ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Σχεδιασμός και Ανάπτυξη Ασυρμάτων Δικτύων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Βασίλειος Δ. Λακαφώσης

Επιβλέπων : Νικόλαος Ουζούνογλου
Καθηγητής Ε.Μ.Π.

Αθήνα, Αύγουστος 2006

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Σχεδιασμός και Ανάπτυξη Ασυρμάτων Δικτύων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Βασίλειος Δ. Λακαφώσης

Επιβλέπων : Νικόλαος Ουζούνογλου
Καθηγητής

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 4η Αυγούστου 2006.

.....	.....	.....
Νικόλαος Ουζούνογλου	Παναγιώτης Φράγκος	Δήμητρα Κακλαμάνη
Καθηγητής ΕΜΠ	Καθηγητής ΕΜΠ	Καθηγήτρια ΕΜΠ

Αθήνα, Αύγουστος 2006

.....

Βασίλειος Δ. Λακαφώσης

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΙΝΑΚΑΣ ΕΙΚΟΝΩΝ

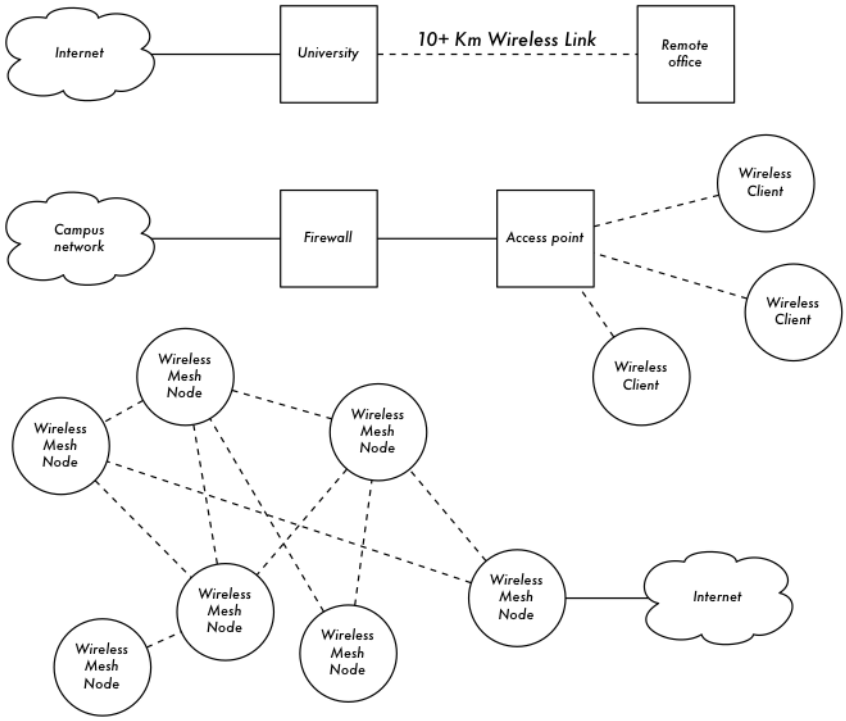
Σκοπός της διπλωματικής – Περίληψη

Η ασύρματη υποδομή μπορεί να χτιστεί με πολύ μικρό κόστος έναντι των παραδοσιακών ενσύρματων εναλλακτικών λύσεων. Παρέχοντας στην τοπική κοινότητα φτηνότερη και ευκολότερη πρόσβαση στις πληροφορίες, δύναται το ευρύ κοινό να ωφεληθεί άμεσα από αυτό που το Διαδίκτυο έχει να προσφέρει.

Αλλά ακόμη και χωρίς πρόσβαση στο Διαδίκτυο, τα ασύρματα τοπικά δίκτυα έχουν τεράστια αξία. Επιτρέπουν στους ανθρώπους να συνεργαστούν από κοινού σε προγράμματα σε μεγάλες αποστάσεις. Οι επικοινωνίες φωνής, το ηλεκτρονικό ταχυδρομείο και άλλα δεδομένα μπορούν να ανταλλαχθούν με πολύ λίγο κόστος.Τελικά, οι χρήστες συνειδητοποιούν ότι τα δίκτυα επικοινωνίας χτίζονται για να επιτρέπουν στους ανθρώπους να συνδέονται ο ένας με τον άλλον. Σε αυτό τη διπλωματική εργασία θα εστιάσω στις ασύρματες τεχνολογίες δικτύωσης δεδομένων στη οικογένεια 802.11. Ενώ ένα τέτοιο δίκτυο μπορεί να φέρει δεδομένα, φωνή, και βίντεο (καθώς επίσης και τον παραδοσιακό Ιστό), τα δίκτυα που περιγράφονται σε αυτή την εργασία είναι δίκτυα δεδομένων. Έμφαση δίνεται στην οικοδόμηση ζεύξεων υποδομής, που προορίζονται για να χρησιμοποιηθούν ως κορμός για τα ασύρματα δίκτυα ευρείας περιοχής.

Από τα πρώτα πειράματα στο γύρισμα του προηγούμενου αιώνα, η ασύρματη μετάδοση είναι ένας γρήγορα εξελισσόμενος τομέας της τεχνολογίας επικοινωνιών. Οι τεχνικές, που περιγράφονται σε αυτό την εργασία, προορίζονται να επεκτείνουν τα υπάρχοντα δίκτυα και να παρέχουν συνδεσιμότητα σε περιοχές όπου το πέρασμα οπτικής ίνας ή άλλου φυσικού καλωδίου δεν θα ήταν πρακτικό.

Η ασύρματη μετάδοση μπορεί να αξιοποιηθεί σε πολλές διαμορφώσεις, από μια απλή επέκταση (όπως ένα αρκετών χιλιομέτρων καλώδιο Ethernet) ως ένα σημείο διανομής (όπως ένα μεγάλο hub). Ακολουθούν μερικά παραδείγματα για το πώς το ενσύρματο δίκτυο μπορεί να ωφεληθεί από την ασύρματη τεχνολογία. Από αυτά μόνο το τελευταίο δεν υλοποιήθηκε στα πλαίσια αυτής της διπλωματικής.



Η τεχνολογία που χρησιμοποιείται για την οικοδόμηση των χαμηλού κόστους ασύρματων δικτύων είναι αυτήν την περίοδο η οικογένεια των πρωτοκόλλων 802.11, επίσης γνωστή ως Wi-Fi. Η οικογένεια των ραδιοπρωτοκόλλων (802.11a, 802.11b και 802.11g) έχει απολαύσει απίστευτη

δημοτικότητα σε όλο τον κόσμο. Με την εφαρμογή ενός κοινού συνόλου πρωτοκόλλων, οι κατασκευαστές παγκοσμίως έχουν χτίσει ιδιαίτερα διαλειτουργικό εξοπλισμό. Η απόφαση αυτή έχει αποδειχθεί σημαντικά ωφέλιμη στη βιομηχανία και τον καταναλωτή.

Ενώ τα νέα πρωτόκολλα όπως το 802.16 (επίσης γνωστό ως WiMax) θα λύσουν πιθανώς μερικά δύσκολα προβλήματα που παρατηρούνται αυτήν την περίοδο με το 802.11, έχουν πολύ δρόμο να κάνουν για να φτάσουν τα επίπεδα δημοτικότητας και τιμών του εξοπλισμού 802.11. Δεδομένου ότι εξοπλισμός που υποστηρίζει WiMax μόλις που γίνεται διαθέσιμος κατά την διάρκεια αυτού του γραψίματος, θα εστιάσω πρώτιστα στη οικογένεια 802.11.

Λέξεις κλειδιά: Wi-Fi, 802.11a, 802.11b ,802.11g, DVB-RCS, Σημείο Πρόσβασης, Ασύρματη Γέφυρα

Purpose of this Thesis - Abstract

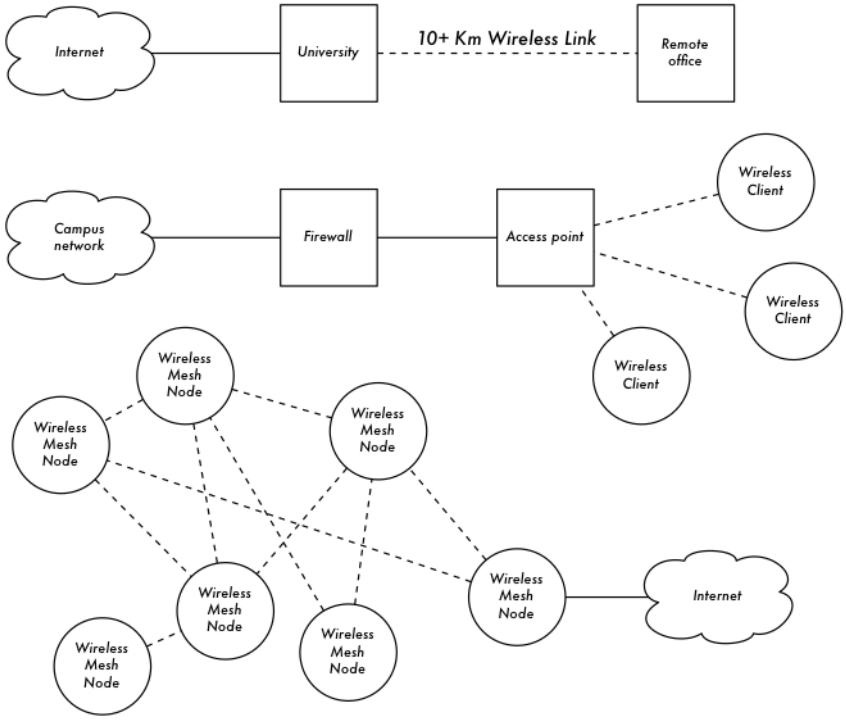
Wireless infrastructure can be built for very little cost compared to traditional wired alternatives. But building wireless networks is only partly about saving money. By providing people in a local community with cheaper and easier access to information, they can directly benefit from what the Internet has to offer.

But even without access to the Internet, wireless community networks have tremendous value. They allow people to collaborate on projects across wide distances. Voice communications, email, and other data can be exchanged for very little cost. Ultimately, they realize that communication networks are built to allow people to connect with each other.

In this Master thesis I will focus on wireless data networking technologies in the 802.11 family. While such a network can carry data, voice, and video (as well as traditional web and Internet traffic), the networks described in this book are data networks. The emphasis is on building infrastructure links intended to be used as the backbone for wide area wireless networks.

Since the first experiments at the turn of the last century, wireless has been a rapidly evolving area of communications technology. The techniques described in this thesis are intended to augment existing systems, and provide connectivity in areas where running fiber or other physical cable would be impractical.

Wireless can serve in many capacities, from a simple extension (like a several kilometer Ethernet cable) to a distribution point (like a large hub). Here are just a few examples of how your network can benefit from wireless technology. Only the last one of these was not deployed in this thesis.



The primary technology used for building low-cost wireless networks is currently the 802.11 family of protocols, also known in many circles as Wi-Fi. The 802.11 family of radio protocols (802.11a, 802.11b, and 802.11g) have enjoyed an incredible popularity in the United States and Europe. By implementing a common set of protocols, manufacturers world wide have built highly

interoperable equipment. This decision has proven to be a significant boon to the industry and the consumer.

While new protocols such as 802.16 (also known as WiMax) will likely solve some difficult problems currently observed with 802.11, they have a long way to go to match the popularity and price point of 802.11 equipment. As this equipment that supports WiMax is just becoming available at the time of this writing, we will focus primarily on the 802.11 family.

Keywords: Wi-Fi, 802.11a, 802.11b ,802.11g, DVB-RCS, Access Point, Wireless Bridge

Ευχαριστώ θερμά τον καθηγητή μου, κ. Ουζούνογλου Νικόλαο, για τη συνεχή υποστήριξη και καθοδήγηση, την ενθάρρυνση και, φυσικά, για όλα τα πολύτιμα γνωστικά εφόδια, που μου έχει προσφέρει.

Ευχαριστώ πολύ τον ερευνητή κ. Μιχαήλ Γεώργιο τόσο για το πραγματικό ενδιαφέρον του όσο και για την πολύωρη υποστήριξή του για την ολοκλήρωση του παρόντος Wi-Fi εγχειρήματος.

Ευχαριστώ την οικογένειά μου.

ΚΕΦΑΛΑΙΟ 1ο
Εισαγωγή

Τι κάνει τα ασύρματα δίκτυα διαφορετικά

Τα ασύρματα δίκτυα είναι ένα άριστο συμπλήρωμα στα σταθερά δίκτυα, αλλά δεν είναι μια τεχνολογία αντικατάστασης. Ακριβώς όπως τα κινητά τηλέφωνα συμπληρώνουν την τηλεφωνία σταθερών γραμμών, τα ασύρματα συμπληρώνουν τα υπάρχοντα σταθερά δίκτυα LANs με την παροχή κινητικότητας στους χρήστες. Οι υπολογιστές πρέπει να έχουν πρόσβαση στα δεδομένα, δηλαδή στους εξυπηρετητές, αλλά η φυσική θέση των πρώτων είναι αδιάφορη. Εφ' όσον δεν κινούνται οι κεντρικοί υπολογιστές, μπορούν επίσης να συνδεθούν με τα καλώδια που δεν κινούνται. Στο άλλο όμως άκρο, τα ασύρματα δίκτυα πρέπει να σχεδιαστούν για να καλύψουν μεγάλες περιοχές προκειμένου να φιλοξενήσουν γρήγορα κινούμενους πελάτες.

Έλλειψη Φυσικών Συνόρων

Η παραδοσιακή ασφάλεια των δικτύων δίνει μεγάλη έμφαση στη φυσική ασφάλεια των τμημάτων δικτύων. Τα δεδομένα ταξιδεύουν πάνω σε καλά καθορισμένα μονοπάτια, συνήθως χαλκού ή οπτικής ίνας, και η δικτυακή υποδομή προστατεύεται από τον ισχυρό φυσικό έλεγχο πρόσβασης. Ο εξοπλισμός είναι με ασφάλεια κλειδωμένος και εγκατεστημένος έτσι ώστε δεν μπορεί να επαναρυθμιστεί από τους χρήστες. Η βασική ασφάλεια προέρχεται από τη ασφάλεια του φυσικού στρώματος. Αν και είναι δυνατό να τρυπηθούν ή να επαναπροσανατολιστούν τα σήματα, ο

φυσικός έλεγχος πρόσβασης το κάνει πολύ δυσκολότερο για έναν εισβολέα να κερδίσει λαθραία πρόσβαση στο δίκτυο.

Τα ασύρματα δίκτυα έχουν ένα πολύ πιο ανοικτό μέσο. Εξ' ορισμού, το μέσο σε ένα ασύρματο δίκτυο δεν είναι ένα καθορισμένο με σαφήνεια μονοπάτι, που αποτελείται από ένα φυσικό καλώδιο, αλλά μια ραδιοζεύξη με μια ιδιαίτερη κωδικοποίηση και διαμόρφωση. Τα σήματα μπορούν να σταλούν ή να παραληφθούν από οποιονδήποτε που γνωρίζει ραδιοτεχνικές, οι οποίες φυσικά είναι ευρέως γνωστές επειδή αποτελούν ανοικτά πρότυπα. Η παρεμπόδιση δεδομένων μπορεί να είναι εύκολη, δεδομένου ότι το μέσο είναι ανοικτό σε οποιονδήποτε με τη σωστή δικτυακή διεπαφή.

Επιπλέον, τα ραδιοκύματα τείνουν να ταξιδέψουν έξω από την προοριζόμενη θέση τους. Δεν υπάρχει κανένα απότομο φυσικό όριο του μέσου και το εύρος μέχρι το οποίο οι μεταδόσεις μπορούν να παραληφθούν μπορεί να επεκταθεί με κεραίες υψηλός-κέρδους από κάθε πλευρά. Κατά την οικοδόμηση ενός ασύρματου δικτύου, πρέπει προσεκτικά να εξεταστεί πώς να προστατευτεί η σύνδεση προκειμένου να αποτραπεί η αναρμόδια χρήση, η έγχυση δικτυακού φόρτου και η ανάλυση της δικτυακής κυκλοφορίας. Με την ωρίμανση των ασύρματων πρωτοκόλλων, τα εργαλεία για την επικύρωση ασύρματων χρηστών και την κατάλληλη κρυπτογράφηση της κυκλοφορίας είναι τώρα προσιτά.

Δυναμικό Φυσικό Μέσο

Μόλις τεθεί ένα συνδεμένο με καλώδιο δίκτυο σε ισχύ, τείνει να είναι προβλέψιμο. Υπό τον όρο ότι το δίκτυο έχει σχεδιαστεί σύμφωνα με τους κανόνες εφαρμοσμένης μηχανικής που σχεδιάζονται στην προδιαγραφή, το δίκτυο πρέπει να λειτουργήσει όπως αναμένεται. Χωρητικότητα μπορεί να προστεθεί σε ένα συνδεμένο με καλώδιο δίκτυο εύκολα με την αναβάθμιση των switches.

Αντίθετα, το φυσικό μέσο στα ασύρματα LANs είναι δυναμικότερο. Τα ραδιοκυμάτα αναπηδούν γύρω από αντικείμενα, διαπερνούν τοίχους, και μπορεί συχνά να συμπεριφερθούν κάπως απρόβλεπτα. Τα ραδιοκύματα μπορούν να υποφέρουν από διάφορα προβλήματα διάδοσης, που μπορούν να διακόψουν τη ραδιοσύνδεση, όπως η πολλαπλών διαδρομών παρεμβολή και οι σκιές. Χωρίς ένα αξιόπιστο μέσο δικτύων, τα ασύρματα δίκτυα πρέπει προσεκτικά να επικυρώσουν τα λαμβανόμενα πλαίσια (frames) για να αποτρέψουν την απώλεια πλαισίων. Η θετική αναγνώριση (acknowledgment), η τακτική που χρησιμοποιείται από το 802.11, κάνει μια άριστη εργασία στη βεβαίωση της παράδοσης με κάποιο κόστος στη ρυθμαπόδοση.

Οι ραδιοζεύξεις υπόκεινται σε διάφορους πρόσθετους περιορισμούς σε αντίθεση με τα σταθερά δίκτυα. Επειδή το ραδιοφάσμα είναι ένας σχετικά λιγοστός πόρος, είναι προσεκτικά ρυθμισμένο. Δύο τρόποι υπάρχουν για να κάνουν τα ραδιοδίκτυα να πάνε γρηγορότερα. Είτε μπορεί να διατεθεί περισσότερο φάσμα, ή η κωδικοποίηση στη σύνδεση μπορεί να γίνει πιο ευαίσθητη έτσι ώστε να συσκευάζει περισσότερα δεδομένα ανά μονάδα του χρόνου. Οι πρόσθετες κατανομές φάσματος είναι σχετικά σπάνιες, ειδικά για τα άδεια-ελεύθερα δίκτυα. Τα 802.11 δίκτυα έχουν τηρήσει το εύρος ζώνης του ραδιοκαναλιού ενός σταθμού περίπου στα 30 MHz, αναπτύσσοντας παράλληλα την απέραντα βελτιωμένη κωδικοποίηση για να βελτιώσουν την ταχύτητα. Γρηγορότερες μέθοδοι κωδικοποίησης μπορούν να αυξήσουν την ταχύτητα, αλλά έχουν ένα πιθανό μειονέκτημα. Επειδή η γρηγορότερη μέθοδος κωδικοποίησης εξαρτάται από το δέκτη για να διαλέξει τις λεπτές διαφορές σημάτων, απαιτείται πολύ υψηλότερος σηματοθορυβικός λόγος. Οι υψηλότεροι ρυθμοί διέλευσης δεδομένων, επομένως, απαιτούν ο σταθμός να βρίσκεται πιο κοντά στο σημείο πρόσβασής του.

Το ραδιόφωνο είναι εγγενώς ένα μέσο ραδιοφωνικής μετάδοσης. Όταν ένας σταθμός διαβιβάζει, όλοι οι άλλοι σταθμοί πρέπει να ακούσουν. Τα σημεία πρόσβασης ενεργούν σαν τα παλαιά κοινά Ethernet hubs δεδομένου ότι υπάρχει ένα σταθερό ποσό ικανότητας μετάδοσης ανά σημείο πρόσβασης και πρέπει να μοιραστεί από όλους τους χρήστες. Η προσθήκη χωρητικότητας απαιτεί ο διαχειριστής δικτύου να προσθέσει σημεία πρόσβασης μειώνοντας ταυτόχρονα την περιοχή κάλυψης των υπαρχόντων σημείων πρόσβασης.

Ασφάλεια

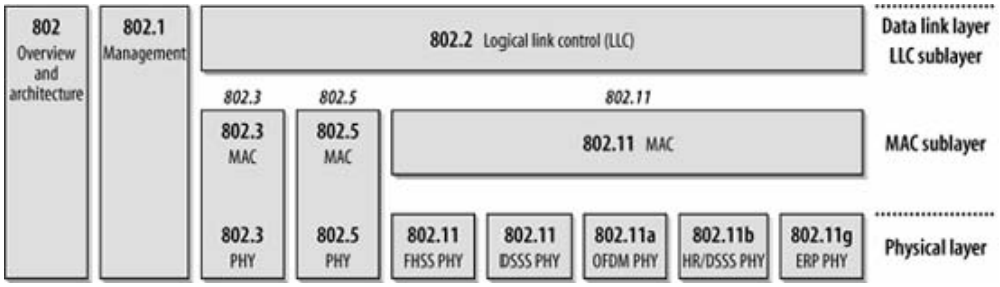
Πολλά ασύρματα δίκτυα είναι βασισμένα στα ραδιοκύματα, κάτι που καθιστά το μέσο των δικτύων αυτών εγγενώς ανοικτό στην παρεμβολή. Η κατάλληλη προστασία των ραδιομεταδόσεων σε οποιοδήποτε δίκτυο είναι πάντα μια ανησυχία για τους σχεδιαστές πρωτοκόλλων. Η αντιμετώπιση της έμφυτης αναξιοπιστίας του ασύρματου μέσου και της κινητικότητας απαίτησε διάφορα χαρακτηριστικά του πρωτοκόλλου για να επιβεβαιώσει την παράδοση πλαισίων, να εξασφαλίσει ισχύ και να προσφέρει κινητικότητα. Η ασφάλεια ήταν αρχικά αρκετά χαμηλά στον κατάλογο και αποδείχθηκε ανεπαρκής στις πρώτες προδιαγραφές.

Τα ασύρματα δίκτυα πρέπει να απαιτούν αυστηρή επικύρωση για να αποτρέψουν τη χρήση από αναρμόδιους χρήστες και οι επικυρωμένες συνδέσεις πρέπει να κρυπτογραφηθούν αυστηρά για να αποτρέψουν την παρεμβολή και την έγχυση κυκλοφορίας από αναρμόδια μέρη. Οι τεχνολογίες που προσφέρουν ισχυρή κρυπτογράφηση και επικύρωση έχουν αναπτυχθεί πολύ κατά στο πέρας του χρόνου.

Επισκόπηση των δικτύων 802.11

Οικογενειακό Δένδρο Τεχνολογίας Δικτύων IEEE 802

Το 802.11 είναι μέλος της οικογένειας IEEE 802, η οποία είναι μια σειρά προδιαγραφών για τις τεχνολογίες δικτύων τοπικής περιοχής (LAN). Το σχήμα 1-1 παρουσιάζει τη σχέση μεταξύ των διάφορων συστατικών της οικογένειας 802 και τη θέση τους στο πρότυπο της OSI.



Εικόνα 1-1 Η οικογένεια IEEE 802 και η σχέση της με το μοντέλο OSI

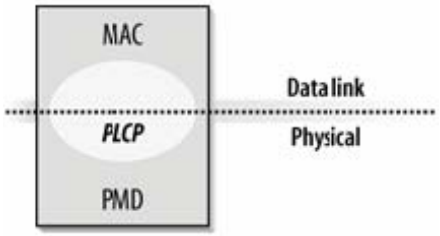
Οι προδιαγραφές IEEE 802 στρέφονται στα δύο χαμηλότερα στρώματα του προτύπου OSI επειδή ενσωματώνουν τα στοιχεία τόσο του φυσικού στρώματος όσο και του στρώματος ζεύξης. Όλα τα 802 δίκτυα έχουν και MAC και φυσικό (PHY) τμήμα . Η MAC είναι ένα σύνολο κανόνων για να καθοριστεί η πρόσβαση στο μέσο και η αποστολή δεδομένων, αλλά οι λεπτομέρειες της μετάδοσης και της λήψης αφήνονται στο PHY.

Μεμονωμένες προδιαγραφές στην 802 σειρά προσδιορίζονται από έναν δεύτερο αριθμό. Παραδείγματος χάριν, 802,3 είναι η προδιαγραφή για ένα δίκτυο Πολλαπλής Πρόσβασης Ανίχνευσης Φέροντος με ανίχνευση σύγκρουσης (CSMA/CD), που συσχετίζεται με το Ethernet, και 802,5 είναι η προδιαγραφή δικτύου δακτυλίου σκυτάλης. Άλλες προδιαγραφές περιγράφουν άλλα μέρη της στοίβας πρωτοκόλλων 802. Το 802.2 διευκρινίζει ένα κοινό στρώμα ζεύξης, τον λογικό έλεγχο συνδέσεων (LLC), ο οποίος μπορεί να χρησιμοποιηθεί από οποιαδήποτε τεχνολογία LAN χαμηλού στρώματος. Τα διαχειριστικά χαρακτηριστικά των 802 δικτύων διευκρινίζονται στο 802.1. Μεταξύ των 802.1, υπάρχουν πολλές παροχές για bridging (802.1D) και εικονικά LANs, ή VLANs (802.1Q).

Το 802.11 είναι απλώς ένα άλλο στρώμα συνδέσεων που μπορεί να χρησιμοποιήσει την ενθυλάκωση 802.2/LLC. Η προδιαγραφή του βασικού 802.11 περιλαμβάνει το 802.11 MAC και δύο φυσικά στρώματα: ένα φυσικό στρώμα απλωμένου φάσματος αναπήδησης συχνότητας (FHSS) και ένα στρώμα ζεύξης απλωμένο φάσμα άμεσης ακολουθίας (DSSS). Πιο πρόσφατες αναθεωρήσεις 802.11 προσέθεσαν επιπρόσθετα φυσικά στρώματα. Το 802.11b περιγράφει ένα στρώμα υψηλού ρυθμού άμεσης ακολουθίας (HR/DSSS)' προϊόντα βασισμένα σε 802.11b χτύπησαν την αγορά το 1999 και ήταν το πρώτο μαζικής αγοράς PHY. Το 802.11a περιγράφει ένα φυσικό στρώμα βασισμένο στην πολυπλεξία ορθογώνιας διαίρεσης συχνότητας (OFDM)' τα πρώτα προϊόντα βασισμένα σε 802.11a έγιναν διαθέσιμα το 2005. Το 802.11g είναι το νεότερο φυσικό στρώμα. Προσφέρει την υψηλότερη ταχύτητα μέσω της χρήσης OFDM αλλά με προς τα πίσω τη συμβατότητα με 802.11b. Η προς τα πίσω συμβατότητα δεν είναι χωρίς κόστος, εν τούτοις. Όταν οι χρήστες 802.11b και 802.11g συνυπάρχουν στο ίδιο σημείο πρόσβασης, απαιτείται πρόσθετος φόρτος για τις επικεφαλίδες πρωτοκόλλου, μειώνοντας τη μέγιστη ταχύτητα για τους χρήστες 802.11g.

Το 802.11 επιτρέπει την κινητή πρόσβαση στο δίκτυο' για την επίτευξη αυτού του στόχου, ενσωματώθηκαν διάφορα πρόσθετα χαρακτηριστικά στη MAC. Κατά συνέπεια, η 802.11 MAC μπορεί να φανεί αρκετά σύνθετη έναντι άλλων IEEE 802 προδιαγραφών της MAC.

