«ΑΝΑΛΥΣΗ ΠΡΟΣΟΜΟΙΩΣΗ ΚΑΙ ΠΕΡΙΓΡΑΦΗ ΠΡΩΤΟΚΟΛΛΩΝ ΑΣΦΑΛΕΙΑΣ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ»

ΣΠΟΥΔΑΣΤΗΣ

ΜΠΑΡΟΥΤΑΣ ΑΛΕΞΑΝΔΡΟΣ

ΕΙΣΗΓΗΤΗΣ

ΡΙΖΟΣ ΓΕΩΡΓΙΟΣ

Στα αδέρφια μου και τους γονείς μου
που με στήριξαν σε ότι έχω κάνει ως τώρα
στην ζωή μου πνευματικά
και οικονομικά .

Στον καθηγητή μου που με βοήθησε
όλο αυτόν τον καιρό με τις γνώσεις
και τις ιδέες του.

Στους συμφοιτητές και κολλητούς μου
φίλους που με στήριξαν ψυχολογικά
κατά την διάρκεια της εργασίας.

Μπαρούτας Αλέξανδρος

Φοιτητής ΤΕΙ Ηπείρου

Baroutas_alex@yahoo.gr

Επιβλέπων καθηγητής: Ρίζος Γεώργιος

Καθηγητής λειτουργίας δικτύου δεδομένων, φωνής-τηλεματικών υπηρεσιών και πολυμέσων

georizos@teiep.gr

Περίληψη

Σκοπός της πτυχιακής εργασίας είναι να περιγράψει τα πρωτόκολλα ασφαλείας αλλά και κρυπτογράφησης, που είναι εγκατεστημένα μέσα στις ασύρματες συσκευές που χρησιμοποιούμε στη καθημερινότητά μας. Με τη χρήση προγράμματος γνωστής εταιρίας πάνω στα δίκτυα, θα υλοποιηθεί προσομοίωση ενός τοπικού ασύρματου δικτύου κάνοντας χρήση ενός πρωτοκόλλου που θα έχουμε αναφερθεί μέσα στην εργασίας.

Πιο συγκεκριμένα, το πρώτο κεφάλαιο θα παρέχει γενικές πληροφορίες που αφορούν τα δίκτυα, όπως επίσης και την ανάγκη του ανθρώπου να τα εξελίξει ώστε να μπορέσει να επικοινωνήσει πιο εύκολα και γρήγορα. Στο αμέσως επόμενο κεφάλαιο γίνεται περιγραφή των ασύρματων δικτύων, με αναφορά των πλεονεκτημάτων και των μειονεκτημάτων τους, τρόποι λειτουργίας αλλά και βασικές λειτουργίες των ασύρματων συσκευών. Το τρίτο κεφάλαιο αναφέρεται στα είδη των αλγορίθμων κρυπτογράφησης και στη σύγκρισή τους με τα πρωτόκολλα κρυπτογράφησης WEP και WPA/WPA2. Το τέταρτο κεφάλαιο επικεντρώνεται πάνω στα είδη των ασύρματων επιθέσεων αλλά και στους τρόπους αντιμετώπισης αυτών με χρήση βοηθητικών προγραμμάτων αλλά και αλλαγών πάνω στην ασύρματη συσκευή. Στο πέμπτο κεφάλαιο θα γίνει η γνωριμία μας με το πρόγραμμα προσομοίωσης . Τρόποι λειτουργίας, εντολές και παράμετροι είναι τα βασικά στοιχεία που αναφέρονται και πρέπει να ασκηθούν πάνω στις ενσύρματες και ασύρματες συσκευές προκειμένου να υλοποιηθεί η προσομοίωση του ασύρματου δικτύου.

Baroutas Alexandros

Student TEI Epirus

Baroutas_alex@yahoo.gr

Thesis Supervisor: Rizos George

Professor data network operation, voice-telematic and multimedia

georizos@teiep.gr

Abstract

The aim of the thesis is to describe the security protocols and encryption, which is installed into the wireless devices we use in our daily lives. By using known company program on the networks will be implemented simulation of a local wireless network by using a protocol that we will mention in the work.
More specifically, the first chapter provides general information on the network as well as the human need to progress in order to be able to communicate more easily and quickly. In the next chapter is a description of wireless networks, indicating the advantages and disadvantages of operating modes and basic functions of the wireless devices. The third chapter discusses the types of encryption algorithms and their comparison with the WEP encryption protocols and WPA / WPA2. The fourth chapter focuses on the types of wireless attacks and ways to tackle them using utilities and changes on the wireless device. The fifth chapter will make our acquaintance with the simulation program. Modes, commands and parameters are the key elements listed and must be exercised on the wired and wireless devices in order to realize the simulation of the wireless network.

Analysis simulation and description of wireless network security protocols.

By

Baroutas Alexandros

Thesis Supervisor: Rizos George

Ευχαριστίες

Θερμές ευχαριστίες στο Κύριο Γεώργιο Ρίζο, υπεύθυνο λειτουργίας δικτύου δεδομένων, φωνής-τηλεματικών υπηρεσιών και πολυμέσων του ΤΕΙ Ηπείρου ,που με βοήθησε καθ' όλη την διάρκεια του εξαμήνου όπου μου χρειάστηκε προκειμένου να υλοποιήσω την πτυχιακή αυτή εργασία. Ακόμα θα ήθελα να ευχαριστήσω την οικογένεια μου και τους κολλητούς μου φίλους ,που με στήριξαν ψυχολογικά όλη αυτή την διάρκεια.

Δήλωση Πνευματικής ιδιοκτησίας

Δηλώνω ότι η πτυχιακή εργασία που παραδίδω είναι αποτέλεσμα πρωτότυπης έρευνας και δεν χρησιμοποιεί πνευματική ιδιοκτησία τρίτων χωρίς αναφορές. Επίσης όλες οι πηγές που χρησιμοποιήθηκαν για την εργασία αναγράφονται στις βιβλιογραφικές αναφορές στο τέλος κάθε κεφαλαίου και στο τέλος της πτυχιακής εργασίας.

Λίστα εικόνων (1/2)

Λίστα εικόνων (2/2)

Περιεχόμενα

ΚΕΦΑΛΑΙΟ 1ο Γενικές πληροφορίες-Εισαγωγικά

Εισαγωγή 1ου κεφαλαίου

Το πρώτο κεφάλαιο της πτυχιακής αυτής εργασίας έχει ως στόχο να ενημερώσει τους αναγνώστες για την σπουδαία ανακάλυψη του ασύρματου δικτύου, αλλά και για την ραγδαία (σε σύγκριση με τον χρόνο) ανάπτυξή του. Γίνεται ιστορική αναδρομή προκειμένου να αναφερθεί ο εφευρέτης της ανακάλυψης αυτής, ο τρόπος βελτίωσής της μέσα στις δεκαετίες ,οι τεχνικές που χρησιμοποιήθηκαν για την ανάπτυξής της όπως επίσης και η μεγάλη ζήτηση που επικρατεί στις μέρες μας από ένα μεγάλο πλήθος χρηστών υπηρεσιών του διαδικτύου έχοντας ως στόχο την καθημερινή τους ενημέρωση με εύκολο και γρήγορο τρόπο μέσω των ασύρματών τους συσκευών .

1.1Γενικά

Ζούμε σε μία εποχή όπου η τεχνολογία αναπτύσσετε με ραγδαίους ρυθμούς και σε όλους τους κλάδους της. Η εξάπλωση του δικτύου υπολογιστών είναι ένας από αυτούς και αποτελεί ένα αναπόσπαστο κομμάτι στη ζωή του σύγχρονου ανθρώπου. Η αλματώδη εξέλιξή του τόσο στον τομέα των ενσύρματων δικτύων όσο και στον τομέα των ασύρματων δικτύων έχει καταφέρει να το φέρει στις πρώτες θέσεις μελέτης και έρευνας μεγάλων επιστημόνων. Ιδιαίτερα αν σκεφτεί κανείς ότι μόλις τον $20^{ο}$ αιώνα καταφέραμε την απομακρυσμένη επικοινωνία και την μετάδοση πληροφορίας μέσω ηλεκτρονικών συσκευών ,τότε μπορεί εύκολα να συμπεράνει κανείς πως με τον καιρό ο άνθρωπος χρειάστηκε να δημιουργήσει τα δίκτυα υπολογιστών που είναι υπεύθυνα για την επεξεργασία και την διακίνηση της πληροφορίας έχοντας ως πρωτεύων στόχο την γρηγορότερη και αποτελεσματικότερη μετάδοσή της.

Σκοπός του ανθρώπου ήταν να ξεφύγει από τα πλαίσια εργασίας εντός γραφείου και να καταφέρει να εργαστεί εκτός αυτού κάνοντας χρήση του φορητού του υπολογιστή και κάποιου είδους δικτύου υπολογιστών. Με την έννοια του δικτύου υπολογιστών αναφερόμαστε σε μία ομάδα από δύο ή περισσότερους υπολογιστές οι οποίοι είναι συνδεδεμένοι μεταξύ τους ενσύρματα ή ασύρματα, ώστε να μπορούν να ανταλλάζουν πληροφορίες.

Ακόμα, δεν μπορεί κανείς να παραλείψει και την μεγάλη απήχηση που έχει τα τελευταία χρόνια το ασύρματο δίκτυο ,που με την δημιουργία του Wi-Fiεπετεύχθητε η γρηγορότερη και απλούστερη διαδικασία σύνδεση ενός χρήστη στο Internet.Πλέον ,εγκαταστάσεις τοπικών ασύρματων δικτύων υπάρχουν σε πολλούς δημόσιους χώρους, εταιρίες και πανεπιστήμια δίνοντας την δυνατότητα στους χρήστες να συνδεθούν με την τηλεφωνική ή και ασύρματη συσκευή του.

1.2 Ιστορική αναδρομή

Η τρίτης χιλιετίας μπορεί εύκολα να χαρακτηριστεί ως δικτυακή εποχή και αυτό οφείλεται στο Μαρκόνι που από το 1901 ανακάλυψε και έθεσε σε χρήση ένα ασύρματο τηλέγραφο ανάμεσα στα πλοία και στη ξηρά προκειμένου να επικοινωνήσουν. Ως κώδικα ο Μαρκόνι ,χρησιμοποίησε τα σήματα μορς τα οποία αποτελούνταν από τελείες και παύλες(δυαδικό σύστημα). Από το σημείο αυτό και έπειτα τα ψηφιακά ασύρματα δίκτυα βελτιώθηκαν έχοντας πάντα ως βασική ιδέα αυτό το είδος της επικοινωνίας.

Τα πρώτα ασύρματα δίκτυα εμφανίστηκαν κάνοντας χρήση τεχνολογίας TCP/IP. Οι πρώτες τεχνικές μεταγωγής πακέτων αναπτύχθηκαν κοντά στο 1964, ενώ ο όρος “Packet” πρωτοχρησιμοποιήθηκε από τον D. W. Davies του National Physical Laboratory της Μεγ. Βρετανίας. Τα πρώτα αποτελέσματα των ερευνών έφεραν στο φώς της δημοσιότητας το δίκτυο μεταγωγής πακέτων, ενώ το ίδιο έτος ο οργανισμός ARPA (Advanced Research Projects Agency) των Η.Π.Α. άρχισε να χρηματοδοτεί τα προγράμματα που οδήγησαν στη δημιουργία του ARPAnet το 1969.

Η τεχνολογία των ασυρμάτων δικτύων μετάδοσης πακέτων άρχισε να αναπτύσσεται στην δεκαετία 1970-1980, ενώ η μεγαλύτερη ζήτηση έγινε τον καιρό των μικροϋπολογιστών δηλαδή κοντά στο 1980 με 1990. Λόγω των ιδιαίτερων χαρακτηριστικών του μέσου μεταδόσεως τα ασύρματα δίκτυα χρησιμοποιούσαν και χρησιμοποιούν ακόμα εξειδικευμένα πρωτόκολλα για το επίπεδο πρόσβασης μέσου και το επίπεδο σύνδεσης δεδομένων (Data Link Layer) .

Σήμερα είναι διαθέσιμος ένας αριθμός από καινούργιες συσκευές και προϊόντα ασύρματης επικοινωνίας που βασίζονται σε νέες τεχνολογίες και νέα πρότυπα. Τα τελευταία χρόνια οι κινητοί υπολογιστές (tablet,notebook, laptop) είναι διαθέσιμοι και ελκυστικοί για το ευρύ κοινό, αφού έχουν πλέον συγκρίσιμο κόστος, υπολογιστική ισχύ και ποιότητα υπηρεσιών ίδια με τους σταθερούς υπολογιστές. Όλα αυτά έχουν σαν αποτέλεσμα την έρευνα για την ανάπτυξη προτύπων για την υποστήριξη των ασύρματων επικοινωνιών.

Βιβλιογραφικές αναφορές κεφαλαίου

[1] https://en.wikipedia.org/wiki/Guglielmo_Marco

[2] https://en.wikipedia.org/wiki/Internet_protocol_suite

[3]https://el.wikipedia.org/wiki/%CE%91%CF%83%CF%8D%CF%81%CE%BC%CE%B1%CF%84%CE%BF_%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF

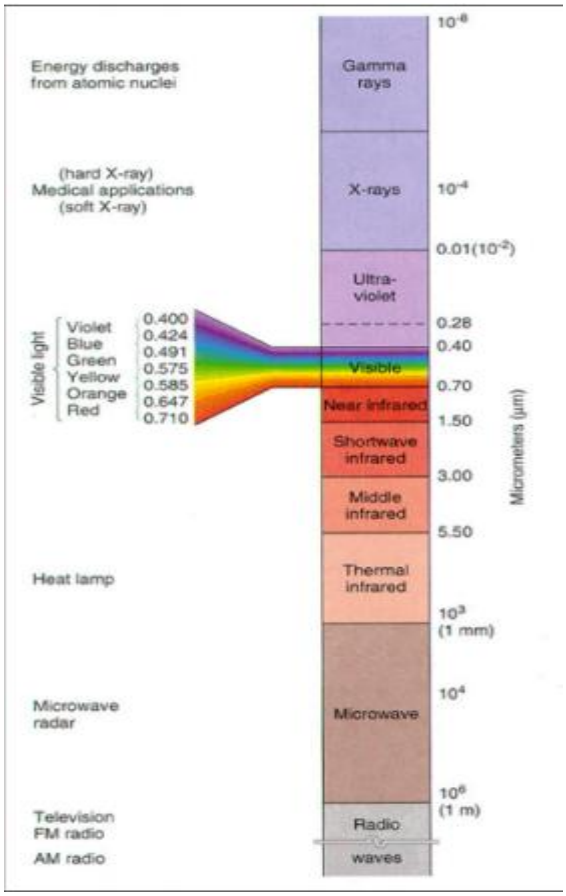
ΚΕΦΑΛΑΙΟ 2ο Ασύρματα Δίκτυα

Εισαγωγή 2ου κεφαλαίου

Στο δεύτερο κεφάλαιο που ακολουθεί αναφέρονται τα βασικά χαρακτηριστικά του ασύρματου δικτύου, ο τρόπος υλοποίησης της επικοινωνίας όπως επίσης και τα χαρακτηριστικά των μεθόδων αυτών. Γίνεται αναφορά των πολυπλεξιών χρόνου και συχνοτήτων και στη συνέχεια αναλύονται τα είδη των ασύρματων δικτύων που χωρίζονται στις εξής τέσσερις κατηγορίες : προσωπικά, τοπικά, μητροπολιτικά και ευρείας εμβέλειας . Μετά την ανάλυση των κατηγοριών αυτών ,παραθέτουμε τα κυριότερα πλεονεκτήματα αλλά και μειονεκτήματα των ασύρματων δικτύων.

2.1 Χαρακτηριστικά ασύρματων δικτύων

Η ασύρματη επικοινωνία υλοποιείται μεταξύ ενός πομπού και ενός δέκτη μεταδίδοντας την πληροφορία μέσω του αέρα και χρησιμοποιώντας ένα είδος κωδικοποίησης. Τα ραδιοκύματα τα οποία είναι υπεύθυνα για την μετάδοση του μηνύματος και που αποτελούν το βασικότερο χαρακτηριστικό στην ασύρματη επικοινωνία, δεν παύουν να είναι τίποτα άλλο από ηλεκτρομαγνητικά σήματα τα οποία έχουν μικρό μήκος κύματος και μεταδίδονται σε διάφορες συχνότητες όπως τα FM και τα AM.



Εικόνα1:Το ηλεκτρομαγνητικό φάσμα

2.1.1 Τρόποι μετάδοσης

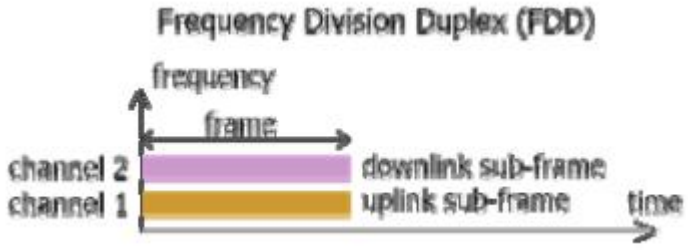
Οι ασύρματες επικοινωνίες υλοποιούνται με δύο τρόπους. Ο πρώτος τρόπος αφορά την μετάδοση της πληροφορίας από ένα άτομο σε πολλά (one to many) και χαρακτηρίζεται ως Broadcast επικοινωνία. Τέτοιου είδους επικοινωνία είναι η εκπομπή του ραδιοφώνου. Ο δεύτερος τρόπος επικοινωνίας παρέχει την δυνατότητα εκπομπής και λήψης ραδιοκυμάτων προς άλλους χρήστες. Αυτές οι επικοινωνίες χαρακτηρίζονται αμφίδρομες και μπορούν να υλοποιούνται σημείο με σημείο (point to point) και σημείο με πολλά σημεία (point to multipoint).

