και με το test του Levene.

10 Η ΠΡΑΓΜΑΤΟΠΟΙΗΣΗ ΤΩΝ ΜΕΤΡΗΣΕΩΝ.

Στο κεφάλαιο αυτό περιγράφουμε, μέχρι την τελευταία λεπτομέρεια, τα πειράματα που κάναμε για να εξετάσουμε την επίδραση των πέντε παραμέτρων που αναφέραμε προηγουμένως. Επίσης εξετάζουμε κατά πόσο, κάτω από τις ίδιες συνθήκες, διαφορετικά εργαλεία αναφέρουν διαφορετικά αποτελέσματα.

Σε κάθε περίπτωση, διατυπώνουμε μια στατιστική υπόθεση, περιγράφουμε την τοπολογία, τον εξοπλισμό και το εργαλείο που χρησιμοποιήσαμε. Κατόπιν, παραθέτουμε ορισμένα μεγέθη και διαγράμματα περιγραφικής στατιστικής και κάποια σχόλια πάνω σε αυτά, που μας δίνουν μια αρχική εικόνα της κατάστασης. Τέλος, πραγματοποιούμε τον έλεγχο της στατιστικής υπόθεσης, αιτιολογώντας την επιλογή του συγκεκριμένου test και σχολιάζοντας τα αποτελέσματα.

Καθ' όλη την διάρκεια του κεφαλαίου, αναφερόμαστε σε κάποιους αριθμούς πειραμάτων. Οι αριθμοί αυτοί συνοψίζονται, σε μορφή πίνακα, στο τέλος αυτού του κεφαλαίου, μαζί με τα βασικά χαρακτηριστικά του κάθε πειράματος.

Πριν, όμως, από όλα τα παραπάνω, αναφέρουμε κάποιους ορισμούς για την αποσαφήνιση των όρων Υπόθεση – Πείραμα – Μέτρηση. Επίσης, ορίζουμε κάποια βασικά, περιγραφικά, στατιστικά μεγέθη που θα χρησιμοποιήσουμε σε όλη την διάρκεια του κεφαλαίου.

10.1 ΥΠΟΘΕΣΗ – ΠΕΙΡΑΜΑ – ΜΕΤΡΗΣΗ.

Οι τρεις όροι, Υπόθεση, Πείραμα και Μέτρηση χρησιμοποιούνται συνεχώς, σε όλη την έκταση αυτού του κειμένου. Θεωρούμε απαραίτητο να δοθεί σαφής εξήγηση της σημασίας τους και της, μεταξύ τους, συσχέτισης.

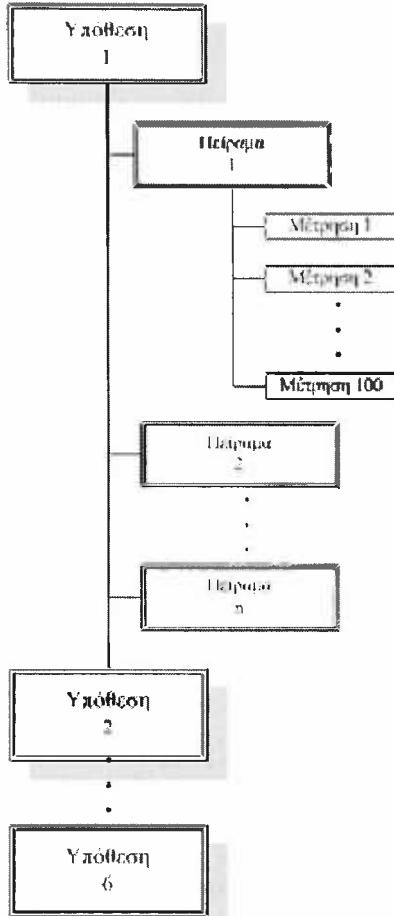
Υπόθεση αποκαλούμε μια στατιστική υπόθεση. Κάθε μία από τις παραμέτρους του συστήματος, της οποίας την επίδραση θέλουμε να ελέγξουμε, αντιστοιχεί σε μία ακριβώς υπόθεση. Συνεπώς το πλήθος των υποθέσεων είναι έξι.

Για τον έλεγχο μιας υπόθεσης επιλέγουμε έναν αριθμό πειραμάτων. Σε καθένα από αυτά αλλάζει μία μόνο παράμετρος του συστήματος.

Κατά την διάρκεια ενός πειράματος, εκτελούμε συνεχείς μετρήσεις, πάντα κάτω από τις ίδιες συνθήκες. Μία μέτρηση αποτελείται από μια TCP σύνδεση μεταξύ πελάτη και εξυπηρετητή, για μια μεταφορά δεδομένων μεγέθους 16MByte. Για κάθε μέτρηση μετριέται η ρυθμοαπόδοση και η καθυστέρηση. Ένα πείραμα ολοκληρώνεται με την επιτυχή ολοκλήρωση 100 επιτυχών μετρήσεων, δηλαδή με την ολοκλήρωση 100 μεταφορών των 16MByte.

Αν μια μέτρηση διακοπεί, για κάποιον λόγο, πριν την ολοκλήρωση της μεταφοράς αυτής της ποσότητας δεδομένων, θεωρείται άκυρη και επαναλαμβάνεται.

Έτσι, η συσχέτιση των παραπάνω εννοιών απεικονίζεται στο παρακάτω διάγραμμα.



Σχήμα 50 - Υπόθεση - Πείραμα - Μέτρηση.

10.2 ΤΑ ΣΤΑΤΙΣΤΙΚΑ ΜΕΓΕΘΗ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΗΘΗΚΑΝ.

Για την εκτίμηση της ισχύος ή μη, των υποθέσεων που κάναμε, βασιστήκαμε σε ορισμένα στατιστικά μεγέθη. Τα μεγέθη αυτά περιγράφουμε ευθύς αμέσως, πριν προχωρήσουμε στην περαιτέρω περιγραφή των υποθέσεων.

1. Ο Αριθμός n :

Το πλήθος των μετρήσεων που παίρνουμε από κάθε εκτέλεση ενός πειράματος. Για παράδειγμα αν εκτελέσουμε το TCP 100 φορές, τότε $n=100$.

2. Ο Αριθμός i :

Ο αύξων αριθμός της μέτρησης μέσα στο ίδιο πείραμα. Προφανώς θα ισχύει:

$$i = \{1, \dots, n\}$$

3. Καθυστέρηση Μέτρησης D_i :

Ο χρόνος που χρειάστηκε για την ολοκλήρωση της i -οστής μέτρησης.

4. Μέση (Mean) Καθυστέρηση Πειράματος \bar{D}_{exNo} :

$$\bar{D}_{exNo} = \frac{l}{n} \cdot \sum_{i=1}^n D_i$$

Τύπος 11 - Μέση Καθυστέρηση Πειράματος.

Όπου $exNo$ ο αριθμός του πειράματος με βάση τον παρακάτω πίνακα.

5. Διακύμανση (Variance) Καθυστέρησης Πειράματος S^2_{DexNo} :

$$S^2_{DexNo} = \frac{l}{n} \cdot \sum_{i=1}^n (D_i - \bar{D}_{exNo})^2$$

Τύπος 12 - Δειγματική Διακύμανση της Καθυστέρησης πειράματος.

Η διακύμανση είναι ένα στατιστικό μέτρο που περιγράφει πόσο πολύ απέχουν οι επιμέρους μετρήσεις από τον μέσο.

6. Τυπική Απόκλιση (Standard Deviation) Καθυστέρησης Πειράματος S_{DexNo} :

Η τετραγωνική ρίζα της διακύμανσης.

7. Μέγεθος Μέτρησης L_i :

Περιγράφει το μέγεθος των δεδομένων που μεταδόθηκαν στην μέτρηση i .

8. Ρυθμοαπόδοση Μέτρησης T_i :

Το Throughput που μετρήθηκε και αναφέρθηκε από τα εργαλεία ως το αποτέλεσμα της i -οστής μέτρησης.

9. Μέση (Average) Ρυθμοαπόδοση Πειράματος \bar{T}_{exNo} :

$$\bar{T}_{exNo} = \frac{\sum_{i=1}^n L_i}{\sum_{i=1}^n D_i}$$

Τύπος 13 - Μέση Ρυθμοαπόδοση Πειράματος.

Όπου $exNo$ ο αριθμός του πειράματος με βάση τον σχετικό πίνακα.

10.3 ΥΠΟΘΕΣΗ 1 – Η ΕΠΙΔΡΑΣΗ ΤΩΝ ΕΡΓΑΛΕΙΩΝ.

Όπως αναφέραμε και νωρίτερα, θελήσαμε να εκτιμήσουμε αν διαφορετικά εργαλεία δίνουν διαφορετικά αποτελέσματα, όταν κάνουν μετρήσεις κάτω από πανομοιότυπες συνθήκες.

10.3.1 Διατύπωση της Υπόθεσης.

Η στατιστική υπόθεση που ελέγχαμε ήταν:

“Οι μέσες καθυστερήσεις που αναφέρει κάθε εργαλείο δεν είναι, στατιστικώς σημαντικά, διαφορετικές μεταξύ τους”

Δηλαδή:

$$H_0 : \overline{D}_0 = \overline{D}_{11} = \overline{D}_{12}$$

vs

$$H_1 : \begin{cases} \overline{D}_0 \neq \overline{D}_{11} \\ \text{ή} \\ \overline{D}_{11} \neq \overline{D}_{12} \\ \text{ή} \\ \overline{D}_0 \neq \overline{D}_{12} \end{cases}$$

Τύπος 14 - Η Στατιστική Έκφραση της Υπόθεσης 1.

10.3.2 Εργαλεία – Εξοπλισμός – Τοπολογία.

Εκτελέσαμε τα πειράματα 0, 11 και 12. Ο αποστολέας ήταν ο υπολογιστής με Windows 98 και ο παραλήπτης ο υπολογιστής με Windows 2000. Η τοπολογία ήταν Wireless to Ethernet. Οι παράμετροι της MIB παρέμειναν αμετάβλητες. Σε κάθε πείραμα χρησιμοποιήσαμε διαφορετικό εργαλείο και με κάθε εργαλείο πήραμε 100 μετρήσεις. Μετρήσαμε την μέση ρυθμοαπόδοση και την μέση καθυστέρηση κάθε πειράματος.

10.3.3 Περιγραφική Στατιστική.

Εκτινώντας την περιγραφική ανάλυση των τριών πειραμάτων, παραθέτουμε τον ακόλουθο πίνακα. Ο πίνακας έχει στις στήλες τα περιγραφικά μεγέθη και στις γραμμές τα διαφορετικά εργαλεία. Η τελευταία γραμμή περιέχει τα στατιστικά επί του συνόλου των 300 μετρήσεων.

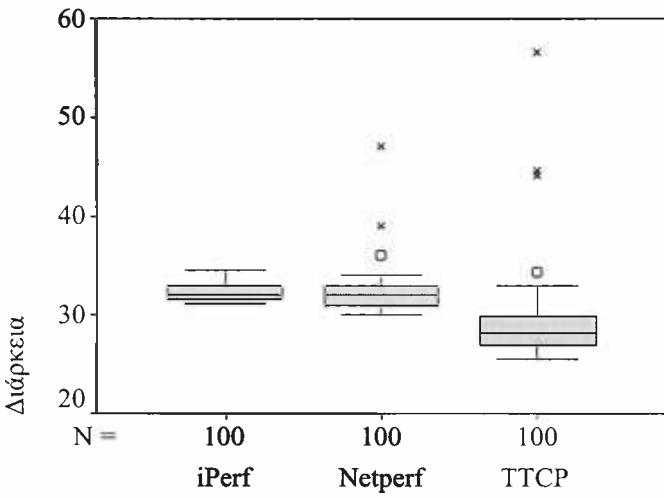
Περιγραφική Στατιστική για την Διάρκεια							
Κατηγορία Πειράματος	N	Mean	Variance	Std. Deviation	Minimum	Maximum	Avg. Thr/put
iPerf	100	32.303	0.653	0.808	31.100	34.500	4057.579
Netperf	100	32.330	3.900	1.975	30.000	47.000	4054.191
TTCP	100	29.084	16.411	4.051	25.627	56.651	4506.685
Total	300	31.239	9.271	3.045	25.627	56.651	4195.784

Πίνακας 18 - Περιγραφική Ανάλυση της Υπόθεσης 1.

Με την πρώτη κιόλας ματιά, υπάρχουν κάποιες σημαντικές παρατηρήσεις που μπορούν να γίνουν.

Η πρώτη είναι ότι, όταν χρησιμοποιήθηκαν, τα εργαλεία NetPerf και iPerf, οι τιμές της καθυστέρησης ήταν πολύ κοντινές μεταξύ τους. Αντίθετα το TTCP δείχνει να έχει διαφορετικά αποτέλεσμα και, συγκεκριμένα, δείχνει να έχει ως αποτέλεσμα μικρότερη αναφερόμενη μέση καθυστέρηση. Το αποτέλεσμα αυτού φαίνεται και από το ότι η αναφερόμενη μέση ρυθμοαπόδοση από το TTCP είναι σημαντικά μεγαλύτερη.

Μια δεύτερη παρατήρηση είναι ότι, στις μετρήσεις που έγιναν με τα δύο πρώτα εργαλεία, η παρατηρούμενη καθυστέρηση περιορίστηκε σε μικρό διάστημα τιμών και σαν αποτέλεσμα, είχε σαφώς χαμηλότερη διακύμανση. Αυτά ακριβώς καταδεικνύει το παρακάτω boxplot διάγραμμα.



Κατηγορία Πειράματος

Σχήμα 51 - BoxPlot για την Υπόθεση 1.

10.3.4 Ελεγχος της Υπόθεσης.