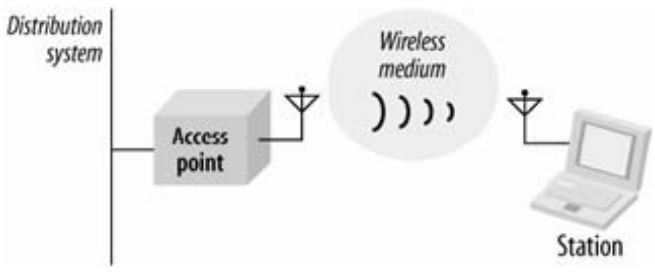
Η χρήση των ραδιοκυμάτων ως φυσικό στρώμα απαιτεί επίσης ένα σχετικά σύνθετο PHY. Το 802.11 χωρίζει το PHY σε δύο γενικά συστατικά: τη Φυσική Διαδικασία Σύγκλισης Στρώματος (Physical Layer Convergence Procedure - PLCP), για τη χαρτογράφηση των πλαισίων της MAC επάνω στο μέσο, και ένα Φυσικό Εξαρτώμενο από το Μέσο σύστημα (Physical Medium Dependent - PMD) για να διαβιβάσει εκείνα τα πλαίσια. Το PLCP καβαλικεύει το όριο της MAC και των φυσικών στρωμάτων, όπως φαίνεται στο σχήμα 1-2. Στο 802.11 το PLCP προσθέτει έναν αριθμό από πεδία στο πλαίσιο καθώς αυτό διαβιβάζεται "στον αέρα."



Εικόνα 1-2 Συστατικά του PHY

802.11 Ονοματολογία

Τα 802.11 δίκτυα αποτελούνται από τέσσερα σημαντικά φυσικά συστατικά, τα οποία συνοψίζονται στο σχήμα 1-3.



Εικόνα 1-3 Συστατικά των 802.11 LANs

Τα συστατικά είναι:

- **Σταθμοί**
  Τα δίκτυα χτίζονται για να μεταφέρουν δεδομένα μεταξύ των σταθμών. Οι σταθμοί υπολογίζουν τις συσκευές με ασύρματες διεπαφές δικτύου. Συνήθως οι σταθμοί είναι φορητοί υπολογιστές ή υπολογιστές χειρός, που λειτουργούν με μπαταρία. Εν τούτοις, δεν υπάρχει κανένας λόγος οι σταθμοί να πρέπει να είναι φορητές συσκευές. Σε μερικά περιβάλλοντα, η ασύρματη δικτύωση χρησιμοποιείται για να αποφευχθεί η τοποθέτηση νέων καλωδίων και οι υπολογιστές γραφείου συνδέονται με ασύρματα LANs. Μεγάλες ανοικτές περιοχές μπορούν επίσης να επωφεληθούν από την ασύρματη δικτύωση. Το 802.11 γίνεται γρήγορα de facto πρότυπο για τη διασύνδεση ηλεκτρονικών ειδών ευρείας κατανάλωσης. Διάφορες εταιρίες ηλεκτρονικών ειδών ευρείας κατανάλωσης έχουν προσχωρήσει στη ομάδα εργασίας 802.11, προφανώς με την πρόθεση να παρέχουν τη δυνατότητα γρήγορης μεταφοράς δεδομένων πάνω σε 802.11.

- **Σημεία Πρόσβασης**
  Τα πλαίσια σε ένα 802.11 δίκτυο πρέπει να μετατραπούν σε έναν άλλο τύπο πλαισίου για παράδοση στον υπόλοιπο κόσμο. Οι συσκευές αποκαλούμενες σημεία πρόσβασης εκτελούν τη λειτουργία γεφύρωσης ασύρματο-σε-ενσύρματο. Τα σημεία πρόσβασης φυσικά εκτελούν και διάφορες άλλες λειτουργίες, αλλά το γεφύρωμα είναι κατά πολύ το σημαντικότερο. Αρχικά, λειτουργίες σημείου πρόσβασης τέθηκαν σε αυτόνομες συσκευές, αν και διάφορα νεότερα προϊόντα διαιρούν το 802.11 πρωτόκολλο μεταξύ των "λεπτών" σημείων πρόσβασης και των ελεγκτών AP.

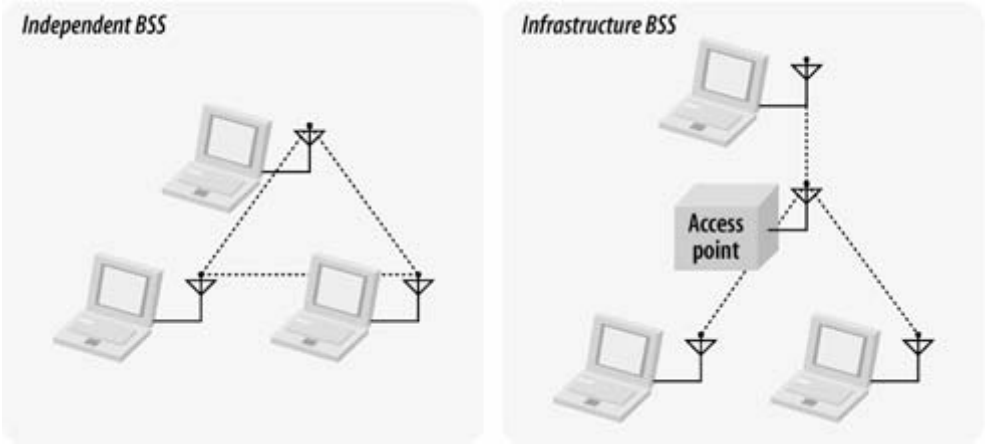
- **Ασύρματο Μέσο**
  Για την κίνηση των πλαισίων από το ένα σταθμό στον άλλο, τα πρότυπα χρησιμοποιούν ένα ασύρματο μέσο. Έχουν καθοριστεί διάφορα διαφορετικά φυσικά στρώματα' η αρχιτεκτονική επιτρέπει την ανάπτυξη πολλαπλών φυσικών στρωμάτων, που μπορούν να υποστηρίξουν το 802.11 MAC. Αρχικά, προτυποποιήθηκαν δύο φυσικά στρώματα ραδιοσυχνότητας (RF) και ένα υπέρυθρο φυσικό στρώμα, αν και τα στρώματα RF έχουν αποδειχθεί πολύ δημοφιλέστερα. Διάφορα πρόσθετα στρώματα RF έχουν επίσης προτυποποιηθεί.

- **Σύστημα Διανομής**
  Όταν πολλά σημεία πρόσβασης συνδέονται για να διαμορφώσουν μια μεγάλη περιοχή κάλυψης, πρέπει να επικοινωνήσουν το ένα με το άλλο για να παρακολουθήσουν τις μετακινήσεις των κινητών σταθμών. Το σύστημα διανομής είναι το λογικό συστατικό του 802.11 που χρησιμοποιείται για να διαβιβάσει τα πλαίσια στον προορισμό τους. Το 802.11 δεν διευκρινίζει καμία ιδιαίτερη τεχνολογία για το σύστημα διανομής. Στα περισσότερα εμπορικά προϊόντα το σύστημα διανομής εφαρμόζεται ως συνδυασμός μιας μηχανής γεφυρώματος (bridging) και ενός μέσου συστήματος διανομής, το οποίο είναι το δίκτυο κορμός που χρησιμοποιείται για να αναμεταδώσει τα πλαίσια μεταξύ των σημείων πρόσβασης' καλείται συχνά απλά δίκτυο κορμός (backbone network). Σχεδόν σε όλα τα εμπορικά επιτυχημένα προϊόντα, το Ethernet χρησιμοποιείται ως τεχνολογία δικτύων κορμού.

Τύποι Δικτύων

Η βασική δομική μονάδα ενός 802.11 δικτύου είναι το βασικό σύνολο υπηρεσιών (Basic Service Set - BSS), το οποίο είναι απλά μια ομάδα σταθμών που επικοινωνούν ο ένας με τον άλλον. Οι επικοινωνίες πραγματοποιούνται μέσα σε μια κάπως συγκεχυμένη περιοχή, αποκαλούμενη βασική περιοχή υπηρεσιών (basic service area), που καθορίζεται από τα χαρακτηριστικά διάδοσης

του ασύρματου μέσου. Όταν ένας σταθμός είναι στη βασική περιοχή υπηρεσιών, μπορεί να επικοινωνήσει με τα άλλα μέλη του BSS. Τα BSSs έρχεται σε δύο τύπους, που απεικονίζονται στο σχήμα 1-4.



Εικόνα 1-4 Ανεξάρτητα BSSs και BSSs υποδομής

Ανεξάρτητα Δίκτυα

Στα αριστερά είναι ένα ανεξάρτητο BSS (independent BSS - IBSS). Οι σταθμοί σε ένα IBSS επικοινωνούν άμεσα ο ένας με τον άλλον και πρέπει έτσι να είναι μέσα σε απόσταση άμεσης επικοινωνίας. Το μικρότερο πιθανό 802.11 δίκτυο είναι ένα IBSS με δύο σταθμούς. Συνήθως IBSSs αποτελούνται από έναν μικρό αριθμό σταθμών που εγκαθίστανται για έναν συγκεκριμένο σκοπό και για μια μικρή χρονική περίοδο. Μια συνηθισμένη χρήση είναι η δημιουργία ενός βραχύβιου δικτύου για να υποστηρίξει μια συνεδρίαση σε ένα δωμάτιο διασκέψεων. Όταν η συνεδρίαση αρχίζει, οι συμμετέχοντες δημιουργούν ένα IBSS για να μοιραστούν δεδομένα. Όταν η συνεδρίαση τελειώνει, το IBSS διαλύεται. Λόγω της σύντομης διάρκειας, του μικρού μεγέθους και του σκοπού τους, τα IBSSs αναφέρονται μερικές φορές ως ad hoc BSSs ή ad hoc δίκτυα.

Δίκτυα υποδομής

Στα δεξιά της εικόνας 2-4 είναι μια υποδομή BSS. Τα δίκτυα υποδομής διακρίνονται με την χρήση ενός σημείου πρόσβασης. Τα σημεία πρόσβασης χρησιμοποιούνται για όλες τις επικοινωνίες στα δίκτυα υποδομής, συμπεριλαμβανομένης της επικοινωνίας μεταξύ των κινητών κόμβων στην ίδια περιοχή υπηρεσιών. Εάν ένας κινητός σταθμός σε μια υποδομή BSS πρέπει να επικοινωνήσει με έναν δεύτερο κινητό σταθμό, η επικοινωνία πρέπει να πάρει δύο hops. Κατ' αρχάς, ο κινητός σταθμός πηγή μεταφέρει το πλαίσιο στο σημείο πρόσβασης. Δεύτερον, το σημείο πρόσβασης μεταφέρει το πλαίσιο στο σταθμό προορισμού. Με όλες τις επικοινωνίες που αναμεταδίδονται μέσω ενός σημείου πρόσβασης, η βασική περιοχή υπηρεσιών που αντιστοιχεί σε μια υποδομή BSS καθορίζεται από τα σημεία στα οποία οι μεταδόσεις από το σημείο πρόσβασης μπορούν να παραληφθούν. Αν και η μετάδοση multihop καταναλώνει μεγαλύτερη χωρητικότητα μετάδοσης απ' ό,τι ένα απ' ευθείας πλαίσιο από τον αποστολέα στο δέκτη, έχει δύο σημαντικά πλεονεκτήματα:

- Μια υποδομή BSS καθορίζεται από την απόσταση από το σημείο πρόσβασης. Όλοι οι κινητοί σταθμοί πρέπει να είναι τοποθετημένοι εντός εύρους κάλυψης του σημείου πρόσβασης, αλλά κανένας περιορισμός δεν τίθεται στην απόσταση μεταξύ των κινητών σταθμών. Η άμεση επικοινωνία μεταξύ των κινητών σταθμών θα εξοικονομούσε χωρητικότητα μετάδοσης αλλά με κόστος την αυξημένη πολυπλοκότητα του φυσικού στρώματος επειδή οι κινητοί σταθμοί θα πρέπει να διατηρήσουν γειτονικές σχέσεις με όλους τους άλλους κινητούς σταθμούς μέσα στην περιοχή υπηρεσιών.

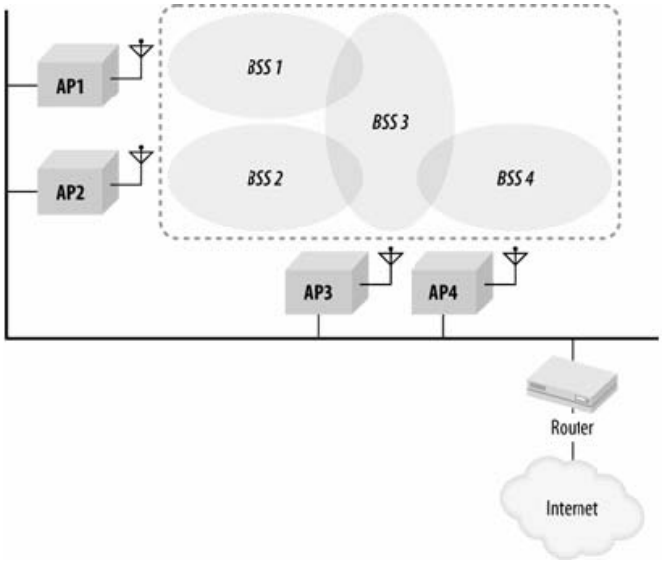
- Τα σημεία πρόσβασης στα δίκτυα υποδομής είναι σε θέση να βοηθήσουν τους σταθμούς που προσπαθούν να εξοικονομήσουν ισχύ (μπαταρίας). Τα σημεία πρόσβασης μπορούν να σημειώσουν πότε ένας σταθμός μπαίνει σε λειτουργία εξοικονόμησης ισχύος και αποθηκεύει πλαίσια για το λόγο αυτό. Οι με λειτουργία μπαταρίας σταθμοί μπορούν να κλείσουν τον ασύρματο πομποδέκτη και να τον ανοίξουν μόνο για να διαβιβάσουν και να ανακτήσουν τα αποθηκευμένα (buffered) πλαίσια από το σημείο πρόσβασης.

Σε ένα δίκτυο υποδομής, οι σταθμοί πρέπει να συνδεθούν με ένα σημείο πρόσβασης για να λάβουν υπηρεσίες δικτύων. Η σύνδεση (association) είναι η διαδικασία με την οποία ένας κινητός σταθμός εισάγεται σε ένα 802.11 δίκτυο' είναι λογικά ισοδύναμο με τη σύνδεση καλωδίου σε ένα Ethernet. Δεν είναι μια συμμετρική διαδικασία. Οι κινητοί σταθμοί κινούν πάντα τη διαδικασία σύνδεσης και τα σημεία πρόσβασης μπορούν να επιλέξουν να χορηγήσουν ή να αρνηθούν την πρόσβαση βασισμένη στο περιεχόμενο ενός αιτήματος σύνδεσης. Οι συνδέσεις είναι επίσης αποκλειστικές εκ μέρους του κινητού σταθμού: ένας κινητός σταθμός μπορεί να συνδεθεί με μόνο ένα σημείο πρόσβασης. πρότυπο 802.11 δεν θέτει κανένα όριο στον αριθμό κινητών σταθμών που ένα σημείο πρόσβασης μπορεί να εξυπηρετήσει. Στην πράξη, εντούτοις, η σχετικά χαμηλή ρυθμαπόδοση των ασύρματων δικτύων είναι πολύ πιθανό να περιορίσει τον αριθμό σταθμών που εισάγονται σε ένα ασύρματο δίκτυο.

Εκτεταμένες περιοχές υπηρεσιών

Τα BSSs μπορούν να δημιουργήσουν κάλυψη σε μικρά γραφεία και σπίτια, αλλά δεν μπορούν να παρέχουν κάλυψη δικτύου σε μεγαλύτερες περιοχές. Το 802.11 επιτρέπει ασύρματα δίκτυα ενός αυθαίρετα μεγάλου μεγέθους να δημιουργηθούν με τη σύνδεση BSSs σε ένα εκτεταμένο σύνολο υπηρεσιών (Extended Service Set - ESS). Ένα ESS δημιουργείται συνδέοντας BSSs μαζί με ένα δίκτυο κορμού. Σε όλα τα σημεία πρόσβασης σε ένα ESS δίνεται το ίδιο καθορισμένο προσδιοριστικό υπηρεσιών (Service Set Identifier - SSID), το οποίο χρησιμεύει ως ένα δίκτυο "όνομα" για τους χρήστες.

Το 802.11 δεν διευκρινίζει μια ιδιαίτερη τεχνολογία κορμού' απαιτεί μόνο ο κορμός να παρέχει ένα σαφές σύνολο υπηρεσιών. Στο σχήμα 2-5 το ESS είναι η ένωση των τεσσάρων BSSs (υπό τον όρο ότι όλα τα σημεία πρόσβασης διαμορφώνονται για να είναι μέρος του ίδιου ESS). Στις πραγματικές επεκτάσεις ο βαθμός επικάλυψης μεταξύ των BSSs θα ήταν πιθανώς πολύ μεγαλύτερος από την επικάλυψη στο σχήμα 1-5.



Εικόνα 1-5 Εκτεταμένη περιοχή υπηρεσιών

Σταθμοί μέσα στο ίδιο ESS μπορούν να επικοινωνήσουν ο ένας με τον άλλον, ακόμα κι αν αυτοί οι σταθμοί είναι σε διαφορετικές βασικές περιοχές υπηρεσιών ή ακόμη μετακινούνται μεταξύ βασικών περιοχών υπηρεσιών. Για να επικοινωνήσει ο ένας σταθμός με τον άλλο σε ένα ESS, το ασύρματο μέσο πρέπει να ενεργήσει όπως μια σύνδεση ενός ενιαίου στρώματος 2. Τα σημεία πρόσβασης ενεργούν ως γέφυρες (bridges), ώστε η άμεση επικοινωνία μεταξύ των σταθμών σε ένα ESS να απαιτεί ότι το δίκτυο κορμού μοιάζει επίσης με μια σύνδεση στρώματος 2. Τα πρώτης γενιάς σημεία πρόσβασης απαιτούσαν άμεσες συνδέσεις στρώματος 2 μέσω hubs ή εικονικών LANs' τα νεότερα προϊόντα εφαρμόζουν μια ποικιλία τεχνολογιών σήραγγας (tunneling) για να προσομοιώσουν το περιβάλλον του στρώματος 2 .

Το 802.11 προσφέρει κινητικότητα στο στρώμα ζεύξης μέσα σε ένα ESS, αλλά μόνο εάν το δίκτυο κορμού εμφανίζεται να είναι μια ενιαία περιοχή στρώματος ζεύξης. Αυτός ο σημαντικός περιορισμός στην κινητικότητα είναι συχνά ένας σημαντικός παράγοντας για τον τρόπο που τα ασύρματα LANs επεκτείνονται, και ένας από τους σημαντικότερους τρόπους που οι προμηθευτές διαφοροποιούν τα προϊόντα τους.

Τα πρώτα σημεία πρόσβασης απαιτούσαν το δίκτυο κορμού να είναι ένα ενιαίο hub ή VLAN, αλλά τα νεότερα προϊόντα μπορούν να διασυνδεθούν άμεσα με το κορμό. Πολλά μπορούν να υποστηρίξουν πολλαπλά VLANs ταυτόχρονα με τις ετικέτες 802.1Q και μερικά μπορούν ακόμη και δυναμικά να δημιουργήσουν VLANs.

Οι εκτεταμένες περιοχές υπηρεσιών είναι η υψηλότερου επιπέδου αφαίρεση που υποστηρίζεται από τα δίκτυα 802.11. α σημεία πρόσβασης σε ένα ESS λειτουργούν σε συμφωνία για να επιτρέψουν στον εξωτερικό κόσμο να χρησιμοποιήσει τη διεύθυνση MAC του σταθμού για να μιλήσει σε έναν σταθμό ανεξάρτητα της θέσης αυτού μέσα στο ESS. Στο σχήμα 2-5, ο δρομολογητής χρησιμοποιεί τη διεύθυνση MAC του σταθμού ως προορισμό για να παραδώσει τα πλαίσια σε έναν κινητό σταθμό' μόνο το σημείο πρόσβασης με το οποίο εκείνος ο κινητός σταθμός έχει συνδεθεί παραδίδει το πλαίσιο. Ο δρομολογητής παραμένει ανίδεος της θέσης του κινητού σταθμού και βασίζεται στα σημεία πρόσβασης για να παραδώσει το πλαίσιο.

Πολλαπλού BSS περιβάλλοντα: "εικονικά APs"

Τα πρώτα 802.11 ραδιοτσιπ είχαν τη δυνατότητα να δημιουργήσουν ένα ενιαίο βασικό σύνολο υπηρεσιών. Ένα AP μπορούσε να συνδέσει χρήστες σε μόνο ένα "ασύρματο δίκτυο" και όλοι οι χρήστες σε εκείνο το δίκτυο είχαν παρόμοια, εάν όχι ολόιδια, προνόμια. Στις πρώτες υλοποιήσεις με περιορισμένο αριθμό χρηστών, ένα ενιαίο λογικό δίκτυο ήταν ικανοποιητικό. Δεδομένου ότι η ασύρματη δικτύωση αυξήθηκε σε δημοτικότητα, ένα δίκτυο δεν αρκεί πλέον.

Για παράδειγμα, οι περισσότερες οργανώσεις δέχονται κανονικούς επισκέπτες, πολλοί από τους οποίους έχουν 802.11 εξοπλισμό και χρειάζονται πρόσβαση στο Διαδίκτυο. Οι φιλοξενούμενοι δεν είναι έμπιστοι χρήστες. Ένας κοινός τρόπος για την αντιμετώπιση της πρόσβασης φιλοξενούμενων είναι να δημιουργηθούν δύο εκτεταμένα σύνολα υπηρεσιών στην ίδια φυσική υποδομή. Τα τρέχοντα 802.11 chipsets μπορούν να δημιουργήσουν πολλαπλά δίκτυα με το ίδιο ράδιο. Χρησιμοποιώντας τα σύγχρονα chipsets, κάθε συσκευή υλικού σημείου πρόσβασης μπορεί να δημιουργήσει δύο BSSs, ένα για το δίκτυο που ονομάζεται φιλοξενούμενων και ένα για το δίκτυο που ονομάζεται εσωτερικό. Εντός του AP κάθε SSID συσχετίζεται με ένα VLAN. Το δίκτυο φιλοξενούμενων συνδέεται με ένα VLAN δημιουργημένο για τη δημόσια πρόσβαση από άγνωστους και μη έμπιστους χρήστες και είναι σχεδόν πάντα τοποθετημένο έξω από το τείχος προστασίας (firewall).

Οι ασύρματες συσκευές βλέπουν δύο χωριστά δίκτυα στη ραδιοπεριοχή και μπορούν να συνδεθούν με οποιοδήποτε ανταποκρίνεται στις ανάγκες τους. Φυσικά, το εσωτερικό δίκτυο προστατεύεται από επικύρωση, που αποτρέπει αναρμόδια χρήση. Οι χρήστες που συνδέονται με το ασύρματο δίκτυο που ονομάζεται φιλοξενούμενων θα τοποθετηθούν στο VLAN φιλοξενούμενων, ενώ οι χρήστες που συνδέονται με το ασύρματο δίκτυο που ονομάζεται εσωτερικό θα επικυρωθούν και θα τοποθετηθούν στο εσωτερικό δίκτυο.

Ισχυρά δίκτυα ασφάλειας (RSNs)

Τα πρώτα ασύρματα LANs αποδείχθηκε ότι είχαν αδύναμη ενσωματωμένη ασφάλεια. Το 802.11i, που επικυρώθηκε τον Ιούνιο του 2004, περιγράφει ένα σύνολο βελτιωμένων μηχανισμών ασφάλειας που παρέχουν τις ισχυρές συνδέσεις δικτύων ασφάλειας. Η υποστήριξη του 802.11i μπορεί να συντίθεται από το υλισμικό, το λογισμικό ή τα δύο, ανάλογα με την αρχιτεκτονική μιας συγκεκριμένης συσκευής. Το υλικό που δεν υποστηρίζει τα βελτιωμένα πρωτόκολλα αναφέρεται ως προ-RSN ικανό.

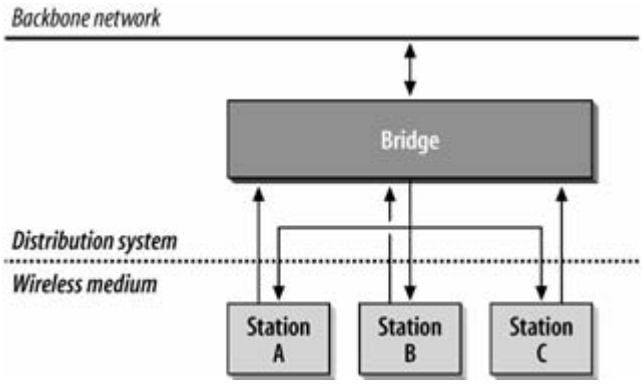
Το σύστημα διανομής

Το 802.11 περιγράφει το σύστημα διανομής από την άποψη των υπηρεσιών που παρέχει στους ασύρματους σταθμούς. Το σύστημα διανομής παρέχει κινητικότητα με τη σύνδεση σημείων πρόσβασης. Όταν ένα πλαίσιο δίνεται στο σύστημα διανομής, αυτό παραδίδεται στο σωστό σημείο πρόσβασης και αναμεταδίδεται από εκείνο το σημείο πρόσβασης στον προοριζόμενο προορισμό.

Το σύστημα διανομής είναι αρμόδιο για την εύρεση του που ένας σταθμός βρίσκεται φυσικά και τη σωστή παράδοση των πλαισίων. Όταν ένα πλαίσιο στέλνεται σε έναν κινητό σταθμό, το σύστημα διανομής αναλαμβάνει να παραδώσει το πλαίσιο αυτό στο σημείο πρόσβασης που εξυπηρετεί τον κινητό σταθμό. Για παράδειγμα, εξετάστε το δρομολογητή στο σχήμα 2-5. Ο δρομολογητής χρησιμοποιεί απλά τη διεύθυνση MAC ενός κινητού σταθμού ως προορισμό του. Το σύστημα διανομής του ESS που απεικονίζεται στο σχήμα 2-5 πρέπει να παραδώσει το πλαίσιο στο σωστό σημείο πρόσβασης. Προφανώς, μέρος του μηχανισμού παράδοσης είναι ο κορμός Ethernet, αλλά ο κορμός δεν μπορεί να είναι ολόκληρο το σύστημα διανομής επειδή δεν έχει κανέναν τρόπο να επιλέξει μεταξύ σημείων πρόσβασης. Στη γλώσσα 802.11, ο κορμός Ethernet είναι το μέσο του συστήματος διανομής, αλλά δεν είναι ολόκληρο το σύστημα διανομής.

Για να ευρεθεί το υπόλοιπο του συστήματος διανομής, πρέπει να κοιτάξουμε στα σημεία πρόσβασης. Τα περισσότερα σημεία πρόσβασης αυτήν την περίοδο στην αγορά λειτουργούν ως γέφυρες. Έχουν τουλάχιστον μια ασύρματη διεπαφή και τουλάχιστον μια διεπαφή Ethernet. Η πλευρά Ethernet μπορεί να συνδεθεί με ένα υπάρχον δίκτυο και η ασύρματη πλευρά γίνεται μια επέκταση εκείνου του δικτύου. Η αναμετάδοση των πλαισίων μεταξύ των δύο μέσων δικτύων ελέγχεται από μια μηχανή γεφυρώματος.

Το σχήμα 1-6 επεξηγεί τη σχέση μεταξύ του σημείου πρόσβασης, του δικτύου κορμού και του συστήματος διανομής. Το σημείο πρόσβασης συνδέει δύο διεπαφές με μια μηχανή γεφυρώματος (bridging engine). Τα βέλη δείχνουν τις πιθανές πορείες προς και από τη μηχανή γεφυρώματος. Τα πλαίσια μπορούν να σταλούν από τη γέφυρα στο ασύρματο δίκτυο' οποιαδήποτε πλαίσια που στέλνονται από την ασύρματη θύρα της γέφυρας διαβιβάζονται σε όλους τους συνδεδεμένους σταθμούς. Κάθε συνδεδεμένος σταθμός μπορεί να διαβιβάσει πλαίσια στο σημείο πρόσβασης. Τέλος, ο θύρα κορμού στη γέφυρα μπορεί να αλληλεπιδράσει άμεσα με το δίκτυο κορμού. Το σύστημα διανομής στο σχήμα 2-6 αποτελείται από τη μηχανή γεφυρώματος συν το ενσύρματο δίκτυο κορμού.



Εικόνα 1-6 Σύστημα διανομής σε κοινές υλοποιήσεις σημείων πρόσβασης 802.11

Κάθε πλαίσιο που στέλνεται από έναν κινητό σταθμό σε ένα δίκτυο υποδομής πρέπει να χρησιμοποιήσει το σύστημα διανομής. Είναι εύκολο να γίνει κατανοητό γιατί η αλληλεπίδραση με τους οικοδεσπότες στο δίκτυο κορμού πρέπει να χρησιμοποιήσει το σύστημα διανομής.Οι ασύρματοι σταθμοί σε ένα δίκτυο υποδομής εξαρτώνται από το σύστημα διανομής για να επικοινωνήσουν ο ένας με τον άλλον επειδή δεν συνδέονται άμεσα ο ένας με τον άλλον. Ο μόνος τρόπος για το σταθμό Α για να στείλει ένα πλαίσιο στο σταθμό Β είναι με την αναμετάδοση του πλαισίου μέσω της μηχανής γεφυρώματος στο σημείο πρόσβασης. Εντούτοις, η γέφυρα είναι ένα συστατικό του συστήματος διανομής.