2.1.2 Τρόποι αμφίδρομης μετάδοσης

Η αμφίδρομη επικοινωνία που επικρατεί στις μέρες μας για την μετάδοση της πληροφορίας στα ασύρματα δίκτυα χωρίζεται στις δύο εξής κατηγορίες:

FrequencyDivisionDuplex (FDD)

Στη συγκεκριμένη μέθοδο χρησιμοποιούνται δύο διαφορετικά κανάλια συχνοτήτων, ένα για την λήψη και ένα για την μετάδοση. Βασικός στόχος ήταν να μπορεί να αποστέλλει και να λαμβάνει δεδομένα ταυτόχρονα χωρίς παρεμβολές.

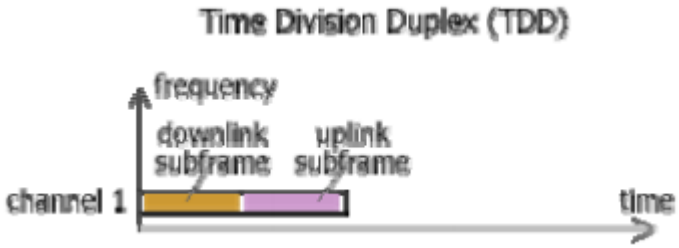


Εικόνα2:Frequency Division Duplex

Time Division Duplex (TDD)

Με αυτή τη μέθοδο γίνεται χρήση ενός και μόνο καναλιού για την λήψη και την μετάδοση. Το κανάλι λειτουργεί μεταξύ των καταστάσεων εκπομπής

και λήψης περιοδικά. Η ταυτόχρονη υλοποίηση δεν μπορεί να πραγματοποιηθεί παρόλο που υπάρχει αμφίδρομη επικοινωνία.



Εικόνα3:TimeDivisionDuplex

2.2 Ανάλυση Ασύρματων Δικτύων

Η ραγδαία και ταχύτατη ανάπτυξη του ασύρματου δικτύου τα τελευταία χρόνια όπως και η έντονη παρουσία του, οφείλεται στην ανεπάρκεια του ενσύρματου δικτύου να παρέχει λύσεις σε διάφορα προβλήματα εφαρμογών.

Ασύρματο δίκτυο χαρακτηρίζετε το τηλεπικοινωνιακό δίκτυο, συνήθως τηλεφωνικό ή δίκτυο υπολογιστών, το οποίο χρησιμοποιεί ραδιοκύματα ως φορείς πληροφορίας. Τα δεδομένα μεταφέρονται μέσω ηλεκτρομαγνητικών κυμάτων με συχνότητα φέροντος η οποία εξαρτάται κάθε φορά από τον ρυθμό μετάδοσης δεδομένων που απαιτείται να υποστηρίζει το δίκτυο. Η ασύρματη επικοινωνία, σε αντίθεση με την ενσύρματη, δεν χρησιμοποιεί ως μέσο μετάδοσης κάποιον τύπο καλωδίου.

Γενικά μπορούμε να αναφέρουμε πως τα ασύρματα δίκτυα τα πρώτα χρόνια της δημιουργίας τους, λόγο των μειονεκτημάτων έλλειψης προτύπων δεν ήταν εύκολα αποδεκτά από το κοινό. Αργότερα όμως, με την εξέλιξη της τεχνολογίας τα ασύρματα δίκτυα έγιναν ευρέος γνωστά λόγο του χαμηλού κόστους εγκατάστασής τους.

Οι ασύρματες συσκευές που χρησιμοποιούνται σήμερα είναι συνήθως ασύμμετρες, δηλαδή τα δύο άκρα είναι κόμβοι διαφορετικού είδους. Πιο συγκεκριμένα το ένα άκρο δεν έχει κινητικότητα αλλά έχει ενσύρματη επικοινωνία με το Διαδίκτυο(μέσω Router) και στο άλλο άκρο έχουμε μια κινητή συσκευή που συνδέεται με το ακίνητο μέρος της ζεύξης .

2.3 Είδη ασύρματων δικτύων

Τα ασύρματα δίκτυα δημιουργήθηκαν πάνω στα πρότυπα των ενσύρματων δικτύων με την διαφορά να βρίσκεται στον τρόπο μετάδοσης την πληροφορίας. Τα είδη των ασύρματων δικτύων που δημιουργήθηκαν και χρησιμοποιούνται τα τελευταία χρόνια είναι τέσσερα και παρουσιάζονται αναλυτικά παρακάτω.

2.3.1 Ασύρματα προσωπικά δίκτυα (WPAN)

Τα ασύρματα προσωπικά δίκτυα επιτρέπουν την διασύνδεση και επικοινωνία ασύρματων συσκευών σε αποστάσεις που δεν ξεπερνούν τα 10 μέτρα. Η επικοινωνία αυτή επιτρέπει την ανταλλαγή αρχείων ,την αποστολή εφαρμογών και την γρήγορη επικοινωνία. Ένα είδος WPAN είναι το Bluetooth το οποίο υπάρχει σε ένα μεγάλο εύρος συσκευών όπως τα κινητά τηλέφωνα, τους υπολογιστές, τα fax κ.α και επιτρέπουν την γρήγορη σύνδεση και επικοινωνία μεταξύ τους. Το Bluetooth χρησιμοποιεί ίδια πρότυπα με το wi-fi αλλά σε μικρότερη ισχύ και με διαφορετικό τρόπο πολύπλεξης του σήματος. Επίσης χρησιμοποιείται για εφαρμογές όπως:

- Επικοινωνία μεταξύ κινητών τηλεφώνων και ασύρματων συσκευών.
- Έλεγχος και εντοπισμός περιφερειακών συσκευών υπολογιστή(ποντίκι ,πληκτρολόγιο).
- Έλεγχος και εντοπισμός χειριστηρίων σε παιχνιδοκονσόλες.

Εικόνα4:Επικοινωία προσωπικού δικτύου με Bluetooth

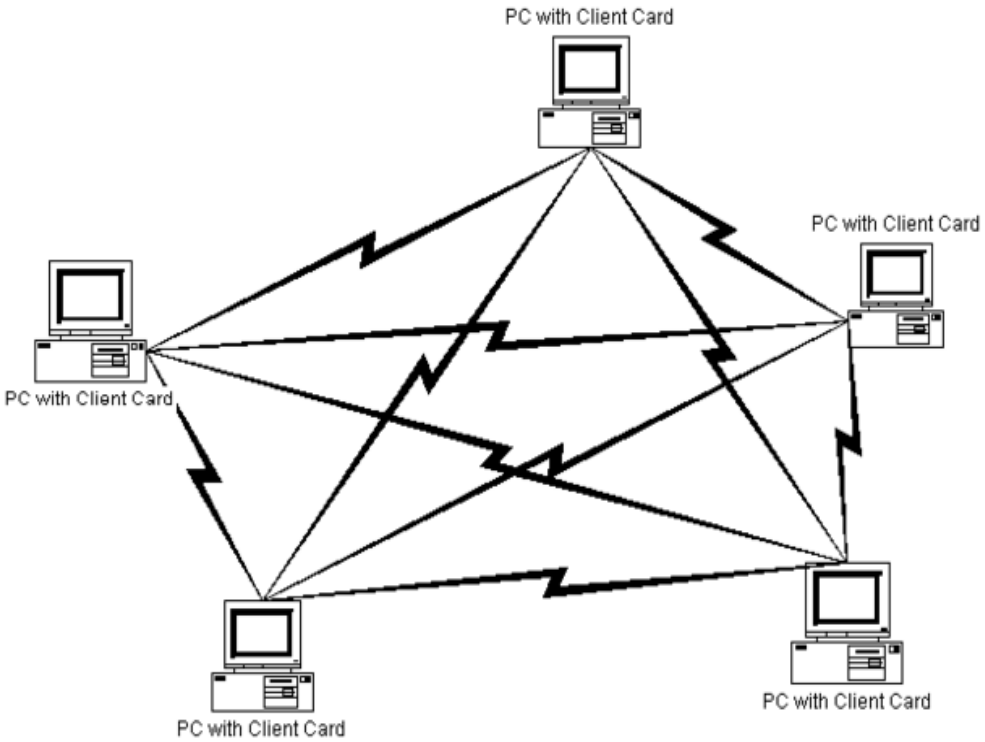
2.3.2 Ασύρματα τοπικά δίκτυα (WLAN)

Τα ασύρματα τοπικά δίκτυα βασίστηκαν και λειτουργούν όπως ένα τοπικό Ethernet δίκτυο. Η λειτουργία του παραμένει ίδια. Τα δεδομένα που είναι για αποστολή χωρίζονται σε μικρά πακέτα και αποστέλλονται στον παραλήπτη. Προκειμένου όμως να επικοινωνήσουν οι σταθμοί μεταξύ τους απαιτείται μια ασύρματη κάρτα δικτύου στην συσκευή.

Τα ασύρματα τοπικά δίκτυα έχουν δύο βασικούς τρόπους λειτουργίας. Χωρίζονται σε απλά και αρκετά σύνθετα. Παρακάτω αναφέρονται οι δύο αυτές τοπολογίες:

Ανεξάρτητο σύνολο βασικής υπηρεσίας (IBSS, Independent Basic Service Set ή Peer-to-Peer ή Ad-Hoc)

Είναι η βασική τοπολογία ασύρματης δικτύωσης. Όλοι οι σταθμοί επικοινωνούν μεταξύ τους, ένας προς ένας (peer to peer) , λειτουργία ad-hoc δηλαδή χωρίς να υπάρχει κάποιος κεντρικός σταθμός AP.



Εικόνα5:Βασική τοπολογία ασύρματου δικτύου με IBSS.

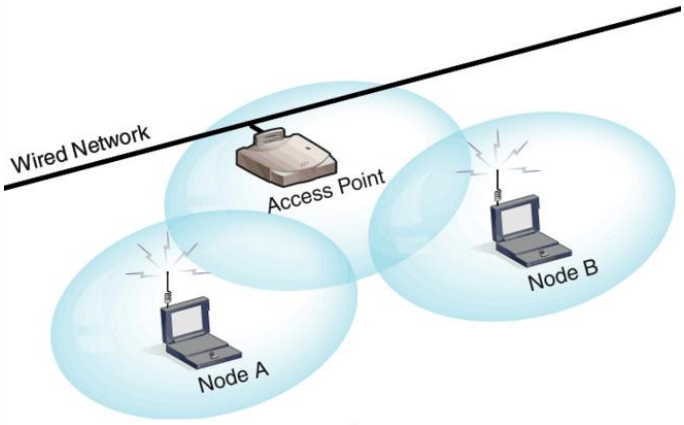
Για να επιτευχθεί αυτό το μόνο που χρειάζεται είναι οι σταθμοί να βρίσκονται ο ένας εντός της εμβέλειας του άλλου. Ο βασικός λόγος ύπαρξης αυτής την λειτουργίας είναι για την εύκολη και γρήγορη διαμόρφωση ενός ασύρματου δικτύου σε μέρη που δεν υπάρχουν υποδομές ή για κάλυψη μικρών περιοχών.

- Λειτουργία υποδομής (Infrastructure Mode)

Είναι ο πιο σύνθετος τρόπος ασύρματου δικτύου. Όλες οι συσκευές επικοινωνούν μεταξύ τους μέσω ενός AP(AccessPoint). Ο αριθμός τον ασύρματων σταθμών που μπορούν να συνδεθούν πάνω σε ένα AP κυμαίνετε από 15-50 και είναι εξολοκλήρου υπεύθυνοι για τον διαχωρισμό του εύρους ζώνης και τον ρυθμό μετάδοσης που μπορεί να έχει ο καθένας. Επίσης το εύρος ζώνης δεν χωρίζετε στους χρήστες ισοδύναμα ,αλλά σύμφωνα με την ποιότητα της σύνδεσης και την απόστασή του από το AP. Ένα μεγάλο πρόβλημα που συναντάται συχνά είναι η αυξημένη πιθανότητα συγκρούσεων σε σχέση με τον μεγάλο αριθμό συνδεδεμένων χρηστών. Γενικά ,οι τύποι υπηρεσιών στην λειτουργία υποδομής χωρίζετε σε δύο κατηγορίες.

1. Σύνολο βασικής υπηρεσίας υποδομής (Infrastructure Basic Service Set)
   Στη συγκεκριμένη κατηγορία όλοι οι ασύρματοι σταθμοί επικοινωνούν με το AP και όταν θελήσουν να επικοινωνήσουν με έναν άλλο σταθμό τότε το μήνυμα επανεκπέμπεται από το AP προς τον τελικό προορισμό. Ο βασικός λόγος αυτής της υπηρεσίας είναι η εξασφάλιση μεγαλύτερης εμβέλειας ,επειδή οι σταθμοί δεν χρειάζονται να είναι κοντά ο ένας με τον άλλο,

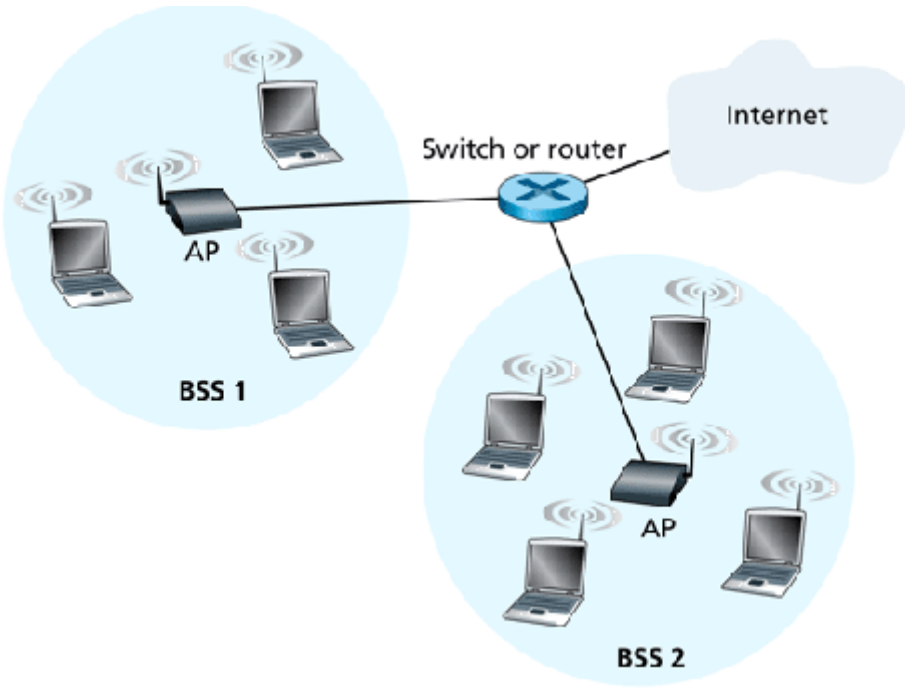
αλλά πρέπει να είναι εντός εμβέλειας του AP.



Εικόνα6: Σύνολο βασικής υπηρεσίας υποδομής (BSS)

2.Εκτεταμένο σύνολο υπηρεσιών (Extended Service Set)

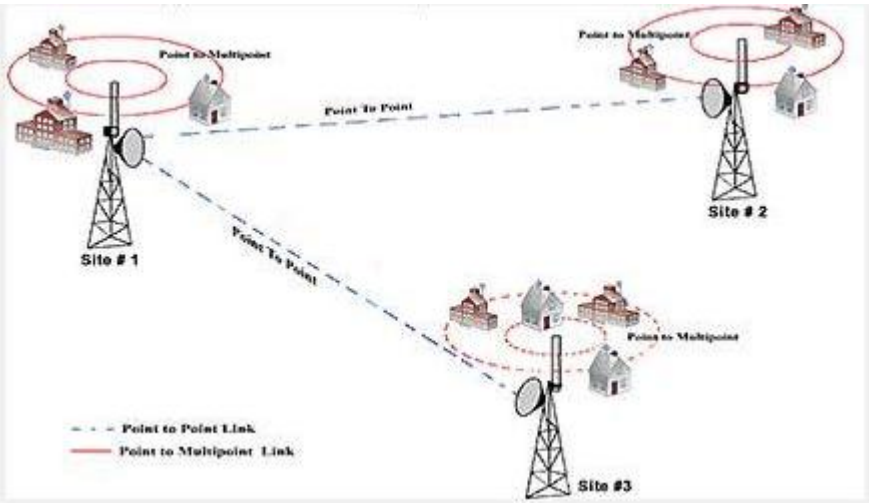
Στη συγκεκριμένη κατηγορία οι ασύρματοι σταθμοί χωρίζονται σε ομάδες(κυψέλες), όπου κάθε ομάδα έχει το δικό της AP(AccessPoint) τα οποία με τη σειρά τους είναι συνδεδεμένα μεταξύ τους με μία δομή δικτύου μετάδοσης. Ο βασικός λόγος αυτής της υπηρεσίας είναι για την μεγαλύτερη εμβέλεια κάλυψης την οποία ένα μόνο του AP δεν μπορεί να καλύψει. Τέτοιου είδους εκτεταμένου συνόλου υπηρεσίες χρησιμοποιούνται για την ολική κάλυψη ενός κτιρίου. Τα AP μπορούν απλά να είναι διασυνδεμένα σε ένα απλό ενσύρματο Ethernet δίκτυο.