Αφού παρουσιάσαμε τα περιγραφικά μεγέθη που σχετίζονται με την υπόθεση, μπορούμε να περάσουμε στο στάδιο του ελέγχου.

Παρατηρούμε ότι έχουμε να κάνουμε έναν έλεγχο ισότητας μέσων τριών διαφορετικών δειγμάτων που διαφοροποιούνται από έναν παράγοντα. Άρα, η μέθοδος που θα ακολουθήσουμε είναι ή ανάλυση διακύμανσης κατά έναν παράγοντα. Επιλέγουμε επίπεδο σημαντικότητας 5%.

AN.O.V.A.					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	696.679	2	348.339	49.849	0.000
Within Groups	2075.396	297	6.988		
Total	2772.075	299			

Πίνακας 19 - Ανάλυση Διακύμανσης για την Υπόθεση 1.

Από αυτό τον πίνακα και συγκεκριμένα από την τιμή 0.000 στο κελί Sig. συμπεραίνουμε ότι η μηδενική υπόθεση απορρίπτεται. Η τιμή του κελιού αυτού είναι το επίπεδο σημαντικότητας του test και είναι μικρότερο από 0.05.

Αρα λοιπόν η καθυστέρηση στις μετρήσεις από διαφορετικά εργαλεία είναι διαφορετική.

Για να προχωρήσουμε, μπορούμε να κάνουμε έναν Post – Hoc έλεγχο, ώστε να διαπιστώσουμε ποια ομάδα μετρήσεων οδηγεί στην απόρριψη της μηδενικής υπόθεσης.

Test of Homogeneity of Variances			
Levene Statistic	df1	df2	Sig.
13.824	2	297	.000

Πίνακας 20 - Ομοιογένεια Διακυμάνσεων Ανάμεσα στις Ομάδες της Υπόθεσης 1.

Εκτελούμε το παραπάνω test ομοιογένειας διακυμάνσεων, για να διαπιστώσουμε αν στην Post Hoc ανάλυση μπορούμε να θεωρήσουμε ίσες διακυμάνσεις ή όχι. Η τιμή Sig. 0.000 μας οδηγεί στο συμπέρασμα ότι οι διακυμάνσεις είναι άνισες. Με αυτό το δεδομένο προχωράμε στο test των Games – Howell.

Multiple Comparisons							
Games-Howell		Mean	Std. Error	Sig.	95% Confidence Interval		
(I) Κατηγορία	(J) Κατηγορία	Πειράματος	Difference (I-J)		Lower Bound	Upper Bound	
iPerf	Netperf		-.027	.3738	.991	-.5271	.4731
	TTCP		3.219 *	.3738	.000	2.2373	4.2009
Netperf	iPerf		,027	.3738	.991	-.4731	.5271
	TTCP		3.246 *	.3738		2.1898	4.3023
TTCP	iPerf		-3.219 *	.3738	.000	-4.2009	-2.2373
	Netperf		-3.246 *	.3738		-4.3023	-2.1898

* The mean difference is significant at the .05 level.

Πίνακας 21 - Games – Howell για την Υπόθεση 1.

Όλη η ουσία του test Games – Howell, βρίσκεται στην στήλη Sig. Η στήλη αυτή περιέχει την πιθανότητα, η διαφορά των μέσων των δύο κατηγοριών, να είναι 0. αν η πιθανότητα αυτή είναι μεγάλη, τότε οι μέσοι των δύο κατηγοριών δεν διαφέρουν. Στο ίδιο συμπέρασμα μπορούμε να καταλήξουμε, αν το 95% διάστημα εμπιστοσύνης για την διαφορά των μέσων περιέχει την τιμή 0.

Κατά συνέπεια καταλήγουμε στο συμπέρασμα ότι τα εργαλεία NetPerf και iPerf οδηγούν, κατά μέσο όρο, στην ίδια καθυστέρηση, σε αντίθεση με το TTCP.

10.3.5 Σχολιασμός των Αποτελεσμάτων.

Το βασικότερο συμπέρασμα που βγαίνει από τα παραπάνω είναι ότι η Υπόθεση 1 δεν ισχύει. Τα τρία εργαλεία, πράγματι, αναφέρουν διαφορετικά αποτελέσματα όταν χρησιμοποιηθούν κάτω από τις ίδιες συνθήκες.

Αναφορικά στην διαφορά του υπολογιζόμενου Throughput, έχουμε να παρατηρήσουμε και το εξής αξιοσημείωτο. Στην περίπτωση του TTCP, η ρυθμοαπόδοση

είναι ίση με το μέγεθος των δεδομένων που μεταφέρθηκαν προς τον χρόνο. Στην περίπτωση των δύο άλλων εργαλείων, κάτι τέτοιο δεν ισχύει. Για τον λόγο αυτό ορίσαμε την μέση ρυθμοαπόδοση πειράματος, έτσι όπως την ορίσαμε. Δηλαδή ξαναύπολογίζοντάς την χρησιμοποιώντας το μέγεθος των δεδομένων και την καθυστέρηση. Αν λαμβάναμε υπ' όψιν μας την ρυθμοαπόδοση που ανέφεραν τα εργαλεία για να υπολογίσουμε την μέση τιμή της, οι αποκλίσεις θα ήταν ακόμα πιο έντονες.

Οσον αφορά στις παρατηρούμενες καθυστερήσεις των μετρήσεων, δύο παράγοντες θα μπορούσαν να οδηγήσουν σε διαφορές.

Ο πρώτος είναι ο τρόπος υπολογισμού τους.

Ο δεύτερος θα μπορούσε να οφείλεται στην ενδεχόμενη “ικανότητα” ενός εργαλείου να μεταφέρει πιο γρήγορα τα δεδομένα.

Για παράδειγμα, κάποιο εργαλείο μπορεί να εκλαμβάνει ως αρχή του χρονομέτρου την στιγμή που γίνεται η κλήση Connect, ενώ ένα άλλο θα μπορούσε να αρχικοποιεί το χρονόμετρο την στιγμή που γίνεται η πρώτη Write. Αντίστοιχα, κάποιο εργαλείο ενδέχεται να μετράει αφού έχει γεμίσει τους ενταμιευτές προς μετάδοση, ενώ ένα άλλο να μετράει τη στιγμή που αρχίζει να γεμίζει τους ενταμιευτές αυτούς.

Αξιοσημείωτη, επίσης, θεωρείται η ύπαρξη πολλών ακραίων τιμών στην περίπτωση του TTCP, όπως φαίνεται από το BoxPlot. Αυτό θα μπορούσε να οφείλεται σε τυχαίους παράγοντες, ή στον τρόπο λειτουργίας του εργαλείου. Η διερεύνηση αυτού του προβληματισμού ίσως να οδηγούσε σε ενδιαφέροντα συμπεράσματα.

10.4 ΥΠΟΘΕΣΗ 2 – Η ΕΠΙΔΡΑΣΗ ΤΗΣ ΤΟΠΟΛΟΓΙΑΣ.

Ένας άλλος παράγοντας, που θεωρήσαμε ότι θα μπορούσε να επηρεάσει τις επιδόσεις του δικτύου, είναι ο παράγοντας “Τοπολογία”.

Τον παράγοντα αυτόν και την επίδρασή του εξετάζουμε στην παράγραφο αυτήν.

10.4.1 Διατύπωση της Υπόθεσης.

Η στατιστική υπόθεση που ελέγχαμε ήταν:

“Οι μέσες καθυστερήσεις που παρατηρούνται ανά τοπολογία δεν είναι στατιστικά σημαντικά, διαφορετικές μεταξύ τους”

Δηλαδή:

$$H_0 : \bar{D}_0 = \bar{D}_{2l}$$

vs

$$H_1 : \bar{D}_0 \neq \bar{D}_{2l}$$

Τύπος 15 - Η Στατιστική Έκφραση της Υπόθεσης 2.

10.4.2 Εργαλεία – Εξοπλισμός – Τοπολογία.

Εκτελέσαμε τα πειράματα 0, 21. Ο αποστολέας ήταν ο υπολογιστής με Windows 98 και ο παραλήπτης ο υπολογιστής με Windows 2000. Το εργαλείο που χρησιμοποιήθηκε ήταν το TTCP. Οι παράμετροι της MIB παρέμειναν αμετάβλητες. Η τοπολογία ήταν Wireless to Ethernet στην μία περίπτωση και Wireless to Wireless στην δεύτερη. Σε κάθε περίπτωση πήραμε από 100 μετρήσεις. Μετρήσαμε την μέση ρυθμοαπόδοση και την μέση καθυστέρηση κάθε πειράματος.

10.4.3 Περιγραφική Στατιστική.

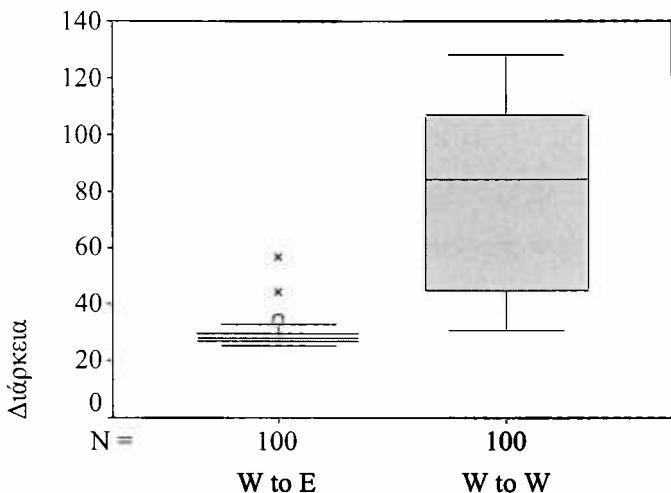
Όπως και στην προηγούμενη υπόθεση, έτσι και για αυτήν, ξεκινάμε με ορισμένα περιγραφικά μεγέθη.

Περιγραφική Στατιστική για την Διάρκεια							
Κατηγορία	N	Mean	Variance	Std. Deviation	Minimum	Maximum	Avg. Thr/put
W to E	100	29.0839	16.411	4.0510	25.63	56.65	4506.685
W to W	100	77.7011	1032.027	32.1252	30.82	128.28	1686.874
Total	200	53.3925	1115.462	33.3985	25.63	128.28	2454.876

Πίνακας 22 - Περιγραφική Ανάλυση της Υπόθεσης 2.

Είναι εντυπωσιακή η διαφορά που παρατηρούμε, αμέσως, στην καθυστέρηση. Η περίπτωση Wireless to Wireless παρουσιάζει σημαντικά μεγαλύτερη καθυστέρηση και μάλιστα και με αξιοσημείωτη διακύμανση.

Η έντονη συμπεριφορά της περίπτωσης Wireless to Wireless αντικατοπτρίζεται με πολύ παραστατικό τρόπο στο BoxPlot που ακολουθεί.



Κατηγορία

Σχήμα 52 - BoxPlot για την Υπόθεση 2.

Από το BoxPlot μπορούμε να παρατηρήσουμε ορισμένα σημαντικά χαρακτηριστικά των πειραμάτων.

Το πρώτο είναι η μεγάλη διακύμανση καθυστέρησης στην περίπτωση Wireless to Wireless. Το πόσο μεγαλύτερο είναι το εύρος τιμών είναι προφανές.

Η μέση τιμή της διακύμανσης είναι πολύ υψηλότερη, στην περίπτωση Wireless to Wireless.

Στην περίπτωση Wireless to Wireless δεν υπάρχουν διαταρακτικές τιμές, σε αντίθεση με την περίπτωση Wireless to Ethernet.

10.4.4 Έλεγχος της Υπόθεσης.

Αφού παρουσιάσαμε, με περιγραφικά μεγέθη, τα αποτελέσματα των πειραμάτων, μπορούμε να ελέγξουμε την ισχύ της μηδενικής υπόθεσης.

Η κατηγοριοποίηση της μεταβλητής σε δύο μόνο ομάδες μας επιτρέπει να κάνουμε τον έλεγχο με t – test.

Με βάση τα προηγούμενα, είναι φυσιολογικό να αναμένουμε ότι η υπόθεση αυτή θα απορριφθεί. Για του λόγου το αληθές έχουμε τον εξής πίνακα αποτελεσμάτων του test.

Διάρκεια	Independent Samples Test							
	Levene's Test		t-test for Equality of Means					
	F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference
Equal variances	346.931	.000	-15.015	198	.000	-48.6172	3.2380	-55.0025 -42.2319
UnEqual variances			-15.015	102.148	.000	-48.6172	3.2380	-55.0395 -42.1948

Πίνακας 23 - Τα Αποτελέσματα του t – test για την Υπόθεση 2.

Τα αποτελέσματα είναι ακριβώς όπως τα φανταζόμασταν. Σύμφωνα με το test του Levene κοιτάμε την δεύτερη γραμμή για άνισες διακυμάνσεις. Το επίπεδο σημαντικότητας του test είναι 0.000 και το 95% διάστημα εμπιστοσύνης για την διαφορά των μέσων δεν περιέχει το 0. Άρα η μηδενική υπόθεση απορρίπτεται.

Συνοψίζουμε. Η διαφορετική τοπολογία έχει σαφή επίδραση στην μέση καθυστέρηση των μετρήσεων. Συγκεκριμένα, η καθυστέρηση στην τοπολογία Wireless to Wireless είναι σαφώς μεγαλύτερη.

10.4.5 Σχολιασμός των Αποτελεσμάτων.

Το γεγονός ότι, τα παραπάνω αποτελέσματα, παρατηρήθηκαν κατ' εξακολούθηση (persistency), μας απαγορεύει να τα αποδώσουμε σε τυχαίους, αστάθμητους παράγοντες. Θεωρούμε πως υπάρχει σαφής και ξεκάθαρος λόγος που οδήγησε σε αυτά.