Επικοινωνία μεταξύ σημείων πρόσβασης ως τμήμα του συστήματος διανομής

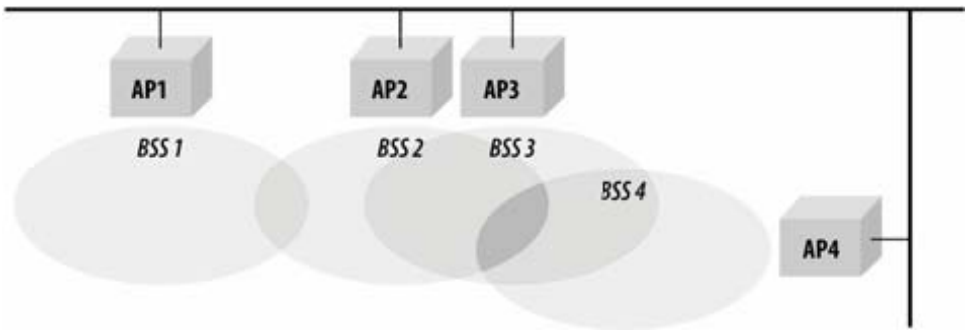
Συμπεριλαμβανόμενη σε αυτό το σύστημα διανομής είναι μια μέθοδος για τη διαχείριση των συνδέσεων. Ένας ασύρματος σταθμός συνδέεται με μόνο ένα σημείο πρόσβασης τη φορά. Εάν ένας σταθμός έχει συνδεθεί με ένα σημείο πρόσβασης, όλα τα άλλα σημεία πρόσβασης στο ESS πρέπει να μάθουν για εκείνο τον σταθμό. Στο σχήμα 2-5, το AP4 πρέπει να ξέρει για όλους τους σταθμούς που συνδέονται με το AP1. Εάν ένας ασύρματος σταθμός που συνδέεται με το AP4 στέλνει ένα πλαίσιο σε έναν σταθμό που έχει συνδεθεί με το AP1, τότε η μηχανή γεφυρώματος μέσα στο AP4 πρέπει να στείλει το πλαίσιο πάνω στον κορμό Ethernet στο AP1 έτσι ώστε αυτό να μπορεί να παραδοθεί στον προορισμό του. Για την πλήρη εφαρμογή του συστήματος διανομής, τα σημεία πρόσβασης πρέπει να ενημερώσουν τα άλλα σημεία πρόσβασης για τους συνδεδεμένους σταθμούς. Φυσικά, πολλά σημεία πρόσβασης στην αγορά χρησιμοποιούν δια-σημείων πρόσβασης πρωτόκολλο (Interaccess Point Protocol - IAPP). Πολλοί προμηθευτές ανέπτυξαν ιδιόκτητα πρωτόκολλα μεταξύ των σημείων πρόσβασης για να μεταφέρουν δεδομένα σύνδεσης. Ένα τυποποιημένο IAPP παρήχθη ως 802.11F, αλλά δεν είναι γνωστή η χρήση του σε κάποιο προϊόν.

Ασύρματες γέφυρες (bridges) και το σύστημα διανομής

Ενώ συχνά συμβαίνει το μέσο συστημάτων διανομής να είναι ένα υπάρχον σταθερό δίκτυο, η 802.11 προδιαγραφή υποστηρίζει ρητά τη χρησιμοποίηση του ίδιου του ασύρματου μέσου ως σύστημα διανομής. Η διαμόρφωση ασύρματου συστήματος διανομής (Wireless Distribution System - WDS) καλείται συχνά διαμόρφωση "ασύρματων γεφυρών" επειδή επιτρέπει στους μηχανικούς δικτύων να συνδέσουν δύο LANs στο στρώμα ζεύξης. Οι ασύρματες γέφυρες μπορούν να χρησιμοποιηθούν για να συνδέσουν γρήγορα απομακρυσμένες φυσικές θέσεις και είναι κατάλληλες προς χρήση από προμηθευτές πρόσβασης. α περισσότερα 802.11 σημεία πρόσβασης στην αγορά υποστηρίζουν τώρα την διαμόρφωση ασύρματων γεφυρών.

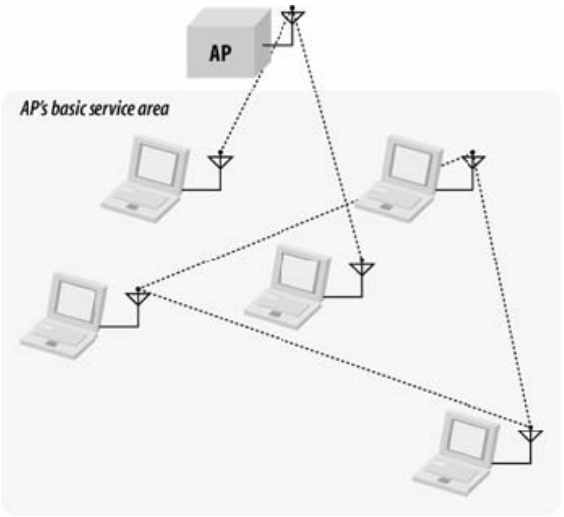
Όρια δικτύων

Λόγω της φύσης του ασύρματου μέσου, τα δίκτυα 802.11 έχουν συγκεχυμένα όρια. Στην πραγματικότητα, κάποιος βαθμός ασάφειας είναι επιθυμητός. Όπως με τα δίκτυα κινητών τηλεφώνων, αυξάνεται η πιθανότητα επιτυχών μεταβάσεων μεταξύ των βασικών περιοχών υπηρεσιών και προσφέρεται το πιο υψηλό επίπεδο κάλυψης δικτύων όταν επιτρέπεται στις βασικές περιοχές υπηρεσιών να επικαλύπτονται. Οι βασικές περιοχές υπηρεσιών στα αριστερά του σχήματος 1-7 επικαλύπτονται σημαντικά. Αυτό σημαίνει ότι ένας σταθμός που κινείται από το BSS2 προς το BSS4 είναι πιθανό να μη χάσει την κάλυψη' επίσης αυτό σημαίνει ότι το AP3 μπορεί να αποτύχει. Αφ' ετέρου, εάν το AP2 "πέσει", το δίκτυο κόβεται σε δύο χωριστά μέρη και οι σταθμοί στο BSS1 χάνουν τη συνδεσιμότητα κατά την κίνηση από το BSS1 προς το BSS3 ή BSS4. Η αντιμετώπιση των "τρυπών κάλυψης" από παύση λειτουργίας σημείου πρόσβασης είναι μια εργασία που απαιτεί προσοχή κατά τη διάρκεια της φάσης σχεδιασμού του δικτύου' πολλά νεότερα προϊόντα προσφέρουν ικανότητες δυναμικού ραδιοσυντονισμού προκειμένου να συμπληρώσουν αυτόματα τρύπες που δημιουργούνται κατά τη διάρκεια της λειτουργίας του δικτύου.



Εικόνα 1-7 Επικαλυπτόμενα BSSs σε μία ESS

Διαφορετικοί τύποι δικτύων 802.11 μπορούν επίσης να επικαλυφθούν. Ανεξάρτητα BSSs μπορούν να δημιουργηθούν μέσα στο βασικό τομέα υπηρεσιών ενός σημείου πρόσβασης. Το σχήμα 1-8 απεικονίζει τη χωρική επικάλυψη. Ένα σημείο πρόσβασης εμφανίζεται στην κορυφή του σχήματος' η βασική του περιοχή υπηρεσιών είναι σκιασμένη. Δύο σταθμοί βρίσκονται σε λειτουργία υποδομής και επικοινωνούν μόνο με το σημείο πρόσβασης. Τρεις σταθμοί έχουν ιδρυθεί ως ανεξάρτητο BSS και επικοινωνούν ο ένας με τον άλλον. Αν και οι πέντε σταθμοί ορίζονται σε δύο διαφορετικά BSSs, μπορούν να μοιραστούν το ίδιο ασύρματο μέσο. Οι σταθμοί μπορούν να λάβουν πρόσβαση στο μέσο μόνο με τη χρησιμοποίηση των κανόνων που διευκρινίζονται στη 802.11 MAC' αυτοί οι κανόνες είχαν σχεδιαστεί προσεκτικά να επιτρέψουν σε πολλαπλά 802.11 δίκτυα να συνυπάρξουν στην ίδια χωρική περιοχή. Και τα δύο BSSs πρέπει να μοιραστούν την χωρητικότητα ενός ενιαίου ραδιοκαναλιού, έτσι μπορεί να υπάρξουν δυσμενείς επιπτώσεις απόδοσης από BSSs, που βρίσκονται στον ίδιο χώρο.



Εικόνα 1-8 Επικαλυπτόμενοι τύποι δικτύων

Λειτουργίες Δικτύου 802.11

Εξ' αρχής το 802.11 είχε σχεδιαστεί να είναι απλώς άλλο ένα στρώμα ζεύξης σε πρωτόκολλα υψηλότερου επιπέδου. Οι διαχειριστές δικτύων, που είναι εξοικειωμένοι με το

Ethernet, θα είναι αμέσως άνετοι με το 802.11. Η κοινή κληρονομιά είναι τόσο βαθιά που το 802.11 αναφέρεται μερικές φορές ως "ασύρματο Ethernet."

Τα βασικά στοιχεία που είναι παρόντα στο Ethernet είναι παρόντα και στο 802.11. Οι σταθμοί προσδιορίζονται από 48-bit IEEE 802 διευθύνσεις MAC. Τα πλαίσια παραδίδονται με βάση τη διεύθυνση MAC. Η παράδοση πλαισίων είναι αναξιόπιστη, αν και το 802.11 ενσωματώνει μερικούς βασικούς μηχανισμούς αξιοπιστίας για να υπερνικήσει την εγγενώς χαμηλή ποιότητα των ραδιοκαναλιών που χρησιμοποιεί.

Υπηρεσίες δικτύου

Ένας τρόπος για να καθοριστεί μια δικτυακή τεχνολογία είναι να καθοριστούν οι υπηρεσίες που αυτή προσφέρει και να επιτραπεί στους προμηθευτές εξοπλισμού να εφαρμόσουν αυτές τις υπηρεσίες με οποιοδήποτε τρόπο νομίζουν αυτοί σωστό. Το 802.11 παρέχει εννέα υπηρεσίες. Μόνο τρεις από τις υπηρεσίες χρησιμοποιούνται για την μεταφορά των δεδομένων' τα υπόλοιπα έξι είναι διαχειριστικές λειτουργίες που επιτρέπουν στο δίκτυο να παρακολουθεί τους κινητούς κόμβους και να παραδίδει τα πλαίσια αναλόγως.

Οι υπηρεσίες περιγράφονται στον ακόλουθο κατάλογο και συνοψίζονται στον πίνακα 2-1:

- **Διανομή (Distribution)**

  Αυτή η υπηρεσία χρησιμοποιείται από τους κινητούς σταθμούς σε ένα δίκτυο υποδομής κάθε φορά που στέλνουν δεδομένα. Μόλις γίνει αποδεκτό ένα πλαίσιο από ένα σημείο πρόσβασης, το τελευταίο χρησιμοποιεί την υπηρεσία διανομής για να παραδώσει το πλαίσιο στον προορισμό του. Οποιαδήποτε επικοινωνία που χρησιμοποιεί ένα σημείο πρόσβασης ταξιδεύει μέσω της υπηρεσίας διανομής, συμπεριλαμβανομένων των επικοινωνιών μεταξύ δύο κινητών σταθμών που συνδέονται με το ίδιο σημείο πρόσβασης.

- **Ενσωμάτωση (Integration)**

  Η ενσωμάτωση είναι μια υπηρεσία που παρέχεται από το σύστημα διανομής' επιτρέπει τη σύνδεση του συστήματος διανομής με ένα μη-IEEE 802.11 δίκτυο. Η λειτουργία ενσωμάτωσης είναι συγκεκριμένη για το χρησιμοποιούμενο σύστημα διανομής και επομένως δεν διευκρινίζεται από το 802.11, εκτός από την άποψη των υπηρεσιών που πρέπει να προσφέρει.

- **Σύνδεση (Association)**

  Η παράδοση των πλαισίων σε κινητούς σταθμούς πραγματοποιείται επειδή οι κινητοί σταθμοί καταχωρούνται σε, ή συνδέονται με, σημεία πρόσβασης. Το σύστημα διανομής μπορεί έπειτα να χρησιμοποιήσει τις πληροφορίες εγγραφής για να καθορίσει ποιο σημείο πρόσβασης να χρησιμοποιήσει για οποιοδήποτε κινητό σταθμό. Οι μη συνδεδεμένοι σταθμοί δεν είναι "στο δίκτυο," όπως οι τερματικοί σταθμοί με αποσυνδεμένα καλώδια Ethernet. Το 802.11 διευκρινίζει τη λειτουργία που πρέπει να παρασχεθεί από το σύστημα διανομής χρησιμοποιώντας τα δεδομένα σύνδεσης, αλλά δεν εξουσιοδοτεί οποιαδήποτε ιδιαίτερη εφαρμογή. Όταν ισχυρά πρωτόκολλα ασφάλειας δικτύων είναι σε χρήση, η σύνδεση είναι ένας πρόδρομος της επικύρωσης. Πριν από την ολοκλήρωση της επικύρωσης, ένα σημείο πρόσβασης θα "ρίξει" όλη την δικτυακή κυκλοφορία από έναν σταθμό.

- **Επανασύνδεση (Reassociation)**

  Όταν ένας κινητός σταθμός κινείται μεταξύ βασικών περιοχών υπηρεσιών μέσα σε μια ενιαία εκτεταμένη περιοχή υπηρεσιών, πρέπει αυτός να αξιολογήσει την ισχύ των σημάτων και ίσως να αλλάξει το σημείο πρόσβασης με το οποίο συνδέεται. Οι επανασυνδέσεις εκκινούνε από τους κινητούς σταθμούς όταν οι συνθήκες των σημάτων δείχνουν ότι μια διαφορετική σύνδεση θα ήταν ευεργετική' δεν εκκινούνε ποτέ άμεσα από το σημείο πρόσβασης. Είναι πιθανό ορισμένα APs να διώξουν ένα σταθμό προκειμένου να αναγκαστεί ο πελάτης αυτός να εισαχθεί στη διαδικασία επανασύνδεσης.

Αφότου η επανασύνδεση είναι πλήρης, το σύστημα διανομής ενημερώνει τα αρχεία θέσης του για να απεικονίσει την χωρική προσιτότητα του κινητού σταθμού μέσω ενός διαφορετικού σημείου πρόσβασης. Όπως με την υπηρεσία σύνδεσης, ένα ισχυρό δίκτυο ασφάλειας θα "ρίξει" την δικτυακή κυκλοφορία πριν από την επιτυχή ολοκλήρωση της επικύρωσης.

- **Αποσύνδεση (Disassociation)**

  Για να τερματιστεί μια υπάρχουσα σύνδεση, οι σταθμοί μπορούν να χρησιμοποιήσουν την υπηρεσία αποσύνδεσης. Όταν οι σταθμοί επικαλούνται την υπηρεσία αποσύνδεσης, οποιοδήποτε δεδομένο κινητικότητας που αποθηκεύεται στο σύστημα διανομής αφαιρείται. Η αποσύνδεση είναι μια ευγενική κίνηση που οφείλει να γίνεται κατά τη διάρκεια της διαδικασίας σβησίματος σταθμού. Το MAC, εντούτοις, έχει σχεδιαστεί να φιλοξενεί τους σταθμούς που αφήνουν το δίκτυο χωρίς τυπικά να αποσυνδεθούν.

- **Επικύρωση (Authentication)**

  Η φυσική ασφάλεια είναι ένα σημαντικό συστατικό μιας λύσης ασφάλειας ενσύρματου LAN.Ο δικτυακός εξοπλισμός μπορεί να εξασφαλιστεί σε κλειδωμένα ντουλάπια καλωδίωσης. Εντούτοις, τα ασύρματα δίκτυα δεν μπορούν να προσφέρουν το ίδιο επίπεδο φυσικής ασφάλειας και επομένως εξαρτώνται από τις πρόσθετες ρουτίνες επικύρωσης για να διασφαλίσουν ότι οι χρήστες που έχουν πρόσβαση στο δίκτυο είναι εξουσιοδοτημένοι. Η επικύρωση είναι μια απαραίτητη προϋπόθεση στην σύνδεση επειδή μόνο οι επικυρωμένοι χρήστες εξουσιοδοτούνται για να χρησιμοποιήσουν το δίκτυο.

  Η επικύρωση μπορεί να συμβεί πολλαπλές φορές κατά τη διάρκεια της σύνδεσης ενός πελάτη σε ένα ασύρματο δίκτυο. Πριν από την σύνδεση, ένας σταθμός θα εκτελέσει μια βασική ανταλλαγή ταυτότητας με ένα σημείο πρόσβασης που αποτελείται από τη διεύθυνση MAC του. Αυτή η ανταλλαγή αναφέρεται συχνά ως "802.11" επικύρωση, η οποία είναι διαφορετική από τη ισχυρή κρυπτογραφική επικύρωση χρηστών που συχνά ακολουθεί.

- **Deauthentication**

  Η αποεπικύρωση τερματίζει μια επικυρωμένη σχέση. Επειδή η επικύρωση απαιτείται προτού να εγκριθεί η χρήση του δικτύου, μια παρενέργεια της αποεπικύρωσης είναι η λήξη οποιασδήποτε τρέχουσας σύνδεσης. Σε ένα ισχυρό δίκτυο ασφάλειας, η αποεπικύρωση καθαρίζει επίσης τις πληροφορίες κλειδιών.

- **Εμπιστευτικότητα (Confidentiality)**

  Οι ισχυροί φυσικοί έλεγχοι μπορούν να αποτρέψουν έναν μεγάλο αριθμό επιθέσεων στη μυστικότητα των δεδομένων στο ενσύρματο LAN. Οι επιτιθέμενοι πρέπει να λάβουν φυσική πρόσβαση στο μέσο πριν προσπαθήσουν να υποκλέψουν την κυκλοφορία. Σε ένα ενσύρματο δίκτυο, η φυσική πρόσβαση στην καλωδίωση είναι ένα υποσύνολο της φυσικής πρόσβασης σε άλλους υπολογιστικούς πόρους. Εκ σχεδιασμού, η φυσική πρόσβαση στα ασύρματα δίκτυα είναι ένα συγκριτικά απλούστερο ζήτημα σωστών κεραιών και μεθόδων διαμόρφωσης.

  Στην αρχική αναθεώρηση του 802.11, η υπηρεσία εμπιστευτικότητας ονομάστηκε μυστικότητα και παρασχέθηκε από το τώρα-δυσφημημένο πρωτόκολλο μυστικότητας ισοδύναμο με ενσύρματο (Wired Equivalent Privacy - WEP). Επιπρόσθετα στα νέα σχέδια κρυπτογράφησης, το 802.11i αυξάνει την υπηρεσία εμπιστευτικότητας με την παροχή της βασισμένης στο χρήστη επικύρωσης και των βασικών διαχειριστικών λειτουργιών, δύο κρίσιμα ζητήματα που το WEP απέτυχε να αντιμετωπίσει.

- **Παράδοση MSDU**

  Τα δίκτυα δεν είναι καθόλου χρήσιμα χωρίς τη δυνατότητα να φτάνουν τα δεδομένα στον παραλήπτη. Οι σταθμοί παρέχουν την υπηρεσία παράδοσης μονάδων δεδομένων

υπηρεσιών MAC (MAC Service Data Unit - MSDU), η οποία είναι αρμόδια για να φτάσουν τα δεδομένα στον πραγματικό προορισμό.

- **Έλεγχος ισχύος εκπομπής (Transmit Power Control - TPC)**

  Το TPC είναι μια νέα υπηρεσία που καθορίστηκε από 802.11h. Τα ευρωπαϊκά πρότυπα για τη ζώνη των 5 GHz απαιτούν οι σταθμοί να ελέγχουν την ισχύ των ραδιομεταδόσεων προκειμένου να αποφύγουν την παρεμβολή με άλλους χρήστες της ζώνης των 5 GHz. Ο έλεγχος της ισχύος εκπομπής βοηθά επίσης να αποφευχθεί η παρεμβολή με άλλα ασύρματα LANs. Το εύρος κάλυψης είναι συνάρτηση της ισχύος' ρυθμίσεις υψηλής ισχύος εκπομπής καθιστούν πιθανότερο το μεγαλύτερο εύρος κάλυψης ενός πελάτη να παρεμποδίσει ένα γειτονικό δίκτυο. Με τον έλεγχο της ισχύος σε ένα επίπεδο που είναι "ακριβώς το κατάλληλο", είναι λιγότερο πιθανό ότι ένας σταθμός θα παρεμβάλει τους γειτονικούς σταθμούς.

- **Δυναμική επιλογή συχνότητας (Dynamic Frequency Selection - DFS)**

  Μερικά συστήματα ραντάρ λειτουργούν στα 5 GHz. Κατά συνέπεια, μερικές ρυθμιστικές αρχές έχουν αναγκάσει ασύρματα LANs να ανιχνεύσουν τα συστήματα ραντάρ και να κινηθεί προς τις συχνότητες που δεν είναι σε χρήση από το ραντάρ. Μερικές ρυθμιστικές αρχές απαιτούν επίσης την ομοιόμορφη χρήση της ζώνης 5 GHz για ασύρματο LANs, έτσι τα δίκτυα πρέπει να έχουν τη δυνατότητα να αλλάζουν τα κανάλια έτσι ώστε η χρήση να εξισώνεται.

Υπηρεσία	**Υπηρεσία σταθμού ή διανομής;**	**Περιγραφή**
Distribution	διανομής	Υπηρεσία που χρησιμοποιείται στην παράδοση πλαισίων για να καθορίσει τη διεύθυνση προορισμού στα δίκτυα υποδομής
Integration	διανομής	Παράδοση πλαισίων σε LAN IEEE 802 έξω από το ασύρματο δίκτυο
Association	διανομής	Χρησιμοποιημένη για να καθιερώσει το AP που χρησιμεύει ως η πύλη σε έναν συγκεκριμένο κινητό σταθμό
Reassociation	διανομής	Χρησιμοποιημένη για να αλλάξει το AP που χρησιμεύει ως η πύλη σε έναν συγκεκριμένο κινητό σταθμό
Disassociation	διανομής	Αφαιρεί τον ασύρματο σταθμό από το δίκτυο
Authentication	σταθμού	Καθιερώνει την ταυτότητα σταθμού (διεύθυνση MAC) πριν από την καθιέρωση της σύνδεσης
Deauthentication	σταθμού	Χρησιμοποιημένη για να τερματίσει την επικύρωση και, κατ' επέκταση, τη σύνδεση
Confidentiality	σταθμού	Παρέχει προστασία ενάντια στο κρυφάκουσμα
MSDU delivery	σταθμού	Παραδίδει δεδομένα στον παραλήπτη
Transmit Power Control (TPC)	διαχείριση σταθμού/φάσματος	Μειώνει την παρεμβολή με την ελαχιστοποίηση της ισχύος εκπομπής του σταθμού
Dynamic Frequency Selection (DFS)	διαχείριση σταθμού/φάσματος	Αποφεύγει την παρεμβολή με τη λειτουργία των ραντάρ στη ζώνη των 5 GHz

Υπηρεσίες σταθμού

Οι υπηρεσίες σταθμών είναι μέρος κάθε σταθμού συμβατού με το 802.11 και πρέπει να ενσωματωθούν από οποιοδήποτε προϊόν που επικαλείται συμμόρφωση με το 802.11. Οι υπηρεσίες σταθμών παρέχονται και από τους κινητούς σταθμούς και από την ασύρματη διεπαφή στα σημεία πρόσβασης. Οι σταθμοί παρέχουν τις υπηρεσίες παράδοσης πλαισίων για να επιτρέψουν την παράδοση μηνυμάτων και, για αυτό το λόγο, μπορεί να πρέπει να χρησιμοποιήσουν τις υπηρεσίες επικύρωσης για να καθιερώσουν συνδέσεις. Οι σταθμοί μπορούν επίσης να επιθυμούν να εκμεταλλευθούν τις λειτουργίες εμπιστευτικότητας για να προστατεύσουν τα μηνύματα δεδομένου ότι διαπερνούν την τρωτή ασύρματη σύνδεση.

Υπηρεσίες συστήματος διανομής

Οι υπηρεσίες συστημάτων διανομής συνδέουν τα σημεία πρόσβασης με το σύστημα διανομής. Ο σημαντικότερος ρόλος των σημείων πρόσβασης είναι να επεκτείνουν τις υπηρεσίες του ενσύρματου δικτύου στο ασύρματο δίκτυο. Αυτό γίνεται με την παροχή των υπηρεσιών διανομής και ενσωμάτωσης στην ασύρματη πλευρά. Η διαχείριση των συνδέσεων κινητών σταθμών είναι ο άλλος σημαντικός ρόλος του συστήματος διανομής. Για να διατηρήσει τα δεδομένα σύνδεσης και τις πληροφορίες θέσης σταθμών, το σύστημα διανομής παρέχει την σύνδεση, την επανασύνδεση και τις υπηρεσίες αποσύνδεσης.

Εμπιστευτικότητα και έλεγχος πρόσβασης

Οι υπηρεσίες ελέγχου εμπιστευτικότητας και πρόσβασης συνδυάζονται. Εκτός από τη μυστικότητα των δεδομένων κατά τη μεταφορά, η υπηρεσία εμπιστευτικότητας αποδεικνύει επίσης την ακεραιότητα του περιεχομένου των πλαισίων. Η υπηρεσία εμπιστευτικότητας εξαρτάται απαραιτήτως από άλλες υπηρεσίες για να παρέχει επικύρωση και διαχείριση κλειδιών.

- **Επικύρωση και διαχείριση κλειδιού (Authentication and key management - AKM)**

  Η κρυπτογραφική ακεραιότητα είναι άνευ αξίας εάν δεν αποτρέπει τους αναρμόδιους χρήστες από να συνδεθούν με το δίκτυο. Η υπηρεσία εμπιστευτικότητας εξαρτάται από την επικύρωση και τη ακολουθία διαχείρισης κλειδιού για να καθιερώσει την ταυτότητα των χρηστών και τα κλειδιά κρυπτογράφησης. Η επικύρωση μπορεί να ολοκληρωθεί μέσω ενός εξωτερικού πρωτοκόλλου, όπως το 802.1X ή με τα προ-μοιρασμένα κλειδιά.

- **Αλγόριθμοι κρυπτογράφησης**

  Τα πλαίσια μπορούν να προστατευθούν από τον παραδοσιακό αλγόριθμο WEP χρησιμοποιώντας μυστικά κλειδιά των 40- ή 104-bit , το πρωτόκολλο προσωρινής ακεραιότητας κλειδιού (Temporal Key Integrity Protocol - TKIP) ή το πρωτόκολλο Counter Mode CBC-MAC (CCMP).

- **Αυθεντικότητα προέλευσης**

  Τα TKIP και CCMP επιτρέπουν στο δέκτη να επικυρώσει τη διεύθυνση MAC του αποστολέα για να αποτρέψει τις επιθέσεις υποκρισίας (spoofing attacks). Η προστασία αυθεντικότητας προέλευσης είναι μόνο διαθέσιμη για τα δεδομένα μονοεκπομπής (unicast data).

- **Ανίχνευση επανάληψης**

  Τα TKIP και CCMP προστατεύουν από τις επιθέσεις επανάληψης με την ενσωμάτωση ενός μετρητή ακολουθίας που επικυρώνεται στην παραλαβή. Τα πλαίσια που είναι "πάρα πολύ παλαιά" για να είναι ισχύοντα απορρίπτονται.

- **Εξωτερικά πρωτόκολλα και συστήματα**

  Η υπηρεσία εμπιστευτικότητας εξαρτάται σε μεγάλο βαθμό από τα εξωτερικά πρωτόκολλα που τρέχουν. Η διαχείριση κλειδιού παρέχεται από το 802.1X, το οποίο μαζί

με το EAP φέρει τα δεδομένα επικύρωσης. Το 802.11 δεν θέτει κανένα περιορισμό στα χρησιμοποιούμενα πρωτόκολλα, αλλά οι πιο κοινές επιλογές είναι EAP για επικύρωση, και RADIUS για τη διασύνδεση με τον κεντρικό υπολογιστή επικύρωσης.