Εικόνα7: Εκτεταμένο σύνολο υπηρεσιών(ESS)

2.3.3 Ασύρματα μητροπολιτικά δίκτυα (WMAN)

Τα ασύρματα μητροπολιτικά δίκτυα διαφέρουν με τα αντίστοιχα μητροπολιτικά δίκτυα τα οποία ενώνουν πολλά σημεία σε μεγάλες αποστάσεις. Τα WMAN , χρησιμοποιούνται για την επικοινωνία δύο σημείων (Point to Point) σε μεγάλες αποστάσεις αρκεί να έχουν ορατότητα μεταξύ τους. Απαιτείται μια κατευθυντική κεραία υψηλής ισχύος ώστε το σήμα να στέλνεται προτού εξασθενίσει.



Εικόνα8:Ασύρματο μητροπολιτικό δίκτυο

Όσο αφορά τα πρωτόκολλα ασφαλείας που χρησιμοποιούνται στα ασύρματα μητροπολιτικά δίκτυα είναι ίδια με αυτά των ασύρματων τοπικών δικτύων με ιδιαίτερη σημασία στην ισχύ του σήματος ,την εξασθένηση και την κατευθυντικότητα και γι αυτό θα αναφερθούν στο επόμενο κεφάλαιο.

2.3.4 Ασύρματα Ευρείας εμβέλειας δίκτυα (WWAN)

Ένα ασύρματο ευρείας εμβέλειας δίκτυο θεωρείτε η σύνδεση ενός υπολογιστή στο internet χωρίς όμως την χρήση καλωδίου. Την δυνατότητα της σύνδεσης μας την παρέχουν οι κινητές τηλεφωνίες έναντι κάποιου χρηματικού ποσού αλλά και με χρήση ειδικής προπληρωμένης κάρτας. Ένα ακόμα WWAN δίκτυο είναι η σύνδεση ορισμένων κινητών τηλεφώνων απευθείας σε ένα φορητό υπολογιστή χρησιμοποιώντας ένα USB. Το κινητό τηλέφωνο λειτουργεί ως μόντεμ παρέχοντας δυνατότητα σύνδεσης στο διαδίκτυο αλλά με χαμηλό ρυθμό δεδομένων.

Εικόνα9:Χρήση SIM κάρτας για WWAN

2.4 Πλεονεκτήματα-Μειονεκτήματα Ασύρματων δικτύων

Όπως έχουμε αναφέρει και παραπάνω τα ασύρματα δίκτυα στις μέρες μας έχουν μεγάλη άνθιση. Λογικό όμως είναι, ότι όπως όλα τα τεχνολογικά επιτεύγματα έτσι και τα ασύρματα δίκτυα έχουν πλεονεκτήματα αλλά και μειονεκτήματα.

Τα κυριότερα πλεονεκτήματα των ασύρματων επικοινωνιών έναντι των ενσύρματων είναι τα εξής:

i) Υποστήριξη Κινητικότητας χρήστη

Η εμβέλεια εκπομπής υπηρεσιών ασύρματου δικτύου δίνει το δικαίωμα στους χρήστες να μπορούν να μετακινούνται μέσα στο χώρο ,αρκεί να είναι επαρκές το σήμα διατηρώντας δηλαδή την συνδεσιμότητα τους. Πολύ βασικό πλεονέκτημα για ένα εργασιακό χώρο, έχοντας ως αποτέλεσμα την μεγαλύτερη αποδοτικότητα.

ii) Χαμηλό κόστος εγκατάστασης

Παρόλο που το αρχικό κόστος εγκατάστασης είναι υψηλότερο σε σχέση με την εγκατάσταση οποιουδήποτε άλλου ενσύρματου δικτύου, το τελικό κόστος φτάνει να είναι λιγότερο λόγο της μεγαλύτερης διάρκειας ζωής και ευελιξίας και ιδίως αν αναλογιστή κανείς το κόστος που θα χρειαστεί μια αναδιάρθρωση και μετακίνηση ενός ενσύρματου δικτύου σε ένα εργασιακό χώρο. Με την εμφάνιση κιόλας περισσότερων κατασκευαστών και τον μεταξύ τους ανταγωνισμό, η τιμή της ασύρματης συσκευής έφτασε σε ικανοποιητικά επίπεδα παρέχοντας μας περισσότερα ποιοτικά χαρακτηριστικά στη συσκευή.

iii) Ευκολία και ευελιξία εγκατάστασης

Η μη χρήση επιπρόσθετων καλωδίων κάνει την εγκατάσταση την ασύρματης ευκολότερη κυρίως σε χώρους που είναι αδύνατη ή μη επιθυμητή η χρήση καλωδίων.

iv) Δυνατότητα επέκτασης

Όλα τα δίκτυα έτσι και τα ασύρματα διαμορφώνονται σε ένα χώρο σύμφωνα με την τοπολογία που ταιριάζει. Από μικρό πλήθος χρηστών ως και μεγάλο ,δίνετε η δυνατότητα της εύκολης και γρήγορης αλλαγής τοπολογίας.

v) Εμβέλεια

Σε σύγκριση με το ενσύρματο δίκτυο που η μέγιστη απόσταση μετάδοσης της πληροφορίας μέσω ενός καλωδίου είναι τα 100 μέτρα ,τα ασύρματα δίκτυα ξεκινούν την εκπομπής τους τοπικά, επεκτείνονται σε απόσταση δεκάδων μέτρων σε κλειστούς χώρους και σε ανοιχτούς χώρους η απόσταση ξεπερνάει αυτή του ενσύρματου δικτύου.

vi) Ταχύτητα μετάδοσης

Αρχικά η ασύρματη επικοινωνία ήταν σε μη ικανοποιητικά επίπεδα λόγο του μικρού ρυθμού μετάδοσης που κυμαίνονταν στα 2 Mbps. Με την ανάπτυξη όμως της τεχνολογίας οι ρυθμοί αυτοί αυξήθηκαν φτάνοντας πλέον στις μέρες μας σε ταχύτητες πάνω από 300Mbps και περιμένοντας ακόμα μεγαλύτερες.

Τα κυριότερα μειονεκτήματα των ασύρματων επικοινωνιών έναντι των ενσύρματων είναι τα εξής:

i) Ασφάλεια πληροφορίας

Είναι γνωστό ότι η μετάδοση των πληροφοριών γίνεται μέσω του αέρα που είναι πιο εύκολο στην υποκλοπή πληροφοριών σε σχέση πάντα με τα καλώδια και τις οπτικές ίνες.

ii) Παρεμβολές-αξιοπιστία

Όπως μπορούμε να γνωρίζουμε τα ασύρματα δίκτυα εκπέμπουν σε δύο ζώνες συχνοτήτων .Η ζώνη χαμηλών συχνοτήτων είναι και η πιο ευάλωτη γιατί σε περίπτωση που άλλος αναμεταδότης εκπέμψει στην ίδια ραδιοσυχνότητα καταστεί άχρηστο το δικό μας και ταυτόχρονα διαπιστώνουμε ότι είναι και ένας τρόπος επίθεσης πάνω στο δίκτυό μας. Από την άλλη η ζώνη υψηλών

συχνοτήτων είναι πιο ασφαλή αλλά έχει μικρότερη εμβέλεια εκπομπής και μεγαλύτερη επίπτωση πάνω στην ανθρώπινη υγεία.

iii) Επιπτώσεις στην υγεία

Γνωρίζουμε ότι τα καλώδια για να μην έχουν απώλεια ακτινοβολίας έχουν εξωτερική θωράκιση ,δυστυχώς όμως κάτι παρόμοιο δεν μπορεί να γίνει και με την ασύρματη μετάδοση και την ηλεκτρομαγνητική ενέργεια που εκπέμπουν οι κεραίες, με συνέπεια οι ακτινοβολίες να προκαλούν αρνητικές επιπτώσεις στην ανθρώπινη υγεία. Το μόνο που μπορούμε να πούμε είναι ότι πρέπει οι κεραίες να ρυθμίζονται σύμφωνα με τους κανόνες που έχει ορίσει το Ευρωπαϊκού Ινστιτούτο Τηλεπικοινωνιακών Προτύπων.

Βιβλιογραφικές αναφορές κεφαλαίου

[1] http://www.smarteck.gr/info_wlan.html

[2]https://el.wikipedia.org/wiki/%CE%91%CF%83%CF%8D%CF%81%CE%BC%CE%B1%CF%84%CE%BF_%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF

[3] WILLIAMSTALLINGS(2007),*ΑΣΥΡΜΑΤΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ ΚΑΙ ΔΙΚΤΥΑ.* Αθήνα:Τζιόλα

[4] ΒΑΣΣΗΣ ΔΗΜΗΤΡΙΟΣ (2014),*ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ ΕΠΙΚΟΙΝΩΝΙΩΝ, Με επίγειες μικροκυματικές ζεύξεις* , ΑΡΤΑ)

[5] Καψάλης.Χ & Κωττής.Π (2002),*ΚΕΡΑΙΕΣ ΑΣΥΡΜΑΤΕΣ ΖΕΥΞΕΙΣ* .Αθήνα : Τζιόλα

ΚΕΦΑΛΑΙΟ 3ο Περιγραφή προτύπων-πρωτοκόλλων ασφαλείας

Εισαγωγή 3ου κεφαλαίου

Το παρακάτω κεφάλαιο περιγράφει την εξέλιξη των ενσύρματων δικτύων σε ασύρματων. Γίνεται αναφορά των βασικών χαρακτηριστικών του Wi-Fi, όπως επίσης και των υπόλοιπων αναβαθμισμένων προτύπων ασφαλείας προκειμένου να επιτυγχάνεται η εκπομπή σε διαφορετικές συχνότητες και ρυθμούς μετάδοσης.

3.1 Ασύρματη ζεύξη (Wi-Fi)

Τα ασύρματα τοπικά δίκτυα είναι η εξέλιξη των ενσύρματων δικτύων σε κλειστούς χώρους και αποκαλούνται διεθνώς ως Wireless Local Area Networks (WLANs) , τα οποία χρησιμοποιούν αποκλειστικά το πρωτόκολλο IEEE 802.11 που είναι γνωστό και ως Wi-Fi. Γενικός το Wi-Fi είναι ένα πιστοποιημένο πρόγραμμα το οποίο καθορίζει την σωστή λειτουργία και επικοινωνία των ασύρματων συσκευών. Βασίζεται στα δύο κατώτερα επίπεδα του OSI ,δηλαδή το φυσικό επίπεδο (physical layer) και το επίπεδο ζεύξης δεδομένων (Medium Access Control).Η IEEE με αυτόν τον τρόπο επιτρέπει την μεταφορά τις πληροφορίας των ανώτερων επιπέδων και την επεξεργάζεται με τον ίδιο τρόπο που λειτουργεί και τοEthernet.

Αρχικός σκοπός της IEEE (Institute of Electrical and Electronics Engineers) ήταν να καταφέρει να πιστοποιήσει όλες τις ασύρματες συσκευές που είχαν ως βάση το πρότυπο 802.11. Το 1999 δημιουργήθηκε η WECA (Wireless Ethernet Compatibility Alliance) μια ομάδα που θα πραγματοποιούσε τον αρχικό στόχο της IEEE. Μετά από καιρό οι συσκευές που περνούσαν από επιτυχία τις δοκιμές αποκτούσαν το λογότυπο Wi-Fi που θεωρούνταν ως εγγύηση για τον υποψήφιο αγοραστή.

3.1.1 Βασικά χαρακτηριστικά Wi-Fi

- Λειτουργεί στα 2.4GHz ή στα 5GHz
- Μη αδειοδοτημένη ζώνη συχνοτήτων
- Ρυθμοί μετάδοσης υψηλοί
- Μικρότερες αποστάσεις κάλυψης σε σχέση με το 3G
- Φθηνός εξοπλισμός

Εικόνα10: Σήμα παροχής υπηρεσιών Wi-Fi

3.2 Πρωτόκολλο ασύρματου δικτύου 802.11

Το πρωτόκολλο 802.11 δημιουργήθηκε από μία νέα ομάδα εργασίας της επιτροπής IEEE 802 με σκοπό την δημιουργία ενός πρωτοκόλλου MAC ειδικό για τα ασύρματα δίκτυα. Ορίζει εννέα υπηρεσίες που χρειάζονται να υποστηρίζονται από το ασύρματο δίκτυο για να παρέχει λειτουργικότητα όμοια με αυτή που είναι βασισμένα τα δίκτυα LAN.

Το στρώμα MAC του IEEE 802.11 περιέχει τρία βασικά χαρακτηριστικά λειτουργίας τα οποία αναφέρουμε αναλυτικά παρακάτω:

- *Αξιόπιστη παράδοση δεδομένων*, όπως και κάθε άλλο ασύρματο δίκτυο έτσι και αυτό χρησιμοποιεί το φυσικό στρώμα του επιπέδου OSI με αποτέλεσμα να υπάρχει σε μεγάλο βαθμό αναξιοπιστία. Ο Θόρυβος και οι παρεμβολές οδηγούν στην απώλεια πληροφοριών και στην μείωση των αριθμών πλαισίου. Για τον λόγο αυτό το 802.11 στέλνει μεγαλύτερο αριθμό πλαισίων που ανέρχεται στον αριθμό 4 προκειμένου ο παραλήπτης να λαμβάνει και να στέλνει μήνυμα απάντησης.
- *Έλεγχος πρόσβασης*, χρησιμοποιεί τα πρωτόκολλα κατανεμημένης πρόσβασης για να μεταδώσουν την απόφαση για εκπομπή σε όλους τους κόμβους ,και τα πρωτόκολλα κεντρικής πρόσβασης που περιλαμβάνουν ρύθμιση της εκπομπής από έναν συγκεκριμένο αποστολέα. Γίνεται έλεγχος δεδομένων ως προς την ευαισθησία χρόνου και υψηλής προτεραιότητας.
- *Ασφάλεια* ,παρέχει μηχανισμούς ιδιωτικότητας και πιστοποίησης οι οποίοι αναφέρονται στο Κεφάλαιο 3.

Γενικά χαρακτηριστικά που πρέπει να γνωρίζουμε για το πρότυπο 802.11 είναι τα εξής:

Το 802.11 είναι ένα πρότυπο το οποίο εκτελείτε με ελεύθερη άδεια χρήσης ζώνης συχνοτήτων στα 2,4GHz. Ο ρυθμός μετάδοσης δεδομένων ανέρχεται στις ταχύτητες των 1Mbps και 2Mbps. Για την μετάδοση του σήματος χρησιμοποιεί τεχνική διάχυσης φάσματος.

3.3 Ασύρματα πρότυπα-πρωτόκολλα δικτύωσης

Παρακάτω αναφέρουμε συνοπτικά τις πέντε παραλλαγές/αναβαθμίσεις του πρωτοκόλλου 802.11:

- **Πρότυπο 802.11b**

Το 802.11b είναι ένα πρότυπο φυσικού επιπέδου το οποίο εκτελείτε και αυτό με ελεύθερη άδεια χρήσης ζώνης συχνοτήτων όπως και το πρότυπο 802.11 στα 2.4GHz.Ο ρυθμός μετάδοσης δεδομένων περιλαμβάνει τις τιμές των 1, 2, 5.5 και 11Mbps . Για την μετάδοση του σήματος χρησιμοποιεί και αυτό τεχνική διάχυσης φάσματος.

- **Πρότυπο 802.11a**

Το 802.11a ως πρότυπο δημιουργήθηκε αργότερα για να εκπέμπει σε ζώνη συχνοτήτων 5GHz . Ο ρυθμός μετάδοσης των δεδομένων όπως είναι φυσικό είναι μεγαλύτερος σε σχέση με πρότυπα που εκπέμπουν στα 2,4GHz. Οι τιμές στον ρυθμό μετάδοσης είναι 6 , 9 , 12 ,18 ,24 ,36 ,48 και 54Mbps. Για να μεταδώσει με αυτόν τον ρυθμό χρειάστηκε να χρησιμοποιήσει Ορθογωνική Πολύπλεξη με Διαίρεση Συχνότητας (orthogonal frequency division multiplexing, OFDM).

- **Πρότυπο 802.11g**

Το πρότυπο 802.11g δημιουργήθηκε για να διασφαλίζει τη συμβατότητα με κάθε συσκευή που υποστηρίζει πρότυπο ασφαλείας. Εκπέμπει στη συχνότητα ζώνης των 2,4GHz.Ο ρυθμός μετάδοσης περιλαμβάνει όλες τις τιμές τον προτύπων 802.11a και 802.11b ,με μέγιστη τιμή τα 54Mbps.Η Ορθογωνική Πολύπλεξη με Διαίρεση Συχνότητας είναι η μέθοδος που χρησιμοποιεί για μετάδοση.