Θα μπορούσε κανείς να βρει πολλούς πιθανούς λόγους που να τα εξηγούν.

Θα μπορούσε, για παράδειγμα, να αναφερθεί σε σφάλματα μετάδοσης και αναμεταδόσεις που, κατά κανόνα, προκαλούν καθυστέρηση. Κάτι τέτοιο δεν πιστεύουμε ότι ισχύει για τους εξής δύο λόγους.

- Η απόσταση των σταθμών από το Access Point και η διάρθρωση του χώρου ήταν τέτοια που εξασφάλιζε την ύπαρξη δυνατού σήματος καθ' όλη την διάρκεια των μετρήσεων. Η δύναμη του σήματος, πιστεύουμε, είναι αρκετή για να εξασφαλίσει την μη ύπαρξη τέτοιων σφαλμάτων.
- Ακόμα και αν δεν ισχύουν τα παραπάνω, η αύξηση της καθυστέρησης είναι πολύ μεγάλη για να δικαιολογείται από σφάλματα. Η αντικατάσταση του ενσύρματου κομματιού του δικτύου από ασύρματο δεν θα μπορούσε, κρίνουμε, να προκάλεσε τόσο μεγάλο αριθμό σφαλμάτων.

Για τα αποτελέσματα της συγκεκριμένης υπόθεσης, ωστόσο, είμαστε πολύ επιφυλακτικοί. Το πρώτο θέμα που πρέπει να θίξουμε είναι ότι, στην δεύτερη τοπολογία, είχαμε και διαφορετικά λειτουργικά συστήματα (Windows 2000 και Windows XP). Έτσι η υπόθεση, ότι διατηρούμε σταθερές όλες τις παραμέτρους του συστήματος, εκτός από την υπό έλεγχο, δεν ευσταθεί απολύτως.

Πέρα από αυτό, κατά την διάρκεια των πειραμάτων, παρατηρήσαμε και μία ιδιαίτερα χαρακτηριστική συμπεριφορά από τα Windows XP και το αντίστοιχο μηχάνημα. Όλα αυτά αναλύονται εκτενώς στο επόμενο κεφάλαιο.

Πάντως, διατηρούμε έντονη την πεποίθηση ότι η τοπολογία, πράγματι, επηρεάζει τις επιδόσεις ενός ασύρματου τοπικού δικτύου.



10.5 ΥΠΟΘΕΣΗ 3 – Η ΕΠΙΔΡΑΣΗ ΤΩΝ ΛΕΙΤΟΥΡΓΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ.

Όπως αναφέραμε νωρίτερα, η τεχνολογία των ασύρματων τοπικών δικτύων είναι πολύ νέα. Οι οδηγοί των καρτών δικτύου δεν έχουν ακόμα τελειοποιηθεί. Έτσι θεωρήσαμε ότι, από λειτουργικό σύστημα σε λειτουργικό σύστημα, οι επιδόσεις θα είναι διαφορετικές.

Στις παρακάτω σελίδες θα αναλύσουμε την υπόθεση αυτή. Τα λειτουργικά συστήματα που ελέγχαμε ήταν τα Windows 2000 Professional και τα Windows XP.

10.5.1 Διατύπωση της Υπόθεσης.

Η στατιστική υπόθεση που ελέγχαμε ήταν:

"Η Μέση Ρυθμοαπόδοση δεν επηρεάζεται από το λειτουργικό σύστημα του εξυπηρετητή."

Χρησιμοποιήθηκαν τα πειράματα 0 και 61.

Δηλαδή:

$$\begin{aligned} H_0 : \bar{D}_0 &= \bar{D}_{61} \\ \text{vs} \\ H_1 : \bar{D}_0 &\neq \bar{D}_{61} \end{aligned}$$

Τύπος 16 - Η Στατιστική Έκφραση της Υπόθεσης 3.

10.5.2 Εργαλεία – Εξοπλισμός – Τοπολογία.

Εκτελέσαμε τα πειράματα 0, 61. Ο αποστολέας ήταν ο υπολογιστής με Windows 98. Το εργαλείο που χρησιμοποιήθηκε ήταν το TTCP. Οι παράμετροι της MIB παρέμειναν αμετάβλητες. Η τοπολογία ήταν Wireless to Ethernet και στις δύο περιπτώσεις. Και στις δύο περιπτώσεις, ο υπολογιστής που είχε διεπαφή με το δίκτυο IEEE 802.11, ήταν ο εξυπηρετητής. Στο πείραμα 0, όπως φαίνεται από τον συνοπτικό πίνακα, ο εξυπηρετητής ήταν ο υπολογιστής με τα Windows 2000 Professional. Στο πείραμα 61 ο εξυπηρετητής ήταν ο υπολογιστής με Windows XP. Σε κάθε περίπτωση πήραμε από 100 μετρήσεις. Μετρήσαμε την μέση ρυθμοαπόδοση και την μέση καθυστέρηση κάθε πειράματος.

10.5.3 Περιγραφική Στατιστική.

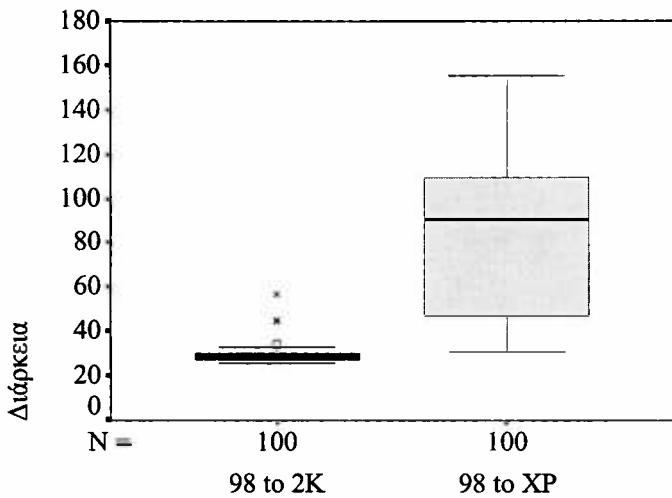
Ξεκινώντας την ανάλυση της υπόθεσης 3, παραθέτουμε έναν πίνακα με περιγραφικά μεγέθη.

Περιγραφική Στατιστική για την Διάρκεια							
Κατηγορία	N	Mean	Variance	Std. Deviation	Minimum	Maximum	Avg. Thr/put
98 to 2K	100	29.0839	16.411	4.0510	25.63	56.65	4506.658
98 to XP	100	82.6904	1243.757	35.2669	30.82	155.26	1585.093
Total	200	55.8872	1348.942	36.7280	25.63	155.26	2345.295

Πίνακας 24 - Περιγραφική Ανάλυση της Υπόθεσης 3.

Όπως και στην υπόθεση υπ' αριθμόν 2, έτσι και στην υπόθεση 3, παρατηρούμε ότι η αλλαγή του λειτουργικού συστήματος, προκαλεί μεγάλη διαφορά στην απόδοση του δικτύου.

Η μέση καθυστέρηση αυξάνει δραματικά και αποκτά πολύ μεγάλη διασπορά. Τα παραπάνω φαίνονται παραστατικά στο BoxPlot που ακολουθεί.



Κατηγορία

Σχήμα 53 - BoxPlot για την Υπόθεση 3.

10.5.4 Έλεγχος της Υπόθεσης.

Μετά από την περιγραφική ανάλυση των αποτελεσμάτων, μπορούμε να προχωρήσουμε στον έλεγχο της 3^{ης} υπόθεσης..

Η κατηγοριοποίηση της μεταβλητής σε δύο μόνο ομάδες μας επιτρέπει να κάνουμε τον έλεγχο με t – test, ακριβώς όπως και στην υπόθεση 2.

Με κριτήριο την προηγούμενη ανάλυση, είναι φυσιολογικό να αναμένουμε ότι η υπόθεση αυτή θα απορριφθεί. Ο παρακάτω πίνακας με τα αποτελέσματα του test μας επιβεβαιώνει τις υποψίες.

Διάρκεια	Independent Samples Test								
	Levene's Test		t-test for Equality of Means						
	F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
Equal variances	35.171	.000	93.177	198	.000	4313.79575	46.29680	4222.49765	4405.09385
UnEqual variances			93.177	117.603	.000	4313.79575	46.29680	4222.11228	4405.47922

Πίνακας 25 - Τα Αποτελέσματα του t – test για την Υπόθεση 3.

Από την τιμή του επιπέδου σημαντικότητας του test Levene για ομοιογένεια διακύμανσης, συμπεραίνουμε ότι δεν μπορούμε να θεωρήσουμε ίσες διακυμάνσεις στις δύο κατηγορίες.

Έτσι. Από την δεύτερη γραμμή αποτελεσμάτων, παρατηρούμε ότι το επίπεδο σημαντικότητας του t – test είναι 0.000 και ότι το 95% διάστημα εμπιστοσύνης δεν περιέχει την τιμή 0.

Είναι ηλίου φαεινότερο ότι η μηδενική υπόθεση για ισότητα των μέσων είναι απορριπτέα.

Έτσι, αυτό που μπορούμε να πούμε είναι ότι τα διαφορετικά λειτουργικά συστήματα έχουν επίπτωση στις επιδόσεις του δικτύου.

10.5.5 Σχολιασμός των Αποτελεσμάτων.

Όπως και στην προηγούμενη υπόθεση, έτσι και εδώ, παρατηρούμε μια μεγάλη αύξηση της καθυστέρησης, μεταβάλλοντας μόνο ένα από τα χαρακτηριστικά του πειράματος.

Η επίδραση που έχει το λειτουργικό σύστημα και μάλιστα τα Windows XP δείχνει να είναι καταλυτική στην υποβάθμιση των επιδόσεων.

Πιθανοί λόγοι που θα μπορούσαν να οδηγούν σε αυτό είναι πολλοί.

Είναι πολύ πιθανόν, η θύρα που είχαμε συνδέσει την PCMCIA κάρτα δικτύου να είχε κάποιο πρόβλημα. Ήα μπορούσε επίσης να υπάρχει κάποιο πρόβλημα με τους οδηγούς της κάρτας για το εν λόγω λειτουργικό σύστημα.

Πρέπει να αναφέρουμε, εξ' άλλου, ότι ενώ το σήμα από το Access Point ήταν πολύ δυνατό, πολύ συχνά ο υπολογιστής “έχανε” το δίκτυο και αποσυνδέόταν. Σε αυτές τις περιπτώσεις, συνήθως, η επανασύνδεση με το δίκτυο γινόταν αυτόματα μετά από λίγα δευτερόλεπτα. Άλλες φορές έπρεπε να αφαιρέσουμε την κάρτα και να την ξανατοποθετήσουμε. Το αποτέλεσμα ήταν να έχουμε πολλές άκυρες μετρήσεις, λόγω του ότι οι TCP συνδέσεις πελάτη – εξυπηρετητή, φυσιολογικά τερματίζονταν. Επίσης, οι συνδέσεις – αποσυνδέσεις με το δίκτυο, είναι πολύ πιθανόν να προκαλούσαν πολλές αναμεταδόσεις.

Σε οποιαδήποτε περίπτωση, πρέπει να αναφέρουμε ότι η κάρτα δικτύου δεν είχε πρόβλημα, καθώς λειτούργησε χωρίς πρόβλημα στα άλλα μηχανήματα που δοκιμάστηκε.

Ήα ήταν, πραγματικά, πολύ ενδιαφέρον, να ξαναγίνονταν παρόμοιες μετρήσεις και με άλλα λειτουργικά συστήματα, όπως UNIX, LINUX κλπ.



10.6 ΥΠΟΘΕΣΗ 4 – Η ΕΠΙΔΡΑΣΗ ΤΗΣ ΕΝΑΛΛΑΓΗΣ CLIENT - SERVER.

Ένα άλλο ερώτημα ήταν κατά πόσο θα επηρεαστεί η Μέση Καθυστέρηση αν ο Server ενός πειράματος γίνει Client στο επόμενο και αντίστροφα. Πιο συγκεκριμένα, θελήσαμε να δούμε τι διαφορά υπάρχει αν το αργότερο από τα δύο PC είναι στην πλευρά του ασύρματου δικτύου με την περίπτωση να είναι από την πλευρά του ενσύρματου.

10.6.1 Διατύπωση της Υπόθεσης.

Η στατιστική υπόθεση που ελέγχαμε ήταν:

“Η Μέση Ρυθμοαπόδοση δεν επηρεάζεται από την εναλλαγή των ρόλων των δύο σταθμών.”

Χρησιμοποιήθηκαν τα πειράματα 21 και 51.

Δηλαδή:

$$H_0 : \bar{D}_{21} = \bar{D}_{51}$$

vs

$$H_1 : \bar{D}_{21} \neq \bar{D}_{51}$$

Τύπος 17 - Η Στατιστική Έκφραση της Υπόθεσης 4.

10.6.2 Εργαλεία – Εξοπλισμός – Τοπολογία.

Για τον έλεγχο της υπόθεσης χρησιμοποιήσαμε τα πειράματα 21, 51. Οι υπολογιστές που χρησιμοποιήσαμε ήταν ο υπολογιστής με Windows 2000 και το Laptop με τα Windows XP. Ο δύο υπολογιστές είχαν, εναλλάξ, τον ρόλο του πελάτη στο ένα πείραμα και του εξυπηρετητή στο άλλο. Το εργαλείο που χρησιμοποιήθηκε ήταν το TTCP. Οι παράμετροι της MIB παρέμειναν αμετάβλητες. Η τοπολογία ήταν Wireless to Wireless και στις δύο περιπτώσεις. Σε κάθε περίπτωση πήραμε από 100 μετρήσεις. Μετρήσαμε την μέση ρυθμοαπόδοση και την μέση καθυστέρηση κάθε πειράματος.