Υπηρεσίες Διαχείρισης φάσματος

Οι υπηρεσίες διαχείρισης φάσματος είναι ένα ειδικό υποσύνολο των υπηρεσιών των σταθμών. Έχουν σχεδιαστεί να επιτρέπουν στο ασύρματο δίκτυο να αντιδρά στις συνθήκες και να αλλάζει δυναμικά τις ρυθμίσεις του ραδίου. Δύο υπηρεσίες καθορίστηκαν στο 802.11h για να βοηθήσουν να ικανοποιηθούν ρυθμιστικές απαιτήσεις.

Η πρώτη υπηρεσία, ελέγχου ισχύος εκπομπής (Transmit Power Control - TPC), μπορεί δυναμικά να ρυθμίσει τη ισχύ μετάδοσης ενός σταθμού. Τα σημεία πρόσβασης είναι σε θέση να χρησιμοποιήσουν τις διαδικασίες TPC για να διαφημίσουν τη μέγιστη επιτρεπόμενη ισχύ και να απορρίψουν συνδέσεις από πελάτες που δεν συμμορφώνονται με τους τοπικούς ραδιοκανονισμούς. Οι πελάτες μπορούν να χρησιμοποιήσουν TPC για να ρυθμίσουν τη ισχύ έτσι ώστε το εύρος κάλυψης να είναι "ακριβώς το κατάλληλο". Τα ψηφιακά κυψελοειδή συστήματα έχουν μια παρόμοια δυνατότητα να επεκτείνουν τη ζωή μπαταριών των κινητών τηλεφώνων. Χαμηλότερη ισχύς εκπομπής επίσης θα έχει κάποιο όφελος υπό μορφή αυξημένης ζωής της μπαταρίας.

Η δεύτερη υπηρεσία, δυναμική επιλογή συχνότητας (Dynamic Frequency Selection - DFS), αναπτύχθηκε κυρίως για να αποφύγει τη παρεμβολή με συστήματα ραντάρ των 5GHz σε χρήση στην Ευρώπη. Αν και αναπτύχθηκαν αρχικά για να ικανοποιήσουν τους ευρωπαϊκούς ρυθμιστές, οι ελλοχεύουσες αρχές έχουν επίσης απαιτηθεί από άλλους ρυθμιστές. Το DFS ήταν βασικό στην απόφαση των Η.Π.Α. να ανοιχτεί περισσότερο φάσμα στη ζώνη των 5 GHz το 2004. Το DFS επιτρέπει στο σημείο πρόσβασης να σβήσει ένα κανάλι έτσι ώστε μπορεί να ψάξει για ραντάρ χωρίς παρεμβολή, αλλά το σημαντικότερο μέρος του DFS είναι ο τρόπος με τον οποίο μπορεί να επαναεκχωρήσει άμεσα το κανάλι σε ένα σημείο πρόσβασης. Οι πελάτες ενημερώνονται για το νέο κανάλι προτού να αλλαχτεί το ισχύον κανάλι.

Υποστήριξη Κινητικότητας

Η κινητικότητα είναι το συνήθως αρχικό κίνητρο για την ανάπτυξη ενός δικτύου 802.11. Η διαβίβαση των πλαισίων δεδομένων ενώ ο σταθμός κινείται θα κάνει για τις μεταδόσεις δεδομένων ό,τι κάνει η κινητή τηλεφωνία για τη φωνή.

Το 802.11 παρέχει κινητικότητα μεταξύ των βασικών περιοχών υπηρεσιών στο στρώμα ζεύξης. Εντούτοις, δεν γνωρίζει τίποτα από το τι συμβαίνει επάνω από το στρώμα ζεύξης. Κατά το σχεδιασμό υλοποίησης 802.11, οι μηχανικοί δικτύων πρέπει να φροντίσουν έτσι ώστε η διάφανη μετάβαση στο στρώμα του ραδίου να υποστηρίζεται και από το στρώμα πρωτοκόλλου δικτύου. Όσον αφορά το 802.11, υπάρχουν τρεις τύποι μεταβάσεων μεταξύ των σημείων πρόσβασης:

- **Καμία μετάβαση**

  Όταν οι σταθμοί δεν κινούνται από την περιοχή υπηρεσιών του τρέχοντος σημείου πρόσβασής τους, καμία μετάβαση δεν είναι απαραίτητη. Αυτό συμβαίνει επειδή ο σταθμός δεν κινείται ή κινείται μέσα στο βασικό τομέα υπηρεσιών του τρέχοντος σημείου πρόσβασής του.

- **BSS μετάβαση**

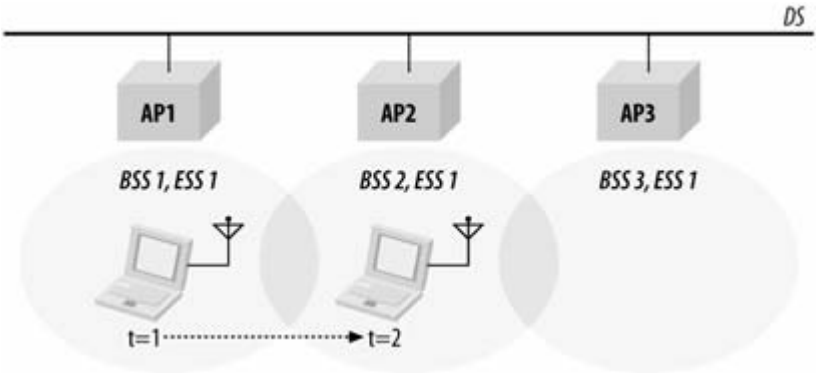
  Οι σταθμοί ελέγχουν συνεχώς την ισχύ και την ποιότητα των σημάτων από όλα τα σημεία πρόσβασης που έχουν οριστεί από το διαχειριστή να καλύψουν μια εκτεταμένη περιοχή υπηρεσιών. Μέσα σε μια εκτεταμένη περιοχή υπηρεσιών, το 802.11 παρέχει κινητικότητα στο στρώματος MAC. Οι σταθμοί που συνδέονται με το σύστημα διανομής μπορούν να στείλουν πλαίσια που απευθύνονται στη διεύθυνση MAC ενός κινητού σταθμού και να αφήσουν τα σημεία πρόσβασης να χειριστούν το τελικό hop στον κινητό

σταθμό. Οι σταθμοί συστημάτων διανομής δεν χρειάζεται να γνωρίζουν τη θέση ενός κινητού σταθμού εφ' όσον είναι μέσα στην ίδια εκτεταμένη περιοχή υπηρεσιών.

Το σχήμα 2-9 απεικονίζει μια μετάβαση BSS. Τα τρία σημεία πρόσβασης στην εικόνα είναι όλα ορισμένα στο ίδιο ESS. Στην έναρξη, που δείχνεται από t=1, ο φορητός υπολογιστής με μια 802.11 κάρτα δικτύου κάθεται μέσα στη βασική περιοχή υπηρεσιών του AP1 και είναι συνδεδεμένος με το AP1. Όταν ο φορητός υπολογιστής έχει κινηθεί έξω από τη βασική περιοχή υπηρεσιών του AP1 προς εκείνη του AP2 τη χρονική στιγμή t=2, μια μετάβαση BSS εμφανίζεται. Ο κινητός σταθμός χρησιμοποιεί την υπηρεσία επανασύνδεσης για να συνδεθεί με το AP2, το οποίο αρχίζει έπειτα να στέλνει τα πλαίσια στον κινητό σταθμό.

Οι μεταβάσεις BSS απαιτούν τη συνεργασία των σημείων πρόσβασης. Σε αυτό το σενάριο, το AP2 πρέπει να ενημερώσει το AP1 ότι ο κινητός σταθμός συνδέεται τώρα με το AP2. Το 802.11 δεν διευκρινίζει τις λεπτομέρειες των επικοινωνιών μεταξύ των σημείων πρόσβασης κατά τη διάρκεια των μεταβάσεων BSS.

Να σημειωθεί ότι ακόμα κι αν δύο σημεία πρόσβασης είναι μέλη του ίδιου εκτεταμένου συνόλου μπορούν εν τούτοις να είναι συνδεδεμένα με έναν δρομολογητή, ο οποίος είναι ένα όριο στρώματος 3 . Σε ένα τέτοιο σενάριο, δεν υπάρχει κανένας τρόπος να είναι εγγυημένη η διάφανη συνδεσιμότητα χρησιμοποιώντας μόνο πρωτόκολλα 802.11.

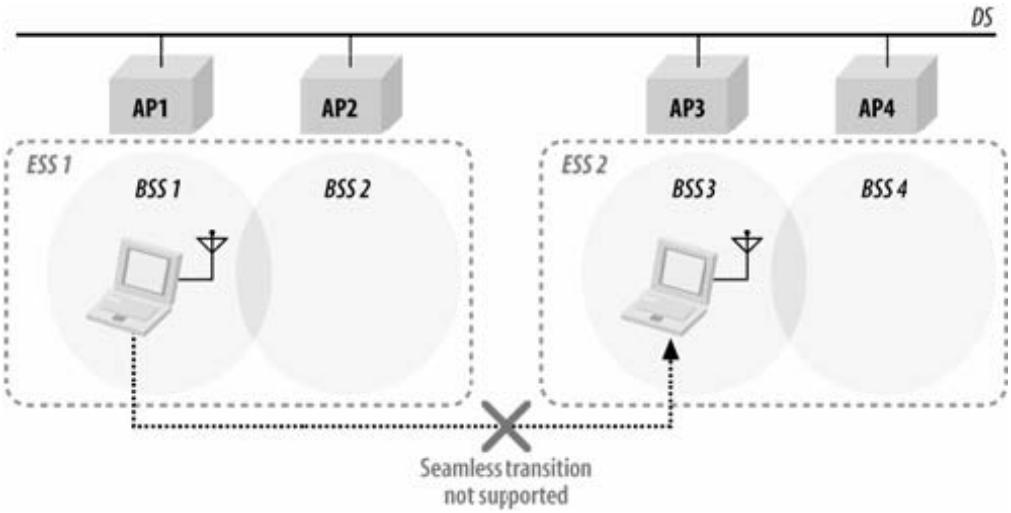


Εικόνα 1-9 BSS διαπομπή

- **ESS μετάβαση**

  Μια μετάβαση ESS αναφέρεται στη μετακίνηση από ένα ESS σε ένα δεύτερο διαφορετικό ESS. Το 802.11 δεν υποστηρίζει αυτόν τον τύπο μετάβασης, εκτός από το να επιτρέψει στο σταθμό να συνδεθεί με ένα σημείο πρόσβασης στο δεύτερο ESS μόλις αυτός αφήσει το πρώτο. Οι συνδέσεις υψηλότερων στρωμάτων είναι σχεδόν εγγυημένο ότι θα διακοπούν. Θα ήταν δίκαιο να ειπωθεί ότι το 802.11 υποστηρίζει μεταβάσεις ESS μόνο μέχρι το σημείο που είναι σχετικά εύκολο να επιχειρηθεί σύνδεση με ένα σημείο πρόσβασης στη νέα εκτεταμένη περιοχή υπηρεσιών. Η διατήρηση των υψηλότερου επιπέδου συνδέσεων απαιτεί την υποστήριξη από σουίτες πρωτοκόλλων. Στην περίπτωση του TCP/ IP, το κινητό IP (Mobile IP) απαιτείται για να υποστηρίξει διαφανώς μια μετάβαση ESS.

  Το σχήμα 2-10 απεικονίζει μια μετάβαση ESS. Τέσσερις βασικές περιοχές υπηρεσιών είναι οργανωμένες σε δύο εκτεταμένες περιοχές υπηρεσιών. Διαφανείς μεταβάσεις από το αριστερό ESS στο δεξί ESS δεν υποστηρίζονται. Μεταβάσεις ESS υποστηρίζονται μόνο επειδή ο κινητός σταθμός θα συνδεθεί γρήγορα με ένα σημείο πρόσβασης στο δεύτερο ESS. Οποιεσδήποτε ενεργές συνδέσεις δικτύου είναι πιθανό να διακοπούν όταν αφήσει ο κινητός σταθμός το πρώτο ESS.



Εικόνα 1-10 ESS διαπομπή

Σχεδιασμός δικτύων για κινητικότητα

Τα περισσότερα δίκτυα σχεδιάζονται έτσι ώστε μια ομάδα σημείων πρόσβασης να μπορεί να παρέχει πρόσβαση σε ένα σύνολο πόρων. Όλα τα σημεία πρόσβασης ορίζονται στο ίδιο SSID και οι πελάτες διαμορφώνονται για να χρησιμοποιήσουν εκείνο το SSID όταν συνδέονται με το ασύρματο δίκτυο.

Καθώς οι πελάτες κινούνται ελέγχουν συνεχώς τη συνδεσιμότητα με το δίκτυο και μετατοπίζονται μεταξύ σημείων πρόσβασης στο ίδιο SSID. Το 802.11 εξασφαλίζει ότι οι πελάτες θα είναι σε θέση να μετακινήσουν συνδέσεις μεταξύ σημείων πρόσβασης του ίδιου SSID, αλλά οι αρχιτέκτονες του δικτύου πρέπει να χτίσουν το δίκτυο ώστε αυτό να υποστηρίζει τους κινητούς πελάτες. Τα μικρά δίκτυα υλοποιούνται συχνά σε ένα ενιαίο VLAN με ένα ενιαίο υποδίκτυο, οπότε σ' αυτή την περίπτωση δεν υπάρχει καμία ανάγκη για ανησυχία περί κινητικότητας. Τα μεγαλύτερα δίκτυα που εκτείνονται πέραν των ορίων ενός υποδικτύου πρέπει να εφαρμόσουν κάποια πρόσθετη τεχνολογία για να παρέχουν την υποστήριξη κινητικότητας. Πολλά προϊόντα μπορούν να λειτουργήσουν με έναν πυρήνα VLAN, ο οποίος επιτρέπει στους πελάτες να συνδέονται πάντα με το ίδιο VLAN κατά μήκος ενός οργανισμού. Τα νέα προϊόντα επιτρέπουν ακόμη και τη δυναμική ανάθεση VLAN βασισμένη σε δεδομένα επικύρωσης. Όταν οι χρήστες συνδέονται με το δίκτυο, είναι συνδεμένοι με το ίδιο VLAN παντού. Μερικά προϊόντα υποστηρίζουν το πρότυπο κινητού IP ή χρησιμοποιούν την τεχνολογία VPN δημιουργικά.

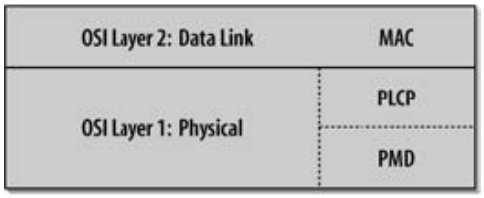
Στην πράξη, οι μεταβάσεις ESS είναι αρκετά σπάνιες. Εμφανίζονται συνήθως μόνο όταν οι χρήστες αφήνουν μια διαχειριστική περιοχή για μια άλλη (έστω το εταιρικό δίκτυο για ένα hot spot), οπότε σε αυτή την περίπτωση τα δύο εν λόγω δίκτυα θα είχαν διαφορετική διεύθυνση IP και καμία σχέση εμπιστοσύνης για να συνδέσουν διαφανώς έναν πελάτη χωρίς να διακοπεί η συνδεσιμότητα στρώματος ζεύξης.

Τεχνολογίες Φυσικού Στρώματος 802.11

Έννοιες Ασύρματου Φυσικού Στρώματος

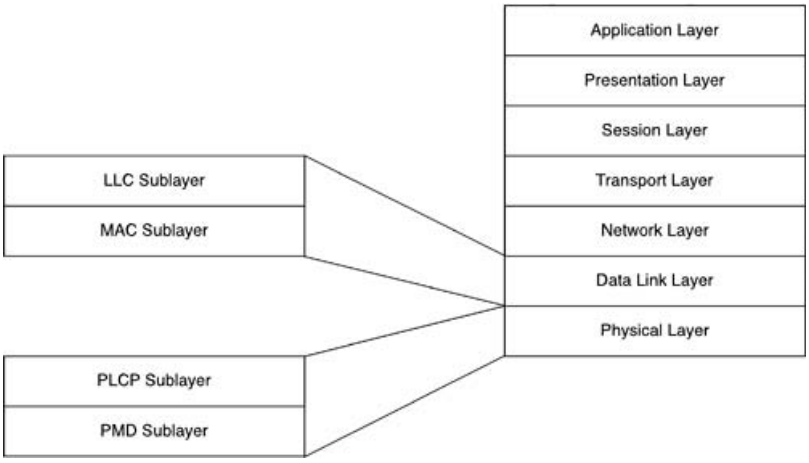
Το φυσικό στρώμα διαιρείται σε δύο υποστρώματα: το υπόστρωμα διαδικασίας σύγκλισης φυσικού στρώματος (Physical Layer Convergence Procedure - PLCP) και το υπόστρωμα το

εξαρτώμενο από το φυσικό μέσο (Physical Medium Dependent - PMD). Το PLCP (σχήμα 10-1) είναι η κόλλα μεταξύ των πλαισίων MAC και των ραδιομεταδόσεων στον αέρα. Προσθέτει την επικεφαλίδα του. Κανονικά, τα πλαίσια περιλαμβάνουν έναν πρόλογο για να βοηθήσουν στο συγχρονισμό των εισερχόμενων μεταδόσεων. Ωστόσο οι απαιτήσεις του προλόγου μπορούν να εξαρτηθούν από τη μέθοδο διαμόρφωσης, έτσι το PLCP προσθέτει την επικεφαλίδα του σε οποιαδήποτε διαβιβασθέντα πλαίσια. Το PMD είναι αρμόδιο για τη διαβίβαση οποιωνδήποτε bits λαμβάνει από το PLCP στον αέρα χρησιμοποιώντας την κεραία. Το φυσικό στρώμα ενσωματώνει επίσης μια λειτουργία αξιολόγησης καθαρών καναλιών (Clear Channel Assessment - CCA) που δείχνει στη MAC όταν ανιχνεύεται ένα σήμα.



Εικόνα 1-11 Λογική αρχιτεκτονική φυσικού στρώματος

Το σχήμα 3-1 επιδεικνύει πώς τα υποστρώματα είναι οριοθετημένα το ένα όσον αφορά το άλλο και τα ανώτερα στρώματα.



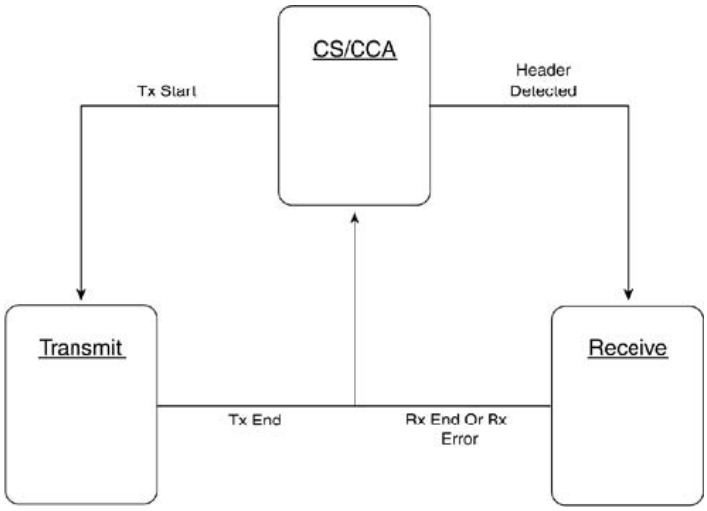
Εικόνα 1-12 Υποστρώματα PHY στο μοντέλο OSI

Το PLCP είναι ουσιαστικά ένα στρώμα χειραψίας που επιτρέπει στις μονάδες δεδομένων του πρωτοκόλλου MAC (MAC Protocol Data Units - MPDUs) να μεταφερθούν μεταξύ σταθμών MAC πάνω στο PMD, που είναι η μέθοδος εκπομπής και λήψης δεδομένων μέσω του ασύρματου μέσου. Από μία άποψη, μπορείτε κανείς να σκεφτεί το PMD ως υπηρεσία ασύρματης μετάδοσης που διασυνδέεται μέσω του PLCP. Τα υποστρώματα PLCP και PMD ποικίλλουν με βάση τους τύπους 802.11.

Όλα τα PLCPs, ανεξάρτητα από τον τύπο PHY 802.11, έχουν πρωταρχικά δεδομένα που παρέχουν τη διεπαφή για τη μεταφορά δεδομένων μεταξύ του MAC και του PMD. Επιπλέον, παρέχουν τα δεδομένα που επιτρέπουν στο MAC να πει στο PHY πότε να αρχίσει τη μετάδοση και στο PHY να πει στο MAC πότε έχει ολοκληρώσει τη μετάδοσή του. Από την πλευρά της λήψης, τα πρωταρχικά PLCP από το PHY στο MAC δείχνουν πότε έχει αρχίσει να λαμβάνει μια μετάδοση από έναν άλλο σταθμό και πότε εκείνη η μετάδοση είναι ολοκληρωμένη. Για να υποστηρίξουν τη λειτουργία αξιολόγησης καθαρών καναλιών (Clear Channel Assessment - CCA), όλα τα PLCPs

παρέχουν έναν μηχανισμό για το MAC να επανεκκινήσει τη μηχανή PHY CCA και για το PHY να εκθέσουν την παρούσα κατάσταση του ασύρματου μέσου.

Γενικά, τα 802.11 PLCPs λειτουργούν σύμφωνα με το διάγραμμα καταστάσεων στο σχήμα 3-2. Το βασική λειτουργική κατάσταση τους είναι η διαδικασία ανίχνευσης φέροντος / αξιολόγησης καθαρών καναλιών (CS/CCA). Αυτή η διαδικασία ανιχνεύει την έναρξη ενός σήματος από έναν διαφορετικό σταθμό και καθορίζει εάν το κανάλι είναι καθαρό για τη μετάδοση. Με τη λήψη ενός αιτήματος Έναρξης Tx, μεταβαίνει στη κατάσταση μετάδοσης αλλάζοντας το PMD από λήψη σε εκπομπή και στέλνει τη μονάδα δεδομένων του πρωτοκόλλου PLCP (PLCP Protocol Data Unit - PPDU). Κατόπιν, εκδίδει ένα Τέλος Tx και επιστρέφει στην κατάσταση CS/CCA. Το PLCP μεταβαίνει στην κατάσταση λήψης όταν η διαδικασία CS/CCA ανιχνεύει τον πρόλογο PLCP και έγκυρη επικεφαλίδα PLCP. Εάν το PLCP ανιχνεύει ένα λάθος, δείχνει το λάθος στο MAC και προχωρά στη διαδικασία CS/CCA.



Εικόνα 1-13 Διάγραμμα καταστάσεων PLCP

Η ραδιοζεύξη

Τρία φυσικά στρώματα τυποποιήθηκαν στην αρχική αναθεώρηση 802.11, η οποία δημοσιεύθηκε το 1997:

- Frequency-hopping (FH) spread-spectrum radio PHY
- Direct-sequence (DS) spread-spectrum radio PHY
- Infrared light (IR) PHY

Αργότερα, αναπτύχθηκαν τρία περαιτέρω φυσικά στρώματα:

- 802.11a: Orthogonal Frequency Division Multiplexing (OFDM) PHY
- 802.11b: High-Rate Direct Sequence (HR/DS or HR/DSSS) PHY
- 802.11g: Extended Rate PHY (ERP)
- Το μελλοντικό 802.11n, το οποίο καλείται και MIMO PHY ή υψηλής ρυθμαπόδοσης PHY

Στην διπλωματική αυτή εργασία συζητείται το φυσικό στρώμα υπέρυθρων ακτινών, το οποίο πιθανότατα να μην έχει εφαρμοστεί ποτέ σε ένα εμπορικό προϊόν.

Χορήγηση Αδειών και Κανονισμός

Η κλασική προσέγγιση στις ραδιοεπικοινωνίες είναι ο περιορισμός ενός σήματος που φέρει πληροφορία σε μια στενή ζώνη συχνοτήτων και η τοποθέτηση το δυνατόν μεγαλύτερης ισχύος (ή νόμιμα επιτρεπόμενης) στο σήμα. Ο θόρυβος είναι απλά η φυσικά παρούσα διαστρέβλωση στη ζώνη συχνοτήτων. Η μετάδοση ενός σήματος παρά το θόρυβο εξασφαλίζεται όταν η ισχύ του εκπεμπόμενου σήματος είναι πολύ μεγαλύτερη από το θόρυβο.

Με έξοδο υψηλής ισχύος σε στενές ζώνες, μια νομική αρχή πρέπει να επιβάλει κανόνες στον τρόπο με τον οποίο το φάσμα RF χρησιμοποιείται. Στις Ηνωμένες Πολιτείες η Ομοσπονδιακή Επιτροπή Επικοινωνιών (Federal Communications Commission - FCC) είναι αρμόδια να ρυθμίζει τη χρήση του φάσματος RF. Η ευρωπαϊκή κατανομή εκτελείται από το Ευρωπαϊκό Γραφείο Ραδιοεπικοινωνιών (European Radiocommunications Office - ERO) και το Ευρωπαϊκό Ίδρυμα Τηλεπικοινωνιακών Προτύπων (European Telecommunications Standards Institute - ETSI). Στην Ιαπωνία, το Υπουργείο Εσωτερικών Επικοινωνιών (Ministry of Internal Communications - MIC) ρυθμίζει τη ραδιοχρήση. Παγκοσμίως η εργασία "εναρμόνισης" γίνεται συχνά υπό την αιγίδα της Διεθνούς Ένωσης Τηλεπικοινωνιών (International Telecommunications Union - ITU). Πολλοί εθνικοί ρυθμιστές υιοθετούν τις συστάσεις ITU. Κάθε μια από αυτές τις αρχές έχει διαφορετικές παραμέτρους για το επιτρεπόμενο κέρδος των κεραιών, ισχύ εκπομπής, επιλογή καναλιών και τα λοιπά που πρέπει να ακολουθούνται.

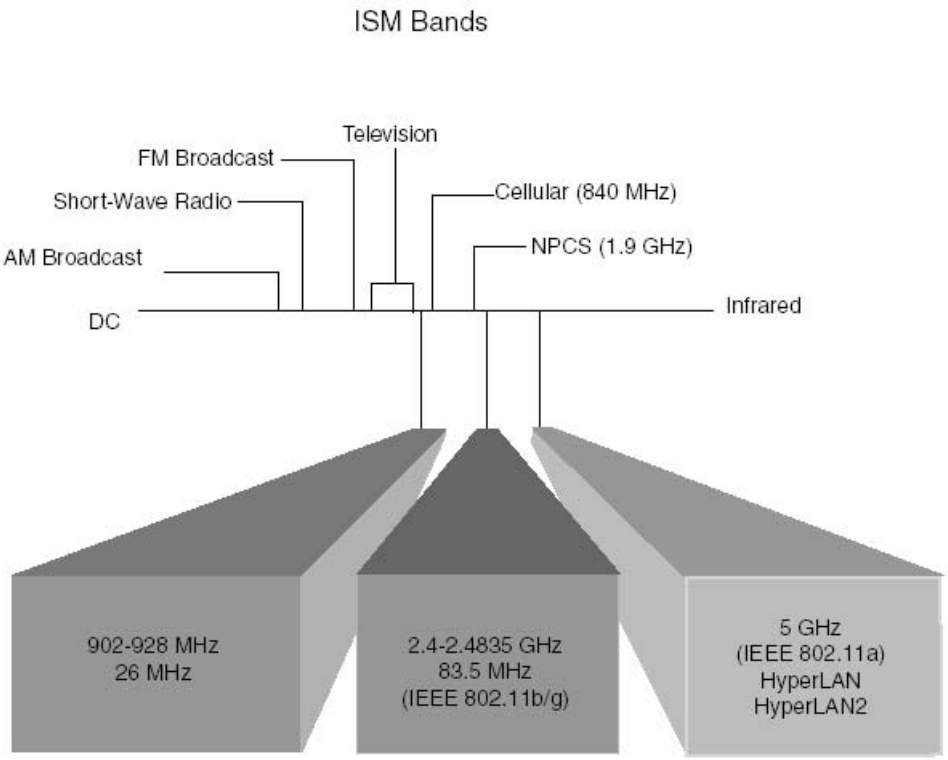
Ως επί το πλείστον, ένας οργανισμός πρέπει να έχει άδεια για να μεταδίδει σε μια δεδομένη συχνότητα. Οι άδειες μπορούν να περιορίσουν τις χρησιμοποιούμενες συχνότητες και την ισχύ μετάδοσης, καθώς επίσης και την περιοχή στην οποία τα ραδιοσήματα μπορούν να μεταδοθούν. Παραδείγματος χάριν, οι σταθμοί ραδιοφωνικής μετάδοσης πρέπει να έχουν μια άδεια. Επιπλέον, τα δίκτυα κινητών τηλεφώνων πρέπει να λάβουν τις άδειες για να χρησιμοποιήσουν το ραδιοφάσμα σε μια δεδομένη αγορά. Η χορήγηση αδειών εγγυάται την αποκλειστική χρήση ενός συγκεκριμένου συνόλου συχνοτήτων. Όταν τα εξουσιοδοτημένα σήματα παρεμποδίζονται, ο κάτοχος της άδειας μπορεί να απαιτήσει από τη ρυθμιστική αρχή να επέμβει και να επιλύσει το πρόβλημα, συνήθως με τη διακοπή της πηγής παρεμβολής. Η σκόπιμη παρεμβολή είναι ισοδύναμη με καταπάτηση και μπορεί να υπόκειται σε ποινικές ή αστικές κυρώσεις.