- **Πρότυπο 802.11n**

Το 802.11n είναι ένα καινούργιο πρότυπο με διαχείριση φάσματος στο 802.11^{α}.Χρησιμοποιεί (DCS, Dynamic Channel Selection και TPC, Transmit Power Control)και εκπέμπει σε ζώνη συχνοτήτων 2,4 και 5GHz.Έχει ρυθμό μετάδοσης μέχρι και 600Mbps. Χρησιμοποιεί εύρος ζώνης συχνοτήτων στα 20 και στα 40MHz.

- **Πρότυπο 802.11i**

Μαζί με το 802.11n δημιουργήθηκε και το 802.11i, το οποίο είναι για ασφάλεια συστημάτων που χρησιμοποιούν μεθόδους κρυπτογράφησης τύπου Wired Equivalent Privacy (WEP).Έχει επεκτάσεις πάνω στο δεύτερο επίπεδο του OSI για ενισχυμένη ασφάλεια και έχει περιγραφή πρωτοκόλλων 802.1X ,TKIP,AES.

Έκδοση	Ημερομηνία	Ζώνη συχνοτήτων	Συνήθης ρυθμός μετάδοσης	Ονομαστικός ρυθμός μετάδοσης	Μέθοδοι μετάδοσης	Εμβέλεια εσωτερικών χώρων
802.11	1997	2.4 GHz	0.9 Mbit/s	2 Mbit/s	IR / FHSS / DSSS	~20 m
802.11b	1999	2.4 GHz	4.3 Mbit/s	11 Mbit/s	DSSS	~38 m
802.11a	1999	5 GHz	23 Mbit/s	54 Mbit/s	OFDM	~35 m
802.11g	2003	2.4 GHz	19 Mbit/s	54 Mbit/s	OFDM	~38 m

Εικόνα11: Πίνακας πρωτόκολλα IEEE 802.11 τα οποία υπάρχουν στην αγορά.

Βιβλιογραφικές αναφορές κεφαλαίου

[1] https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

[2] ΠΡΕΒΕΣ ΝΙΚΟΛΑΟΣ(2008),*ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ ,ΑΣΦΑΛΕΙΑ ΚΑΙ ΑΠΟΔΟΣΗ ΤΩΝ ΠΡΩΤΟΚΟΛΛΩΝ TCP/IP*. Αθήνα :Εκδόσεις νέων τεχνολογιών

[3] http://digilib.lib.unipi.gr/dspace/bitstream/unipi/4992/1/Kefalas,%20Grigorios%20I..pdf

[4] http://www.smarteck.gr/info_wlan.html

ΚΕΦΑΛΑΙΟ 4ο Ασφάλεια ασύρματων δικτύων με την χρήση των πρωτοκόλλων

Εισαγωγή 4ου κεφαλαίου

Το τέταρτο κεφάλαιο της εργασίας επικεντρώνεται στα δύο βασικά είδη της κρυπτογράφησης, την κρυπτογράφηση συμμετρικού και δημόσιου κλειδιού. Μετά την πλήρη περιγραφή και τον τρόπο λειτουργίας τους, συναντούμε τα δύο είδη πρωτοκόλλων ασφαλείας και γίνεται μια σύγκριση μεταξύ τους προκειμένου να δούμε το ασφαλέστερο για την ασύρματή μας συσκευή.

4.1 Κρυπτογράφηση

Κρυπτογράφηση είναι μία μορφή αλλοιωμένου κείμενου που προκειμένου να το φέρεις σε μορφή ανάγνωσης πρέπει να διαθέτεις το κατάλληλο κλειδί. Η κρυπτογράφηση χωρίζετε σε δύο κατηγορίες:

- Κρυπτογράφηση συμμετρικού κλειδιού
- Κρυπτογράφηση δημόσιου κλειδιού

Ο σκοπός της κρυπτογράφησης είναι να καταφέρει να μεταδώσει πληροφορία μέσα από ένα μη ασφαλές κανάλι με τέτοιο τρόπο ώστε, από τον έναν χρήστη σε έναν άλλο να μην υπάρχει πιθανότητα υποκλοπής δεδομένων και πληροφοριών. Τα βασικά χαρακτηριστικά της κρυπτογράφησης είναι :

- Εμπιστευτικότητα: Η μετάδοση γίνεται ανάμεσα σε δύο χρήστες οι οποίοι έχουν στην διάθεσή τους τα κατάλληλα κλειδιά κρυπτογράφησης και αποκρυπτογράφησης του αρχικού κειμένου. Το μήνυμα είναι ακατανόητο για όποιον κρυφακούει, με την προϋπόθεση ότι δεν γνωρίζει το κλειδί αποκρυπτογράφησης.

- Ακεραιότητα : Η πληροφορία που μεταδίδετε μέσα από το ασύρματο μέσο μετάδοσης δεν μπορεί να αλλοιωθεί παρά μόνο από τους δύο αρχικούς χρήστες.

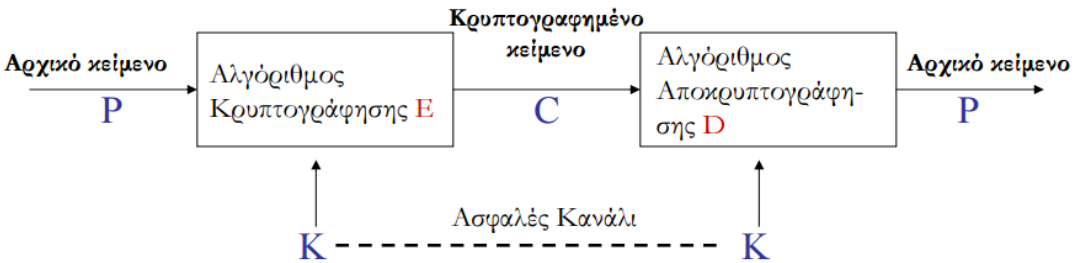
- Μη Απάρνηση : Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της.

- Πιστοποίηση : Οι χρήστες των κλειδιών μπορούν να επιβεβαιώσουν τα στοιχεία τους προκειμένου να μπορέσουν αν συνεχίσουν την μεταξύ τους επικοινωνία, αρκεί τα στοιχεία τους να είναι αληθή .

Εικόνα 12:Κρυπτογράφηση-Αποκρυπτογράφηση

4.1.1 Κρυπτογράφηση συμμετρικού κλειδιού

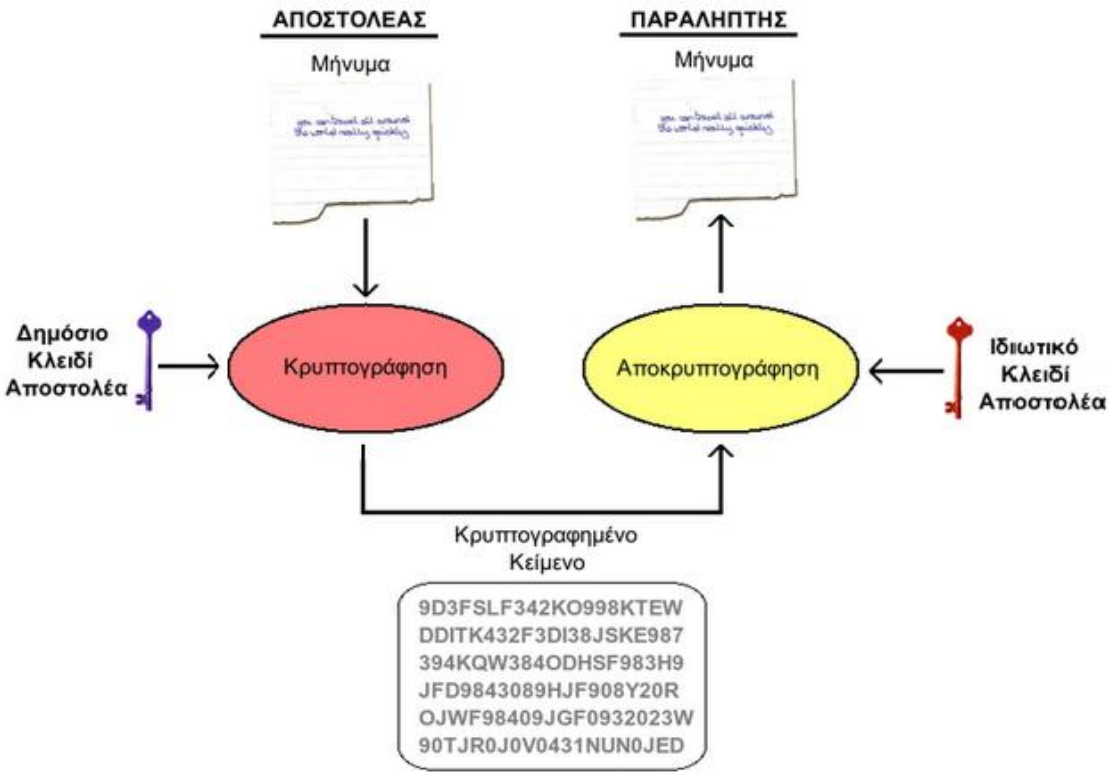
Σε μία κρυπτογραφία συμμετρικού κλειδιού και οι δύο συμμετέχοντες που επικοινωνούν μοιράζονται το ίδιο κλειδί. Με λίγα λόγια ,αν κρυπτογραφηθεί με ένα συγκεκριμένο κλειδί απαιτείται το ίδιο για την αποκρυπτογράφηση του μηνύματος. Γενικά όμως ,ένα μεγάλο πρόβλημα είναι η ανταλλαγή του κλειδιού μέσα από ένα ασφαλές κανάλι επικοινωνίας χωρίς να υπάρχει περίπτωση παρεμβολής τρίτου προσώπου. Αυτός είναι και ο κύριος λόγος που η επικοινωνία γίνεται δύσκολη μεταξύ απομακρυσμένων ατόμων.



Εικόνα 13: Κρυπτογράφηση συμμετρικού κλειδιού

4.1.2 Κρυπτογράφηση δημόσιου κλειδιού

Η κρυπτογράφηση δημόσιου κλειδιού ή ασύμμετρου κλειδιού επινοήθηκε για να διευκολύνει τους δύο χρήστες για την μεταξύ τους επικοινωνία. Ο λόγος που κάνει την κρυπτογράφηση πιο εύκολη είναι ότι χρησιμοποιεί ένα ζευγάρι από κλειδιά, ένα για την κρυπτογράφηση και ένα διαφορετικό για την αποκρυπτογράφηση . Ο χρήστης που κρατάει το ιδιωτικό κλειδί είναι υποχρεωμένος να το κρατήσει απόρρητο έτσι ώστε να είναι ο μοναδικός που μπορεί να κάνει την ανάγνωση του αρχικού κειμένου , ενώ το δημόσιο κλειδί μπορεί να το δημοσιεύσει προκειμένου να μπορεί ο οποιοσδήποτε να κρυπτογραφεί ένα κείμενο για αποστολή προς τον παραλήπτη.



Εικόνα 14: Κρυπτογράφηση δημόσιου ή ασύμμετρου κλειδιού

4.1.3 Σύγκριση κρυπτογραφήσεων

Σύμφωνα με τα παραπάνω στοιχεία κρυπτογραφήσεων μπορούμε να βγάλουμε κάποια εύκολα συμπεράσματα σχετικά με τα πλεονεκτήματα και τα μειονεκτήματα της κάθε μίας κρυπτογράφησης.

Τα πλεονεκτήματα της συμμετρικής κρυπτογράφησης είναι:

- Χαμηλό κόστος υλοποίησης, λόγο της δημιουργίας ενός και μόνο κλειδιού.
- Εύκολη υλοποίηση από την πλευρά του Hardware.

Τα Πλεονεκτήματα της δημόσιας κρυπτογράφησης είναι:

- Υψηλή ασφάλεια, δεν χρειάζεται να μεταδοθεί ποτέ μέσα από ένα μη ασφαλές κανάλι το ιδιωτικό κλειδί επειδή το κρατάει μόνιμα ο παραλήπτης.
- Παροχή ψηφιακής υπογραφής , αυτό οφείλετε στην μοναδικότητα του ιδιωτικού κλειδιού του κάθε ένα παραλήπτη.
- Ένας παραλήπτης→Ένα ιδιωτικό κλειδί

Τα μειονεκτήματα της συμμετρικής κρυπτογράφησης είναι:

- Δημοσίευση και μετάδοση του κλειδιού, μέσα από ένα μη ασφαλές κανάλι.
- Εκτεταμένη ζημιά εφόσον έχει χαθεί το κλειδί.

Τα μειονεκτήματα της δημόσιας κρυπτογράφησης είναι:

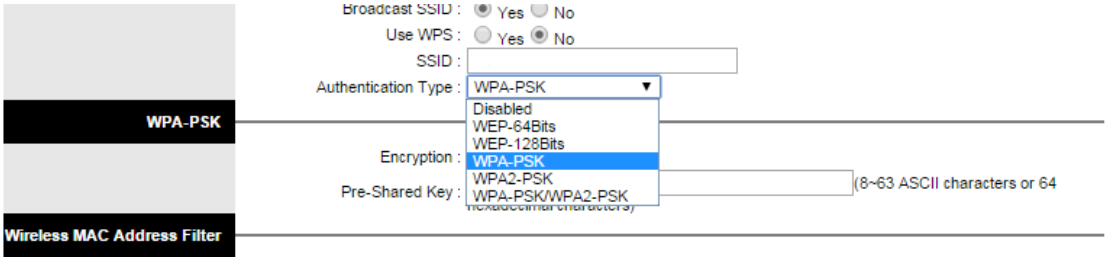
- Ταχύτητα κρυπτογράφησης, αρκετά μικρή ταχύτητα που δίνει την δυνατότητα σε οποιονδήποτε με γρήγορη μέθοδο αποκρυπτογράφησης να το βρει.
- Ευάλωτη στη πλαστοπροσωπία ,σε περίπτωση μίμησης άλλου προσώπου έχει την δυνατότητα να αποσπάσει το ιδιωτικό κλειδί του παραλήπτη.

4.2 Πρωτόκολλα κρυπτογράφησης

Μετά από τόσα χρόνια εξέλιξης της τεχνολογίας αλλά και ανακάλυψης των ασύρματων δικτύων ,φτάσαμε σε ένα σημείο όπου η ασφάλεια των τοπικών ασύρματων δικτύων βασίζονται σε δύο βασικές κατηγορίες πρωτοκόλλων κρυπτογράφησης οι οποίες είναι οι εξής:

- Πρωτόκολλο κρυπτογράφησης WEP
- Πρωτόκολλο κρυπτογράφησης WPA/WPA2

Όπως θα δούμε παρακάτω αναλυτικά ,και τα δύο πρωτόκολλα ασφαλείας βασίζονται στο πρότυπο 802.11 το οποίο και αυτό με την σειρά του κατανέμετε στο δεύτερο επίπεδο του μοντέλου OSI.



Εικόνα 15: Πρωτόκολλα κρυπτογράφησης σε ασύρματη συσκευή

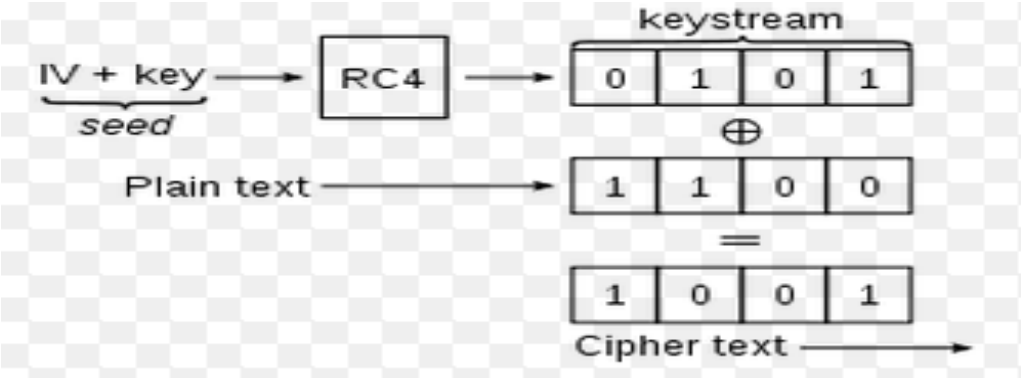
4.3 Περιγραφή πρωτοκόλλου WEP

Το WEP ήταν το πρώτο πρωτόκολλο ασφαλείας που δημιούργησε το 802.11 προκειμένου να διασφαλίσει την ασφαλή επικοινωνία μέσω ασύρματων συσκευών. Το WEP παρέχει ένα ικανοποιητικό επίπεδο ασφαλείας και μπορούμε να το εντοπίσουμε εύκολα σε παλιές ασύρματες συσκευές. Για την παροχή προστασίας καθώς και την προστασία των δεδομένων ,χρησιμοποιεί έναν αλγόριθμο κρυπτογράφησης που βασίζεται στον αλγόριθμο κρυπτογράφησης RC4, μήκους 64 ή 128 bit. Το WEP δημιουργεί τα κλειδιά των 64 bit με δέσμευση 40 bit για την κρυπτογράφηση του κλειδιού και άλλα 24 bits για τα δεδομένα του συστήματος. Αντίστοιχα για την δημιουργία των 128 bit ,δεσμεύει 104 bit για την κρυπτογράφηση και άλλα 24 bit για τα δεδομένα του συστήματος. Ο τρόπος προστασίας περιγράφετε αναλυτικά στην παρακάτω υπό ενότητα.