10.6.3 Περιγραφική Στατιστική.

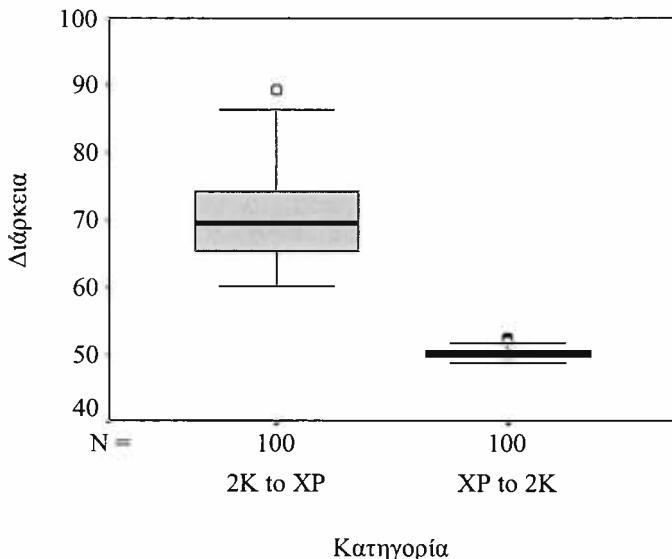
Όπως και σε όλες τις προηγούμενες υποθέσεις και σύμφωνα με αυτά που αναφέραμε στην αρχή του κεφαλαίου, ξεκινάμε με την παρουσίαση των περιγραφικών στατιστικών των δύο πειραμάτων.

Περιγραφική Στατιστική για την Διάρκεια							
Κατηγορία	N	Mean	Variance	Std. Deviation	Minimum	Maximum	Avg. Thr/put
2K to XP	100	70.39496	43.946	6.62918	60.136	89.348	1861.951
XP to 2K	100	50.10392	.524	.72411	48.780	52.321	2616.003
Total	200	60.24944	125.572	11.20590	48.780	89.348	2175.489

Πίνακας 26 - Περιγραφική Ανάλυση της Υπόθεσης 4.

Ο παραπάνω πίνακας μας παρέχει ορισμένα σημεία αξια σχολιασμού. Παρατηρούμε λοιπόν ότι, ενώ έχουμε μια σημαντική αύξηση στην μέση καθυστέρηση, η αύξηση αυτή δεν είναι εξίσου αλματώδης, όσο στις περιπτώσεις των δύο προηγούμενων υποθέσεων.

Ωστόσο, στο πείραμα που είχε σαν αποστολέα τα Windows XP, παρατηρούμε και πολύ χαμηλή διακύμανση. Οι επιμέρους τιμές της καθυστέρησης σε κάθε μέτρηση, είναι χαρακτηριστικά κοντά στην μέση καθυστέρηση. Αυτά φαίνονται και από το παρακάτω BoxPlot.



Σχήμα 54 - BoxPlot για την Υπόθεση 4.

Παρατηρεί κανείς, με την πρώτη ματιά, το πόσο κοντά βρίσκονται οι επιμέρους τιμές της καθυστέρησης, σε σχέση με την μέση καθυστέρηση. Παρατηρούμε, επίσης, ότι υπάρχει πλήρης απουσία ακραίων τιμών, ωστόσο υπάρχουν πολλές διαταρακτικές στο δεύτερο πείραμα. Αυτό όμως είναι λογικό, αν σκεφτεί κανείς τα εξής. Το αν μια τιμή είναι διαταρακτική ή ακραία, καθορίζεται από την απόστασή της από τα άκρα του ενδοτεταρτημοριακού εύρους και από το ίδιο το εύρος. Μικρή διακύμανση σημαίνει μικρό ενδοτεταρτημοριακό εύρος. Άρα η ύπαρξη των outliers οφείλεται στο ότι, γενικά, η διακύμανση της καθυστέρησης του πειράματος ήταν πολύ μικρή και όχι στο ότι απέχουν πραγματικά πολύ από την διάμεσο τιμή της καθυστέρησης.

10.6.4 Έλεγχος της Υπόθεσης.

Αφού κάναμε αυτές τις σημαντικές παρατηρήσεις, μπορούμε να προχωρήσουμε με το t-test, για τον έλεγχο της υπόθεσης 4.

Η χρήση αυτού του test δικαιολογείται, για μια ακόμη φορά από το ότι τα δεδομένα μας χωρίζονται μόνο σε δύο ομάδες.

Στον παρακάτω πίνακα, από το test Levene, ομοιογένειας διακυμάνσεων, προκύπτει ότι οι δύο πληθυνσμοί δεν μπορούν να θεωρηθούν ομοσκεδαστικοί. Από την δεύτερη σειρά του πίνακα, προκύπτει ότι οι δύο μέσοι διαφέρουν. Αυτό, τόσο από την τιμή του επιπέδου σημαντικότητας του test, όσο και από την μη ύπαρξη της τιμής 0 στο 95% διάστημα εμπιστοσύνης για την διαφορά των μέσων.

Independent Samples Test								
Διάρκεια	Levene's Test		t-test for Equality of Means					
	F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference
Equal variances	137.030	.000	30.428	198	.000	20.29104	.66686	18.97598 21.60610
UnEqual variances			30.428	101.362	.000	20.29104	.66686	18.96822 21.61386

Πίνακας 27 - Τα Αποτελέσματα του t – test για την Υπόθεση 4.

Κατά συνέπεια έχουμε να πούμε ότι η υπόθεση περί ισότητας των μέσων απορρίπτεται.

10.6.5 Σχολιασμός των Αποτελεσμάτων.

Στην περίπτωση της υπόθεσης τέσσερα, είχαμε και πάλι αύξηση της μέσης καθυστέρησης, που είναι στατιστικώς σημαντική.

Ωστόσο, από την περιγραφική ανάλυση προκύπτει ότι η αύξηση αυτή δεν ήταν τόσο αλματώδης όσο ήταν οι παρατηρηθείσες αυξήσεις στις υποθέσεις δύο και τρία.

Αξίζει, επίσης να αναφέρουμε ότι, η μικρή καθυστέρηση παρατηρήθηκε στην περίπτωση που η μεγαλύτερη υπολογιστική ισχύς ήταν από την πλευρά του αποστολέα – πελάτη. Το γεγονός αυτό μας υποδηλώνει ότι ο μεγαλύτερος φόρτος βρίσκεται από την πλευρά του αποστολέα. Εκεί, τα δεδομένα πρέπει να υποστούν επεξεργασία και να προετοιμαστούν για να εισέλθουν στο δίκτυο. Αντίθετα, ο φόρτος φαίνεται μικρότερος στην πλευρά του παραλήπτη, όπου τα δεδομένα εξάγονται από τα πεδία “Data” των πρωτοκόλλων, των επιπέδων της στοίβας TCP/IP. Έτσι, ουσιαστικά, αφού η καθυστέρηση διάδοσης είναι ίδια και στις δύο περιπτώσεις, η συνολική καθυστέρηση καθορίζεται περισσότερο από το πόσο γρήγορα τα δεδομένα θα “κατέβουν” την στοίβα πρωτοκόλλων, στην πλευρά του αποστολέα και λιγότερο από το πόσο γρήγορα θα την “ανέβουν” στο άκρο του παραλήπτη. Για τον λόγο αυτό, ισχυρότερος αποστολέας ισοδυναμεί με μικρότερη καθυστέρηση.

Τέλος, στο θέμα που έχει προκύψει με τις επιδόσεις των Windows XP, παρατηρούμε ότι το λειτουργικό αυτό συμπεριφέρεται πολύ καλύτερα και σταθερά σαν αποστολέας δεδομένων απ' ότι σαν παραλήπτης.

10.7 ΥΠΟΘΕΣΗ 5 – Η ΕΠΙΔΡΑΣΗ ΤΩΝ ΑΝΤΙΚΕΙΜΕΝΩΝ ΤΗΣ MIB.

Αυτή η υπόθεση είναι και η πολυπλοκότερη από όλες. Θέλουμε να ελέγξουμε αν τα αντικείμενα της MIB των δικτύων IEEE 802.11, επηρεάζουν την μέση καθυστέρηση των πειραμάτων.

Όταν αναφερόμαστε στα αντικείμενα της MIB, εξυπακούεται πως δεν αναφερόμαστε στο σύνολό τους, αλλά μόνο σε αυτά που χαρακτηρίσαμε ως ενδιαφέροντα σε προηγούμενο κεφάλαιο.

10.7.1 Διατύπωση της Υπόθεσης.

Η στατιστική υπόθεση που ελέγχαμε ήταν:

“Η μέση καθυστέρηση ενός πειράματος δεν μεταβάλλεται στατιστικώς σημαντικά, όταν αλλάζουμε την τιμή ενός αντικειμένου της MIB”.

Δηλαδή:

$$H_0 : \overline{D}_0 = \overline{D}_{41} = \overline{D}_{42} = \overline{D}_{43} = \overline{D}_{44}$$

Τύπος 18 - Η Στατιστική Έκφραση της Υπόθεσης 1.

Η εναλλακτική υπόθεση είναι η H_1 : κάποια από τις παραπάνω ισότητες δεν ισχύει.

10.7.2 Εργαλεία – Εξοπλισμός – Τοπολογία.

Εκτελέσαμε τα πειράματα 0, 41, 42, 43 και 44. Ο αποστολέας ήταν ο υπολογιστής με Windows 98 και ο παραλήπτης ο υπολογιστής με Windows 2000. Η τοπολογία ήταν Wireless to Ethernet. Το εργαλείο που χρησιμοποιήσαμε ήταν το TTCP. Σε κάθε πείραμα χρησιμοποιήσαμε διαφορετικό εργαλείο και με κάθε εργαλείο πήραμε 100 μετρήσεις. Μετρήσαμε την μέση ρυθμοαπόδοση και την μέση καθυστέρηση κάθε πειράματος.

Σε κάθε πείραμα μεταβάλαμε μία παράμετρο της MIB ως εξής.

- **Πείραμα 0:** Οι αρχικές ρυθμίσεις του κατασκευαστή.
- **Πείραμα 41:** Θέσαμε στο αντικείμενο **dot11PrivacyOptionImplemented** την τιμή TRUE και χρησιμοποιήσαμε κλειδί μήκους 64 bit.
- **Πείραμα 42:** Θέσαμε στο αντικείμενο **dot11PrivacyOptionImplemented** την τιμή TRUE και χρησιμοποιήσαμε κλειδί μήκους 128 bit.
- **Πείραμα 43:** Θέσαμε στο αντικείμενο **dot11BeaconPeriod** την τιμή 65536. Η αρχική ήταν 100.
- **Πείραμα 44:** Θέσαμε στο αντικείμενο **dot11RTSThreshold** την τιμή 0, ενεργοποιώντας την ακολουθία πλαισίων RTS/CTS για όλα τα πλαίσια ανεξαρτήτως μεγέθους. Η αρχική τιμή ήταν 2347, που είναι και η μέγιστη επιτρεπόμενη.

Πέρα από τα παραπάνω αντικείμενα, θελήσαμε να συμπεριλάβουμε και το **dot11FragmentationThreshold**. Ξεκινήσαμε ένα πείραμα, θέτοντας την ελάχιστη τιμή (256). Όμως, με την εκκίνηση του πειράματος, η πρώτη μέτρηση διήρκησε περίπου 5 λεπτά. Έτσι θεωρήσαμε ότι θα χάναμε πολύτιμο χρόνο ύσχανοντας να βρούμε το προφανές, ότι δηλαδή, μία μικρή τιμή σε αυτήν την παράμετρο υποβιβάζει κατά πολύ τις επιδόσεις. Το πείραμα 45 ματαιώθηκε.

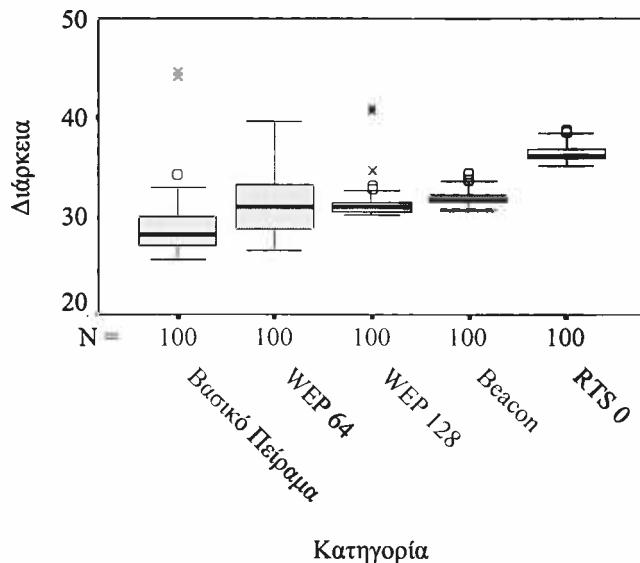
10.7.3 Περιγραφική Στατιστική.

Ξεκινώντας την περιγραφική ανάλυση των πειραμάτων, παραθέτουμε τον ακόλουθο πίνακα.

Περιγραφική Στατιστική για την Διάρκεια							Avg.
Κατηγορία Πειράματος	N	Mean	Variance	Std. Deviation	Minimum	Maximum	Thr/put
Βασικό Πείραμα	100	29.08391	16.411	4.05101	25.627	56.651	4506.684
WEP 64	100	31.33416	9.864	3.14065	26.468	39.637	4183.038
WEP 128	100	31.53639	11.858	3.44360	30.054	61.999	4156.214
Beacon	100	31.77710	.547	.73956	30.634	34.230	4124.731
RTS 0	100	36.37400	.670	.81883	35.141	38.655	3603.453
Total	500	32.02111	13.487	3.67240	25.627	61.999	4093.299

Πίνακας 28 - Περιγραφική Ανάλυση της Υπόθεσης 5.