Διάθεση συχνοτήτων και μη αδειοδοτούμενες ζώνες συχνοτήτων

Το ραδιοφάσμα διατίθεται σε ζώνες που αφιερώνονται για έναν ιδιαίτερο σκοπό. Μια ζώνη καθορίζει τις συχνότητες που μια συγκεκριμένη εφαρμογή μπορεί να χρησιμοποιήσει. Περιλαμβάνει συχνά ζώνες φρουράς, οι οποίες είναι αχρησιμοποίητα τμήματα της ολικής κατανομής και οι οποίες αποτρέπουν την "διαρροή" από εξουσιοδοτημένη μετάδοση να επηρεάσει άλλης διατιθέμενη ζώνη.

Διάφορες ζώνες έχουν διατηρηθεί για χρήση χωρίς άδεια. Για να επιτραπεί στις καταναλωτικές εταιρίες να αναπτύξουν οικιακές συσκευές, οι ρυθμιστικές αρχές υπέδειξαν ορισμένες ζώνες για τη χρήση "βιομηχανικού, επιστημονικού, και ιατρικού" εξοπλισμού. Αυτές οι ζώνες συχνότητας αναφέρονται συνήθως ως ISM (Industrial, Scientific and Medical) ζώνες. Η χρήση εξοπλισμού στις ISM ζώνες γίνεται γενικά χωρίς άδεια, υπό τον όρο ότι οι συσκευές που λειτουργούν σε αυτές δεν εκπέμπουν σημαντικά ποσά ακτινοβολίας. Οι φούρνοι μικροκυμάτων είναι μεγάλης ισχύος συσκευές, αλλά έχουν εκτενές προστατευτικό κάλυμμα για να περιορίσουν τις ραδιοεκπομπές. Οι χωρίς άδεια ζώνες έχουν δει μεγάλη δραστηριότητα τα τελευταία έτη δεδομένου ότι νέες τεχνολογίες επικοινωνιών έχουν αναπτυχθεί για να εκμεταλλευτούν τη χωρίς άδεια ζώνη. Οι χρήστες μπορούν να εγκαταστήσουν νέες συσκευές, που λειτουργούν στις ISM ζώνες, χωρίς να περάσουν από οποιαδήποτε διαδικασία χορήγησης άδειας.

Τα χωρίς άδεια WLANs εμπίμπτουν σε τρεις βασικές ζώνες συχνοτήτων: 900 MHz, 2,4 GHz, και 5 GHz. Καθεμιά έχει τα πλεονεκτήματα και τα μειονεκτήματά της και χωρίζεται σε κανάλια ή ομάδες καναλιών. Το σχήμα 3-1 παρουσιάζει που τοποθετούνται αυτές οι ζώνες στο ολικό φάσμα συχνοτήτων.

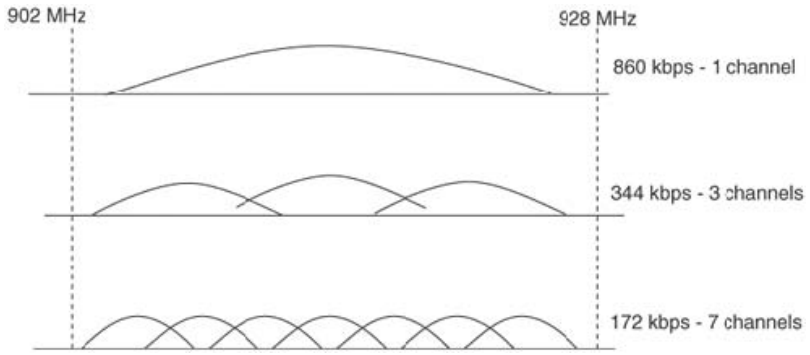


Εικόνα 1-14 Ζώνες ISM

Η ζώνη συχνοτήτων 900-MHz

Η ζώνη των 900 MHz ήταν η πρώτη περιοχή για την οποία το απλωμένο φάσμα WLANs αναπτύχθηκε. Ένας κοντινός γείτονας της ζώνης των 900 MHz ήταν η ζώνη των κυψελοειδών τηλεφωνικών επικοινωνιών. Αυτό βοήθησε την πρόωρη ανάπτυξη της βιομηχανίας WLAN στη ζώνη 900 MHz λόγω της διαθεσιμότητας των φθηνών και μικρών τμημάτων RF που είχαν αναπτυχθεί για χρήση στη βιομηχανία των κινητών τηλεφώνων.

Ένα μεγάλο μειονέκτημα της ζώνης των 900 MHz ήταν το περιορισμένο εύρος ζώνης. Οι ρυθμοί διέλευσης δεδομένων ήταν περιορισμένοι στα 1 και 2 Mbps το μέγιστο λόγω της περιορισμένης έκτασης συχνότητας που ήταν διαθέσιμη. Το σχήμα 3-2 απεικονίζει την ολική απαίτηση εύρους ζώνης σε 900 MHz με εφαρμογή διαφορετικών ρυθμών δεδομένων. Όπως μπορείτε να δείτε, η εφαρμογή υψηλότερων ρυθμών δεδομένων περιορίζει τον αριθμό καναλιών σε ένα, το οποίο απασχολεί ολόκληρη τη ζώνη και περιορίζει σοβαρά την εξελιξιμότητα.



Εικόνα 1-15 Σχήμα καναλιών στα 900 MHz

Καθώς αναπτυσσόταν η προδιαγραφή IEEE 802.11, η IEEE αναγνώρισε τις ανεπάρκειες αυτής της ζώνης και επέλεξε να μην την περιλάβει στο πρότυπο.

Η ζώνη συχνοτήτων 2.4-GHz

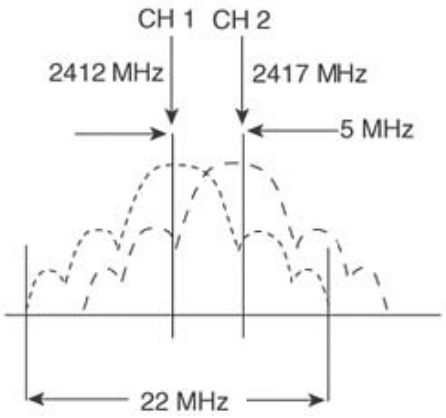
Η επιθυμία για υψηλότερους ρυθμούς διέλευσης δεδομένων και περισσότερη εξελιξιμότητα οδήγησε την ανάπτυξη στη ζώνη των 2,4 GHz. Αυτή η ζώνη ήταν γενικά διαθέσιμη σχεδόν σε κάθε μεγάλη χώρα παγκοσμίως. Αν και αρχικά επέτρεπε ρυθμούς διέλευσης δεδομένων μόνο μέχρι 2 Mbps, πρόσφερε μεγαλύτερη ικανότητα καναλιών. Η ανάπτυξη των συσκευών 2.4-GHz ενθαρρύνθηκε από το γεγονός ότι η ζώνη των 2.4 GHz είχε γείτονες τα PCS (Personal Communication Services) ασύρματα συστήματα καθώς επίσης και μερικά συστήματα ραντάρ. Οι κοντινές συχνότητες σήμαναν ότι μερικά από τα συστατικά RF και δαπάνες ανάπτυξης θα μπορούσαν να μοιραστούν μεταξύ των διαφορετικών τεχνολογιών. Καθώς η βιομηχανία άρχισε να επενδύει στην τεχνολογία 2.4 GHz, το IEEE ανέπτυσσε μια προδιαγραφή για να παρέχει διαλειτουργικότητα για τη νέα αγορά WLAN.

Το 1997, το IEEE ολοκλήρωσε τη προδιαγραφή 802.11, που καθορίζει ρυθμούς δεδομένων μέχρι 2 Mbps για τη ζώνη των 2.4 GHz και που καθορίζει ένα σχέδιο καναλιών που παρείχε τρία μη επικαλυπτόμενα και μη παρεμβαλλόμενα κανάλια. Στη περιοχή της Βόρειας Αμερικής υπήρξε ανάγκη να περιοριστούν τα ανώτερα κανάλια λόγω ενός πολύ σφιχτού περιορισμού για τα σήματα RF με αποτέλεσμα να καθοριστούν μόνο 11 κανάλια. Για την ETSI, ο περιορισμός στο ανώτερο τμήμα της ζώνης δεν ήταν ανάγκη και, έτσι, καθορίστηκαν 13 κανάλια. Στην Ιαπωνία, ένας πολύ ακριβής κανονισμός περιόρισε τη χρήση WLAN μόνο σε ένα στενό τμήμα και περιόρισε τον αριθμό καναλιών σε ένα και εκείνο το κανάλι ήταν ασύμβατο τόσο με την ETSI όσο και με τα βορειοαμερικανικά κανάλια. Αρκετά έτη αργότερα, η ιαπωνική TELEC άλλαξε τους κανονισμούς, επιτρέποντας τη λειτουργία των 13 καναλιών ETSI συν το παλαιό μοναδικό κανάλι της Ιαπωνίας.

Λόγω της απαίτησης για υψηλότερους ρυθμούς δεδομένων, το IEEE προσέθεσε μια τροποποίηση το 1999 για να αυξήσει το ρυθμό δεδομένων για τα συστήματα άμεσης ακολουθίας (Direct Sequence - DS) 2.4-GHz ώστε να περιλάβουν 5,5 Mbps και 11 Mbps. Αυτή η τροποποίηση είναι γνωστή ως προδιαγραφή 802.11b. Ο αριθμός καναλιών δεν άλλαξε και η νέα προδιαγραφή απαίτησε τα προϊόντα να είναι προς τα πίσω συμβατά με τα παλαιότερα 802.11 προϊόντα των 1 και 2 Mbps.

Παρομοίως, το 2003, το IEEE προσέθεσε ένα άλλο μέρος στις προδιαγραφές 802.11. Το πρότυπο 802.11g είναι ακόμα ένα σχέδιο, ακόμα υψηλότερου ρυθμού δεδομένων στη ζώνη 2.4 GHz, που παράγει ρυθμούς τόσο υψηλούς όσο τα 54 Mbps. Το πρότυπο αυτό προσφέρει συμβατότητα προς τα πίσω με την προδιαγραφή 802.11b.

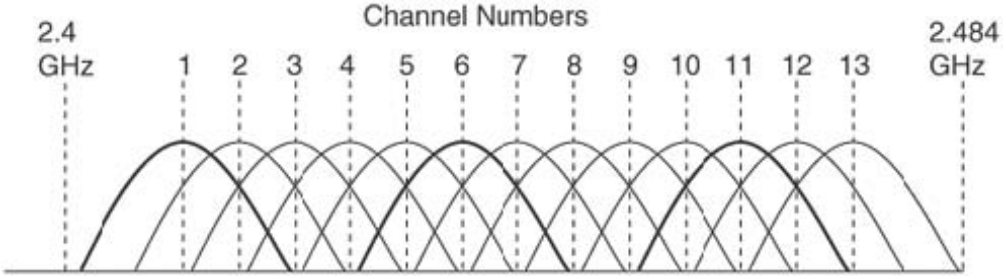
Η προδιαγραφή 802.11 καθορίζει το σχέδιο καναλιών να έχει εύρος 22 MHz, αρχίζοντας από την κεντρική συχνότητα του πρώτου καναλιού στα 2.412 GHz. Οι κεντρικές συχνότητες για τα κανάλια είναι μεταξύ τους απομακρυσμένες κατά διαστήματα των 5 MHz' αυτό το σχέδιο καναλιών οδηγεί σε δύο επικαλυπτόμενα κανάλια, όπως φαίνεται στο σχήμα 3-3.



Εικόνα 1-16 Επικάλυψη καναλιών 802.11 στα 2,4 GHz

Για πολλούς, το γεγονός ότι υπάρχουν 11 (ή 13 ή 14) διαθέσιμα κανάλια σημαίνει ότι λογικά είναι δυνατό να χρησιμοποιηθεί ένα σύστημα WLAN σε ένα κανάλι στην ίδια εγγύτητα με ένα άλλο σύστημα σε διαφορετικό κανάλι. Αν και αυτό ισχύει, ο μηχανικός πρέπει να είναι σίγουρος ότι χρησιμοποιεί κανάλια που δεν επικαλύπτονται.

Με βάση το καθορισμένο σχέδιο καναλιών και για τον ETSI και για τη Βόρεια Αμερική, τρία μη επικαλυπτόμενα κανάλια μπορούν να χρησιμοποιηθούν στην ίδια περιοχή χωρίς παρεμβολή μεταξύ τους. Αν και υπάρχουν papers, σχετικά με τη δυνατότητα να χρησιμοποιηθούν τέσσερα ή ακόμα και πέντε χωριστά κανάλια, που ελαφρώς επικαλύπτονται, στην ίδια περιοχή, η βιομηχανία WLAN γενικά συστήνει τη χρήση του σχήματος των τριών μη επικαλυπτόμενων καναλιών (βλ. σχήμα 3-4).

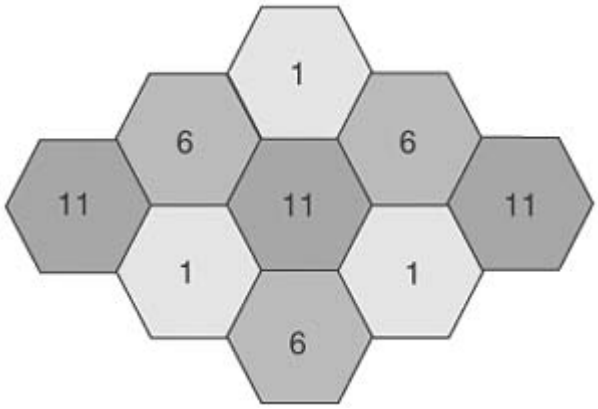


Εικόνα 1-17 Σχήμα καναλιών 802.11 στα 2,4 GHz

Αριθμός καναλιού	Συχνότητα	Βόρεια Αμερική	ETSI	Ιαπωνία
1	2.412	X	X	X
2	2.417	X	X	X
3	2.422	X	X	X
4	2.427	X	X	X
5	2.432	X	X	X
6	2.437	X	X	X
7	2.442	X	X	X
8	2.447	X	X	X
9	2.452	X	X	X
10	2.457	X	X	X

11	2.462	X	X	X
12	2.467		X	X
13	2.472		X	X
14	2.484			X

Χρησιμοποιώντας τα τρία μη επικαλυπτόμενα κανάλια, είναι δυνατή η επαναχρησιμοποίηση των κανάλια σε ένα περιστρεφόμενο σχέδιο και η προσεκτική ανάθεση σε παρακείμενες κυψέλες καναλιών που δεν παρεμβάλλονται (βλ. σχήμα 3-5).



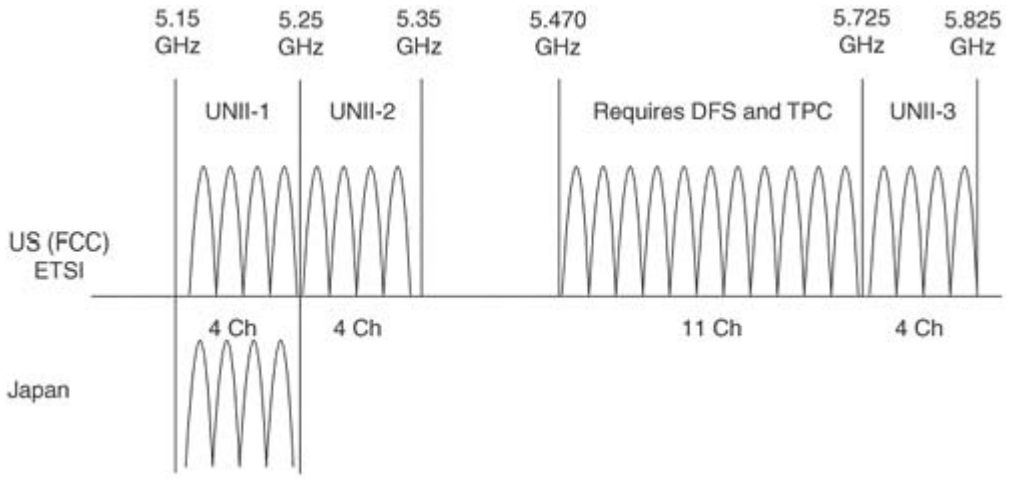
Εικόνα 1-18 Επαναχρησιμοποίηση καναλιών 802.11 στα 2,4 GHz

Η ζώνη συχνοτήτων 5-GHz

Η ζώνη των 5 GHz χρησιμοποιήθηκε αρχικά στην Ευρώπη για την προδιαγραφή ETSI HiperLAN, αλλά η έλξη για αυτήν την τεχνολογία ποτέ δεν φάνηκε να είναι μεγάλη και προσπεράστηκε από την ανάπτυξη ενός ανταγωνιστικού προτύπου 802.11 από το IEEE. Η προδιαγραφή 802.11a, που ολοκληρώθηκε το 1999, καθόρισε αρκετές διαφορετικές ομάδες καναλιών μέσα στη ζώνη των 5 GHz. Λόγω πολλών διαφορετικών κανονισμών σε όλο τον κόσμο με τη ζώνη των 5 GHz, οι επιτρεπόμενες κατά τόπους ομάδες καναλιών πρέπει να ελεγχθούν προσεκτικά.

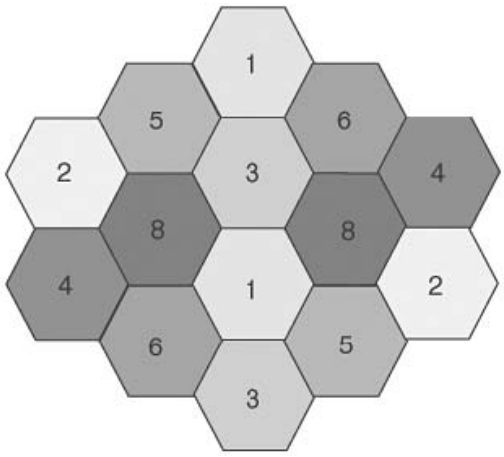
Έχει υπάρξει πρόσφατα μεγάλη δραστηριότητα στους ρυθμιστικούς οργανισμούς σχετικά με τις ζώνες WLAN των 5 GHz . Το 2003 υπήρξε μια συνεδρίαση των ρυθμιστικών οργανισμών όλου του κόσμου που συζήτησαν την αναθεώρηση πολλών από αυτούς τους κανονισμούς και το άνοιγμα νέων συχνοτήτων.

Όπως προαναφέρθηκε, η ζώνη των 5 GHz χωρίζεται σε αρκετές διαφορετικές ομάδες καναλιών. Στις Ηνωμένες Πολιτείες αυτοί αναφέρονται ως ζώνες εθνικής υποδομής πληροφοριών χωρίς άδεια (Unlicensed National Information Infrastructure - UNII). Οι τρεις ζώνες ή ομάδες UNII1, UNII2, και UNII3 επιτρέπουν λειτουργία στα φάσματα συχνοτήτων 5,215 ως 5,225 GHz, 5,225 ως 5,235 GHz και 5,725 ως 5,825 GHz, αντίστοιχα. Μετά από τις πρόσφατες αλλαγές στους κανονισμούς, μια νέα ζώνη συχνοτήτων είναι τώρα διαθέσιμη εκτεινόμενη από 5,470 έως 5.725 GHz (βλ. σχήμα 3-6). Η τελευταία αυτή ζώνη χρησιμοποιείται στον ευρωπαϊκό χώρο.



Εικόνα 1-19 Σχήμα καναλιών 802.11a στα 5 GHz

Συγκρινόμενη με τη ζώνη των 2,4 GHz, η ζώνη των 5 GHz προσφέρει τουλάχιστον οκτώ κανάλια. Αν και υπάρχει μια μικρή επικάλυψη στις πλευρικές ζώνες των συχνοτήτων, τα κανάλια αναφέρονται συνήθως ως μη επικαλυπτόμενα. Μερικοί μηχανικοί θεωρούν ότι δεν εμφανίζεται πρόβλημα κατά τη χρησιμοποίηση παρακείμενων καναλιών σε παρακείμενες κυψέλες' εντούτοις, συστήνεται να αποφεύγονται παρακείμενα κανάλια σε παρακείμενες κυψέλες (βλ. σχήμα 3-7).



Εικόνα 1-20 Επαναχρησιμοποίηση καναλιών 802.11a στα 5 GHz

Δυναμική επιλογή συχνοτήτων και έλεγχος ισχύος εκπομπής με το 801.11h

Η ζώνη ETSI των 5 GHz είναι πολύ ευρεία ζώνη, εκτεινόμενη από τα 5,15 GHz ως τα 5,7 GHz. Επειδή ένα μεγάλο μέρος αυτής της περιοχής είναι σε χρήση από άλλες υπηρεσίες ραδίων, η ρυθμιστική αρχή ETSI απαίτησε το συνυπολογισμό δύο χαρακτηριστικών, που δεν υπήρχαν στα αρχικά προϊόντα 802.11a. Αυτά τα δύο χαρακτηριστικά είναι δυναμική επιλογή συχνότητας (Dynamic Frequency Selection - DFS) και ο έλεγχος ισχύος εκπομπής (Transmit Power Control - TPC) και αποτελούν τα αρχικά χαρακτηριστικά της προδιαγραφής IEEE 802.11h.

Με την DFS, το σκεπτικό είναι ότι μια 802.11 συσκευή υποδομής ακούει αρχικά το σύνολο της ζώνης συχνοτήτων, που είναι διαθέσιμη σε αυτήν, και έπειτα αυτόματα επιλέγει το ελάχιστα κορεσμένο διαθέσιμο κανάλι. Η λογική πάλι πίσω από αυτό είναι ότι τμήματα της ζώνης των 5 GHz έχουν ανατεθεί για στρατιωτική χρήση και για συστήματα ραντάρ. Η ιδέα εδώ είναι ότι ακούγοντας

πρώτα πριν καθοριστεί ένα κανάλι για να λειτουργήσει επάνω, το WLAN δεν θα παρεμβάλει με επιβεβλημένους χρήστες. Δεύτερον, η διαθεσιμότητα ενός τέτοιου χαρακτηριστικού γνωρίσματος απλοποιεί τις εγκαταστάσεις σε επιχειρήσεις επειδή οι ίδιες οι συσκευές μπορούν (θεωρητικά) αυτόματα να βελτιστοποιήσουν το σχέδιο επαναχρησιμοποίησης καναλιών τους.

Το TPC είναι μια τεχνολογία που έχει χρησιμοποιηθεί στη βιομηχανία των κυψελοειδών τηλεφώνων για πολλά έτη. Με τον καθορισμό της ισχύος μετάδοσης του AP και του προσαρμοστή του πελάτη, είναι δυνατόν να διαμορφωθούν διαφορετικά μεγέθη περιοχής κάλυψης και, στην περίπτωση του πελάτη, να διατηρηθεί για μεγαλύτερο χρονικό διάστημα η ζωή της μπαταρίας. Οι συσκευές που δεν επιτρέπουν τη ρύθμιση των επιπέδων ισχύος έχουν συνήθως στατικές ρυθμίσεις και είναι εντελώς ανεξάρτητες η μια από την άλλη (AP και πελάτες). Παραδείγματος χάριν, ένα AP μπορεί να τεθεί σε μια χαμηλή ισχύ μετάδοσης των 5 mW ώστε να ελαχιστοποιηθεί το μέγεθος της κυψέλης, το οποίο αποδεικνύεται χρήσιμο σε περιοχές με υψηλή πυκνότητα χρηστών. Οι πελάτες, εντούτοις, θα μεταδίδουν σε προηγουμένως ορισθείσα ρύθμιση ισχύος, η οποία είναι πιθανότατα υψηλότερη ισχύ μετάδοσης από ό,τι απαιτείται για να διατηρηθεί η ένωση με το AP. Αυτό οδηγεί σε περιττή ενέργεια RF, που εκπέμπεται από τους πελάτες, δημιουργώντας ένα πιο υψηλό επίπεδο ενέργειας RF από το απαραίτητο έξω από την προορισμένη περιοχή κάλυψης του AP. Με το TPC, ο πελάτης και το AP ανταλλάσσουν πληροφορίες και έπειτα η συσκευή του πελάτη ρυθμίζει δυναμικά την ισχύ μετάδοσής της έτσι ώστε να χρησιμοποιεί μόνο αρκετή ενέργεια για να διατηρήσει την ένωση με το AP σε ένα δεδομένο ρυθμό διέλευσης δεδομένων. Το τελικό αποτέλεσμα αυτού είναι ότι ο πελάτης συμβάλλει λιγότερο σε παρεμβολή παρακείμενων κυψελών, κάτι που επιτρέπει πιο πυκνά WLANs υψηλής απόδοσης. Σαν δεύτερο όφελος, η χαμηλότερη ισχύς στον πελάτη παρέχει η μεγαλύτερη ζωή για την μπαταρία επειδή λιγότερη ισχύς χρησιμοποιείται από το ραδιόφωνο.

Η Συμμαχία Wi-Fi

Το Wi-Fi είναι μια εμπορική φίρμα που αναπτύσσεται από την WFA και σημαίνει WLAN για πολλούς χρήστες. Η ομάδα είναι αρμόδια για το όρο Wi-Fi (που είναι μια αποκοπή της ασύρματης πιστότητας - wireless fidelity) και, το πιο σημαντικό, ανεξάρτητη να ελέγχει τη διαλειτουργικότητα.

Το Wi-Fi περιγράφει τα προϊόντα WLAN που είναι βασισμένα στα πρότυπα IEEE 802.11 και προορίζεται να είναι ένα φιλικότερο προς το χρήστη όνομα με τον ίδιο τρόπο που το Ethernet και το Token Ring είναι φιλικότερα προς το χρήστη από τα IEEE 802.3 and 802.5, αντίστοιχα. Καμία άλλη οργάνωση δεν έχει κάνει τόσα πολλά για να οδηγήσει στην υιοθέτηση των τεχνολογιών WLAN. Με στόχο τη διαλειτουργικότητας μεταξύ των συσκευών βασισμένων στα πρότυπα 802.11b, τη WFA άρχισε ένα πρόγραμμα για να πιστοποιεί η διαλειτουργικότητα μεταξύ των συσκευών. Ιδρυθέν τον Αύγουστο του 1999 από τις 3Com, Aironet Wireless Communications, Harris Semiconductor (τώρα Intersil), Lucent Technologies (αργότερα Agere), Nokia και Symbol Technologies, το WFA έχει μεγαλώσει με πάνω από 200 μέλη. Προϊόντα όπως ανιχνευτές bar code , κάρτες PCMCIA, APs και ασύρματα συστήματα ψυχαγωγίας έχουν περάσει επιτυχώς τη δοκιμή διαλειτουργικότητας Wi-Fi και έχουν κερδίσει το δικαίωμα να φέρουν την ετικέτα Wi-Fi.

Άλλες Πιστοποιήσεις Wi-Fi

Άλλες δοκιμές έχουν αρχίσει επίσης να πραγματοποιούνται στο WFA. Υπάρχει τώρα μια προδιαγραφή ασφάλειας αποκαλούμενη προστατευμένη πρόσβαση Wi-Fi (Wi-Fi Protected Access - WPA) που ακολουθεί την προδιαγραφή ασφάλειας 802.11i και παρέχει μια δοκιμή για να εξασφαλίσει τη διαλειτουργικότητα μεταξύ των συσκευών κατά χρησιμοποίηση WPA.