4.3.1 Αλγόριθμος WEP

Εύκολα μπορούμε να καταλάβουμε πως με την χρήση της κρυπτογράφησης των 128 bits έχουμε λίγο καλύτερη ασφάλεια σε σχέση με την κρυπτογράφηση των 64 bits. Αυτό οφείλεται στο κόστος δέσμευσης κλειδιού και στον διαμοιρασμό από τα δυο συμμετέχοντα μέρη της ανταλλαγής. Ένα διάνυσμα εκκίνησης γνωστό και ως IV(InitializationVector) ενώνεται με το κρυφό κλειδί. Το αποτέλεσμα της ένωσης είναι η δημιουργία ενός μπλοκ που παίζει τον σημαντικότερο ρόλο στην δημιουργία της γεννήτριας τυχαίων αριθμών που ορίζεται στον αλγόριθμο RC4. Η γεννήτρια τυχαίων αριθμών δημιουργεί μία ακολουθία από bit ίδιου μήκους με το μήκος του πλαισίου MAC. Σε αυτή την ακολουθία προστίθεται το IV κρυπτογράφημα και το μπλοκ, με αποτέλεσμα να έχουμε την δημιουργία ενός κρυπτογραφημένου κειμένου από την πλευρά του αποστολέα . Από την πλευρά του ο δέκτης πρέπει να ξεχωρίσει το IV από το μπλοκ δεδομένων και να χρησιμοποιήσει το δικό του κρυφό κλειδί για να επαναφέρει το κείμενο στην αρχική ακολουθία τον bit που είχε δημιουργήσει η γεννήτρια τυχαίων αριθμών. Στο τελικό στάδιο της αποκρυπτογράφησης πρέπει η ακολουθία των bit να συνδυαστεί κατά XOR με το μπλοκ και έτσι έχουμε το αρχικό κείμενο αποστολής του πομπού.

Η ακαταλληλότητα του πρωτοκόλλου οφείλεται στον χρόνο καθυστέρησης επεξεργασίας των πράξεων XOR και στοχεύουν τον πίνακα αρχικοποίησης (IV). Πιο συγκεκριμένα ένα τρίτο πρόσωπο μπορεί να καταφέρει να υποκλέψει πληροφορίες εξαναγκάζοντας το σύστημα να εκπέμψει ξανά το κρυπτογραφημένο μήνυμα και γνωρίζοντας την ιδιότητα της πράξης XOR του παραλήπτη , μπορεί να αποκρυπτογραφήσει το υπάρχον κρυπτογραφημένο κείμενο.



Εικόνα 16: Κρυπτογράφηση κειμένου με χρήση πρωτοκόλλου WEP

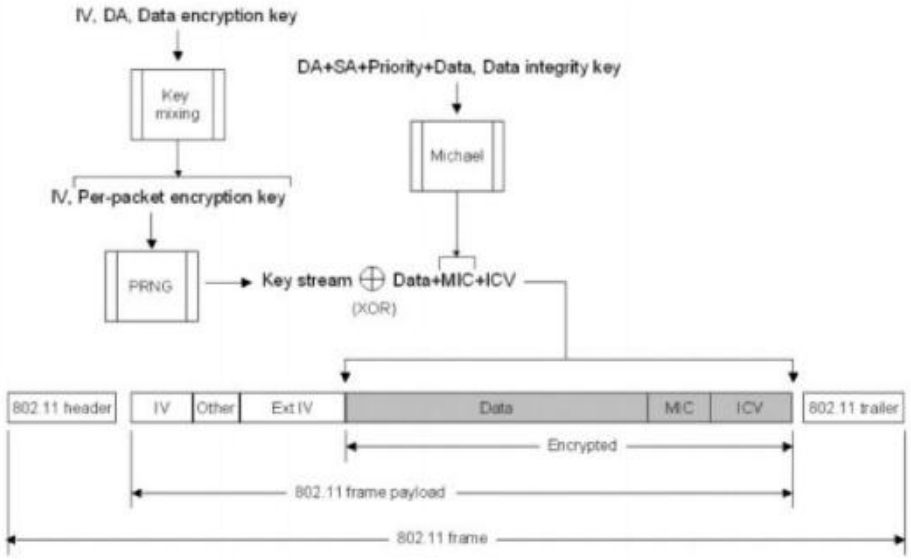
4.4 Περιγραφή πρωτοκόλλου WPA

Το πρωτόκολλο WPA το γνωστό σε όλους μας και ως Wi-Fi ,δημιουργήθηκε το 2004 έχοντας ως πρότυπο την έκδοση 802.11i με σκοπό να καλύψει τα κενά που υπήρχαν στην ασφάλεια ασύρματης επικοινωνίας από το πρωτόκολλο WEP. Το επιπλέον χαρακτηριστικό που πρόσθεσαν στην βελτιωμένη έκδοση της WEP κρυπτογράφησης είναι η εισαγωγή ενός μηχανισμού αυθεντικοποίησης , η οποία γίνεται με δύο διαφορετικούς τρόπους.

Ο πρώτος τρόπος είναι μέσω WPA-Personal γνωστή και ως προσωπική κατάσταση ή κατάσταση προ-κοινόχρηστου κλειδιού (pre-shared key (PSK)) που παρέχει ισχυρή ασφάλεια κατάλληλη για οικιακά δίκτυα. Η λειτουργία γίνεται μέσο μιας ασύρματης συσκευής και ενός σημείου πρόσβασης που έχουν προκαθοριστεί από την αρχή και προκύπτει ένα κρυπτογραφικό ζεύγος πρωτεύοντος κλειδιού.

Ο δεύτερος τρόπος είναι μέσω WPA-Enterprise γνωστή και ως ισχυρότερη κατάσταση πιστοποίησης ταυτότητας ,βασισμένη στο πρότυπο 802.1X που είναι υπεύθυνη για την ασφάλεια ασύρματων δικτύων και χρησιμοποιεί ένα διακομιστή πιστοποίησης ταυτότητας. Παρακάτω στην Λειτουργία και Αλγόριθμο του πρωτοκόλλου WPA θα εξηγήσουμε αναλυτικά τον τρόπο ταυτοποίησής του.

Σκοπός του πρωτοκόλλου WPA είναι να αποτρέψει την πρόσβαση ενός αντιπάλου στο δίκτυο, μέσω του σημείου πρόσβασης, αλλά και να τον εμποδίσει (τον αντίπαλο) να ξεγελάσει την ασύρματή μας συσκευή παραπέμποντάς τον σε ένα ψεύτικο (εικονικό) AccessPoint (AP).



Εικόνα 17: Υλοποίηση WPA πρωτοκόλλου

4.4.1 Αλγόριθμος-Λειτουργία WPA

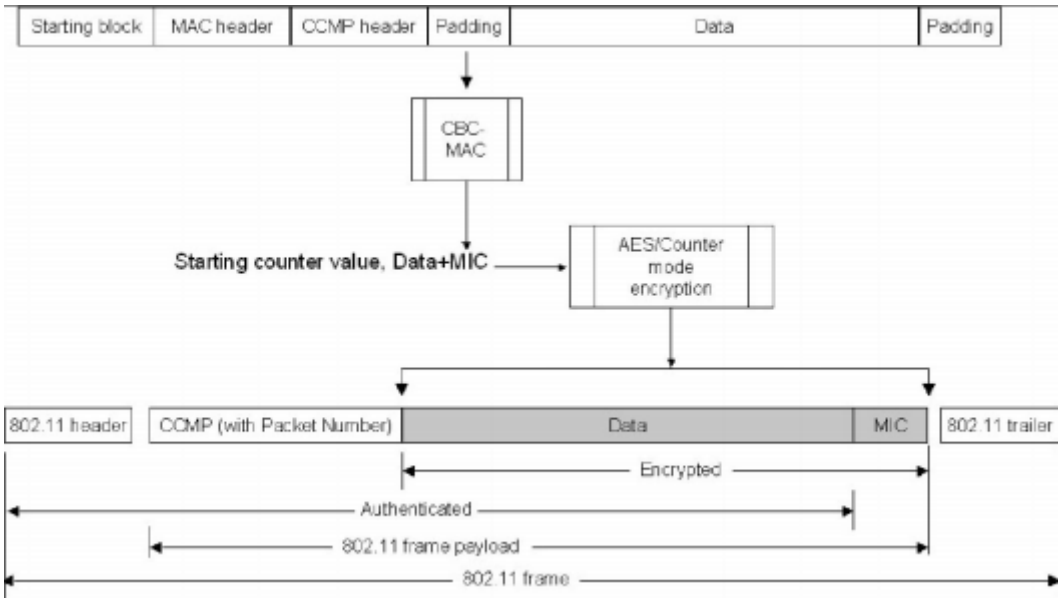
Το πρωτόκολλο WPA χρησιμοποιεί και αυτό την γεννήτρια τυχαίων αριθμών RC4 με δημιουργία μήκους κλειδιού από 64 bits έως και 256 bits. Η διαφορά του με το πρωτόκολλο WEP είναι στη μη χρήση πλαισίου MAC και στη μη επεξεργασίας πράξεων με την XOR ,αλλά βασίζετε στη χρησιμοποίηση της hash συνάρτησης →PBKDF2(Password-Based Key Derivation Function 2) και της χρήσης του αρχικού κωδικού ως κλειδί.

Έχουμε αναφέρει πως ο μηχανισμός αυθεντικοποίησης έχει δύο τρόπος με τελικό κοινό σκοπό την επιτυχημένη πιστοποίηση ταυτότητας και δημιουργίας ενός ζεύγους κοινόχρηστου πρωτεύοντος κλειδιού. Από την μία πλευρά έχουμε την μεταξύ τους επικοινωνία μιας ασύρματης συσκευής και ενός σημείου πρόσβασης και από την άλλη πλευρά έχουμε ένα διακομιστή πιστοποίησης ταυτότητας και ενός σημείου πρόσβασης.

Η ασύρματη συσκευή και το σημείο πρόσβασης έχουν διευθετηθεί εκ των προτέρων με μια κοινόχρηστη συνθηματική φράση ,δημιουργώντας ένα πολύ μεγάλο κωδικό πρόσβασης από τον οποίο προκύπτει το ζεύγος πρωτεύοντος κλειδιού, ενώ ο διακομιστής AS και το σημείο πρόσβασης AP πρέπει να συνδέονται με ασφαλές κανάλι ώστε να μπορούν να έχουν από κοινού τις υπολογιστικές υπηρεσίες. Η ασφάλεια του καναλιού επιτυγχάνετε με την χρήση του Επεκτάσιμου Πρωτοκόλλου Πιστοποίησης Ταυτότητας (EAP) , με σκοπό να υποστηρίζει πολλές μεθόδους πιστοποίησης ταυτότητας.

4.4.2 Διαφορές πρωτοκόλλου WPA με WPA2

Όπως έχουμε αναφέρει το πρωτόκολλο κρυπτογράφησης WPA δημιουργήθηκε για να καλύψει τα κενά του πρωτοκόλλου ασφαλείας WEP. ‘Αν και σχεδόν αδιαπέραστο το WPA η ομάδα του προτύπου IEEE 802.11 πήρε την απόφαση αν δημιουργήσει την βελτιωμένη έκδοση του WPA ,δηλαδή το πρωτόκολλο WPA2. Αυτό που κάνει την διαφορά στα δύο αυτά πρωτόκολλα είναι ο αλγόριθμος κρυπτογράφησης. Στο WPA2 χρησιμοποίησαν τον αλγόριθμο CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol) το οποίο βασίζεται στο πρωτόκολλο CTR (Counter Mode) . Χρησιμοποιεί αλγόριθμο AES(Advanced Encryption Standard) σε κατάσταση λειτουργίας μετρητή ώστε να μπορεί να παρέχει προστασία εμπιστευτικότητας και ιδιωτικότητας .



Εικόνα 18: Υλοποίηση WPA2 πρωτοκόλλου

4.5 Σύγκριση πρωτοκόλλων WEP με WPA/WPA2

Η ομάδα IEEE 802.11 όπως ήταν λογικό δημιούργησε την WPA κρυπτογράφηση για να παρέχει καλύτερη ασφάλεια στις ασύρματες συσκευές. Το μόνο χαρακτηριστικό που έμεινε ανέπαφο σε σχέση με την WEP κρυπτογράφηση είναι η γεννήτρια τυχαίων αριθμών RC4. Οι διαφορές των δύο πρωτοκόλλων ξεκινούν από μήκος του κλειδιού κρυπτογράφησης που η WEP δεσμεύει 40 ή 104 bit και επιπλέον 24 bit για τον πίνακα αρχικοποίησης ,ενώ η WPA δεσμεύει 48 bit IV(initialization vector) με 128 bit κλειδί κρυπτογράφησης. Ο κύριος στόχος επίθεσης πάνω στην WEP ήταν ο πίνακας αρχικοποίησης γι' αυτό και η WPA κρυπτογράφηση λειτουργεί με την χρήση του πρωτοκόλλου TKIP (Temporal Key Integrity Protocol) και την χρήση μεγάλου πίνακα αρχικοποίησης. Πιο συγκεκριμένα το πρωτόκολλο TKIP κάνει χρήση τριών χαρακτηριστικών ασφαλείας μαζί τα οποία είναι : Μυστικό κλειδί, Διανύσματα αρχικοποίησης και γεννήτρια τυχαίων αριθμών RC4.

Οι μηχανισμοί αυθεντικοποίησης που WPA-Personal και WPA-enterprise ήταν τα τελευταία χαρακτηριστικά που προστέθηκαν στην κρυπτογράφηση WPA, με ιδιαίτερο χαρακτηριστικό η αυτόματη παράδοση κλειδιών, έναντι της WEP που διακινούσε το κοινό κλειδί μέσα από ένα μη ασφαλές κανάλι.

Βιβλιογραφικές αναφορές κεφαλαίου

[1] http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/advantages-and-disadvantages.htm

[2] http://science.opposingviews.com/advantages-disadvantages-symmetric-key-encryption-2609.html

[3] https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol

[4] ANDREW S. TANENBAUM (2003),*COMPUTER NETWORKS* , Αθήνα:Κλειδάριθμος

[5] WILLIAMSTALLINGS(2007),*ΑΣΥΡΜΑΤΕΣΕΠΙΚΟΙΝΩΝΙΕΣΚΑΙΔΙΚΤΥΑ*. Αθήνα:Τζιόλα

ΚΕΦΑΛΑΙΟ 5ο Επιθέσεις δικτύων και τρόποι αντιμετώπισης

Εισαγωγή 5ου κεφαλαίου

Το πέμπτο και τελευταίο θεωρητικό κεφάλαιο την εργασίας έχει ως στόχο την ενημέρωση των αναγνωστών όσον αναφορά τις διαφορετικές κατηγορίες επιθέσεων που επικρατούν στις μέρες μας ως προς τις ασύρματες συσκευές. Γίνεται λεπτομερή περιγραφή των διαφόρων ειδών επιθέσεων και παρουσίαση λειτουργίας μέσω εικόνων. Στο τελευταίο σκέλος του κεφαλαίου αναφέρονται οι βασικότεροι τρόποι προφύλαξης και αντιμετώπισης τέτοιων μελλοντικών επιθέσεων.

5.1 Τύποι επιθέσεων ασύρματων δικτύου

Γνωρίζουμε πολύ καλά πως τα ασύρματα δίκτυα είναι πιο ευάλωτα από τα ενσύρματα δίκτυα , λόγο του διαφορετικού τρόπου μετάδοσης των πληροφοριών. Τα ασύρματα δίκτυα μεταδίδουν δεδομένα μέσο του αέρα και μπορούν να επηρεαστούν ευκολότερα από τρίτα πρόσωπα αρκεί να βρίσκονται εντός της εμβέλειας εκπομπής της ασύρματης συσκευής. Με την έννοια επίθεση ,εννοούμε την οποιαδήποτε ενέργεια που κάνουν εξωτερικοί παράγοντες προκειμένου να επηρεάσουν την ασφάλεια της πληροφορίας.

Οι επιθέσεις πάνω στην ασφάλεια των ασύρματων δικτύων ,χωρίζονται σε δύο κατηγορίες , οι παθητικές επιθέσεις (passive) και οι ενεργητικές επιθέσεις (active).

5.1.1 Παθητική επίθεση δικτύου

Παθητικές επιθέσεις χαρακτηρίζονται οι επιθέσεις στις οποίες ο επιτιθέμενος λαμβάνει απαραίτητες πληροφορίες τις οποίες μπορεί αργότερα να τις χρησιμοποιήσει για ενεργητικές επιθέσεις. Τέτοιου είδους παθητικών επιθέσεων είναι:

- Υποκλοπή (eavesdropping)
- Συλλογή πληροφοριών (traffic analysis)
- Συλλογή πακέτων (packet sniffing)
- Παρακολούθηση κυκλοφορίας (monitoring)

Ο δημοφιλέστερος τρόπος αποφυγής παθητικών επιθέσεων είναι η χρήση κρυπτογραφίας.