Αυτή είναι η εικόνα της υπόθεσης, από την σκοπιά της περιγραφικής στατιστικής. Αν θέλαμε να κάνουμε κάποια αρχικά σχόλια, θα λέγαμε ότι οι μέσες καθυστερήσεις είναι πολύ κοντινές μεταξύ τους.



Σχήμα 55 - BoxPlot για την Υπόθεση 5.

Στο παραπάνω BoxPlot, πέρα από όλα τα άλλα, γίνεται φανερό και ότι, σε όλες τις περιπτώσεις, υπάρχουν πολλές διαταρακτικές και ακραίες τιμές, εκτός από αυτήν του

πειράματος 41. Επίσης επαληθεύεται και οπτικά το γεγονός ότι οι περιπτώσεις των πειραμάτων 0 και 42 παρουσιάζουν την μεγαλύτερη διακύμανση.

10.7.4 Έλεγχος της Υπόθεσης.

Αφού παρουσιάσαμε τα περιγραφικά μεγέθη που σχετίζονται με την υπόθεση, μπορούμε να περάσουμε στο στάδιο του ελέγχου.

Παρατηρούμε ότι έχουμε να κάνουμε έναν έλεγχο ισότητας μέσων πέντε διαφορετικών δειγμάτων που διαφοροποιούνται από έναν παράγοντα. Άρα, η μέθοδος που θα ακολουθήσουμε είναι ή ανάλυση διακύμανσης κατά έναν παράγοντα. Επιλέγουμε επίπεδο σημαντικότητας 5%.

AN.O.V.A.					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	2834.119	4	708.530	90.029	.000
Within Groups	3895.668	495	7.870		
Total	6729.787	499			

Πίνακας 29 - Ανάλυση Διακύμανσης για την Υπόθεση 5.

Από αυτό τον πίνακα και συγκεκριμένα από την τιμή 0.000 στο κελί Sig. συμπεραίνουμε ότι η μηδενική υπόθεση απορρίπτεται. Η τιμή του κελιού αυτού είναι το επίπεδο σημαντικότητας του test και είναι μικρότερη από 0.05.

Άρα, λοιπόν, η υπόθεση ότι οι τιμές των αντικειμένων της MIB δεν επηρεάζουν την μέση καθυστέρηση, είναι απορριπτέα.

Για να προχωρήσουμε, μπορούμε να κάνουμε έναν Post – Hoc έλεγχο, ώστε να διαπιστώσουμε ποια ομάδα μετρήσεων οδηγεί στην απόρριψη της μηδενικής υπόθεσης.

Test of Homogeneity of Variances			
Levene Statistic	df1	df2	Sig.
15.904	4	495	.000

Πίνακας 30 - Ομοιογένεια Διακυμάνσεων Ανάμεσα στις Ομάδες της Υπόθεσης 5.

Εκτελούμε το παραπάνω test ομοιογένειας διακυμάνσεων, για να διαπιστώσουμε αν στην Post Hoc ανάλυση μπορούμε να θεωρήσουμε ίσες διακυμάνσεις ή όχι. Η τιμή Sig. 0.000 μας οδηγεί στο συμπέρασμα ότι οι διακυμάνσεις είναι άνισες. Με αυτό το δεδομένο προχωράμε στο test των Games – Howell.

Όλη η ουσία του test Games – Howell, βρίσκεται στην στήλη Sig. Η στήλη αυτή περιέχει την πιθανότητα, η διαφορά των μέσων των δύο κατηγοριών, να είναι 0. αν η πιθανότητα αυτή είναι μεγάλη, τότε οι μέσοι των δύο κατηγοριών δεν διαφέρουν. Στο ίδιο συμπέρασμα μπορούμε να καταλήξουμε, αν το 95% διάστημα εμπιστοσύνης για την διαφορά των μέσων περιέχει την τιμή 0.

Ο παρακάτω πίνακας περιέχει τα αποτελέσματα του test Games – Howell, για την υπόθεση 5. από την μελέτη του βγαίνουν ορισμένα πολύ ενδιαφέροντα συμπεράσματα.

Το βασικότερο είναι ότι όλες οι παράμετροι τη ΜΙΒ, όταν αλλάζουν τιμή, οδηγούν στην υποβάθμιση των επιδόσεων σε σχέση με τις εργοστασιακές ρυθμίσεις του εξοπλισμού.

Ένα δεύτερο συμπέρασμα είναι ότι η απλή ανάλυση διακύμανσης μας κάνει απόκρυψη λεπτομερειών. Πράγματι απορρίπτοντας την μηδενική υπόθεση, δεν ξέρουμε πότες και ποιες από τις ισότητές της δεν ισχύουν. Εκτελώντας Games – Howell test, μπορούμε να εξάγουμε ακριβώς αυτή την πληροφόρηση.

Συγκεκριμένα, και αυτό είναι και το τρίτο συμπέρασμα που βγάζουμε, οι μέσες καθυστερήσεις στα πειράματα 41, 42 και 43 δεν διαφέρουν στατιστικώς σημαντικά. Αυτό φαίνεται από τα σκιασμένα κελιά του πίνακα και από τα αντίστοιχα επίπεδα σημαντικότητας.

Multiple Comparisons

Games-Howell						
(I) Κατηγορία Πειράματος	(J) Κατηγορία Πειράματος	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
Βασικό Πείραμα	WEP 64	-2.25025 *	.39674	.000	-3.64847	-.85203
	WEP 128	-2.45248 *	.39674	.000	-3.90280	-1.00216
	Beacon	-2.69319 *	.39674	.000	-3.83613	-1.55025
	RTS 0	-7.29009 *	.39674	.000	-8.43691	-6.14327
WEP 64	Βασικό Πείραμα	2.25025 *	.39674	.000	.85203	3.64847
	WEP 128	-.20223	.39674	.993	-1.47356	1.06910
	Beacon	-.44294	.39674	.646	-1.33785	.45197
	RTS 0	-5.03984 *	.39674	.000	-5.93972	-4.13996
WEP 128	Βασικό Πείραμα	2.45248 *	.39674	.000	1.00216	3.90280
	WEP 64	.20223	.39674	.993	-1.06910	1.47356
	Beacon	-.24071	.39674	.960	-1.21788	.73646
	RTS 0	-4.83761 *	.39674	.000	-5.81932	-3.85590
Beacon	Βασικό Πείραμα	2.69319 *	.39674	.000	1.55025	3.83613
	WEP 64	.44294	.39674	.646	-.45197	1.33785
	WEP 128	.24071	.39674	.960	-.73646	1.21788
	RTS 0	-4.59690 *	.39674	.000	-4.89788	-4.29592
RTS 0	Βασικό Πείραμα	7.29009 *	.39674	.000	6.14327	8.43691
	WEP 64	5.03984 *	.39674	.000	4.13996	5.93972
	WEP 128	4.83761 *	.39674	.000	3.85590	5.81932
	Beacon	4.59690 *	.39674	.000	4.29592	4.89788

* The mean difference is significant at the .05 level.

Πίνακας 31 - Games – Howell για την Υπόθεση 5.

Αν θέλουμε να προχωρήσουμε ένα βήμα παραπέρα, θα σχολιάσουμε ότι οι μέσες τιμές της καθυστέρησης στα πειράματα 41 και 42 είναι ίσες σε επίπεδο σημαντικότητας 99.3%, το οποίο είναι πάρα πολύ ψηλό.

AN.O.V.A.

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	9.834	2	4.917	.662	.516
Within Groups	2204.633	297	7.423		
Total	2214.467	299			

Πίνακας 32 - AN.O.V.A. Μόνο για τα Πειράματα 41, 42 και 43.

Αν από την ανάλυση διακύμανσης απορρίψουμε τις περιπτώσεις 0 και 44 και επαναλάβουμε το test, παίρνουμε τον παραπάνω πίνακα. Αυτός επιβεβαιώνει τα ευρήματα του test Games – Howell, δίνοντας ως αποτέλεσμα την ισότητα των μέσων της καθυστέρησης και των τριών πειραμάτων, σε επίπεδο σημαντικότητας 51.6%.

10.7.5 Σχολιασμός των Αποτελεσμάτων.

Όπως είπαμε και στην εισαγωγή της παραγράφου, η υπόθεση 5 ήταν και η πολυπλοκότερη από τις έξι. Ο λόγος είναι το ότι είχαμε πολλές κατηγορίες μετρήσεων και πολλούς πιθανούς συνδυασμούς αποτελεσμάτων. Όμως, εκτός από πολύπλοκη, η υπόθεση αυτή ήταν και η ραχοκοκαλιά της έρευνας αυτής. Πραγματικά, από την αρχή θεωρήσαμε πολύ βασικό το κομμάτι της επίδρασης των αντικειμένων της MIB.

Το βασικό συμπέρασμα που εξάγεται από την ανάλυση, είναι ότι οι εργοστασιακές ρυθμίσεις του εξοπλισμού, παρέχουν και τις βέλτιστες επιδόσεις.

Ένα δεύτερο συμπέρασμα που εξάγεται είναι ότι, αν ο διαχειριστής κάποιας εγκατάστασης αποφασίσει να χρησιμοποιήσει WEP, μπορεί να χρησιμοποιήσει κλειδιά μήκους 128 bits, χωρίς να φοβάται μείωση των επιδόσεων. Απ' ότι είδαμε το WEP 128 και το WEP 64, έχουν τις ίδιες τιμές καθυστέρησης. Φαίνεται πως ο αλγόριθμος που κρυπτογραφεί τα δεδομένα με το κλειδί, δεν είναι σημαντικά βαρύτερος όταν εφαρμόζει κλειδί μεγαλύτερου μήκους.

Η ενεργοποίηση της ακολουθίας μηνυμάτων RTS/CTS για όλα τα MAC πλαίσια επιβαρύνει σημαντικά το δίκτυο. Αυτό επιβεβαιώνει την θεωρητική μας γνώση για την λειτουργία του MAC επιπέδου, με βάση την οποία περιμέναμε αυτό ακριβώς το αποτέλεσμα. Η επιβάρυνση του δικτύου με πρόσθετα πλαίσια, από την μία και η καθυστέρηση πριν την αποστολή δεδομένων, εν αναμονή της ολοκλήρωσης της ανταλλαγής RTS/CTS, απ' την άλλη, είναι λογικό να προκαλέσουν καθυστερήσεις στο δίκτυο. Αυτές οι καθυστερήσεις, μπορεί να είναι ανεπαίσθητες στον χρήστη, αλλά σίγουρα γίνονται εντονότερες όσο αυξάνει το μέγεθος του δικτύου.

10.8 ΥΠΟΘΕΣΗ 6 – Η ΕΠΙΔΡΑΣΗ ΤΩΝ ΕΜΠΟΔΙΩΝ.

Η έκτη και τελευταία υπόθεση που κάναμε είναι κατά πόσο η απόσταση και η παρεμβολή εμποδίων, ανάμεσα σε δύο σταθμούς, μπορεί να επηρεάσει τις επιδόσεις του δικτύου.

Η απόσταση και η ύπαρξη εμποδίων έχουν, ουσιαστικά, σαν αποτέλεσμα την εξασθένηση του σήματος, που φτάνει στους σταθμούς από το Access Point.

Η εξασθένηση του σήματος, ενδέχεται, σε ορισμένες περιπτώσεις να προκαλέσει σφάλματα μετάδοσης και αναμεταδόσεις. Είναι λογικό να θεωρήσουμε ότι, οι πολλές αναμεταδόσεις, έχουν άμεση επίπτωση στην καθυστέρηση.

Επιχειρήσαμε να εκτιμήσουμε την στατιστική σημαντικότητα της μεταβολής των επιδόσεων λόγω απόστασης και εμποδίων.

10.8.1 Διατύπωση της Υπόθεσης.

Η στατιστική υπόθεση που ελέγχαμε ήταν:

“Η Μέση Ρυθμοαπόδοση δεν επηρεάζεται από την αύξηση της απόστασης και από την παρεμβολή εμποδίων.”

Δηλαδή:

$$\begin{aligned} H_0 : \bar{D}_{61} &= \bar{D}_{62} \\ \text{vs} \\ H_1 : \bar{D}_{61} &\neq \bar{D}_{62} \end{aligned}$$

Τύπος 19 - Η Στατιστική Έκφραση της Υπόθεσης 6.

Χρησιμοποιήθηκαν τα πειράματα 61 και 62.

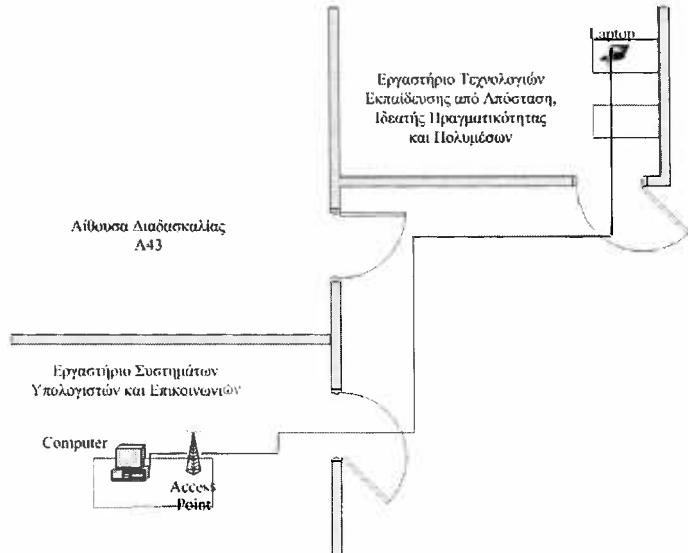
10.8.2 Εργαλεία – Εξοπλισμός – Τοπολογία.