Υπάρχει επίσης μια πιστοποίηση διαλειτουργικότητας QoS διαθέσιμη από το WFA, γνωστή ως πολυμέσα Wi-Fi (WMM), το οποίο χρησιμοποιεί μερικά χαρακτηριστικά που προσδιορίζονται από την ομάδα εργασίας 802.11e.

Ετικέτα Ικανοτήτων Wi-Fi

Σήμερα μια συσκευή Wi-Fi φέρει ένα λογότυπο πιστοποίησης Wi-Fi και η συσκευασία φέρει επίσης μια ετικέτα ικανοτήτων (βλ. σχήμα 1-4). Αυτή η ετικέτα καθορίζει ποια πιστοποίηση έχει περάσει επιτυχώς η συσκευή, όπως 802.11a, 802.11b, WPA και τα λοιπά. Ένας πελάτης που υλοποιεί ένα δίκτυο WLAN με εξοπλισμό από διαφορετικούς κατασκευαστές ενθαρρύνεται να απαιτήσει να έχουν περάσει όλες οι συσκευές τη δοκιμή και την επαλήθευση διαλειτουργικότητας και να έχουν λάβει το λογότυπο Wi-Fi.

Εικόνα 1-21 Ετικέτα ικανοτήτων Wi-Fi

ΚΕΦΑΛΑΙΟ 2ο
Σχεδίαση ενός πολυκυψελικού δικτύου Wi-Fi

Κεραίες

Η κατάλληλη χρήση των κεραιών μπορεί να βελτιώσει την απόδοση ενός WLAN εντυπωσιακά. Στην πραγματικότητα, οι κεραίες είναι πιθανώς ο ευκολότερος τρόπος να βελτιωθεί η απόδοση ενός WLAN.

Όλες οι κεραίες έχουν τρεις θεμελιώδεις ιδιότητες:

- Κέρδος: Ένα μέτρο της αύξησης ισχύος
- Κατευθυντικότητα: Η μορφή του διαγράμματος ακτινοβολίας
- Πόλωση: Η γωνία κατά την οποία η ενέργεια εκπέμπεται στον αέρα

Και οι τρεις αυτές ιδιότητες συζητούνται λεπτομερώς παρακάτω.

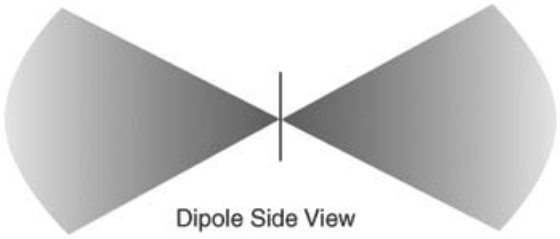
Κέρδος

Το κέρδος είναι το ποσό αύξησης στην ισχύ που μια κεραία εμφανίζεται να προσθέτει σε ένα σήμα RF. Υπάρχουν διαφορετικές μέθοδοι για τη μέτρηση του κέρδους, ανάλογα με το σημείο αναφοράς που επιλέγεται.

Το βασικό κέρδος κεραιών εκτιμάται σε σύγκριση με τις ισοτροπικές κεραίες ή κεραίες διπόλων. Μια ισοτροπική κεραία είναι μια θεωρητική κεραία με ένα ομοιόμορφο τρισδιάστατο διάγραμμα ακτινοβολίας. Η εκτίμηση dBi χρησιμοποιείται για να συγκρίνει το επίπεδο ισχύος μιας δεδομένης κεραίας με τη θεωρητική ισοτροπική κεραία (έτσι προκύπτει η χρήση του i στο dBi). Πολλοί ρυθμιστικοί οργανισμοί χρησιμοποιούν το dBi για τον καθορισμό των επιπέδων ισχύος στους κανονισμούς που καλύπτουν τις κεραίες WLAN. Οι περισσότεροι μαθηματικοί υπολογισμοί

που περιλαμβάνουν απώλειες διάδοσης χρησιμοποιούν επίσης την εκτίμηση dBi. Μια ισοτροπική κεραία λέγεται ότι έχει μια εκτίμηση ισχύος 0 dBi.

Σε αντίθεση με τις ισοτροπικές κεραίες, οι κεραίες διπόλων είναι φυσικές κεραίες που είναι τυποποιημένες σε πολλά προϊόντα WLAN. Οι κεραίες διπόλων έχουν ένα διαφορετικό διάγραμμα ακτινοβολίας συγκρινόμενες με μια ισοτροπική κεραία. Το διάγραμμα ακτινοβολίας διπόλων είναι 360 βαθμοί στο οριζόντιο επίπεδο και συνήθως περίπου 75 βαθμοί στο κάθετο επίπεδο (υποθέτοντας φυσικά ότι το δίπολο στέκεται κατακόρυφα) (βλ. σχήμα 2-1). Επειδή η ακτίνα συγκεντρώνεται ελαφρώς, οι κεραίες διπόλων έχουν ένα κέρδος σε σύγκριση με τις ισοτροπικές κεραίες στο οριζόντιο επίπεδο. Οι κεραίες διπόλων λέγεται ότι έχουν ένα κέρδος 2,14 dBi (σε σύγκριση με μια ισοτροπική κεραία).



Εικόνα 2-1 Διάγραμμα ακτινοβολίας διπόλου

Μερικές κεραίες εκτιμώνται σε σύγκριση με τις κεραίες διπόλων. Αυτό δείχνεται από το επίθεμα dBd. Ως εκ τούτου, οι κεραίες διπόλων έχουν ένα κέρδος 0 dBd (0 dBd = 2,14 dBi).

Για τη μετατροπή οποιουδήποτε αριθμού από dBd σε dBi, προστίθενται ακριβώς 2,14 στον αριθμό dBd. Παραδείγματος χάριν μια κεραία 3dBd θα είχε μια εκτίμηση 5,14 dBi.

Ιδιότητες κατευθυντικότητας

Οποιαδήποτε κεραία, εκτός από μια ισοτροπική κεραία (θεωρητικά τέλεια κεραία που ακτινοβολεί εξίσου σε όλες τις κατευθύνσεις), έχει κάποιο είδος διαγράμματος ακτινοβολίας. Αυτό σημαίνει ότι ακτινοβολεί την ενέργεια σε ορισμένες κατευθύνσεις περισσότερο από άλλες.

Στο RF πρέπει συνήθως να θυσιαστεί κάτι για να κερδηθεί κάτι άλλο. Όσον αφορά το κέρδος κεραιών, αυτό εμφανίζεται υπό μορφή περιοχής κάλυψης ή αυτό που είναι γνωστό ως εύρος δέσμης. Δεδομένου ότι το κέρδος μιας κεραίας ανεβαίνει, το εύρος δέσμης (συνήθως) πηγαίνει κάτω.

Η κάλυψη μιας ισοτροπικής κεραίας μπορεί να θεωρηθεί ως τέλειο στρογγυλό μπαλόνι. Επεκτείνεται σε όλες τις κατευθύνσεις εξίσου. Το μέγεθος του μπαλονιού αντιπροσωπεύει το ποσό ισχύος RF που ο πομπός στέλνει στις κεραίες, και η κεραία μετατρέπει την ισχύ σε ακτινοβολούσα ισχύ RF. Η ολική ισχύς που ακτινοβολείται από την κεραία δεν αυξάνεται, απλά επαναπροσανατολίζεται. Όπως συνέβη με την κεραία διπόλων που συζητήθηκε νωρίτερα σε αυτό το κεφάλαιο, αυτό το τέλειο στρογγυλό μπαλόνι της ενέργειας που μια ισοτροπική κεραία παρέχει γίνεται κάτι τελείως διαφορετικό στη μορφή.

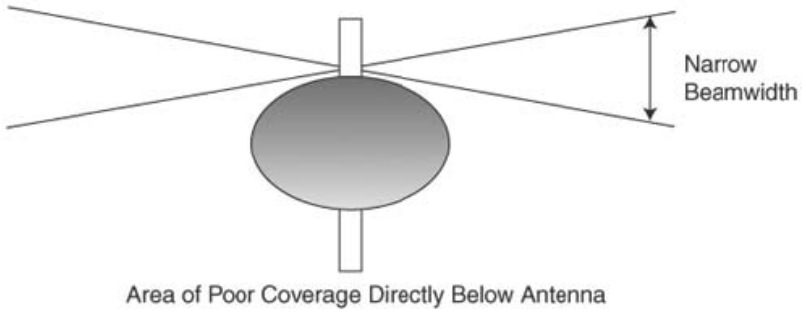
Ομοιοκατευθυντικές κεραίες

Μια κεραία omni σχεδιάζεται για να παρέχει ένα διάγραμμα ακτινοβολίας 360^{o} στο οριζόντιο επίπεδο. Αυτός ο τύπος κεραίας χρησιμοποιείται όταν απαιτείται η κάλυψη σε όλες τις κατευθύνσεις που περιβάλλουν τις κεραίες. Όταν μια κεραία omni σχεδιάζεται για να έχει υψηλότερο κέρδος, οδηγεί σε απώλεια κάλυψης σε ορισμένες περιοχές.

Φανταστείτε πάλι, το μπαλόνι της ενέργειας μιας ισοτροπικής κεραίας, η οποία επεκτείνεται από την κεραία εξίσου σε όλες τις κατευθύνσεις. Τώρα φανταστείτε άσκηση πίεσης στην κορυφή και το κατώτατο σημείο του μπαλονιού. Αυτό αναγκάζει το μπαλόνι να επεκταθεί σε μια εξωτερική κατεύθυνση, που καλύπτει περισσότερη περιοχή στο οριζόντιο επίπεδο, αλλά που μειώνει την

περιοχή κάλυψης επάνω και κάτω από την κεραία. Αυτό παράγει ένα υψηλότερο κέρδος, αφού η κεραία εμφανίζεται να επεκτείνεται σε μια μεγαλύτερη περιοχή κάλυψης. Όσο ψηλότερο είναι το κέρδος σε μια κεραία τόσο μικρότερο είναι το κάθετο εύρος δέσμης.

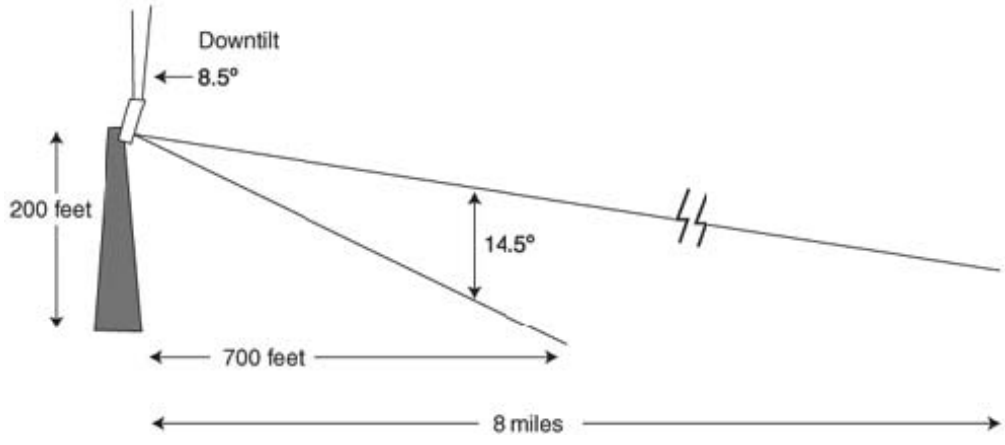
Εάν συνεχιστεί η πίεση στις άκρες του μπαλονιού, αυτό θα οδηγήσει σε μια επίδραση τηγανιτών (pancake effect) με πολύ στενό κάθετο εύρος δέσμης, αλλά πολύ μεγάλη οριζόντια κάλυψη (βλ. σχήμα 2-2). Αυτός ο τύπος σχεδίου κεραιών μπορεί να προσφέρει πολύ μεγάλες αποστάσεις επικοινωνιών, αλλά έχει ένα μειονέκτημα: φτωχή κάλυψη κάτω από την κεραία.



Εικόνα 2-2 Διάγραμμα ακτινοβολίας ομοιοκατευθυντικής κεραίας υψηλού κέρδους

Σε μερικές περιπτώσεις, το κέρδος μιας κεραίας μπορεί να είναι αρκετά υψηλό και τα διαγράμματα ακτινοβολίας τόσο μικρά, ώστε ακόμα και μικρές κινήσεις της κεραίας (από τον αέρα παραδείγματος χάριν) μπορούν να αναγκάσουν το σήμα να απομακρυνθεί από τον προοριζόμενο στόχο και να χαθεί η επικοινωνία. Για αυτόν τον λόγο, κεραίες εξαιρετικά υψηλού κέρδους τοποθετούνται συνήθως σε μια πολύ ισχυρή και μόνιμη δομή και δεν χρησιμοποιούνται σχεδόν ποτέ σε ένα κινητό ή φορητό περιβάλλον.

Με τις κεραίες omni υψηλού κέρδους, αυτό το πρόβλημα μπορεί να λυθεί μερικώς με το σχεδιασμό αυτού που αποκαλείται χαμηλωμένης κλίσης (downtilt). Μια κεραία που χρησιμοποιεί downtilt έχει σχεδιαστεί να ακτινοβολεί σε μια μικρή γωνία από το κατακόρυφο στοιχείο. Το χαμηλωμένη κλίση βοηθά στην τοπική κάλυψη αλλά μειώνει την αποτελεσματικότητα της ικανότητας μεγάλου εύρους (βλ. σχήμα 2-3). Οι κυψελοειδείς κεραίες χρησιμοποιούν downtilt.



Εικόνα 2-3 Χαμήλωμα κλίσης κεραίας

Κατευθυντικές κεραίες

Οι κατευθυντικές κεραίες μπορούν να χρησιμοποιηθούν για να παρέχουν μακρύτερο εύρος σε ορισμένες κατευθύνσεις και για να απομονώσουν το ράδιο από άλλα σήματα. Υπάρχει μια ευρεία γκάμα διαθέσιμων κατευθυντικών κεραιών. Όπως έχει προαναφερθεί, μια κεραία δεν προσθέτει οποιαδήποτε πρόσθετη ισχύ στο σήμα' αντ' αυτού, επαναπροσανατολίζει την ενέργεια από μια κατεύθυνση και στρέφει την ενέργεια σε μια συγκεκριμένη κατεύθυνση. Αυτό οδηγεί σε περισσότερη ενέργεια σε ορισμένες κατευθύνσεις και λιγότερη ακτινοβολούσα ενέργεια σε άλλες κατευθύνσεις. Δεδομένου ότι το κέρδος μιας κατευθυντικής κεραίας αυξάνεται, η ολική περιοχή κάλυψης συνήθως μειώνεται. Κοινοί τύποι κατευθυντικών κεραιών WLAN αποτελούν οι παραβολικές κεραίες, οι κεραίες patch και οι κεραίες Yagi.

Πόλωση

Δύο επίπεδα χρησιμοποιούνται στις ακτινοβολίες RF: το επίπεδο E και H. Το επίπεδο E (ηλεκτρικό πεδίο) καθορίζει τον προσανατολισμό των ραδιοκυμάτων όπως ακτινοβολούνται από την κεραία. Εάν το E είναι κάθετο στη γήινη επιφάνεια, αναφέρεται ως κάθετα πολωμένο. Στα συστήματα WLAN, παραδείγματος χάριν, μια ομοιοκατευθυντική κεραία είναι συνήθως μια κάθετα πολωμένη κεραία.

Οι οριζόντια πολωμένες (γραμμικές) κεραίες έχουν το ηλεκτρικό πεδίο τους παράλληλο στη γήινη επιφάνεια. Τα WLANs σπάνια χρησιμοποιούν οριζόντια πολωμένες κεραίες, εκτός από ορισμένα υπαίθρια, από σημείο σε σημείο συστήματα.

Παραδείγματα κεραιών

Στο υποκεφάλαιο αυτό περιλαμβάνονται οι πιο κοινές κεραίες WLAN που χρησιμοποιούνται σήμερα στη βιομηχανία.

Κεραια Patch

Μια κεραία patch είναι συνήθως μικρή και κάπως επίπεδη και σχεδιάζεται συνήθως για να τοποθετηθεί εφαπτόμενα σε έναν τοίχο ή σε ένα μικρό υποστήριγμα. Έχει ένα εύρος δέσμης που είναι λιγότερο από 180^{o} και αναφέρεται μερικές φορές ως ημισφαιρική κεραία.

Κεραια Panel

Μια κεραία panel (μερικές φορές επίσης αποκαλούμενη ως τομεϊκή (sectorized) κεραία) είναι παρόμοια με μια κεραία patch, αλλά έχει γενικά ένα υψηλότερο κέρδος και είναι φυσικά μεγαλύτερη. Πολλές φορές μια κεραία panel έχει έναν ρυθμιζόμενο πίσω ανακλαστήρα που μπορεί να χρησιμοποιηθεί για να αλλάξει το εύρος δέσμης καθώς επίσης και υποστηρίγματα τοποθέτησης που μπορούν να ρυθμιστούν για χαμηλωμένη κλίση (downtilt).

Οι κεραίες Panel χρησιμοποιούνται συνήθως υπαίθρια και μπορούν να έχουν κέρδη που κυμαίνονται από 5 dBi ως περισσότερα από 20 dBi. Μπορούν να χρησιμοποιηθούν ως ενιαία κεραία ή σε πολλαπλάσια για να καλύψουν μια μεγαλύτερη περιοχή.

Κεραια Yagi

Μια κεραία Yagi έχει μια σειρά από μικρά στοιχείων, που αποκαλούνται ανακλαστήρες ή διευθυντές, και ένα ενεργό στοιχείο. Αυτοί τοποθετούνται σε μια ευθεία γραμμή και κατευθύνουν την ενέργεια σε μια δεδομένη κατεύθυνση. Γενικά οι κεραίες Yagi έχουν αρκετά υψηλό κέρδος. Όσο περισσότερους ανακλαστήρες και διευθυντές έχει μια Yagi, τόσο υψηλότερο είναι κέρδος της. Εξ' αιτίας του μικρού μήκους κύματος για τις συχνότητες που χρησιμοποιούνται στα συστήματα WLAN, τα στοιχεία είναι αρκετά μικρά και οι περισσότερες Yagi που χρησιμοποιούνται για 2.4 ή 5-

GHz περιέχουν κάποιο τύπο κάλυψης που να προστατεύει τα τμήματα της κεραίας από τον καιρό και να παρέχει περισσότερη δομική δύναμη.

Οι κεραίες Yagi μπορούν να κυμανθούν σε κέρδος από 5 dBi μέχρι 17 dBi ή περισσότερο.

Κεραία πιάτο

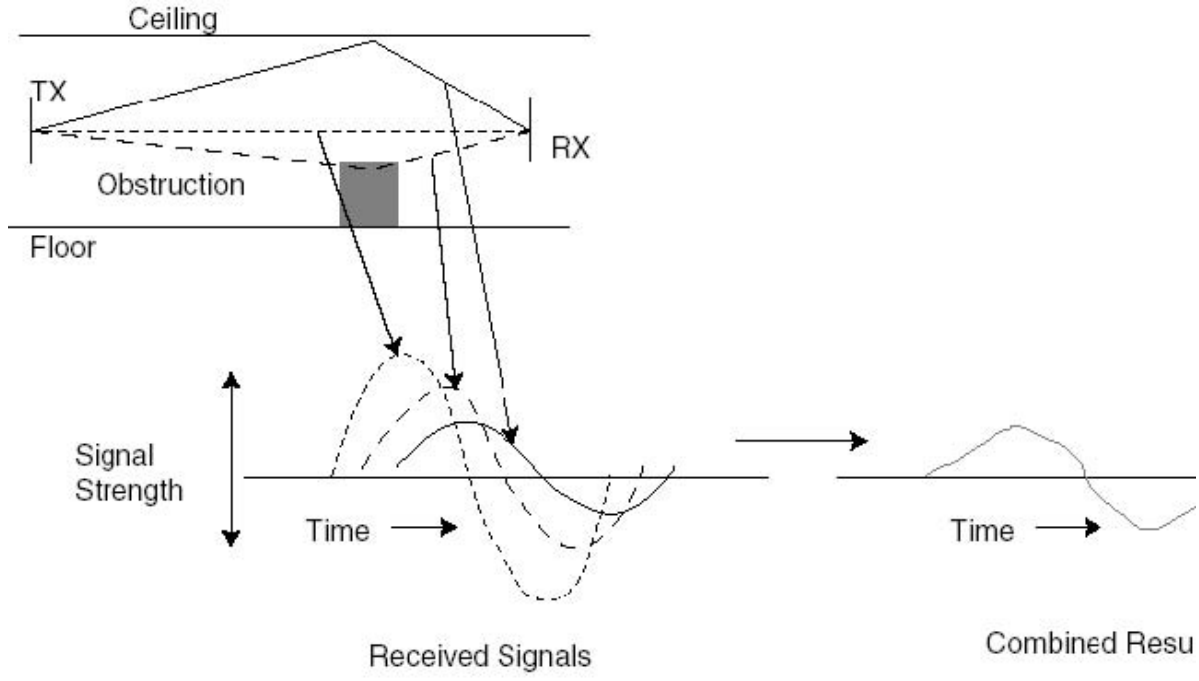
Υπάρχουν δύο κύριοι τύποι κεραιών πιάτων: το παραβολικό και πιάτο πλέγματος. Το παραβολικό πιάτο περιέχει έναν ανακλαστήρα που είναι στερεός στην κατασκευή και ένα οδηγημένο ή ενεργό στοιχείο που υποστηρίζεται στο κέντρο του ανακλαστήρα. Αυτά είναι παρόμοια με αυτά που χρησιμοποιούνται ως μια τυποποιημένη δορυφορική κεραία TV, εκτός από την τοποθέτηση διαφορετικού ενεργού στοιχείου ειδικού για WLAN.

Η κεραία πιάτου πλέγματος είναι πολύ παρόμοια με την παραβολική κεραία, εκτός από το ότι ο ανακλαστήρα δεν είναι στερεός. Αποτελείται από μια δομή πλέγματος που επιτρέπει στον αέρα και τη βροχή να τη διαπεράσει. Αυτό παρέχει λιγότερη αντίσταση στον αέρα και επομένως απαιτεί μια μικρότερη δομή στήριξης.

Διαφορική εκπομπή και λήψη

Τα συστήματα διαφορικών κεραιών χρησιμοποιούνται για να υπερνικηθεί ένα φαινόμενο γνωστό ως παραμόρφωση ή εξασθένιση πολλαπλών διαδρομών (multipath distortion or multipath fading). Χρησιμοποιεί δύο ίδιες κεραίες, που εντοπίζονται σε μια μικρή απόσταση, για να παρέχει κάλυψη στην ίδια φυσική περιοχή.

Η εξασθένιση πολλαπλών διαδρομών είναι μια μορφή RF παρεμβολής που μπορεί να εμφανιστεί όταν ένα ραδιοσήμα έχει περισσότερες από μια διαδρομές μεταξύ της κεραίας εκπομπής και της κεραίας λήψης. Περιβάλλοντα με υψηλή πιθανότητα εξασθένισης πολλαπλών διαδρομών αποτελούν θέσεις όπως τα υπόστεγα αερολιμένων, οι χώροι κατασκευής, τα κέντρα διανομής και άλλες θέσεις όπου η κεραία εκτίθεται σε μεταλλικούς τοίχους, οροφές, ράφια ή άλλα μεταλλικά στοιχεία που ανακλούν τα σήματα και δημιουργούν συνθήκες πολλαπλών διαδρομών (βλ. σχήμα 2-4).

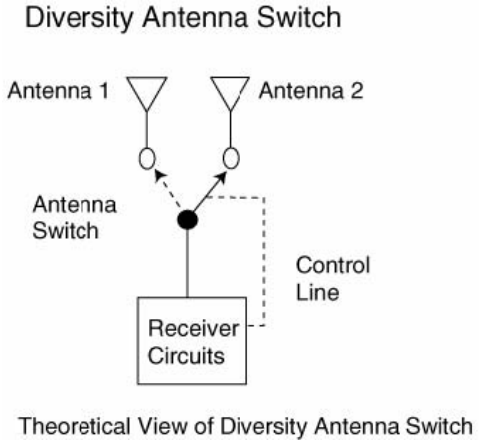


Εικόνα 2-4 Διαδρομές πολλαπλών σημάτων

Όταν μια κεραία εκπέμπει, ακτινοβολεί ενέργεια RF σε περισσότερες από μια καθορισμένες κατευθύνσεις. Αυτό αναγκάζει το RF να μετακινηθεί μεταξύ της κεραίας εκπομπής και λήψης στην αμεσότερη (επιθυμητή) πορεία ανακλώντας ή αναπηδώντας από μεταλλικές και άλλες RF-ανακλούσες επιφάνειες. Η διαδικασία ανάκλασης των κυμάτων RF προκαλεί την εμφάνιση διαφόρων φαινόμενων. Κατ' αρχάς, τα ανακλασμένα κύματα RF ταξίδεψαν μακρύτερα από το επιθυμητό άμεσο κύμα RF. Αυτό σημαίνει ότι τα ανακλασμένα κύματα θα φτάσουν στη κεραία λήψης χρονικά αργότερα. Δεύτερον, λόγω της μακρύτερης διαδρομής μετάδοσης, το ανακλασμένο σήμα χάνει περισσότερη ενέργεια RF από το άμεσου διαδρομής σήμα. Τρίτον, το σήμα θα χάσει κάποια ενέργεια ως αποτέλεσμα της ανάκλασης. Στο τέλος, το επιθυμητό κύμα, μαζί με πολλά ανακλασμένα κύματα, συνδυάζεται στο δέκτη. Αυτά τα διαφορετικά κύματα είναι δυνατόν όχι μόνο να υπερτίθενται αλλά και να αλληλοεξουδετερώνονται προκαλώντας τη διαστρέβλωση του επιθυμητού κύματος και έχοντας επιπτώσεις στην ικανότητα λήψης-αποκωδικοποίησης. Σε μερικές περιπτώσεις, εάν τα σήματα παραλαμβάνονται με ίση ισχύ, αλλά καθυστερημένα με τέτοιο τρόπο ώστε να είναι αντίθετα στην πολικότητα, θα εξουδετερώσουν εντελώς το ένα το άλλο, κάτι που δημιουργεί συνολικά απουσία λαμβανόμενου σήματος από το δέκτη. Αυτό είναι γνωστό ως μηδενικό πολλαπλών διαδρομών (multipath null).

Όταν αυτά τα ανακλασμένα σήματα συνδυάζονται στο δέκτη, αν και η RF ενέργεια (ισχύς σημάτων) μπορεί να είναι υψηλή, τα δεδομένα δεν είναι ανακτήσιμα. Η αλλαγή της θέσης της κεραίας μπορεί να αλλάξει αυτές τις αντανακλάσεις και να μικραίνει την πιθανότητα της πολλαπλών διαδρομών παρέμβασης. Επειδή ένα σημείο (AP) πρόσβασης δεν μπορεί να κινήσει φυσικά την κεραία του, πολλά έχουν σχεδιαστεί με δύο θύρες κεραιών. Το ράδιο εκτελεί μια αξιολόγηση κάθε θύρας κεραίας και επιλέγει να χρησιμοποιήσει την κεραία με την καλύτερη λήψη.

Το σύστημα κεραιών διαφορικής εκπομπής και λήψης περιλαμβάνει δύο κεραίες που συνδέονται με έναν διακόπτη RF, ο οποίος συνδέεται στη συνέχεια με το δέκτη (βλ. σχήμα 2-5). Ο δέκτης μεταστρέφεται περιοδικά μεταξύ των κεραιών όταν αφουγκράζεται ένα έγκυρο σήμα.



Εικόνα 2-5 Διακόπτης διαφορικής κεραίας

Να σημειωθεί ότι αυτή η αλλαγή του διακόπτη γίνεται εξαιρετικά γρήγορα. Το AP δειγματοληπτεί μέρος της επικεφαλίδας και αποφασίζει να χρησιμοποιήσει την καλύτερη κεραία για να λάβει τα δεδομένα του πελάτη και χρησιμοποιεί έπειτα την ίδια κεραία κατά τη μετάδοση πίσω στον πελάτη. Εάν ο πελάτης δεν αποκρίνεται, το AP θα προσπαθήσει έπειτα να στείλει τα δεδομένα από την άλλη κεραία.