Οι επιθέσεις υποκλοπής είναι μη εξουσιοδοτημένης παρακολούθησης, των επικοινωνιών άλλων ανθρώπων. Σκοπός του επιτιθέμενου είναι να λάβει δεδομένα από ανθρώπους που κάνουν χρήση όλων των υπηρεσιών του Διαδικτύου όπως e-mail ,char και κωδικούς ιστοσελίδων ,προκειμένου να τις χρησιμοποιήσει αργότερα για μελλοντικές ενεργητικές επιθέσεις.

Οι επιθέσεις συλλογής πληροφοριών γίνετε από την πλευρά του επιτιθέμενου στην ασύρματη συσκευή μετάδοσης λαμβάνοντας πληροφορίες σχετικά με την φυσική διεύθυνση της συσκευής (MAC address) ,το κανάλι και την συχνότητα εκπομπής ,το πρωτόκολλο κρυπτογράφησης ,ακόμα και τις φυσικές

διευθύνσεις των ασύρματων και ενσύρματων συσκευών που είναι εκείνη την στιγμή συνδεδεμένες.

Οι επιθέσεις συλλογής πακέτων, έχουν ως σκοπό την παρακολούθηση και την καταγραφή της κίνησης των πακέτων του δικτύου, που τηρούν κάποια κριτήρια ,προκειμένου να καταγραφούν σε ένα αρχείο. Ύστερα αυτά τα πακέτα επεξεργάζονται και αποκρυπτογραφούνται ώστε να μάθουν περεταίρω χαρακτηριστικά του δικτύου.

Οι επιθέσεις monitoring είναι ένας συνδυασμός της traffic analysis και της packet sniffing. Λαμβάνει στοιχεία που αφορούν το ασύρματο δίκτυο και παρακολουθεί την ροή των πακέτων για τυχόν αλλαγές που μπορεί να εμφανιστούν.

5.1.2 Ενεργητική επίθεση δικτύου

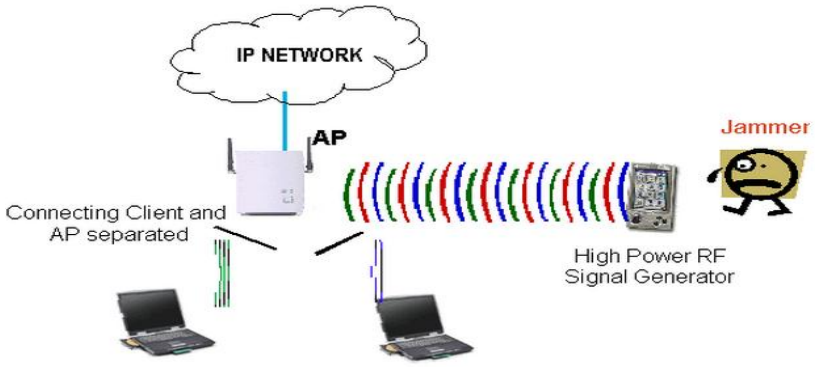
Ενεργητικές επιθέσεις χαρακτηρίζονται οι επιθέσεις στις οποίες λαμβάνει μέρος ο επιτιθέμενος με χρήση είτε ανταλλασσόμενων μηνυμάτων είτε με δημιουργία ψεύτικων μηνυμάτων. Τα είδη των ενεργητικών επιθέσεων διακρίνονται στις εξής κατηγορίες:

- Επιθέσεις με παρεμβολές (jamming)
- Επιθέσεις με τροποποίηση μηνυμάτων (modification)
- Επιθέσεις με μεταμφίεση (impersonating)
- Επιθέσεις με άρνηση υπηρεσιών (Denial Of Service)

Ο δημοφιλέστερος τρόπος για να αποφύγουμε τέτοιου είδους επιθέσεων είναι η συχνή επαλήθευση και εγκυρότητα με χρήση μετρητών εισόδου ,σε οποιαδήποτε δραστηριότητα που ασκούμε στην ασύρματη συσκευή. Δύσκολο και σχεδόν ακατόρθωτο ,γι' αυτό και είμαστε ευάλωτοι στις συγκεκριμένες επιθέσεις δικτύων.

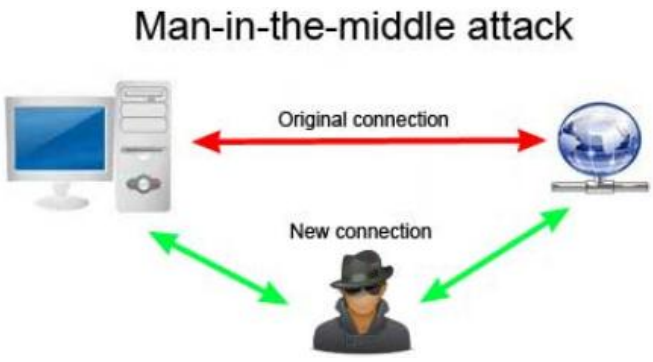
Οι επιθέσεις με παρεμβολές είναι συχνές επιθέσεις που παρατηρούνται στα ασύρματα δίκτυα. Το μόνο που έχει να κάνει ο επιτιθέμενος είναι να καταφέρει να μπλοκάρει τη συχνότητα εκπομπής της ασύρματης συσκευής που συνήθως είναι τα 2,4 GHz, με αποτέλεσμα να πέσει η συχνότητα του σήματος σε πολύ χαμηλά επίπεδα και να μην μπορεί πλέον να λειτουργήσει. Ο κύριος λόγος που

κάνει τους επιτιθέμενους να χρησιμοποιούν αυτό το είδος της επίθεσης είναι, επειδή πολλές ασύρματες συσκευές εκτός από αυτές που παρέχουν υπηρεσίες Διαδικτύου ,εκπέμπουν και αυτές στην συχνότητα των 2,4GHz έχοντας ως αποτέλεσμα τις παρεμβολές.



Εικόνα 19:Επίθεση με χρήση παρεμβολών (jamming)

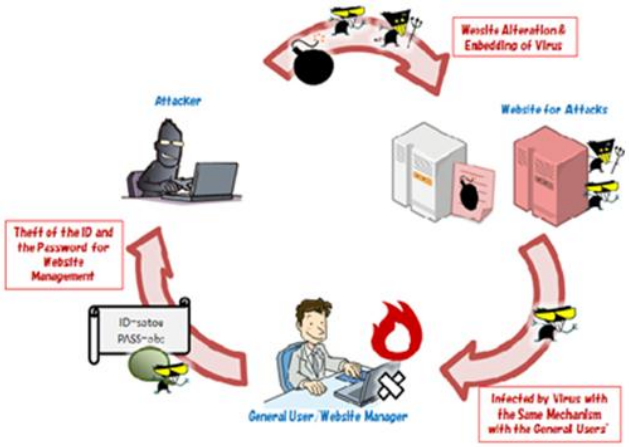
Οι επιθέσεις με τροποποίηση μηνυμάτων έχουν ως στόχο την υποκλοπή δεδομένων σε μία αρχική συνομιλία δύο ατόμων. Ο επιτιθέμενος δεν παίρνει μέρος σε αυτή την συνομιλία ώστε να κρυφακούσει, αλλά παίρνει θέση πάνω στην ασύρματη συσκευή και τα δεδομένα μεταφέρονται πρώτα σε αυτόν πριν φτάσουν στον άλλο εξυπηρετητή.



Εικόνα 20:Επίθεση με τροποποίηση μηνυμάτων (modification)

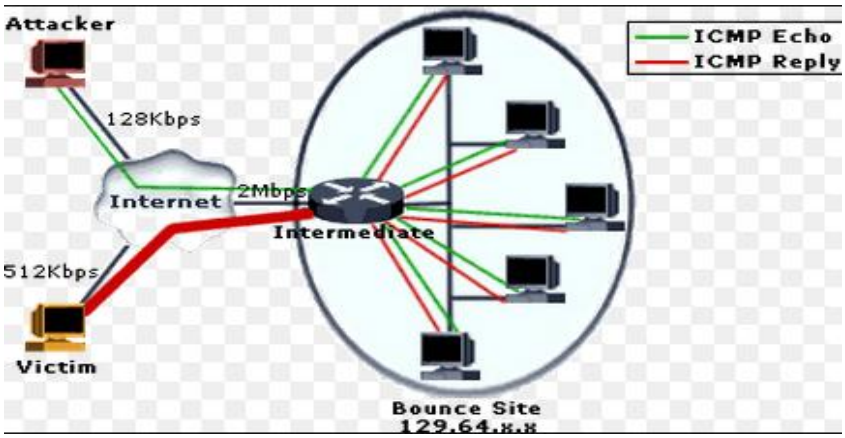
Οι επιθέσεις μεταμφίεσης ονομάστηκαν έτσι γιατί ο επιτιθέμενος χρησιμοποιεί μία ψεύτικη ταυτότητα δικτύου για να αποκτήσει πρόσβαση σε πληροφορίες

του υπολογιστή. Αυτό συμβαίνει μόνο όταν ο υπολογιστής δεν χρησιμοποιεί τα κατάλληλα προγράμματα πλήρης προστασίας.



Εικόνα 21:Επίθεση με μεταμφίεση (impersonating)

Οι επιθέσεις με άρνηση υπηρεσίας είναι η πιο συχνές και διαδεδομένες επιθέσεις πάνω στα ασύρματα δίκτυα και πολλές φορές είναι δύσκολο να αποφευχθούν επειδή οι ασύρματες συσκευές δεν έχουν πολύ μεγάλη υπολογιστική ισχύ. Ο τρόπος με τον οποίο καταρρέει η ασύρματη συσκευή και παρέχει πρόσβαση στον επιτιθέμενο είναι ο χρόνος καθυστέρησης των τεράστιων όγκων δεδομένου που έχει αποστείλει ο επιτιθέμενος καθιστώντας την συσκευή ανίκανη να τα επεξεργαστεί , διακόπτοντας έτσι την επικοινωνία των χρηστών.

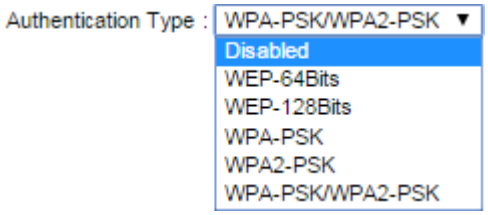


Εικόνα 22:Επίθεση με άρνηση υπηρεσιών (DenialOfService/DOS)

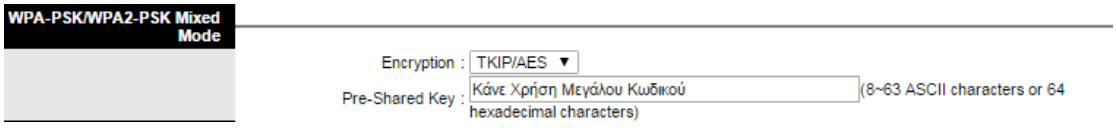
5.2 Τρόποι αντιμετώπισης επιθέσεων

Ο βασικός σκοπός του Διαδικτύου είναι η εύκολη και γρήγορη ανταλλαγή πληροφορίας μεταξύ διαφόρων χρηστών. Το σημαντικότερο όμως θέμα στα σύγχρονα δίκτυα είναι η ασφάλεια την πληροφορίας, τόσο ατομικά για έναν απλό χρήστη όσο και για έναν ολόκληρο οργανισμό. Συγκεκριμένα η ασφάλεια στα ασύρματα δίκτυα βασίζεται στην πρόληψη και λήψη μέτρων στην αρχή προκειμένου να μην αντιμετωπισθούν προβλήματα αργότερα. Τέτοιου είδους μέτρα εφαρμόζονται κυρίως πάνω στις ασύρματες συσκευές και είναι τα εξής:

- *Access Point Security (AP)*, είναι το ασύρματο σημείο πρόσβασης που θα συνδεθούν πάνω σε αυτό όλες οι ασύρματες συσκευές προκειμένου να έχουν παροχή υπηρεσιών Internet. Χρησιμοποιεί ένα από τα δύο είδη κρυπτογράφησης WEP ή WPA/WPA2 ,το οποίο ουσιαστικά είναι το κλειδί-κωδικός για να συνδεθεί ο κάθε χρήστης . Ο σκοπός του κλειδιού είναι να μην μπορεί να βρεθεί εύκολα ,ώστε να εμποδίσει την εισβολή του επιτιθέμενου στο δίκτυό μας ή έστω να τον καθυστερήσει . Ένας ακόμα τρόπος που αφορά την προστασία του ασύρματου δικτύου και βασίζεται πάνω στο AP είναι ο περιορισμός των χρηστών. Μειώνοντας την σύνδεση πολλών χρηστών ,υπάρχει καλύτερος έλεγχος και ελάττωση των πιθανοτήτων να δεχτεί το δίκτυο επίθεση.

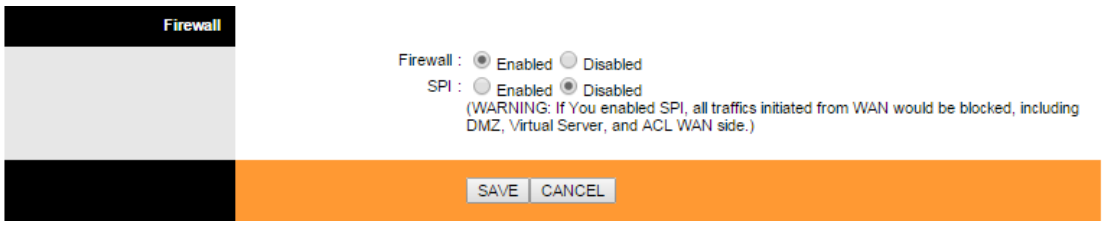


Εικόνα23:Χρήση πρωτοκόλλου κρυπτογράφησης



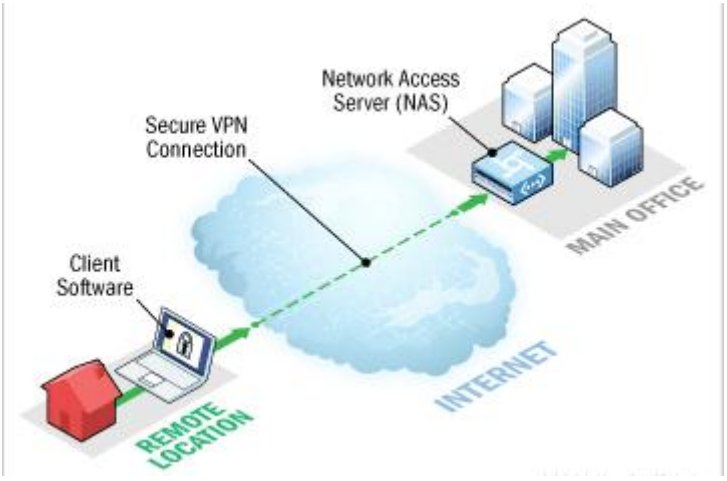
Εικόνα24:Χρήση μεγάλου κωδικού ασφαλείας

- *Ασφάλεια τερματικών σταθμών*, η εισβολή σε ένα ασύρματο δίκτυο δεν μπορεί να αποφευχθεί με μεγάλη σιγουριά. Σε περίπτωση που εισβάλει στο δίκτυο και δεν υπάρχει κίνηση δεδομένων για να υποκλέψει ,μπορεί να λάβει πληροφορίες για άλλους τερματικούς σταθμούς. Ο μόνος τρόπος προστασίας σε αυτό το σημείο είναι η εγκατάσταση λογισμικών διάφορων ιών (Anti-virus) , αλλά και η ενημέρωση-εγκατάσταση προσωπικών Firewalls στον τερματικό μας σταθμό.



Εικόνα25:Ενεργοποίηση τοίχου προστασίας σε ασύρματη συσκευή

- *Ασφαλή μετάδοση πληροφορίας,* η χρήση πρωτοκόλλου ασφαλείας και κωδικού δεν είναι επαρκεί για να προστατέψουν τις πολύτιμες πληροφορίες, την στιγμή που αποστέλλονται μέσω ενός μη ασφαλούς καναλιού επικοινωνίας. Σε τέτοιες περιπτώσεις γίνεται χρήση ενός Εικονικού Προσωπικού Δικτύου(Virtual Private Network) το οποίο κάνει χρήση ισχυρών αλγορίθμων και επιβεβαίωση εμπιστευτικότητας της επικοινωνίας.



Εικόνα26:Μετάδοση πληροφορίας με VPN

- *Αλλαγή ζώνης συχνοτήτων,* τα περισσότερα AP που παρέχουν την δυνατότητα σύνδεσης των χρηστών στο Διαδίκτυο εκπέμπουν στην ζώνη συχνοτήτων 2,4GHz. Σε αυτές τις συχνότητες όμως παρεμβάλουν και άλλες συσκευές όπως το Bluetoothκαι η ασύρματες κάμερες ,παρεμποδίζοντας το σήμα και την μετάδοση των δεδομένων . Συνεπώς αν το AP έχει την δυνατότητα αυτόματης ρύθμισης και ισχύος εκπομπής σήματος στη ζώνη συχνοτήτων των 5GHz είναι προτιμότερο λόγο των μειωμένων παρεμβολών.