Για τον έλεγχο της υπόθεσης χρησιμοποιήσαμε τα πειράματα 61, 62. Ο αποστολέας ήταν ο υπολογιστής με Windows 98 και ο παραλήπτης το Laptop με τα Windows XP. Το εργαλείο που χρησιμοποιήθηκε ήταν το TTCP. Οι παράμετροι της MIB παρέμειναν αμετάβλητες. Η τοπολογία ήταν Wireless to Wireless και στις δύο περιπτώσεις.

Το πρώτο πείραμα έγινε στον χώρο του Εργαστηρίου Συστημάτων Υπολογιστών και επικοινωνιών. Μετά το τέλος του, μεταφέραμε το Laptop στον χώρο του Εργαστηρίου Τεχνολογιών Εκπαίδευσης από Απόσταση, Ιδεατής Πραγματικότητας και Πολυμέσων που βρίσκεται επίσης στον 4^ο όροφο της πτέρυγας Αντωνιάδου του Οικονομικού Πανεπιστημίου Αθηνών. Μετά από την μεταφορά παρατηρήσαμε ότι το σήμα που λάμβανε το Laptop ήταν πολύ αδύναμο.

Σε κάθε περίπτωση πήραμε από 100 μετρήσεις. Μετρήσαμε την μέση ρυθμοαπόδοση και την μέση καθυστέρηση κάθε πειράματος.

Στο σχήμα βλέπουμε μια πρόχειρη κάτοψη του χώρου όπου έγιναν τα πειράματα.



Σχήμα 56 - Κάτοψη του 4^{ου} Ορόφου της Πτέρυγας Αντωνιάδου.

10.8.3 Περιγραφική Στατιστική.

Με τον πίνακα που ακολουθεί παρουσιάζεται η στατιστική επεξεργασία των αποτελεσμάτων των πειραμάτων.

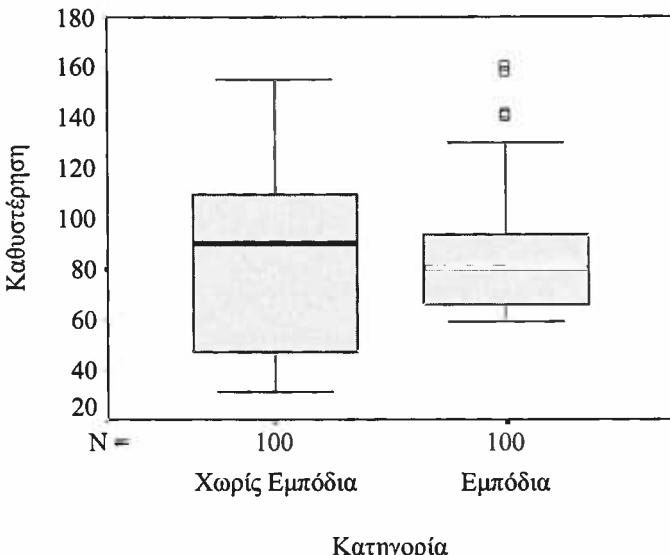
Περιγραφική Στατιστική για την Διάρκεια							
Κατηγορία	N	Mean	Variance	Std. Deviation	Minimum	Maximum	Avg. Thr/put
Χωρίς Εμπόδια	100	82.69044	1243.757	35.26693	30.824	155.263	1585.093
Εμπόδια	100	83.22061	410.453	20.25963	59.625	160.531	1574.994
Total	200	82.95553	823.019	28.68831	30.824	160.531	1580.027

Πίνακας 33 - Περιγραφική Ανάλυση της Υπόθεσης 6.

Η πρώτη και πολύ βασική παρατήρηση που κάνουμε είναι πως η αύξηση της μέσης καθυστέρησης είναι πολύ μικρή, τουλάχιστον συγκριτικά με τις αυξήσεις που παρατηρήθηκαν κατά την επεξεργασία των προηγούμενων υποθέσεων.

Ωστόσο, η διασπορά των τιμών γύρω από τον μέσο είναι μεγαλύτερη στο πείραμα πριν από την μετακίνηση. Ως συνήθως, όλα τα παραπάνω παρουσιάζονται με ένα BoxPlot.

Πριν περάσουμε στον έλεγχο της υπόθεσης 6, αξίζει να επισημάνουμε την ύπαρξη πολλών διαταρακτικών τιμών, στην περίπτωση των μετρήσεων που έγιναν με εμπόδια. Η εξήγηση που μπορεί να δοθεί σε αυτό είναι ότι, ενδεχομένως, στα συγκεκριμένες περιπτώσεις είχαμε σφάλματα μετάδοσης και αναμεταδώσεις, όπως αναφέραμε και στην εισαγωγή αυτής της παραγράφου. Αν ισχύει αυτό, τότε μπορούμε να συμπεράνουμε ότι αριθμός των πειραμάτων που παρουσίασαν αναμεταδώσεις είναι ίσος με το πλήθος των Outliers.



Σχήμα 57 - BoxPlot για την Υπόθεση 6.

10.8.4 Έλεγχος της Υπόθεσης.

Έχουμε, για άλλη μια φορά, να κάνουμε έλεγχο ισότητας των μέσων δύο πληθυσμών. Ως συνήθως, χρησιμοποιήσαμε t – test, του οποίου τα αποτελέσματα φαίνονται στον πίνακα.

Independent Samples Test										
Διάρκεια	Levene's Test			t-test for Equality of Means					95% Confidence Interval of the Difference	
	F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper	
Equal variances	47.038	.000	-.130	198	.896	-.53017	4.06720	-8.55075	7.49041	
UnEqual variances			-.130	157.925	.896	-.53017	4.06720	-8.56329	7.50295	

Πίνακας 34 - Τα Αποτελέσματα του t – test για την Υπόθεση 6.

Κατά τα γνωστά, το test Levene, για ομοιογένεια διακυμάνσεων, μας υπαγορεύει σε ποια γραμμή αποτελεσμάτων πρέπει να κοιτάξουμε. Η τιμή 0.000 του επιπέδου σημαντικότητας του test αυτού μας δηλώνει άνισες διακυμάνσεις.

Άρα, πρέπει να κοιτάξουμε την δεύτερη γραμμή αποτελεσμάτων του t – test. Για το test αυτό, παρατηρούμε την τιμή 0.896 για το επίπεδο σημαντικότητας, καθώς και την παρουσία του αριθμού 0 στο 95% διάστημα εμπιστοσύνης για την διαφορά των μέσων. Αυτά μας υποδηλώνουν ότι η μηδενική υπόθεση δεν απορρίπτεται.

10.8.5 Σχολιασμός των Αποτελεσμάτων.

Στην περίπτωση της υπόθεσης 6, όπως είδαμε, ισχύει η ισότητα των δύο μέσων. Αυτό σημαίνει πως, τα πιθανά σφάλματα μετάδοσης και οι αναμεταδώσεις πλαισίων MAC

που αυτά μπορεί να προκαλέσουν, δεν είναι ικανά να διαταράξουν, στατιστικώς σημαντικά, την μέση καθυστέρηση.

Στην περίπτωση της ύπαρξης εμποδίων, πρέπει να σημειώσουμε ότι ανάμεσα στους δύο υπολογιστές, μεσολαβούσαν δύο τοίχοι και αρκετά μέτρα απόστασης. Το δίκτυο λειτουργούσε με την χειρότερη δυνατή ποιότητα σήματος. Αν οι δύο υπολογιστές απομακρύνονταν και άλλο, θα ήταν αδύνατη οποιαδήποτε σύνδεση με το δίκτυο.

Το συμπέρασμα που μπορεί να βγει από τα παραπάνω είναι ότι, όταν ένα ασύρματο τοπικό δίκτυο λειτουργεί, έστω και με πολύ εξασθενημένο σήμα, η ποιότητα λειτουργίας του και οι επιδόσεις του παραμένουν αμετάβλητες. Αυτό τουλάχιστον δείχνει να ισχύει για τα προϊόντα της συγκεκριμένης εταιρείας.

10.9 ΣΥΝΟΠΤΙΚΟΣ ΠΙΝΑΚΑΣ ΠΕΡΙΓΡΑΦΗΣ ΤΩΝ ΠΕΙΡΑΜΑΤΩΝ.

Πρώτη Ομάδα Πειραμάτων:

Η επίδραση των εργαλείων.

A/a	Τοπολογία	Αποστολέας	Παραλήπτης	MIB	Εργαλείο
0	W/E	Windows 98	Windows 2K	Προεπιλογές ¹	TTCP
11	"	"	"	"	Netperf
12	"	"	"	"	iPerf

Δεύτερη Ομάδα Πειραμάτων:

Η επίδραση της τοπολογίας.

A/a	Τοπολογία	Αποστολέας	Παραλήπτης	MIB	Εργαλείο
0	W/E	Windows 98	Windows 2K	Προεπιλογές ¹	TTCP
21	W/W	Windows XP	Windows 2K	"	TTCP

Τρίτη Ομάδα Πειραμάτων:

Η επίδραση των λειτουργικών συστημάτων.

A/a	Τοπολογία	Αποστολέας	Παραλήπτης	MIB	Εργαλείο
0	W/E	Windows 98	Windows 2K	Προεπιλογές ¹	TTCP
61	W/E	"	Windows XP	"	"

Τέταρτη Ομάδα Πειραμάτων:

Η επίδραση των παραμέτρων της MIB.

A/a	Τοπολογία	Αποστολέας	Παραλήπτης	MIB	Εργαλείο
0	W/E	Windows 98	Windows 2K	Προεπιλογές ¹	TTCP
41	"	"	"	dot11PrivacyOptionImplemented (WEP 64bit)	"
42	"	"	"	dot11PrivacyOptionImplemented (WEP 128bit)	"
43	"	"	"	dot11BeaconPeriod	"
44	"	"	"	dot11RTSThreshold	"
N/A ²	"	"	"	dot11FragmentationThreshold	"

Πέμπτη Ομάδα Πειραμάτων:

Εναλλαγή Αποστολέα Παραλήπτη.

A/a	Τοπολογία	Αποστολέας	Παραλήπτης	MIB	Εργαλείο
51	W/W	Windows 2K	Windows XP	Προεπιλογές ¹	TTCP
21	"	Windows XP	Windows 2K	"	TTCP

Έκτη Ομάδα Πειραμάτων:

Σφάλματα Μετάδοσης λόγω εμποδίων.

A/a	Τοπολογία	Αποστολέας	Παραλήπτης	MIB	Εργαλείο
61	W/E	Windows 98	Windows XP	Προεπιλογές ¹ – Οχι Εμπόδια.	TTCP
62	W/E	"	"	Εμπόδια.	TTCP

Το πείραμα υπ' αριθμόν 0 περιέχει τις βασικές ρυθμίσεις.

¹ Οι τιμές των αντικειμένων της MIB ήταν αυτές που έχει θέσει ο κατασκευαστής.

² Το πείραμα δεν εκτελέστηκε

Πίνακας 35 - Η Κατηγοριοποίηση των Πειραμάτων.

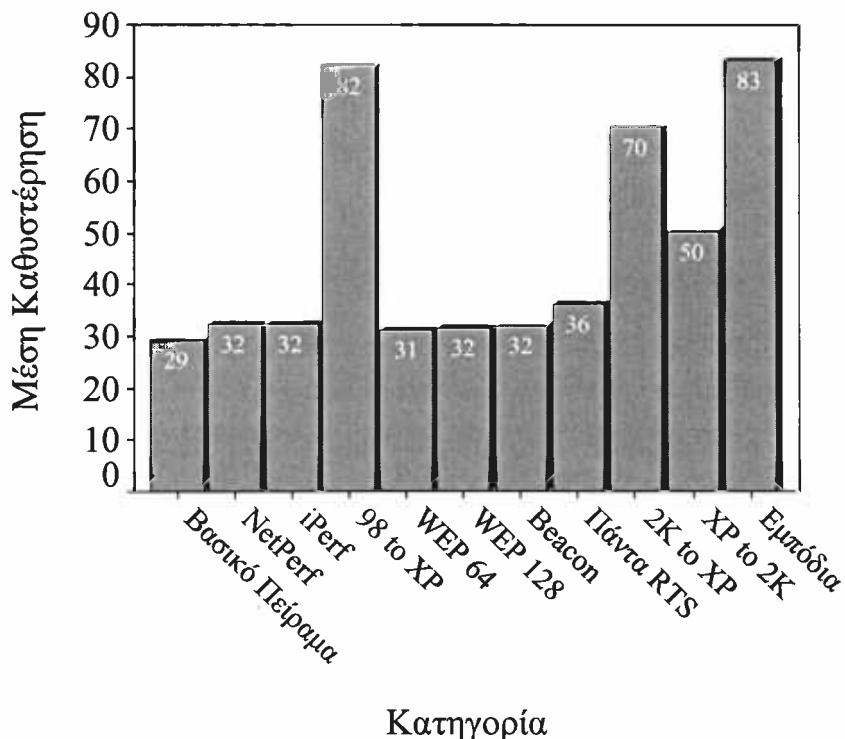
11 ΤΕΛΙΚΑ ΣΥΜΠΕΡΑΣΜΑΤΑ – ΠΕΡΑΙΤΕΡΩ ΕΡΕΥΝΑ.

Έχοντας ολοκληρώσει το μέρος της εργασίας, το σχετικό με την στατιστική επεξεργασία των αποτελεσμάτων, θεωρούμε σκόπιμο να προχωρήσουμε με μία γενικότερη ανάλυση των ευρημάτων μας.