Καλώδια

Η κεραία πρέπει να τοποθετηθεί σε μια θέση που χρησιμοποιεί το διάγραμμα ακτινοβολίας της στη μέγιστη απόδοση για τους χρήστες. Σε μερικές περιπτώσεις, αυτή η θέση δεν είναι ιδανική για να τοποθετηθεί το AP. Επομένως, επιδιώκεται μερικές φορές να χωριστεί η κεραία από το AP ή τη ραδιοσυσκευή. Αυτό μπορεί να οφείλεται στην ανάγκη να τοποθετηθεί η κεραία υπαίθρια και να κρατηθεί το AP στο εσωτερικό ή να τοποθετηθεί το AP πάνω από το ταβάνι και να τοποθετηθεί η κεραία κάτω από αυτό.

Αν και αυτό φαίνεται να είναι ένα τετριμμένο θέμα, δεν είναι πραγματικά. Η καλωδίωση εισάγει απώλειες στο σύστημα, μειώνοντας το επίπεδο σημάτων από το πομπό στην κεραία, καθώς επίσης και μειώνοντας το επίπεδο σημάτων από την κεραία προς το δέκτη. Και στις δύο περιπτώσεις, αυτό έχει μια δραματική επίδραση στην περιοχή κάλυψης RF.

Καλώδιο σχεδιασμένο να μεταφέρει RF γιατί WLAN είναι το ομοαξονικό καλώδιο και πρέπει να επιλεχτεί για να ταιριάξει με την εμπέδηση του πομπού και της κεραίας. Ουσιαστικά όλα τα συστήματα WLAN χρησιμοποιούν σύνθετη αντίσταση κεραιών ίση με 50 Ohm και το καλώδιο που επιλέγεται πρέπει να ταιριάζει με αυτήν την τιμή.

Ένα κύμα που ταξιδεύει είτε μέσω ενός καλωδίου είτε μέσω του αέρα έχει ένα διακριτικό φυσικό χαρακτηριστικό: το μήκος κύματός του. Μια σχέση που εμφανίζεται στο RF είναι ότι καθώς οι ταλαντώσεις ή η συχνότητα ενός κύματος γίνεται γρηγορότερη, τότε το μήκος κύματος γίνεται πιο μικρό.

Καθώς οι συχνότητες των σημάτων αλλάζουν, αυτά επηρεάζονται διαφορετικά από τον περιβάλλοντα χώρο. Σε ένα καλώδιο, καθώς τα ηλεκτρόνια ταξιδεύουν μέσω του αγωγού συναντούν αντίσταση. Καθώς η συχνότητα εκείνου του ηλεκτρικού σήματος αυξάνεται, τα ηλεκτρόνια στο καλώδιο κινούνται ολοένα και γρηγορότερα. Τείνουν να κινηθούν προς την επιφάνεια του αγωγού, πράγμα το οποίο καλείται επιδερμική επίδραση (skin effect). Αυτό ουσιαστικά αυξάνει την αντίσταση στο ταξίδι των ηλεκτρονίων (επειδή χρησιμοποιούν μόνο το δέρμα, ή το εξωτερικό μέρος, του καλωδίου), και επομένως μειώνει το ποσό ενέργειας που φθάνει στο τέλος του καλωδίου. Για την αντιστάθμιση αυτού του skin effect, πολλά ομοαξονικά καλώδια, που έχουν σχεδιαστεί για μικροκυματικές ή υψηλότερες συχνότητες χρησιμοποιούν καλώδια σημαντικής φυσικής διαμέτρου για χαμηλότερη απώλεια.

Πολλοί τύποι καλωδίων κατάλληλοι για περιβάλλοντα WLAN είναι διαθέσιμοι σήμερα. Ο παρακάτω πίνακας παρουσιάζει μερικούς από τους χαρακτηριστικούς τύπους καλωδίων, που μπορούν να χρησιμοποιηθούν, και τις τιμές των ενεργειακών απωλειών που συνδέονται με αυτά τα καλώδια.

Κωδικός καλωδίου	**Μέγεθος (cm)**	**Εξασθένιση (dB) / 10m**		**Μέση Ισχύς (kW)**	
		2.4 GHz	5.7 GHz	2.4 GHz	5.7 GHz
RG-58	0.4953	8,1288	13,3547	0,05	0,03
LMR400	1.0287	2,1703	3,5154	0,34	0,21
LMR600	1.27	1,419	2,3576	0,53	0,32

Υπολογιστής απωλειών χειρισμού ισχύος για μια πλούσια γκάμα από τύπους καλωδίων μπορεί να βρεθεί στην εξής ιστοσελίδα: http://www.timesmicrowave.com/cgi-bin/calculate.pl.

RF Διάδοση

Καθώς τα κύματα RF ταξιδεύουν μέσω του αέρα έχουν επίσης την αντίσταση στη μετακίνηση γνωστή ως απώλεια διαδρομής. Καθώς η συχνότητα αλλάζει, αλλάζει και το μήκος

κύματος. Αυτά είναι μεγέθη αντιστρόφως ανάλογα και μπορούν να μετρηθούν με τον ακόλουθο τύπο $\lambda = c/f$.

Καθώς η συχνότητα αυξάνεται στο εύρος των ultrahigh συχνοτήτων (UHF) και έπειτα στις μικροκυματικές συχνότητες (που χρησιμοποιούνται για WLANs), οι απώλειες από την ατμόσφαιρα αυξάνονται, οι οποίες με τη σειρά τους μειώνουν την ενέργεια που μεταφέρεται. Το τελικό αποτέλεσμα είναι πιο μικρή ραδιοκάλυψη. Αυτός είναι ο κύριος λόγος που ένα σήμα WLAN 5 GHz, που χρησιμοποιεί την ίδια ισχύ εκπομπής και κέρδος κεραίας με ένα WLAN σήμα των 2.4 GHz, έχει μικρότερο εύρος.

Υπάρχουν πολλά ζητήματα που κάποιος πρέπει να εξετάσει προτού να μπορέσει να αρχίσει το κομμάτι έρευνας τοποθεσίας για το WLAN δίκτυο. Μια τέτοια παράμετρος είναι η συχνότητα που θα χρησιμοποιηθεί. Ένας άλλος παράγοντας που πρέπει να καθοριστεί είναι ο ελάχιστος αποδεκτός ρυθμός δεδομένων για τους χρήστες. Και οι δύο παράμετροι έχουν επιπτώσεις στην έρευνα της τοποθεσίας και τις ολική ικανότητα κάλυψης.

Συχνότητα εναντίον Κάλυψης

Από φυσικής πλευράς, η απόσταση της μετάδοσης είναι μια σημαντική παράμετρος της ασύρματης τεχνολογίας. Με τις υπόλοιπες μεταβλητές σταθερές, καθώς η συχνότητα αυξάνεται, μειώνεται το εύρος κάλυψης. Καταρχάς, όσο υψηλότερη είναι η συχνότητα, τόσο κοντύτερο είναι το μήκος κύματος του σήματος. Όσο πιο μικρό είναι το μήκος κύματος, τόσο υψηλότερες είναι οι απώλειες που προκαλούνται από την ατμόσφαιρα.

Δεύτερον, όσο μακρύτερο είναι το μήκος κύματος, τόσο καλύτερα ταξιδεύει το κύμα μέσω και γύρω από πράγματα. Κύματα μακρύτερου μήκους κύματος (και επομένως χαμηλότερη συχνότητα) τείνουν να διαπεράσουν τα αντικείμενα καλύτερα από τα κοντύτερου μήκους κύματος (και επομένως υψηλότερη συχνότητα) κύματα.

Επιπλέον, τα κύματα υψηλότερης συχνότητας είναι πιο τρωτά σε απορρόφηση από οικοδομικά υλικά, όπως ο τοίχος και το σκυρόδεμα.

Τέλος, όσο κοντύτερο είναι το μήκος κύματος, τόσο περισσότερα δεδομένα μπορεί το σήμα αυτό να μεταφέρει. Όσο γρηγορότερα ταλαντεύεται το κύμα, τόσο περισσότερη πληροφορία μπορεί να φέρει - κάθε κύκλος θα μπορούσε παραδείγματος χάριν να χρησιμοποιηθεί για να μεταφέρει ένα ψηφιακό bit, ένα "0" ή ένα "1".

Απορρόφηση Υλικών, Ανάκλαση και Διάθλαση

Άλλοι παράγοντες που έχουν δραστικές επιπτώσεις στο εύρος κάλυψης είναι η απορρόφηση, η ανάκλαση και η διάθλαση των σημάτων. Πολλά υλικά απορροφούν την ενέργεια RF. Στα 2,4 GHz, υλικό που περιέχει ένα υψηλό επίπεδο υγρασίας (όπως πολλά έγγραφο και το χαρτόνι) απορροφά το σήμα. Σε εγκαταστάσεις που περιέχουν έναν σημαντικό αριθμό μεταλλικών αντικειμένων (όπως μια αποθήκη εμπορευμάτων χάλυβα) εμφανίζονται αντανακλάσεις που μπορούν είτε να βοηθήσουν είτε να παρεμποδίσουν την κάλυψη δεδομένου του φαινόμενου πολλαπλών διαδρομών που δημιουργείται.

Πολλές φορές, τα υλικά δεν φαίνονται και είναι πέρα από τη γνώση μας, όπως η ενίσχυση χάλυβα στους τσιμεντένιους τοίχους και το δάπεδο, ορισμένοι τύποι βαψιμάτων στα παράθυρα που περιέχουν ιδιότητες μετάλλων ή ακόμα και μερικοί τύποι μονώσεων που χρησιμοποιούνται στους τοίχους. Ο μόνος αληθινός τρόπος να ανακαλυφθεί πώς το υλικό σε μια τοποθεσία έχει επιπτώσεις στο σήμα και την κάλυψη είναι να εκτελεστεί μια WLAN έρευνα της τοποθεσίας.

Τα ραδιοκύματα ανακλώνται εκτός από επίπεδες επιφάνειες και κατά την είσοδο σε διαφορετικά μέσα. Οι ανακλαστικές ιδιότητες της περιοχής όπου το WLAN πρόκειται να εγκατασταθεί είναι εξαιρετικά σημαντικές και μπορούν να καθορίσουν εάν ένα WLAN λειτουργεί ή όχι. Επιπλέον, τα βύσματα και στις δύο άκρες της γραμμής μετάδοσης, που πηγαίνει στην κεραία, πρέπει να σχεδιαστούν κατάλληλα και να εγκατασταθούν έτσι ώστε καμία αντανάκλαση των ραδιοκυμάτων να μην πραγματοποιείται. Εάν το καλώδιο και τα βύσματα δεν είναι κατάλληλα συνδεδεμένα, κάποια ενέργεια θα ανακλαστεί και θα αποτελέσει απώλεια στην ισχύ.

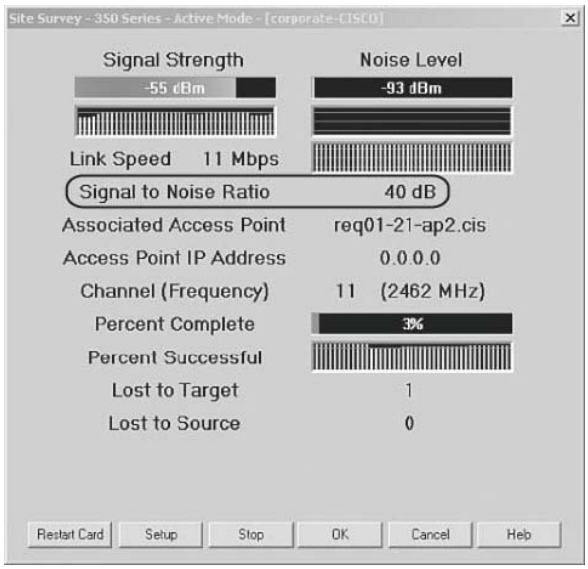
Ισχύς Σημάτων, Θόρυβος και Σηματοθορυβικός Λόγος

Η ισχύς των σημάτων, όπως έχει προαναφερθεί, είναι η τιμή του σήματος (που εκφράζεται συνήθως σε dBm για τα επίπεδα δεκτών στα συστήματα WLAN) που φτάνει στο δέκτη. Οι περισσότεροι δέκτες έχουν κάποια μέθοδο να απεικονίζουν αυτήν την τιμή. Είναι σημαντικό να γίνει κατανοητή και να καθοριστεί η ελάχιστη ισχύς σημάτων που είναι επιθυμητή για μια ιδιαίτερη εφαρμογή, για συγκεκριμένο ρυθμό διέλευσης δεδομένων και για τις ραδιοσυσκευές που χρησιμοποιούνται.

Ο περιβαλλοντικός θόρυβος RF εμφανίζεται στην ατμόσφαιρα. Δεδομένου ότι συνεχώς προστίθενται ηλεκτρονικές συσκευές στο περιβάλλον (ακόμη και οι υπολογιστές έχουν τώρα τις ταχύτητες bus που τρέχουν στο εύρος των GHz και εκπέμπουν ανεπιθύμητα RF σήματα), τα περιβαλλοντικά επίπεδα θορύβου RF βαθμιαία θεωρούνται υψηλότερα. Για να ληφθεί κατάλληλα ένα σήμα, το επιθυμητό σήμα πρέπει να έχει μια ισχύ σημάτων υψηλότερη από τον περιβαλλοντικό θόρυβο κατά ένα καθορισμένο ποσό, το οποίο θα ποικίλει από τον έναν τύπο δεκτών στο ένα άλλο και από έναν ρυθμό διέλευσης δεδομένων σε άλλο.

Το SNR είναι ακριβώς αυτό, ο λόγος του επιθυμητού σήματος (ισχύς σήματος) προς τον περιβαλλοντικό θόρυβος RF. Εκφράζεται σε dB και το απαραίτητο SNR θα ποικίλει με βάση τη διαμόρφωση, το ρυθμό διέλευσης δεδομένων και την ποιότητα του δέκτη.

Το σχήμα 2-6 παρουσιάζει την οθόνη εξόδου μίας συσκευής WLAN που παρουσιάζει την ισχύ του σήματος, το θόρυβο και το SNR.



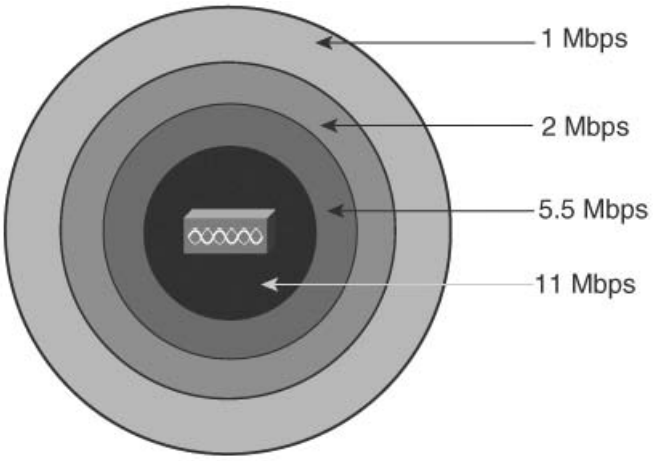
Εικόνα 2-6 Παράδειγμα SNR

Κάλυψη εναντίον Εύρους Ζώνης

Τα APs προσφέρουν στους πελάτες πολλαπλούς ρυθμούς διέλευσης δεδομένων για την ασύρματη σύνδεση. Για το 802.11b, το εύρος είναι από 1 έως 11 Mbps σε τέσσερις αυξήσεις: 1, 2, 5,5 και 11 Mbps. Το εύρος 802.11a είναι από 6 έως 54 Mbps σε οκτώ αυξήσεις: 6, 9, 12, 18, 24, 36, 48 και 54 Mbps. Τα προϊόντα 802.11g περιλαμβάνουν όλους αυτούς τους ρυθμούς. Επειδή οι ρυθμοί διέλευσης δεδομένων έχουν επιπτώσεις στο εύρος κάλυψης, η επιλογή των ρυθμών κατά τη διάρκεια του σταδίου σχεδιασμού είναι εξαιρετικά σημαντική. Οι κάρτες πελατών θα μεταπηδήσουν αυτόματα στο γρηγορότερο πιθανό ρυθμό του AP' το πώς αυτό γίνεται ποικίλλει από προμηθευτή σε προμηθευτή.

Επειδή κάθε ρυθμός διέλευσης δεδομένων έχει μια μοναδική κυψέλη κάλυψης (όσο υψηλότερος ο ρυθμός, τόσο μικρότερη η κυψέλη), ο ελάχιστος ρυθμός δεδομένων πρέπει να καθοριστεί στη φάση του σχεδιασμού. Τα μεγέθη κυψελών στο δεδομένο ρυθμό διέλευσης μπορούν να θεωρηθούν όπως οι ομόκεντροι κύκλοι με τους κύκλους υψηλότερων ρυθμών δεδομένων να έχουν τοποθετηθεί μέσα στον τομέα κάλυψης του αμέσως χαμηλότερου ρυθμού διέλευσης δεδομένων. Η επιλογή να προσφέρεται στους πελάτες μόνο ο υψηλότερος ρυθμός δεδομένων θα απαιτήσει έναν μεγαλύτερο αριθμό APs για να καλύψουν μια δεδομένη περιοχή. Επομένως, πρέπει να αναπτυχθεί ένας συμβιβασμός μεταξύ του απαραίτητου συνολικού ρυθμού διέλευσης δεδομένων και του γενικού κόστους του Wi-Fi συστήματος.

Ένα παράδειγμα του ρυθμού δεδομένων εναντίον του εύρους κάλυψης παρουσιάζεται στο σχήμα 2-7.



Εικόνα 2-7 Ρυθμός διέλευσης δεδομένων εναντίον εύρους κάλυψης

Διαμόρφωση εναντίον Κάλυψης

Ένας άλλος παράγοντας που μπορεί να έχει επιπτώσεις στο εύρος κάλυψης είναι το σχέδιο διαμόρφωσης. Ορισμένα σχέδια διαμόρφωσης όπως το OFDM έχουν την καλύτερη απόδοση σε ορισμένες περιοχές. Έστω ένα ιδιαίτερα ανακλαστικό περιβάλλον, παραδείγματος χάριν, όπου υπάρχει μεγάλη παρεμβολή σημάτων πολλαπλών διαδρομών. Το OFDM προσφέρει μια καλύτερη απόδοση σε αυτόν τον τύπο περιβάλλοντος λόγω του πολλαπλού φέροντος σχήματός του.

Ζητήματα Υπαίθριου RF

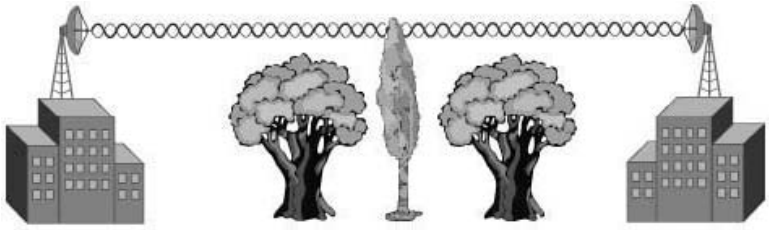
Κατά τη χρησιμοποίηση συστημάτων WLAN σε ένα υπαίθριο περιβάλλον, πολλοί άλλοι παράγοντες εισάγονται. Οι περισσότερες συσκευές WLAN δεν έχουν σχεδιαστεί για να τοποθετηθούν άμεσα υπαίθρια. Επομένως, είτε μια στεγανή περίφραξη πρέπει να χρησιμοποιηθεί, ή το AP θα τοποθετηθεί στο εσωτερικό και ένα καλώδιο θα χρησιμοποιηθεί για να συνδέσει το τελευταίο με την κεραία. Όπως δηλώθηκε νωρίτερα σε αυτό το κεφάλαιο, η χρήση των καλωδίων μπορεί να μειώσει εντυπωσιακά τη διαθέσιμη ισχύ που φθάνει στην κεραία και μπορεί να έχει επιπτώσεις στο ολικό εύρος.

Διάδοση και Απώλειες

Οι υπαίθριες συνδέσεις RF έχουν διαφορετικά χαρακτηριστικά διάδοσης από εκείνες σε εσωτερικούς χώρους. Οι υπολογισμοί μπορούν να παρέχουν ακριβείς πληροφορίες για την πιθανή απόδοση και την απόσταση. Τα εξής συμπεριλαμβάνονται σε υπολογισμούς για τον καθορισμό της υπαίθριας απόδοσης κάλυψης:

- Κέρδος κεραίας
- Ισχύς πομπού
- Απόδοση δέκτη
- Απώλειες καλωδίων
- Δομές του περιβάλλοντος

Οι τέσσερις πρώτες παράμετροι είναι γνωστές τιμές και καθορίζονται εύκολα. Εντούτοις, οι περιβαλλοντικές δομές, όπως τα κτήρια, τα δέντρα και τα λοιπά, και βασικά οτιδήποτε στη γραμμή θέας μεταξύ μιας κεραίας και μίας άλλης, μπορούν να προκαλέσουν σημαντικά προβλήματα στις υπαίθριες συνδέσεις RF. Για τις μακρινές επικοινωνίες που χρησιμοποιούν τις συχνότητες WLAN, μια γραμμή θέας μεταξύ των κεραιών είναι απαραίτητη για τη διατήρηση ποιοτικών RF συνδέσεων (βλ. σχήμα 2-8).

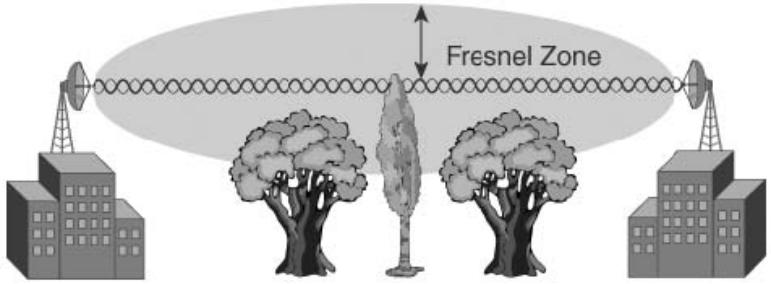


Εικόνα 2-8 Γραμμή οπτικής επαφής

Η καμπύλωση της Γης και η ζώνη Fresnel

Δύο άλλοι παράγοντες που έχουν επιπτώσεις στις υπαίθριες συνδέσεις είναι η ζώνη Fresnel και η καμπύλωση της γης. Οι ασύρματες συνδέσεις που μεταφέρουν δεδομένα σε μεγάλες αποστάσεις απαιτούν την πρόσθετη προσοχή να εξασφαλισθεί κατάλληλη οπτική επαφή. Είναι σημαντικό οι κεραίες να έχουν το κατάλληλο ύψος για να διατηρήσουν τη γραμμή θέας. Είναι σημαντικό να αναφερθεί ότι στην οπτική αυτή, επιπλέον της καμπύλωσης τη γης, θα πρέπει να προστεθεί η ανύψωση άλλων αντικειμένων (όπως κτήρια, δέντρα, λόφοι και τα λοιπά).

Ένας άλλος παράγοντας που εξετάζεται στις μεγάλες αποστάσεις είναι η ζώνη Fresnel, η οποία είναι μια ελλειπτική περιοχή που περιβάλλει την οπτική πορεία (βλ. σχήμα 2-9). Ποικίλλει ανάλογα με το μήκος της πορείας και τη συχνότητα του σήματος. Η ζώνη Fresnel μπορεί να υπολογιστεί και πρέπει να ληφθεί υπόψη κατά τη σχεδιασμό μιας ασύρματης σύνδεσης. Εάν η ζώνη Fresnel εμποδίζεται, η απαραίτητη γραμμή θέας δεν είναι καθαρή και η σύνδεση μπορεί να είναι αναξιόπιστη.



Εικόνα 2-9 Ζώνη Fresnel

Σύμφωνα με τα στάνταρ της βιομηχανίας απαιτείται να κρατείται τουλάχιστον το 60% της πρώτης ζώνης Fresnel καθαρό από εμπόδια. Αυτός ο υπολογισμός πρέπει να θεωρηθεί μόνο ως

αναφορά και δεν λαμβάνει υπόψη το φαινόμενο της διάθλασης από ιδιαίτερα ανακλαστικές επιφάνειες.

Παρακάτω υποενότητα του παρόντος κεφαλαίου καλύπτει αυτό το θέμα λεπτομερέστερα, όπου καλύπτονται σε βάθος οι υπαίθριες συνδέσεις RF γεφυρών (bridges).

Διάφορες αρχιτεκτονικές WLAN

Αρκετά WLANs που εισάγονται στην αγορά έχουν μια κεντρική διαχειριστική συσκευή, η οποία σε πολλές περιπτώσεις μεταγλωττίζεται ως ένα ασύρματο switch. Έναν ορισμό ενός switch δικτύων αποτελεί ο εξής (http://wi-fiplanet.webopedia.com):

Συντομογραφία του port-switching hub, αποτελεί έναν ειδικό τύπο hub που διαβιβάζει τα πακέτα στην κατάλληλη θύρα με βάση τη διεύθυνση του πακέτου. Συμβατικά hubs επανεκπέμπουν κάθε πακέτο σε κάθε θύρα. Επειδή τα switching hubs διαβιβάζουν κάθε πακέτο μόνο στην σωστή θύρα, παρέχουν πολύ καλύτερη απόδοση.

Με απλούς όρους, η "ανεξάρτητη περιοχή συγκρούσεων" προσδιορίζει το στοιχείο κλειδί που οι περισσότεροι μηχανικοί δικτύων αντιλαμβάνονται ως δικτυακό switch. Στο ενσύρματο κόσμο, αυτό σημαίνει ότι μόνο η κυκλοφορία που προορίζεται για ή που φεύγει από έναν δεδομένο σταθμό είναι στο συνδεμένο ενσύρματο τμήμα του δικτύου εκείνου του σταθμού. Για να επιτευχθεί αυτό σε ένα 802.11 ασύρματο δίκτυο, πρέπει να είναι κάθε σταθμός σε δικό του μη επικαλυπτόμενο, μη παρεμβαλλόμενο RF κανάλι. Υποθέτοντας ένα δίκτυο 2.4 GHz, το οποίο έχει συνολικά τρία μη επικαλυπτόμενα κανάλια, αυτό σημαίνει ότι είναι δυνατόν να υπάρχουν μέχρι τρεις χρήστες. Αυτό δεν αποτελεί πραγματικότητα για ένα πραγματικό εξελικτικό δίκτυο!

Συνεπώς η τεχνολογία WLAN δεν είναι ένα σύστημα που μπορεί πραγματικά να "μεταχθεί" (switched) με την πραγματική έννοια του όρου. Οι συσκευές WLAN λειτουργούν σε ένα κοινό, μοιραζόμενο μέσο και ο σχεδιασμός των δικτύων WLAN οφείλει να απεικονίσει εκείνο το γεγονός.

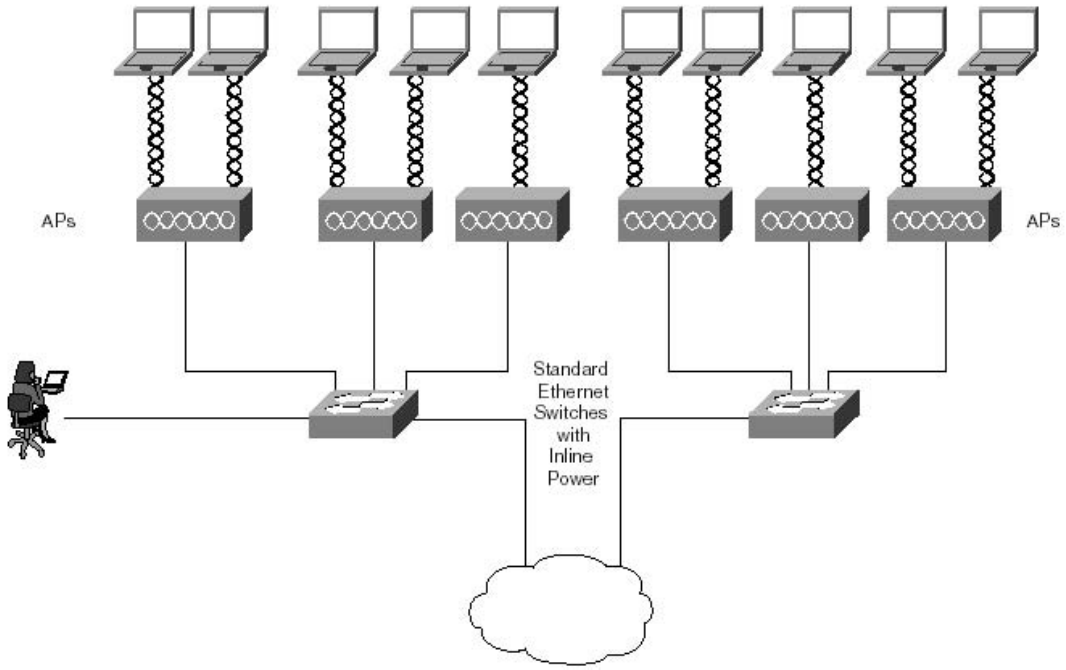
Η ενότητα αυτή καλύπτει έξι από τις δημοφιλέστερες ασύρματες αρχιτεκτονικές, καθεμία από τις οποίες καλύπτει καλύτερα τις ανάγκες συγκεκριμένου δικτύου.