Εικόνα27:Αλλαγή συχνοτήτων από 2,4GHz σε 5GHz

Βιβλιογραφικές αναφορές κεφαλαίου

[1] http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/types-of-attack.html

[2] ΠΡΕΒΕΣ ΝΙΚΟΛΑΟΣ(2008),*ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ ,ΑΣΦΑΛΕΙΑ ΚΑΙ ΑΠΟΔΟΣΗ ΤΩΝ ΠΡΩΤΟΚΟΛΛΩΝ TCP/IP*. Αθήνα :Εκδόσεις νέων τεχνολογιών

[3] http://en.wikipedia.org/wiki/Monitoring

[4] LARRYL.PETERSON&BRUCES.DAVIE(2009) ,*ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ,μια προσέγγιση από τη σκοπιά των συστημάτων* Αθήνα : Κλειδάριθμος

[5] WILLIAMSTALLINGS(2007),*ΑΣΥΡΜΑΤΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ ΚΑΙ ΔΙΚΤΥΑ.* Αθήνα:Τζιόλα

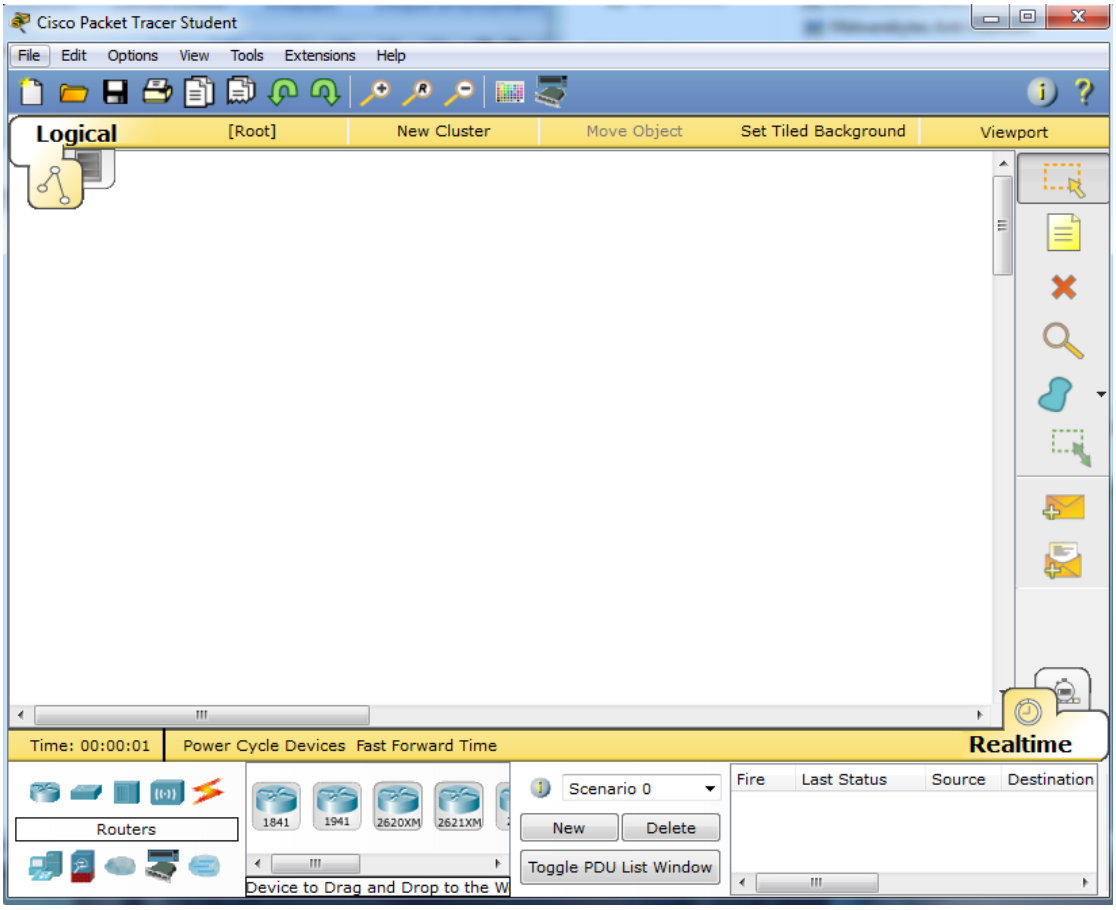
[6] ANDREWS. TANENBAUM (2003),*COMPUTERNETWORKS* , Αθήνα:Κλειδάριθμος

[7]http://www.infosec.gov.hk/english/promotion/files/Script_Eavesdropping.pdf

ΚΕΦΑΛΑΙΟ 6ο ΠΡΟΣΟΜΟΙΩΤΗΣ CISCOPACKETTRACER (CPT)

6.1 Γενικές πληροφορίες για το CPT

Πολλές φορές αναφέρονται συσκευές, έννοιες και τεχνικές πάνω στα δίκτυα οι οποίες είναι δύσκολα κατανοητές. Κάποιες από αυτές αφορούν τις διευθύνσεις IP, τις διευθύνσεις Ethernet , τις δρομολογήσεις ακόμα και την έννοια του υποδικτύου. Κάνοντας όμως χρήση του προγράμματος CPT μπορούν να γίνουν εύκολα κατανοητές λόγο του ιδανικού γραφικού περιβάλλοντος που παρέχει. Η δυνατότητα παροχής κόμβων ,διακοπτών ,δρομολογητών , τερματικών σταθμών , τοίχων προστασίας και πολλών ειδών καλωδίων είναι λίγες από τις δυνατότητες που έχει το πρόγραμμα για να υλοποιήσει μια άσκηση σε περιβάλλον πραγματικού χρόνου ή σε περιβάλλον προσομοίωσης.

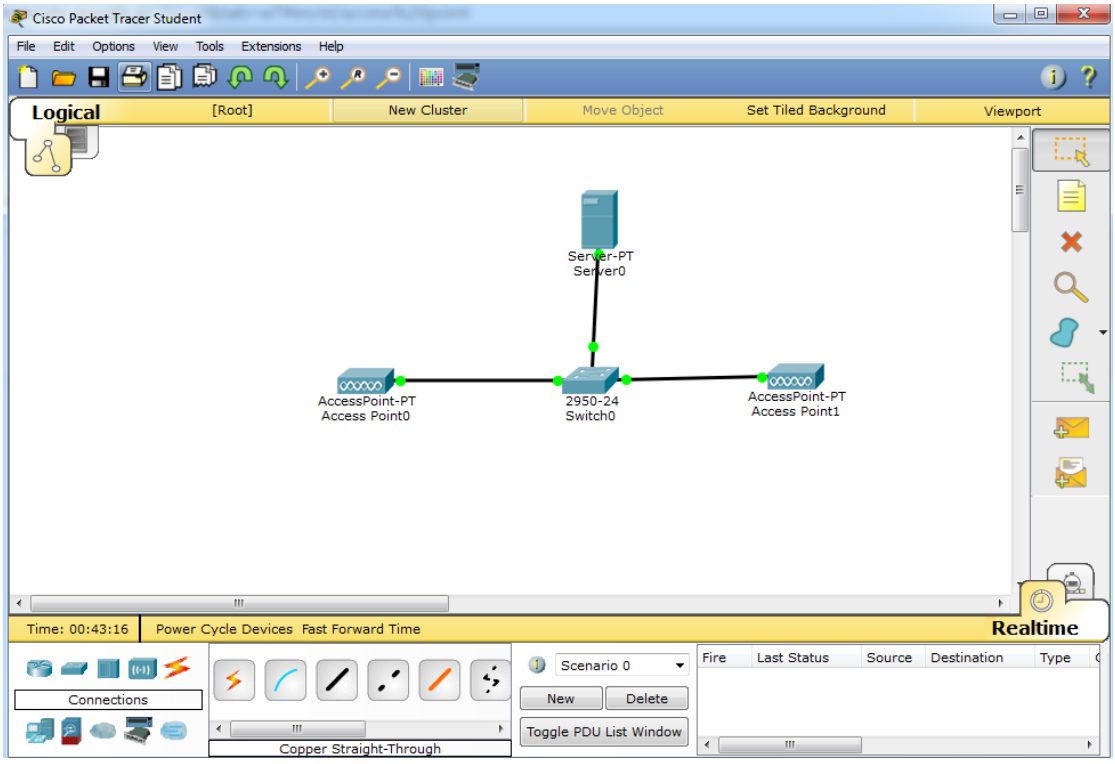


Εικόνα28:Περιβάλλον προσομοίωσης CiscoPacketTracer (CPT)

6.2 Υλοποίηση της προσομοίωσης

Στόχος την προσομοίωσης μας είναι να υλοποιήσουμε ένα εκτεταμένο σύνολο υπηρεσιών (Extended Service Set) δικτύου με την δυνατότητα χρήσης ενός πρωτοκόλλου ασφαλείας. Η επικοινωνία των σταθμών θα γίνεται μέσω ενός AccessPoint (AP) για κάθε μια κυψέλη και μέσω ενός διακόπτη (Switch) και ενός διακομιστή (Server) η επικοινωνία θα διακόπτεται ή θα συνεχίζεται.

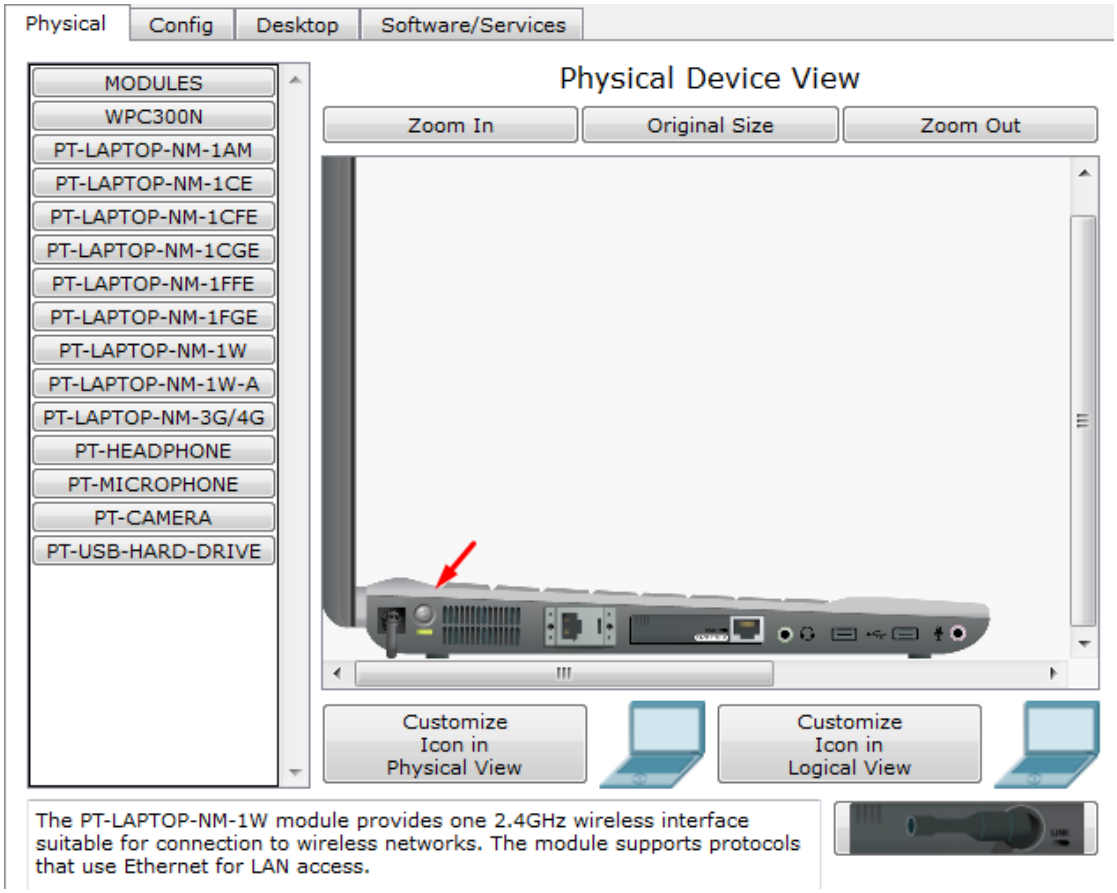
Στο πρώτο στάδιο της προσομοίωσης θα χρειαστούμε να εισάγουμε στο γραφικό μας περιβάλλον τις συσκευές διασύνδεσης , δηλαδή έναν διακομιστή, έναν διακόπτη και δύο σημεία πρόσβασης. Αφού τα τοποθετήσουμε σε μία σειρά (όπως την εικόνα23) επόμενο στάδιο είναι η σύνδεση τους με χρήση καλωδίων Straight-Through. Η σύνδεση μεταξύ Server/Switch θα γίνει στις θύρες FastEthernet0 &FastEthernet0/1 ενώ η σύνδεση Switch/AccessPoint0 θα γίνει στις θύρες FastEthernet0/23 &Port 0 και Switch/AccessPoint1 θα γίνει στις θύρες FastEthernet0/24 &Port 0.



Εικόνα29:Τοποθέτηση και σύνδεση συσκευών στο γραφικό περιβάλλον

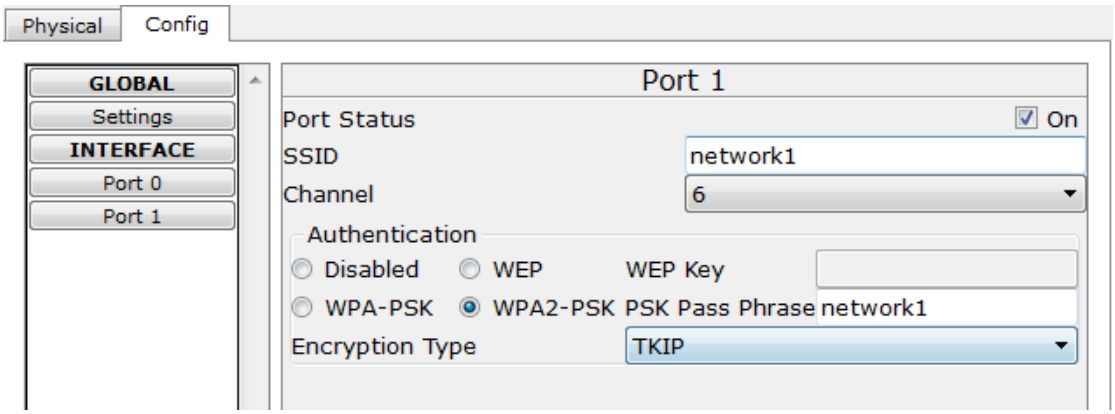
Αφού έχουμε βεβαιωθεί ότι όλα τα led είναι πράσινα ,τότε μπορούμε να προχωρήσουμε στο επόμενο στάδιο που είναι η εισαγωγή των ασύρματων συσκευών (υπολογιστές) στο περιβάλλον προσομοίωσης. Το μόνο που έχουμε να κάνουμε είναι να πάμε στο κάτω αριστερά μέρος του προγράμματός μας ,να επιλέξουμε το εικονίδιο που αναγράφει «End Devices» και από εκεί να εισάγουμε όσους υπολογιστές (laptop ή desktop) που χρειαζόμαστε. Μόλις τους τοποθετήσουμε εντός (σχετικά) της εμβέλειας του AP ,μπορούμε να περάσουμε στο επόμενο στάδιο που είναι η προσθήκη κεραίας σε όλες τις συσκευές μας για να έχουμε την δυνατότητα εντοπισμού ασύρματων δικτύων.

Για να υλοποιήσουμε το συγκεκριμένο στάδιο θα πρέπει να κάνουμε μια φορά ¨κλικ¨ στον υπολογιστή και στο παράθυρο που θα μας βγάλει θα απενεργοποιήσουμε την συσκευή , θα εξάγουμε την θύρα Ethernet και θα εισάγουμε την κεραία ασύρματου δικτύου που εμφανίζεται στο κάτω δεξιά μέρος του παραθύρου. Μόλις το κάνουμε ενεργοποιούμε την συσκευή ξανά.



Εικόνα30:Παραμετροποίηση συσκευής για λήψη ασύρματου δικτύου.

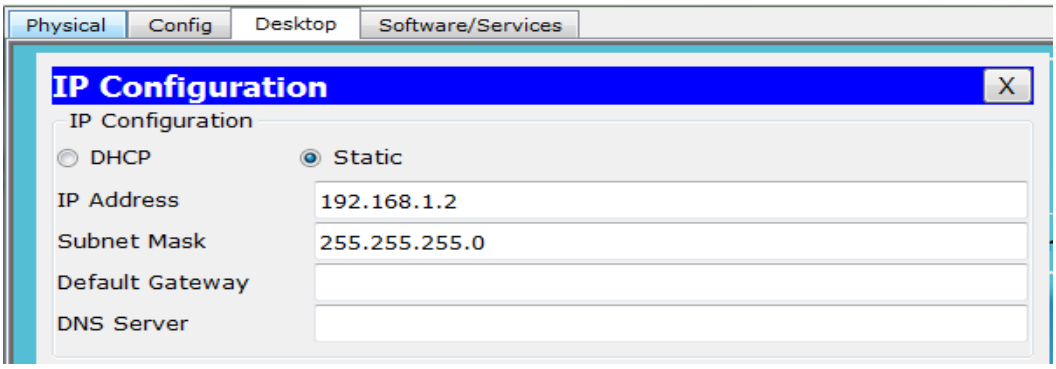
Σε αυτό το σημείο βλέπουμε πως οι υπολογιστές μας έχουν εντοπίσει το ασύρματο δίκτυο και συνδέονται με τα AP. Για να έχουμε όμως ένα καλύτερο επίπεδο ασφάλειας στο δίκτυό μας θα κάνουμε τις απαραίτητες ρυθμίσεις αλλαγής ονόματος και χρήσης ενός είδους πρωτοκόλλου ασφαλείας. Πατώντας πάνω σε ένα AccessPoint και κάνοντας ¨κλικ¨ στην κατηγορία Config→Port1 μας δίνει την δυνατότητα να αλλάξουμε το SSIDπου είναι το όνομα της συσκευής και στην κατηγορία ασφάλειας, επιλέγουμε χρήση WPA2-PSK βάζοντας ένα δικό μας κωδικό.