Γέρα από αυτή την ανάλυση, θα επεκταθούμε σε πειράματα και ελέγχους που επιθυμούσαμε, αλλά τελικά δεν πραγματοποιήσαμε, είτε λόγω πίεσης χρόνου είτε λόγω έλλειψης του απαραίτητου εξοπλισμού. Επίσης, θα σχολιάσουμε ποια πειράματα πρέπει να επαναληφθούν και να προσεχθούν και, κυρίως, με τι ρυθμίσεις.

11.1 ΕΠΙΔΟΣΕΙΣ WINDOWS XP.

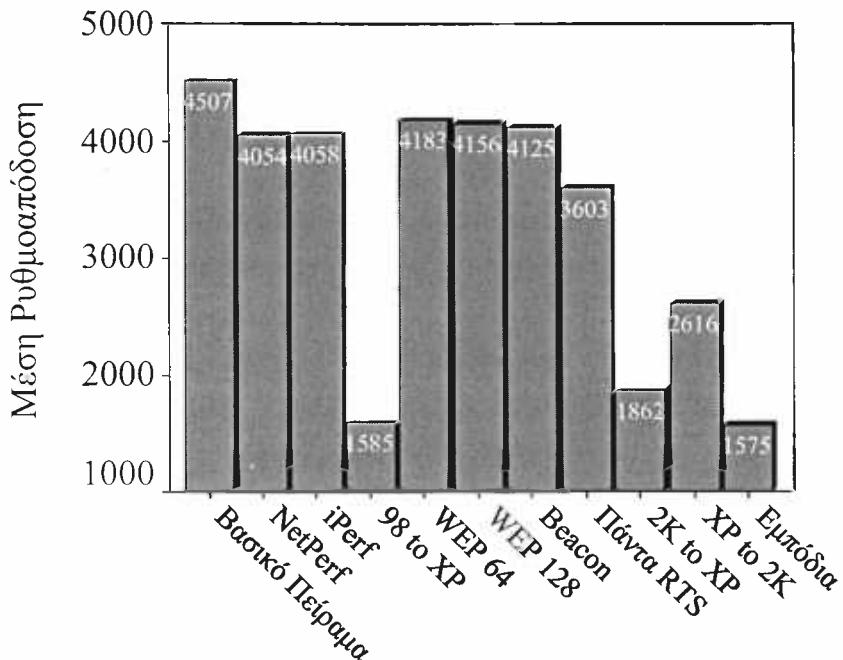
Μία αρχική παρατήρηση που έχουμε να κάνουμε και που θέλουμε να επισημάνουμε, για άλλη μία φορά, είναι η συμπεριφορά των Windows XP.



Σχήμα 58 - Ραβδόγραμμα για την Μέση Καθυστέρηση σε κάθε Πείραμα.

Είναι εντυπωσιακό, το πόσο πολύ αυξάνει η μέση καθυστέρηση στα τέσσερα πειράματα, από τα 11 που απεικονίζονται στο ραβδόγραμμα. Είναι ακόμα πιο ενδιαφέρουσα η παρατήρηση ότι και στα τέσσερα αυτά πειράματα, ο ένας από τους δύο υπολογιστές ήταν αυτός με τα Windows XP.

Όπως αναφέραμε και στο προηγούμενο κεφάλαιο, αυτό το φαινόμενο μπορεί να οφείλεται σε κάποιο πρόβλημα με το υλικό του συγκεκριμένου υπολογιστή (κύριοι υποπτοί είναι η PCMCIA θύρα και η Motherboard) ή με τους οδηγούς της κάρτας για το συγκεκριμένο λειτουργικό σύστημα.



Κατηγορία

Σχήμα 59 - Ραβδόγραμμα για την Μέση Ρυθμοαπόδοση σε κάθε Πείραμα.

Πάντως, από τα τέσσερα παραπάνω πειράματα, στα τρία που παρουσιάζουν μέση καθυστέρηση πάνω από 70 δευτερόλεπτα, ο υπολογιστής με τα Windows XP ήταν ο εξυπηρετητής. Στο δε τέταρτο ήταν ο πελάτης. Με βάση τα παραπάνω νούμερα, δεν θα ήταν παράλογο να υποπτευθούμε ότι το πρόβλημα προκύπτει κυρίως όταν ο υπολογιστής λαμβάνει δεδομένα. Είναι λοιπόν, πιθανό, μια λογική τιμή για την μέση καθυστέρηση της τοπολογίας Wireless to Wireless να είναι γύρω στα 50 δευτερόλεπτα, αν θεωρήσουμε ότι, στην περίπτωση που τα Windows XP στέλνουν, δεν παρουσιάζουν ανώμαλη συμπεριφορά. Αυτό γιατί σε τέτοια τοπολογία αναφέρεται το τέταρτο από τα πειράματα για τα οποία έγινε λόγος σε αυτήν την παράγραφο.

Ας θυμηθούμε, τώρα, τα αποτελέσματα της υπόθεσης 2. Η υπόθεση αυτή έλεγε ότι η μέση καθυστέρηση δεν επηρεάζεται από την τοπολογία. Η υπόθεση, τελικά, απορρίφθηκε, γιατί, για την μέτρηση της δεύτερης τοπολογίας Wireless to Wireless, αναγκαστήκαμε να αλλάξουμε και το λειτουργικό σύστημα του ενός υπολογιστή. Κατά σύμπτωση, στον έλεγχο της τοπολογίας που παρουσίασε ψηλή καθυστέρηση, χρησιμοποιήσαμε τον

υπολογιστή με τα Windows XP. Ίσως τελικά η αύξηση της καθυστέρησης στην υπόθεση 2, να οφείλεται κατά κυριότερο λόγο στην ύπαρξη των Windows XP παρά στην αλλαγή της τοπολογίας. Βέβαια, αν τελικά η παραπάνω υπόθεση περί μέσης καθυστέρησης σε τοπολογία Wireless to Wireless, είναι όντως γύρω στα 50 δευτερόλεπτα, τότε ορθά απορρίψαμε την υπόθεση 2.

Όπως και να έχουν τα πράγματα, εμείς πρέπει να αναφέρουμε ότι θα άξιζε, στο μέλλον, να ξαναγίνουν οι μετρήσεις με κάποιο άλλο Windows XP μηχάνημα και ενδεχομένως, με νέους οδηγούς.

11.2 ΤΑ ANTIKEIMENA ΤΗΣ MIB.

Έχουμε ήδη καταγράψει, σε προηγούμενο κεφάλαιο, το ενδιαφέρον μας για την επίδραση των αντικειμένων της MIB.

Αν θέλουμε να βγάλουμε ένα γενικό συμπέρασμα, θα μπορούσαμε να πούμε ότι οι παράμετροι που διαλέξαμε, εν γένει, επηρεάζουν την απόδοση του δικτύου. Επίσης, θα πρέπει να αναφέρουμε ότι οι εργοστασιακές τιμές ήταν οι βέλτιστες και δεν καταφέραμε επηρεάζοντας κάποια παράμετρο να βελτιώσουμε τις επιδόσεις.

Βέβαια, πρέπει να αναφερθεί εδώ ότι δεν ασχοληθήκαμε με τις παραμέτρους της MIB που δεν είχαν άμεση σχέση με την τεχνολογία IEEE 802.11. Έτσι δεν μεταβάλαμε κανένα αντικείμενο της MIB – II. Τα μόνα αντικείμενα τα οποία μας απασχόλησαν ήταν αυτά που ορίζονται μέσα στο ίδιο το πρότυπο, δηλαδή το group {.1.2.840.10036}.

Συγκεκριμένα, πάντως, θα πρέπει να επαναλάβουμε το συμπέρασμα ότι οι επιδόσεις μεταξύ WEP 64bit και WEP 128bit, δεν παρουσιάζουν διαφορές στην μέση καθυστέρηση. Αυτό μας δείχνει ότι η κρυπτογράφηση των δεδομένων με κλειδί μεγαλύτερου μήκους δεν μας επιβαρύνει με αξιοσημείωτη καθυστέρηση. Είναι, βέβαια, περιττό να αναφέρουμε ότι η χρήση κλειδιών μήκους 128bit, δεν προσθέτει περισσότερη κίνηση στο δίκτυο, ούτε μέσω του πλήθους των πλαισίων ούτε μέσω του μεγέθους τους, σε σχέση με τον αριθμό και το μέγεθος των πλαισίων που κυκλοφορούν στο δίκτυο στην περίπτωση κλειδιών μήκος 64bit.

11.3 FRAGMENTATION THRESHOLD.

Όπως αναφέραμε και σε προηγούμενο κεφάλαιο, μία παράμετρος που θέλαμε να ελέγξουμε ήταν η **dot11FragmentationThreshold**. Αυτό το αντικείμενο της MAC MIB, καθορίζει το μέγιστο μέγεθος πλαισίου MAC που μπορεί να παραδοθεί στο φυσικό επίπεδο.

Ο κατακερματισμός ενός πλαισίου MAC σε μικρότερα, επιβαρύνει την μέση καθυστέρηση για δύο λόγους.

Ο πρώτος είναι ότι προστίθεται overhead στο δίκτυο. Πράγματι αν ένα πλαίσιο έχει μέγεθος δεδομένων (χωρίς την επικεφαλίδα) S και το μέγιστο μέγεθος πλαισίου (χωρίς την επικεφαλίδα) που δεν κατακερματίζεται είναι $SMax$ τότε ο αριθμός πλαισίων N που χρειάζονται για την μετάδοση είναι το πάνω ακέραιο μέρος της διαίρεσης του S με το $SMax$, δηλαδή $N = \left\lceil \frac{S}{SMax} \right\rceil = \left\lceil \frac{S}{SMax} \right\rceil + 1 = S \text{ div } SMax + 1$. Αν θεωρήσουμε ότι η επικεφαλίδα MAC είναι πάντα μήκους 34Bytes τότε, είναι προφανές ότι ισχύει $\text{dot11FragmentationThreshold} = SMax + 34$, αφού η τιμή του εν λόγω αντικειμένου της MIB περιγράφει μέγεθος μαζί με την επικεφαλίδα. (Να σημειωθεί ότι, ειδικά εδώ, στο μήκος της επικεφαλίδας συμπεριλαμβάνουμε και τα 4Bytes του πεδίου FCS).

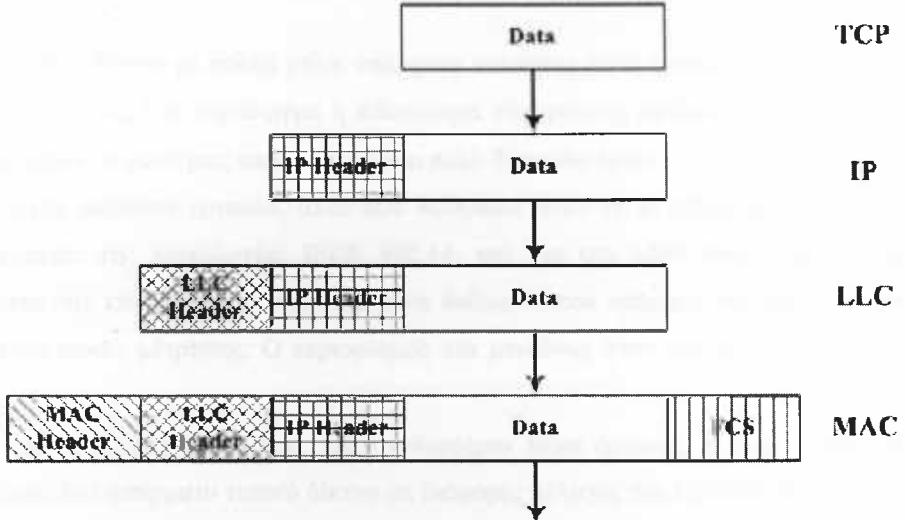
Τα δεδομένα λοιπόν που θα μπουν στο δίκτυο θα είναι το μέγεθος των δεδομένων σε Bytes συν τον αριθμό των πλαισίων επί το μήκος της επικεφαλίδας που, για το επίπεδο MAC του IEEE 802.11, είναι περίπου 34Bytes. Δηλαδή $S + 34 \cdot N$ Bytes περίπου. Στην περίπτωση που δεν υπάρχει κατακερματισμός μεταδίδονται $S + 34$ Bytes, δηλαδή τελικά έχουμε μια διαφορά της τάξης των $34 \cdot (N - 1)$ Bytes από τις $N - 1$ πρόσθετες επικεφαλίδες

Αυτό το overhead προστίθεται μόνο από το μήκος των επιπλέον επικεφαλίδων. Δεν είναι όμως το μοναδικό. Δεν πρέπει να ξεχάσουμε το overhead λόγω των περισσότερων RTS/CTS ανταλλαγών που θα χρειαστούν, ούτε το overhead από τα επιπλέον Headers του φυσικού επιπέδου.

Το δεύτερο είδος Overhead προστίθεται, φυσικά, από τη καθυστέρηση που χρειάζεται ο κατακερματισμός και η δημιουργία των νέων πλαισίων και η ανασύνθεσή τους στον παραλήπτη.