Εικόνα31:Παράμετροι AccessPoint(ονόματος και κωδικού)

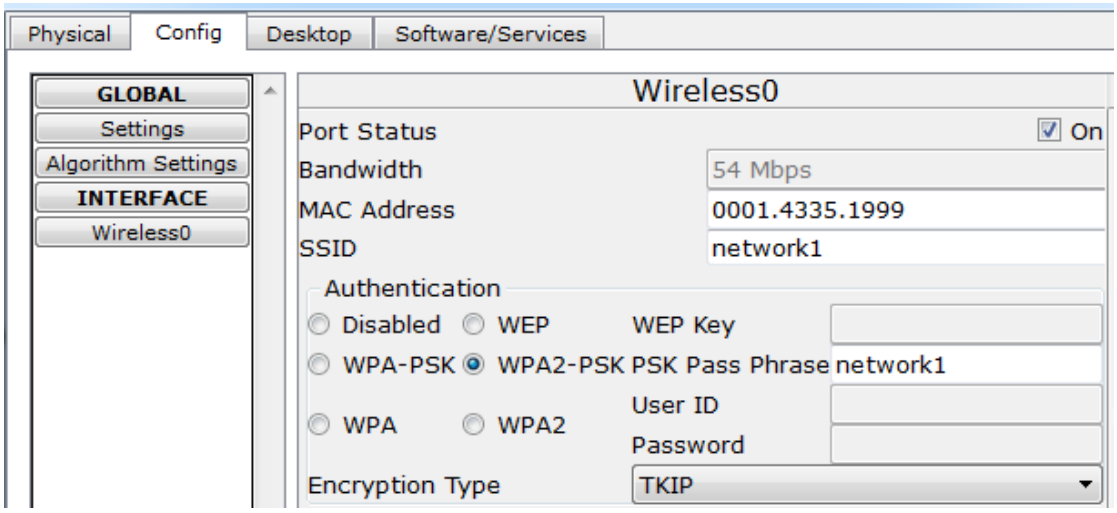
Μόλις ολοκληρώσουμε και αυτό το στάδιο ,μπορούμε να πούμε ότι βρισκόμαστε στην τελική ευθεία της προσομοίωσής μας. Η Χρήση διευθύνσεων IPστον Server και στις ασύρματες συσκευές είναι το προ-τελευταίο στάδιο ,έχοντας ως τελευταίο την εισαγωγή των καινούργιων ονομάτων και κωδικών ασφαλείας που ορίσαμε εμείς στα AP, στις ασύρματες συσκευές μας.

Για να ορίσουμε τις φυσικές διευθύνσεις θα πρέπει να κάνουμε ¨κλικ¨ σε μία συσκευή ,από εκεί επιλέγουμε την κατηγορία Desktop ->IP configuration ενεργοποιούμε την κατηγορία Static και θέτουμε ως IP Address 192.168.1.1 και Subnet Mask 255.255.255.0 .Σε κάθε διαφορετική συσκευή το μόνο που θα αλλάζουμε θα είναι το τελευταίο αριθμό της IP Address στον οποίο θα προσθέτουμε +1 ,η επόμενη δηλαδή συσκευή θα έχει το 192.168.1.2 .



Εικόνα32:Χρήση IPAddress και SubnetMask

Στο τελευταίο στάδιο της προσομοίωσής μας είναι να μπούμε στις ρυθμίσεις της κάθε μία ασύρματης συσκευής, να επιλέξουμε την κατηγορία Config και από εκεί την κατηγορία Wireless0 . Στο παράθυρο που εμφανίζεται τοποθετούμε το αλλαγμένο SSID και τον καινούργιο κωδικό πρόσβασης που ορίσαμε εμείς πριν στα AccessPoint.

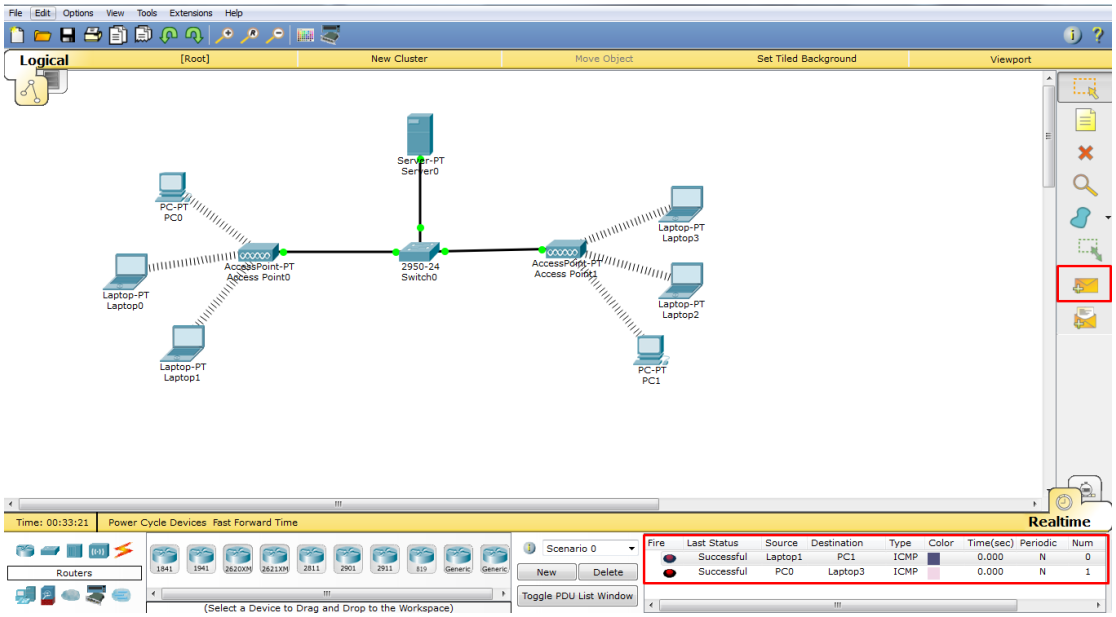


Εικόνα33:Αντικατάσταση SSID και Κωδικού ασύρματου σταθμού σε υπολογιστή

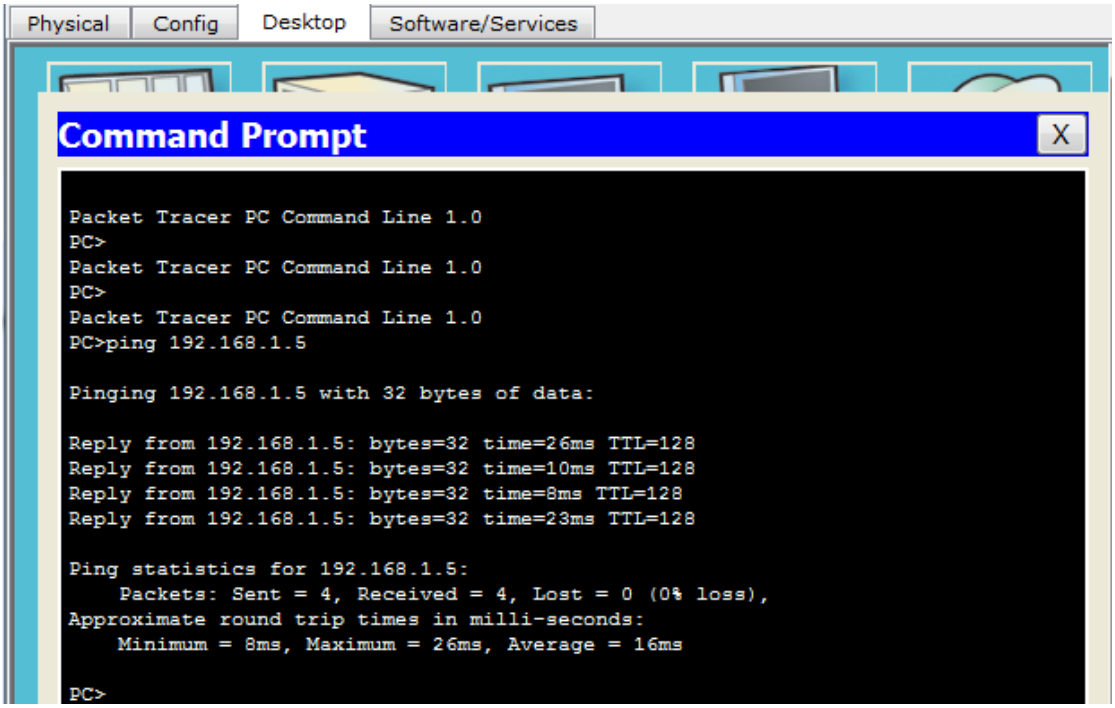
Στο σημείο αυτό ,η προσομοίωση ολοκληρώθηκε και το μόνο πράγμα που απομένει για να σιγουρευτούμε ότι η προσομοίωση λειτουργεί άψογα είναι να βεβαιωθούμε ότι οι υπολογιστές μπορούν να επικοινωνούν όλοι μεταξύ τους. Η επιβεβαίωση μπορεί να γίνει με δύο τρόπους:

Ο πρώτος τρόπος που είναι και πιο εύκολος ,δίνεται από το πρόγραμμα προσομοίωσης. Στο δεξιά μέρος του προγράμματός μας υπάρχει ένα εικονίδιο ενός κλειστού φακέλου(εικόνα 28). Επιλέγοντας το εικονίδιο αυτό μας δίνεται η δυνατότητα να επιλέξουμε δύο υπολογιστές. Αφού γίνει η επιλογή από την πλευρά μας ,στο κάτω μέρος του προγράμματος ανακοινώνεται αν η επικοινωνία πραγματοποιήθηκε ή όχι.

Ο δεύτερος τρόπος για να επιβεβαιώσουμε αν το δίκτυό μας λειτουργεί κανονικά γίνεται στέλνοντας μηνύματα ping μέσω του Command Prompt του κάθε υπολογιστή . Αν λαμβάνουμε απάντηση τότε το δίκτυό μας λειτουργεί κανονικά.



Εικόνα34:Πρώτος τρόπος προβολής λειτουργίας προσομοίωσης



Εικόνα35:Δεύτερος τρόπος προβολής λειτουργίας προσομοίωσης

ΚΕΦΑΛΑΙΟ 7ο Συμπεράσματα

Τα συμπεράσματα που προκύπτουν από την παραπάνω πτυχιακή εργασία είναι αυτά που με ώθησαν να ασχοληθώ με το συγκεκριμένο θέμα. Τα συμπεράσματά μου είναι τα εξής:

- ✓ Τα ασύρματα δίκτυα έχουν μεγάλη ανάπτυξη και ζήτηση στις μέρες μας ,αλλά το μέσο μετάδοσης δεν είναι ασφαλές από πλευράς επιθέσεων.
- ✓ Τα ασύρματα δίκτυα λόγο του τρόπου μετάδοσης είναι βλαβερά για την ανθρώπινη υγεία, περισσότερο απ' ότι τα ενσύρματα δίκτυα.
- ✓ Τα πρότυπα της IEEE αναβαθμίζονται συνεχώς προκειμένου να μπορέσουν να καλύψουν τις ανάγκες των ασύρματων δικτύων.
- ✓ Το πρωτόκολλο WEP παρέχει μια τυπική ασφάλεια σε ένα ασύρματο δίκτυο αλλά μπορεί εύκολα να αποκρυπτογραφηθεί από το επιτιθέμενο άτομο.
- ✓ Το πρωτόκολλο WPA/WPA2 έδωσε ασφάλεια στα δίκτυα μετά το 2004. Η πολυπλοκότητα της κρυπτογράφησής του παραμένει σε αρκετά υψηλά επίπεδα.
- ✓ Η σύγκριση των δύο πρωτοκόλλων βγάζει φανερό νικητή το πρωτόκολλο WPA. Ο λόγος είναι το μεγαλύτερο μήκος κλειδιού και η χρήση του πρωτοκόλλου TKIP, σε συνδυασμό με τον μεγαλύτερο πίνακα αρχικοποίησης.
- ✓ Οι επιθέσεις πάνω στα ασύρματα δίκτυα υπάρχουν και θα συνεχίσουν να υπάρχουν μέχρι κάποια μέρα να καταφέρουμε να δημιουργήσουμε το ΑΠΟΛΥΤΟ πρωτόκολλο .(Αν αυτό θα μπορέσει να υπάρξει ποτέ!)
- ✓ Οι παθητικές επιθέσεις δεν είναι βλαβερές ως προς την ασύρματη συσκευή μας, αλλά μπορούν να υποκλέψουν οποιαδήποτε πληροφορία έχουμε εμείς μέσα σε αυτή.
- ✓ Για να καταφέρουμε να αποφύγουμε τις παθητικές επιθέσεις δημιουργήθηκε η κρυπτογραφία που είναι εγκατεστημένη μέσα στα πρωτόκολλα ασφαλείας της ασύρματης συσκευής.
- ✓ Οι ενεργητικές επιθέσεις είναι βλαβερές και αυτό γιατί τα στοιχεία που μας υποκλέπτουν χρησιμοποιούνται εναντίον

μας. Κλοπή κωδικού, προσωπικά στοιχεία και μεταφορά κακόβουλου λογισμικού είναι οι κυριότεροι στόχοι των επιτεθέντων.

- ✓ Τρόπος αντιμετώπισης ενεργητικών επιθέσεων ,κατά ένα μέρος ,είναι η αύξηση της συχνότητας εκπομπής της ασύρματης συσκευής από τα 2.4GHz στη ζώνη συχνοτήτων των 5GHz.(Αν τηρεί τις προϋποθέσεις η ασύρματή μας συσκευή.)

Και τέλος, ας μην ξεχνάμε ότι η τεχνολογία δεν έχει φτάσει ούτε καν στο αποκορύφωμά της και έχει ακόμα πολλά να μας αποκαλύψει…

Το μόνο που χρειάζεται είναι ο άνθρωπος να είναι υπεύθυνος και συνετός απέναντί της….

ΚΕΦΑΛΑΙΟ 8ο ΒΙΒΛΙΟΓΡΑΦΙΑ

1)(http://www.satspot.gr/technology/connections/201-katigories-diktioy-ilekronikon-ipologiston)

2) (http://www.diktyas.gr)

3)(http://el.wikipedia.org/wiki/%CE%91%CF%83%CF%8D%CF%81%CE%BC%CE%B1%CF%84%CE%BF_%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF)

4) (http://www.smarteck.gr/info_wlan.html)

5)ΒΑΣΣΗΣ ΔΗΜΗΤΡΙΟΣ (2014),*ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ ΕΠΙΚΟΙΝΩΝΙΩΝ, Με επίγειες μικροκυματικές ζεύξεις* , ΑΡΤΑ)

6)Καψάλης.Χ&Κωττής.Π (2002),*ΚΕΡΑΙΕΣ ΑΣΥΡΜΑΤΕΣ ΖΕΥΞΕΙΣ* .Αθήνα : Τζιόλα

7)LARRYL.PETERSON&BRUCES.DAVIE(2009) ,*ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ,μια προσέγγιση από τη σκοπιά των συστημάτων*Αθήνα:Κλειδάριθμος

8)WILLIAMSTALLINGS(2007),*ΑΣΥΡΜΑΤΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ ΚΑΙ ΔΙΚΤΥΑ.* Αθήνα:Τζιόλα

9) ANDREWS. TANENBAUM (2003),*COMPUTERNETWORKS* , Αθήνα:Κλειδάριθμος

10)(https://www.cs.ucy.ac.cy/courses/EPL674/labs/lab1/Lab1-Cryptography.pdf)

11)(http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/advantages-and-disadvantages.htm)

12)(http://science.opposingviews.com/advantages-disadvantages-symmetric-key-encryption-2609.html)

13)(http://digilib.lib.unipi.gr/dspace/bitstream/unipi/4992/1/Kefalas,%20Grigorios%20I..pdf)

14) (http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access)

15) (http://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol)

16)(http://www.infosec.gov.hk/english/promotion/files/Script_Eavesdropping.pdf)

17)(http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/types-of-attack.html)

18) (http://en.wikipedia.org/wiki/Monitoring)

19)ΠΡΕΒΕΣ ΝΙΚΟΛΑΟΣ(2008),*ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ ,ΑΣΦΑΛΕΙΑ ΚΑΙ ΑΠΟΔΟΣΗ ΤΩΝ ΠΡΩΤΟΚΟΛΛΩΝ TCP/IP*. Αθήνα :Εκδόσεις νέων τεχνολογιών

20)https://en.wikipedia.org/wiki/Guglielmo_Marconi

21) https://en.wikipedia.org/wiki/Internet_protocol_suite