Θα ήταν πραγματικά πολύ ενδιαφέρον να δει κανείς και ένα άλλο θέμα. Αυτό που αναφέρεται στην συσχέτιση μεταξύ του μέγιστου πακέτου MAC που μπορεί να περάσει από το δίκτυο και του μέγιστου Datagram που μπορεί να περάσει από το δίκτυο. Θεωρητικά, αν το μέγιστο MAC πλαίσιο είναι μεγαλύτερο ή ίσο από το μέγιστο IP Datagram, συν τα επιπλέον δεδομένα από τα επίπεδα LLC και MAC, δηλαδή αν ισχύει $SMaxMAC \geq SMaxIP + LLCHeader + MACHeader + FCS$, τότε κανένα πλαίσιο δεν θα κατακερματίζεται στο επίπεδο MAC. Όλος ο πιθανός κατακερματισμός θα γίνεται σε επίπεδο IP. Βέβαια το μέγιστο μήκος ενός IP Datagram είναι 64KBytes, συνεπώς η παραπάνω περίπτωση είναι καθαρά θεωρητική. Μια πιο ρεαλιστική υπόθεση είναι, το μέγιστο μέγεθος του IP Datagram συν την επικεφαλίδα LLC να είναι ακέραιο πολλαπλάσιο του μέγιστου MAC payload, ώστε να μην σπαταλούνται MAC πλαίσια για την αποστολή περίσσιας δεδομένων.

Η σωστή ρύθμιση των δύο παραπάνω παραμέτρων, μπορεί να βελτιώσει σημαντικά τις επιδόσεις ενός δικτύου.



Σχήμα 60 - Οι Προσθήκες Headers ανά Επίπεδο Δικτύου.

11.4 RTS / CTS.

Όπως αναφέραμε στην υπόθεση 5, στο προηγούμενο κεφάλαιο, η αρχική τιμή του αντικειμένου `dot11RTSThreshold` ήταν 2347. Το μέγιστο μέγεθος MAC πλαισίου είναι 2346Bytes. Έτσι, με αυτή την τιμή, ουσιαστικά, απενεργοποιείται για όλα τα πλαίσια η ακολουθία μηνυμάτων RTS / CTS.

Ενεργοποιώντας την για όλα τα πλαίσια, παρατηρήσαμε σαφή μείωση των επιδόσεων. Αυτό οφείλεται, σαφώς στην αύξηση του αριθμού των πλαισίων που κυκλοφορούν στο δίκτυο.

Ωστόσο, δεν μπορούμε να ισχυριστούμε ότι αυτό το αποτέλεσμα γενικεύεται, για την περίπτωση που το δίκτυο είναι μεγάλου μεγέθους. Ενδέχεται, η αύξηση του αριθμού των σταθμών, να απαιτεί την ενεργοποίηση του RTS/CTS τουλάχιστον για τα μεγάλα πλαίσια, αν όχι για όλα.

11.5 ΜΕΓΕΘΟΣ ΔΙΚΤΥΟΥ.

Είναι ένα θέμα που έχει ήδη επισημανθεί με έμμεσο τρόπο. Σε αυτή την παράγραφο θα του αφιερώσουμε λίγη περισσότερη έκταση.

Το ασύρματο δίκτυο που εγκαταστήσαμε, ουσιαστικά, αποτελούσαν δύο σταθμοί IEEE 802.11, το Access Point και ένας σταθμός με Ethernet.

Συνεπώς, όλα τα συμπεράσματα που βγάλαμε από τους ελέγχους των έξι υποθέσεων, ισχύουν για δίκτυα μικρού μεγέθους. Και αν μπορούμε να θεωρήσουμε πως οι υποθέσεις για τα λειτουργικά συστήματα, την εναλλαγή ρόλων, τα εμπόδια και τα

εργαλεία γενικεύονται για μεγάλα δίκτυα, σε καμία περίπτωση δεν μπορούμε να κάνουμε την ίδια γενίκευση για τις υποθέσεις σχετικά με την τοπολογία και τις παραμέτρους της MIB.

Σε ένα δίκτυο με πολλά μέλη, υπάρχουν συνθήκες πολύ διαφορετικές από αυτές των πειραμάτων μας. Για παράδειγμα η πιθανότητα σύγκρουσης αυξάνεται κατά πολύ. Το να διατηρηθούν οι συνθήκες υπό έλεγχο είναι πολύ δύσκολο έργο.

Στην παρούσα εργασία, αυτό που θελήσαμε ήταν να μετρήσουμε τις πραγματικές δυνατότητες της τεχνολογίας IEEE 802.11, και για τον λόγο αυτό περιορίσαμε στο ελάχιστο την κίνηση στο δίκτυο. Τα μόνα δεδομένα που υπήρχαν στο δίκτυο ήταν αυτά των εφαρμογών μέτρησης. Ο περιορισμός του μεγέθους ήταν μια θησεία που έπρεπε να γίνει.

Θα αποτελούσε, ωστόσο, πολύ ενδιαφέρον θέμα έρευνας, η διερεύνηση του πώς αντιδράει ένα ασύρματο τοπικό δίκτυο σε διάφορες αλλαγές των συνθηκών.

Για παράδειγμα, πως μεταβάλλεται η καθυστέρηση στην επικοινωνία δύο σταθμών αν, ταυτόχρονα, μεταξύ άλλων σταθμών στο δίκτυο, υπάρχουν άλλης μορφής επικοινωνίας. Άραγε ένα τέτοια δίκτυο να αντιδρά διαφορετικά όταν υπάρχουν πολλές μικρές TCP συνδέσεις (POP3) και διαφορετικά όταν υπάρχουν λίγες με μεταφορά πολλών δεδομένων (FTP); Πώς επηρεάζονται οι επιδόσεις από την ύπαρξη πολλών UDP πακέτων;

Φυσικά δεν πρέπει να αγνοήσουμε ότι το δίκτυο που δοκιμάσαμε ήταν ένα δίκτυο τεχνολογίας IEEE 802.11b. Παρόμοια έρευνα θα μπορούσε να γίνει στο μέλλον με την τεχνολογία IEEE 802.11a.

ΒΙΒΛΙΟΓΡΑΦΙΑ – ΠΗΓΕΣ.

Συγγραφέας	Τίτλος	Εκδόσεις	Έτος
1. Rifaat A. Dayem	Mobile Data & Wireless LAN Technologies.	Prentice Hall	1997
2. Jim Geier	Wireless LANs. Implementing High Performance IEEE 802.11 Networks.	SAMS Publishing	2000
3. James D. Solomon	Mobile IP. The Internet Unplugged.	Prentice Hall	1998
4. William Stallings	SNMP, SNMPv2, SNMPv3, RMON1 and 2.	Addison Wesley	1999
5. Θεόδωρος Αποστολόπουλος	Δίκτυα Υπολογιστών. Μετάδοση Δεδομένων – Επικοινωνιακό Υποδίκτυο.		1994
6. Θεόδωρος Αποστολόπουλος	Ανώτερα Επίπεδα σε Δίκτυα Υπολογιστών.		1998
7. Δημήτριος Αθανασόπουλος	Επαγγεική Στατιστική.	Εκδόσεις Α. Σταμούλης	1990
8. Δημήτριος Αθανασόπουλος	Θεωρία Πιθανοτήτων – Μέρος II. Κατανομές Πιθανότητας Τυχαίων Μεταβλητών.	Εκδόσεις Α. Σταμούλης	1991
9. Δημήτριος Αθανασόπουλος	Περιγραφική Στατιστική.	Εκδόσεις Α. Σταμούλης	1989
10. Δημήτριος Καφέρες	Μαθήματα Ανάλυσης Παλλινδρόμησης.	Εκδόσεις Α. Σταμούλης	1991
11. Δημήτριος Καφέρες	Μαθήματα Ανάλυσεως Διακυμάνσεως.	Εκδόσεις Α. Σταμούλης	1989

11.6 ΠΑΝΕΠΙΣΤΗΜΙΑΚΕΣ ΠΑΡΑΔΟΣΕΙΣ.

- Θεόδωρος Αποστολόπουλος "Δίκτυα Υπολογιστών", Μεταπτυχιακό Πρόγραμμα Σπουδών σε Πληροφοριακά Συστήματα, Ο.Π.Α. 2000 – 2001.
- Γεώργιος Σταμούλης "Ρυθμιστική Πολιτική και Τηλεπικοινωνίες", Μεταπτυχιακό Πρόγραμμα Σπουδών σε Πληροφοριακά Συστήματα, Ο.Π.Α. 2000 – 2001.

11.7 ΠΗΓΕΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ.

- <http://www.caida.org>
- <http://www.ieee> Institute of Electrical and Electronic Engineers
- <http://www.ietf.org> Internet Engineering Task Force
- <http://www.cisco.com>
- <http://www.dlink.com> D – Link
- <http://www.hp.com> Hewlett Packard
- <http://www.lucent.com> Lucent Technologies
- <http://www.wirelesstethernet.com> WECA Wireless Ethernet Compatibility Alliance
- <http://www.wlana.org> WLANA Wireless LAN Alliance
- <http://www.wi-fi.com> WI-FI Wireless Fidelity
- <http://ftp.arl.army.mil/~mike/ttcp.html> The Story of the TTCP Program.
- <http://sat.gmd.de/docs/o-tel-o.html> Internet over satellite and cable networks.

11.8 ΑΡΘΡΑ.

Συγγραφέας	Τίτλος	Δημοσίευση	Έτος
1. Jill Gemmill University of Alabama at Birmingham	Blind Men Feeling The Elephant. Managing Application Network Performance: Standards, Tools And Challenges	Integrated Design and Process Technology, IDPT- Vol.1	2001
2. Jim Brady, Terry Martin, Gomathy Naranan	Evaluation of Throughput Probes for Measuring IP Service Performance		
3. Constantinos Dovrolis	What do packet dispersion techniques measure?	www.caida.org	



Συγγραφέας	Τίτλος	Δημοσίευση	Έτος
Parameswaran Ramanathan David Moore			
4. Nevil Brownlee, Chris Loosley	Fundamentals of Internet Measurement: A Tutorial	Journal of Computer Resource Management	2001
5. Martin Borris, Uwe Dannowski, Hermann H.artig	TCP Performance over ATM on Linux and Windows NT	proceedings of the 1st IEEE Conference on ATM Networking (ICATM'98), Colmar, France	1998
6. Michal Przybylski Szymon Trocha	Network measurement tools tests.	Poznan Supercomputing and Networking Center	2001
7. Serge Tessier Maria Amparo Sanmateu Werner Pommenger	Evaluation of Mobile IPv4. Network Performance Tests and Results.	Active Networks and Mobility T-Nova Deutsche Telekom Innovationsgesellschaft mbH	
8. Kacker, Liu, Yen, Zhang, Wilkinson, Marbukh, Kelley, Mills, Montgomery	Understanding Internet Performance From The User Perspective	DARPA Network Modeling and Simulation Workshop, Albuquerque, NM	2000

11.9 ΠΡΟΤΥΠΑ, RFC ΚΑΙ INTERNET DRAFTS.

Όνομα	Πλήρης Τίτλος
1. IEEE 802.11	“Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”.
2. IEEE 802.11a	“Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. High-speed Physical Layer in the 5 GHz Band”.
3. IEEE 802.11b	“Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification. Higher-Speed Physical Layer Extension in the 2.4 GHz Band”.
4. IEEE 802.11f Draft 2	Recommended Practice for Multi – Vendor Access Point Interoperability via an Inter – Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation.
5. RFC 768	User Datagram Protocol.
6. RFC 791	Internet Protocol.
7. RFC 793	Transmission Control Protocol.
8. RFC 1155	Structure and Identification of Management Information for TCP/IP – based Internets.
9. RFC 1157	A Simple Network Management Protocol (SNMP).
10. RFC 1212	Concise MIB Definition.
11. RFC 1213	Management Information Base for Network Management of TCP/IP– based Internets: MIB – II.
12. RFC 1757	Remote Network Monitoring Management Information Base.
13. RFC 1883	Internet Protocol, Version 6 (IPv6).
14. RFC 1884	IP Version 6 Addressing Architecture.
15. RFC 1901	Introduction to Community – Based SNMPv2.
16. RFC 1902	Structure of Management Information for SNMPv2.
17. RFC 1903	Textual Conventions for SNMPv2.
18. RFC 1904	Conformance Statements for SNMPv2.
19. RFC 1905	Protocol Operations for SNMPv2.
20. RFC 1906	Transport Mappings for SNMPv2.
21. RFC 1907	Management Information Base for SNMPv2.
22. RFC 1908	Coexistence Between Version 1 and Version 2 of the Internet – Standard Network Management Framework
23. RFC 1971	IPv6 Stateless Address Autoconfiguration.
24. RFC 2002	IP Mobility Support.
25. RFC 2003	IP Encapsulation Within IP.
26. RFC 2004	Minimal Encapsulation Within IP.
27. RFC 2021	Remote Network Monitoring Management Information Base – II.



Όνομα	Πλήρης Τίτλος
28. RFC 2074	Remote Network Monitoring MIB Protocol Identifiers.
29. RFC 2271	An Architecture for Describing SNMP Management Frameworks.
30. RFC 2272	Message Processing and Dispatching for SNMP.
31. RFC 2273	SNMPv3 Applications
32. RFC 2274	User – Based Security Model for SNMPv3.
33. RFC 2330	Framework for IP Performance Metrics.
34. RFC 2678	IPPM Metrics for Measuring Connectivity.
35. RFC 2679	A One-way Delay Metric for IPPM.
36. RFC 2680	A One-way Packet Loss Metric for IPPM.
37. RFC 2681	A Round-trip Delay Metric for IPPM.
38. RFC 3148	A Framework for Defining Empirical Bulk Transfer Capacity Metrics.
39. Draft Document	IP Packet Delay Variation Metric for IPPM.
40. Draft Document	One-way Loss Pattern Sample Metrics.
41. Draft Document	Network performance measurement for periodic streams.
42. Draft Document	A One-way Delay Measurement Protocol.
43. Draft Document	A One-way Active Measurement Protocol Requirements.
44. Draft Document	Generic Packet Tunneling in IPv6 Specification.
45. Draft Document	Mobility Support in IPv6.

Dyrd