Διανεμημένη Νοημοσύνη

Όπως έχει συμβεί στα πρώτα WLANs, ένα AP στην αρχιτεκτονική αυτή περιέχει μια σχετικά μεγάλη επεξεργαστική ισχύ και διατηρεί το μεγαλύτερο μέρος της νοημοσύνης RF στο άκρο του δικτύου. Το AP συνδέεται έπειτα άμεσα στο δίκτυο, συνήθως σε έναν network switch και είναι ένα ανεξάρτητο AP, το οποίο σημαίνει ότι δεν εμπιστεύεται κανένα άλλο κεντρικό υπολογιστή ή ελεγκτή στο δίκτυο (εκτός από τη συνδεσιμότητα Ethernet) για να διατηρήσει τις 802.11 επικοινωνίες στους ασύρματους πελάτες.

Το ευφυές AP καλείται συχνά παχύ AP επειδή περιέχει συστατικά ενός ισχυρού επεξεργαστή και σημαντικά ποσά μνήμης RAM και ROM. Περιλαμβάνοντας αυτά τα συστατικά, το AP μπορεί να κάνει περισσότερα από το να γεφυρώνει το Ethernet με το ασύρματο 802.11.

Το σχήμα 2-10 απεικονίζει ένα διανεμημένο σύστημα νοημοσύνης, όπου το AP συνδέεται με ένα Ethernet switch και λειτουργεί ως αυτόνομη συσκευή, χωρίς να απαιτεί την ύπαρξη μίας συσκευής στο δίκτυο που να παρέχει τη γενική λειτουργία του AP.



Εικόνα 2-10 Σύστημα διανεμημένης νοημοσύνης

Ένα κύριο χαρακτηριστικό ενός ευφυούς AP είναι ότι μπορεί να χρησιμοποιηθεί ως πιστοποιητής με βάση τη θύρα. Όταν χρησιμοποιείται υπό αυτήν τη μορφή, το AP εμποδίζει πραγματικά την κυκλοφορία, που προορίζεται από το RF για το Ethernet, να περάσει τη θύρα Ethernet, κρατώντας την έτσι μακριά από το ενσύρματο δίκτυο εκτός αν η κυκλοφορία είναι πιστοποιημένη (authenticated). Εάν ένα πακέτο έχει ληφθεί από το RF και δεν είναι από έναν επικυρωμένο σταθμό, επαναδρομολογείται μόνο στον επικυρωμένο κεντρικό υπολογιστή. Με αυτόν τον τρόπο, μόνο η ασφαλής, επικυρωμένη κυκλοφορία επιτρέπεται στο ενσύρματο δίκτυο.

Η τοπική κρυπτογράφηση και αποκρυπτογράφηση είναι επίσης ένα άλλο βασικό πλεονέκτημα των ευφυών APs. Το AP είναι το σημείο στο οποίο η κυκλοφορία RF κρυπτογραφείται στην πλευρά μετάδοσης και αποκρυπτογραφείται στην πλευρά λήψης. Αν και μερικοί μπορούν να μην θεωρήσουν αυτό ως πλεονέκτημα, ένα υψηλής απόδοσης AP θα χρησιμοποιήσει την επιτάχυνση υλικού στο AP, που εκτελεί την κρυπτογράφηση με πολύ μικρό ολικό κόστος στη ρυθμαπόδοση της κυκλοφορίας δεδομένων WLAN. Με τη διανομή αυτού της εργασίας σε κάθε AP, η πιθανότητα της επιβάρυνσης κάποιου επεξεργαστή, που χειρίζεται όλη την κρυπτογράφηση κυκλοφορίας RF, από αρκετά ίσως εκατοντάδες APs είναι ανύπαρκτη.

Ένα άλλο χαρακτηριστικό ενός ευφυούς AP, που συχνά παραβλέπεται, είναι η ανθεκτικότητα σε περίπτωση δυσλειτουργίας του συστήματος. Εάν, δηλαδή, ένα AP αποτύχει να λειτουργήσει, μόνο αυτό το AP επηρεάζεται και όλες οι άλλες συσκευές συνεχίζουν να λειτουργούν κανονικά. Κάθε AP δεν εξαρτάται από τον κώδικα που τρέχει σε κάποια άλλη συσκευή για να λειτουργήσει.

Σε μικρές εγκαταστάσεις, όπου απαιτείται ίσως μόνο ένας πολύ μικρός αριθμός APs, όπως ένα μικρό λιανικό κατάστημα ή μικρή επιχείρηση, δεν υπάρχει ανάγκη για έναν ακριβό ελεγκτή ή ένα ιδιόκτητο switch. Είναι δυνατή η διαχείριση των APs χρησιμοποιώντας το εσωτερικό λογισμικό τους και έναν απλό browser Ιστού ή το μικρό διαχειριστικό πρόγραμμα που έχει εγκατασταθεί σε έναν από τους δικτυωμένους κεντρικούς υπολογιστές.

Για τη βέλτιστη διαχείριση, μια ευφυής προσέγγιση AP, τουλάχιστον στις μεγάλες εγκαταστάσεις, απαιτεί συνήθως έναν διαχειριστικό κεντρικό υπολογιστή (παραδείγματος χάριν, διευθυντή SNMP) για να παρέχει την επαρκή υποστήριξη, τη διαμόρφωση και τη διαχείριση των πολλών APs.

Κεντρικοποιημένη Νοημοσύνη

Σε αντίθεση με ένα ευφυές AP, τα περισσότερα κεντρικοποιημένα συστήματα νοημοσύνης αφαιρούν το μεγαλύτερο μέρος των εργασιών και της επεξεργασίας από το AP και τοποθετούν την επεξεργασία αυτών των εργασιών σε ένα switch ή έναν κύριο ελεγκτή WLAN τοποθετημένο σε ένα κεντρικό σημείο του ενσύρματου δικτύου. Αυτοί οι τύποι των APs αναφέρονται συχνά ως λεπτά APs. Οι δύο τύποι κεντρικοποιημένων αρχιτεκτονικών νοημοσύνης είναι οι ακόλουθοι:

- Ένα σύστημα που χρησιμοποιεί συσκευές πυρήνες (που εδρεύουν στον πυρήνα του δικτύου) για τη διατήρηση της νοημοσύνης
- Ένα σύστημα που χρησιμοποιεί τις ακραίες συσκευές (που εδρεύουν στην άκρη του ενσύρματου δικτύου, όπως ένα Ethernet switch) για τη διατήρηση της νοημοσύνης του WLAN

Στην περίπτωση του ασύρματου switching, τα APs απλοποιούνται και εκτελούν μόνο λειτουργίες πομποδεκτών και, σε μερικές περιπτώσεις, ελέγχου της ραδιοκυκλοφορίας. Σε μερικά συστήματα, αυτά τα APs συνδέονται με το WLAN switch ή με τον ελεγκτή τους (όπως στα συστήματα συσκευών πυρήνων). Τα APs γίνονται εκτεταμένες θύρες πρόσβασης στο WLAN switch, κατευθύνοντας την κυκλοφορία χρηστών στο switch ή τον ελεγκτή για επεξεργασία.

Οι λειτουργίες ασφάλειας που χρησιμοποιούνται στα συστήματα WLAN switch , όπως η κρυπτογράφηση, η επικύρωση και ο έλεγχος πρόσβασης, προσαρμόζονται για να ακολουθήσουν τους χρήστες καθώς αυτοί κινούνται. Τα περισσότερα ασύρματα συστήματα switch παρέχουν εκτεταμένο switching στρώματow 2/3, επιτρέποντας στους κινητούς χρήστες να περιπλανηθούν μεταξύ APs, switches, VLANs και των υποδικτύων χωρίς απώλεια συνδεσιμότητας.

Το WLAN switching παρέχει επίσης μια διαφορετική προσέγγιση στη λειτουργική διαχείριση των 802.11 δικτύων. Οι διαμορφώσεις των APs αποθηκεύονται στον ελεγκτή ή το διακόπτη WLAN παρά στο ίδιο το AP. Με τη δυνατότητα ελέγχου ρυθμίσεων ισχύος και καναλιών μεμονωμένων APs, μερικά WLAN switches μπορούν αυτόματα να ανιχνεύσουν αποτυχημένα APs και να δώσουν εντολή σε κοντινά APs να ρυθμίσουν την ισχύ και τα κανάλια τους προκειμένου να υπάρξει η ανάλογη αντιστάθμιση. Όταν το αποτυχημένο AP αντικαθίσταται από ένα εργαζόμενο AP, ο διακόπτης WLAN σημειώνει αυτόματα το γεγονός και διαμορφώνει το νέο AP.

Τα περιπλοκότερα WLAN switches ελέγχουν συνεχώς τη ραδιοκυκλοφορία για να παρατηρήσουν το φόρτο του δικτύου και των χρηστών. Μπορούν ακόμη και δυναμικά να ρυθμίσουν το εύρος ζώνης, τον έλεγχο πρόσβασης, το QoS και άλλες παραμέτρους καθώς οι κινητοί χρήστες περιπλανώνται σε όλη την υποδομή.

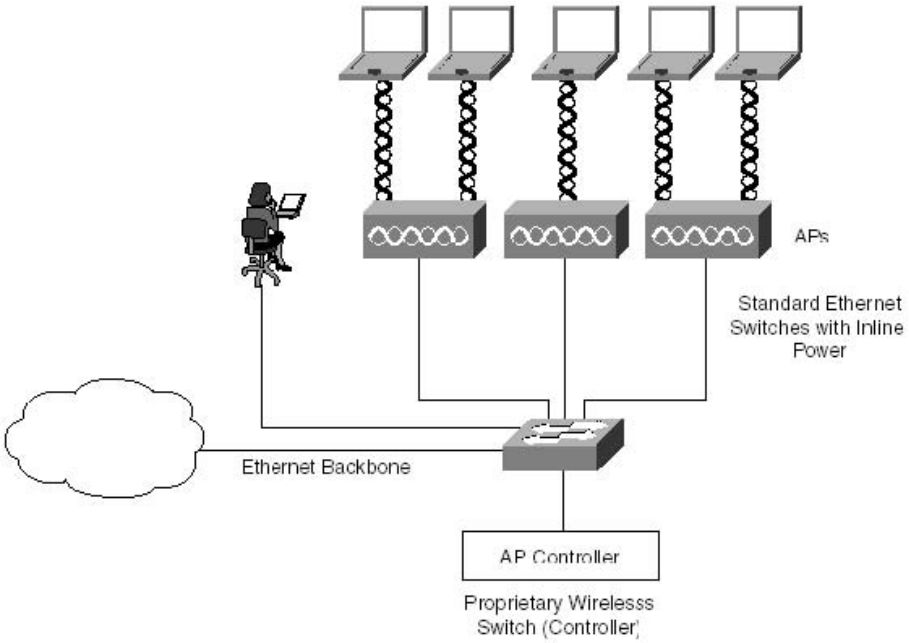
Αρχιτεκτονική συσκευών πυρήνων

Σε μια αρχιτεκτονική συσκευών πυρήνων, η νοημοσύνη κατοικεί οπουδήποτε στο δίκτυο, συνήθως μέσα στο κέντρο λειτουργιών του δικτύου (Network Operations Center - NOC). Παραδόξως, αρκετά από αυτά τα συστήματα χρησιμοποιούν τον όρο ασύρματο switch για να περιγράψουν το κεντρικοποιημένο τους ελεγκτή, παρ' όλο που αυτός δεν έχει καμία ικανότητα δικτυακού switching, όπως ορίστηκε στην αρχή αυτής της ενότητας, και παρέχει μόνο μια θύρα εισόδου και εξόδου.

Σε αυτά τα συστήματα, ένα AP είναι συνήθως γυμνό τόσο από νοημοσύνη όσο και από πολλές ευθύνες που συσχετίζονται με μια ακραία συσκευή. Εκτελεί μόνο τη ραδιολειτουργία και περνά όλη την κυκλοφορία πίσω σε έναν κεντρικά τοποθετημένο ελεγκτή. Αυτή η συσκευή ελεγκτών είναι αρμόδια για όλες τις λειτουργίες διαχείρισης πακέτων, συμπεριλαμβανομένης της ασφάλειας, της ταξινόμησης και επικόλλησης (tagging) QoS και του φιλτραρίσματος πακέτων για όλα τα συνδεδεμένα APs.

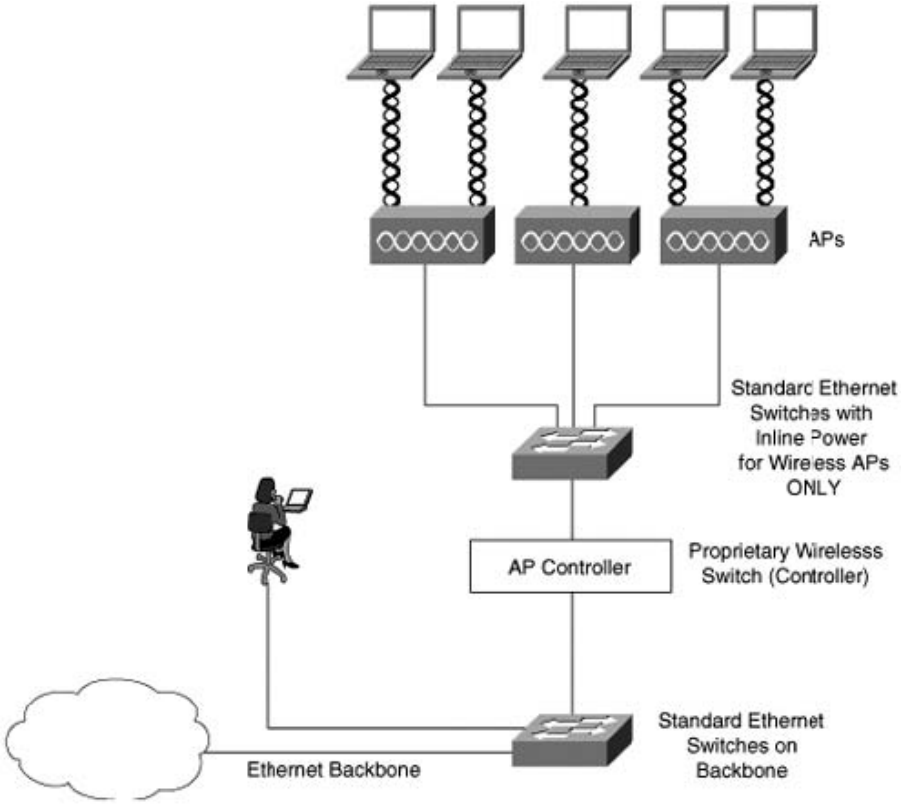
Το επιθυμητό αρχικό όφελος ενός τέτοιου συστήματος είναι το χαμηλότερο κόστος. Με τη μείωση των δαπανών εξοπλισμού, υλοποίησης και συντήρησης, το αποτέλεσμα είναι ένα χαμηλότερο συνολικό κόστος ιδιοκτησίας. Νοημοσύνη (και, επομένως, κόστος) έχει αφαιρεθεί από τα APs και έχει μεταφερθεί μέσα στο δίκτυο στο switch. Εντούτοις, το κόστος μεταφέρεται επίσης στο διακόπτη. Μακροπρόθεσμα υπάρχει ελάχιστος εάν όχι κανένα όφελος δαπανών σε σύγκριση με τα συστήματα διανεμημένης νοημοσύνης.

Η εγκατάσταση μιας συσκευής πυρήνα μπορεί να επιτευχθεί με δύο τρόπους. Το σχήμα 5-2 απεικονίζει τη μέθοδο που προτείνεται από τους περισσότερους προμηθευτές. Στο κέντρο του σχήματος 2-11 βρίσκεται ένας Ethernet switch που εξυπηρετεί διπλό σκοπό: να προσφέρει ισχύ στα APs (inline power) και να αποτελέσει ένα σημείο συνάθροισης για πολλαπλά APs. Ο ελεγκτής σε αυτό το σενάριο λειτουργεί παρόμοια με ένα δρομολογητή υπό την έννοια ότι δέχεται όλη την κυκλοφορία ώστε να παρέχει κάποια λειτουργία υψηλότερου στρώματος (παραδείγματος χάριν, ασφάλεια, QoS, φιλτράρισμα). Σε αυτήν την περίπτωση, όλη η κυκλοφορία θα έπρεπε να ρεύσει προς και από τις ίδιες διεπαφές Ethernet.



Εικόνα 2-11 Κεντρικοποιημένη αρχιτεκτονική συσκευών πυρήνων

Το σχήμα 2-12 παρουσιάζει ένα άλλο σενάριο υλοποίησης με κεντρικοποιημένη αρχιτεκτονική συσκευών πυρήνων. Σε αυτό το διάγραμμα, ο ελεγκτής διασυνδέεται σε ένα κατευθυνόμενο βόρεια switch που αθροίζει APs και ένα κατευθυνόμενο νότια switch που παρέχει πρόσβαση στον κορμό. Κάθε σύνδεση είναι 100 Mbps, πλήρως αμφίδρομη.



Εικόνα 2-12 Εναλλακτική κεντρικοποιημένη αρχιτεκτονική συσκευών πυρήνων

Η ασφάλεια είναι ένα ζήτημα σε οποιοδήποτε ασύρματο δίκτυο. Ακόμα κι αν ισχυρή επικύρωση και κρυπτογράφηση μπορούν να εφαρμοστούν, το γεγονός ότι η νοημοσύνη έχει αφαιρεθεί από τα APs και έχει τοποθετηθεί στον ελεγκτή του δικτύου σημαίνει ότι η κυκλοφορία πρέπει να ρεύσει στον ελεγκτή προτού να ασφαλιστεί. Με αυτήν την αρχιτεκτονική συστημάτων, μη επικυρωμένη κυκλοφορία ταξιδεύει προς το Ethernet switch, το οποίο έχει άμεση σύνδεση στον κορμό. Προκειμένου να γίνει το δίκτυο ασφαλές, πρέπει η ασύρματη κυκλοφορία να τοποθετηθεί σε ένα "βρώμικο" τμήμα ή την αποστρατικοποιημένη ζώνη (Demilitarized Zone - DMZ), έως ότου αυτή επικυρωθεί. Ο μόνος τρόπος να επιτευχθεί αυτό είναι να περάσει μέσω του ελεγκτή σε ένα ξεχωριστό switch που περνά έπειτα την κυκλοφορία στον κορμό. Κάθε σύνδεση είναι 100 Mbps, πλήρως αμφίδρομη.

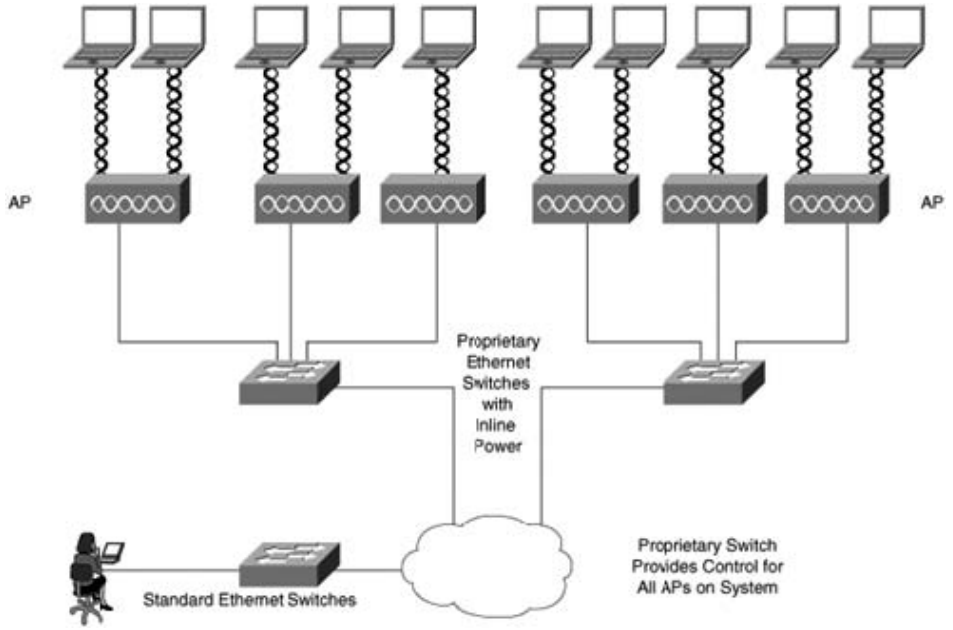
Αρχιτεκτονική ακραίων συσκευών

Στην αρχιτεκτονική αυτή ένα Ethernet switch στεγάζει τη νοημοσύνη για τα APs. Με τη κεντρικοποίηση μερικών από τις ασύρματες υπηρεσίες και των εργαλείων ανίχνευσης λαθών σε ένα δομημένο σύστημα μεταγωγής WLAN, οι μηχανικοί συστημάτων μπορούν να χτίσουν, να διαχειριστούν και να λειτουργήσουν τις μεγάλης κλίμακας 802.11 υποδομές με βελτιωμένες ικανότητες απόδοσης και διαχείρισης. Εντούτοις, συγκεντρώνοντας πάρα πολλή νοημοσύνη και επεξεργασία σε ένα κεντρικό σημείο εμφανίζονται πολλά από τα ίδια ζητήματα που εμφανίζονται σε έναν κεντρικό ελεγκτή πυρήνων.

Τα περισσότερα από τα συστήματα μεταγωγής WLAN μετακινούν σήμερα τις λειτουργίες μεγάλης επεξεργασίας, όπως η κρυπτογράφηση, η επικύρωση και η διαχείριση κινητικότητας, που βρίσκονται σε σημερινά ευφυή APs, σε έναν συγκεντρωμένο διακόπτη WLAN' ενώ κάνουν αυτό προσθέτουν επίσης σημαντικά νέα ασύρματα χαρακτηριστικά, όπως τον έλεγχο της ραδιοκυκλοφορίας και αυτοματοποιημένες έρευνες τοποθεσίας, τα οποία δίνουν στους διαχειριστές δικτύων περισσότερη διαφάνεια, ασφάλεια και έλεγχο. Με τη μεταγωγή WLAN, μια

πολυστρωματική προσέγγιση είναι απαραίτητη για την ασφάλεια στον αέρα, το δίκτυο και το χρήστη.

Η χρήση πραγματικών switches τύπου Ethernet ως ελεγκτή για τα APs είναι μια καλύτερη προσέγγιση από έναν κεντρικοποιημένο ελεγκτή, δεδομένου ότι βελτιώνεται πραγματικά η ασφάλεια καθιστώντας το switch πιστοποιητή των θυρών. Με αυτόν τον τρόπο, η μη επικυρωμένη κυκλοφορία δεν θα περάσει πέρα από τη θύρα switch. Εντούτοις, αυτό εξαρτάται από το εάν το AP συνδέεται άμεσα με το switch, που παρέχει τον έλεγχο για αυτό το συγκεκριμένο AP. Στα περισσότερα ακραία ασύρματα συστήματα switches, είναι δυνατόν να χρησιμοποιηθεί ένα switch για τον έλεγχο πολλών APs, συμπεριλαμβανομένων εκείνων που βρίσκονται σε έναν άλλο διακόπτη (βλ. σχήμα 2-13). Σε αυτήν την περίπτωση, υπάρχουν ακόμα μη επικυρωμένα πακέτα στο δίκτυο.



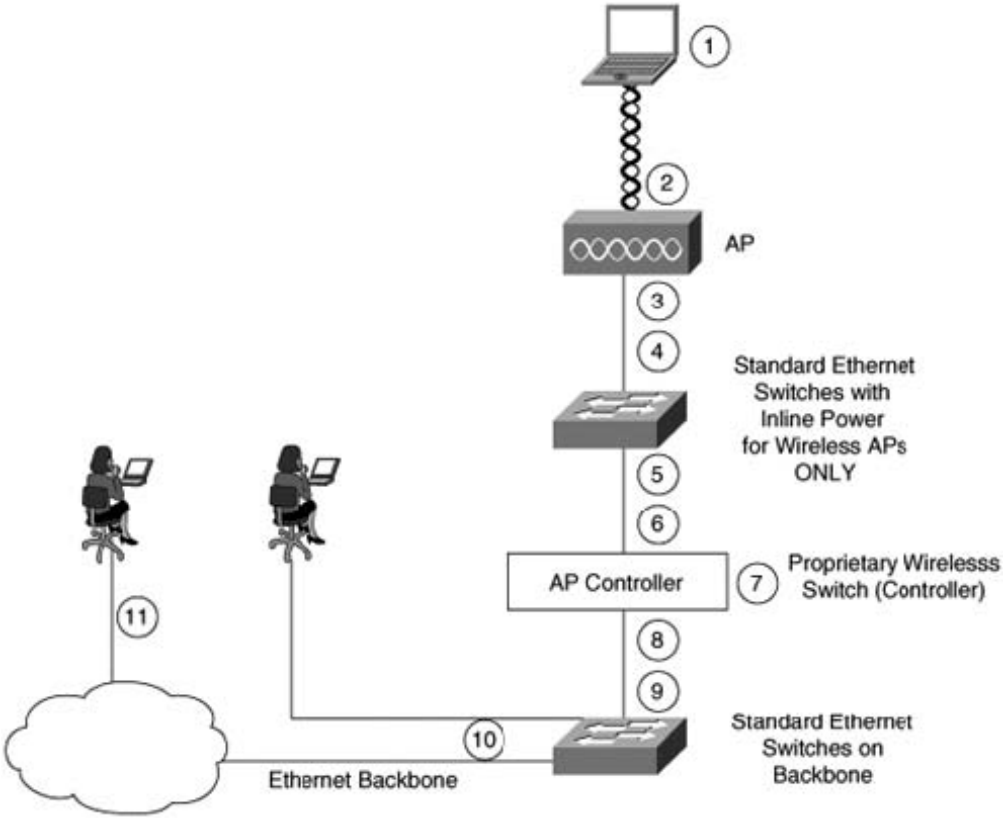
Εικόνα 2-13 Κεντρικοποιημένη αρχιτεκτονική ακραίων συσκευών

Το ένα βασικό στοιχείο που τα κεντρικοποιημένα συστήματα νοημοσύνης καθώς και τα συστήματα συσκευών πυρήνων και ακραίων συσκευών προωθούν είναι η ευκολία της διαχείρισης. Στις περισσότερες περιπτώσεις, εντούτοις, τα switches ή οι ελεγκτές έχουν έναν μέγιστο αριθμό APs που μπορούν να υποστηρίξουν και να διαχειριστούν. Σε ένα μεγάλο σύστημα μίας επιχείρησης, αυτό απαιτεί την προσθήκη ακόμα ενός συστατικού, κάποιου διευθυντή των διευθυντών, που απαιτείται για να διαχειριστεί αυτά τα WLAN switches ή τους ελεγκτές. Σε ένα ιδανικό σύστημα, ο ίδιος διευθυντής που χρησιμοποιείται για να διαχειριστεί τους ενσύρματους δρομολογητές και τους διακόπτες θα χρησιμοποιείτο για να διαχειριστεί και το ασύρματο δίκτυο.

Σύγκριση ροών πακέτων μεταξύ συστημάτων διανεμημένης και κεντρικοποιημένης νοημοσύνης

Στην πραγματικότητα, οι βασικές ταχύτητες δικτύων και οι τροφές τρυπούν μια τρύπα σε αυτήν την αρχιτεκτονική με περισσότερους από έναν τρόπους. Προκειμένου αυτό να γίνει κατανοητό, εξετάστε μια απλή ροή πακέτων μέσω του δικτύου, από έναν ασύρματο πελάτη σε έναν συνδεμένο με καλώδιο πελάτη. Το σχήμα 2-14 παρουσιάζει τη ζωή ενός πακέτου σε ένα σύστημα κεντρικοποιημένης νοημοσύνης συσκευών πυρήνων. Να ληφθεί υπόψη ότι τα APs ήταν

αποτελεσματικά "λοβοτομημένα" αναγκάζοντας κάθε πακέτο να αποστέλλεται πίσω στον ελεγκτή για επιθεώρηση.



Εικόνα 2-14 Η ζωή ενός πακέτου σε σύστημα κεντρικοποιημένης νοημοσύνης συσκευών πυρήνων

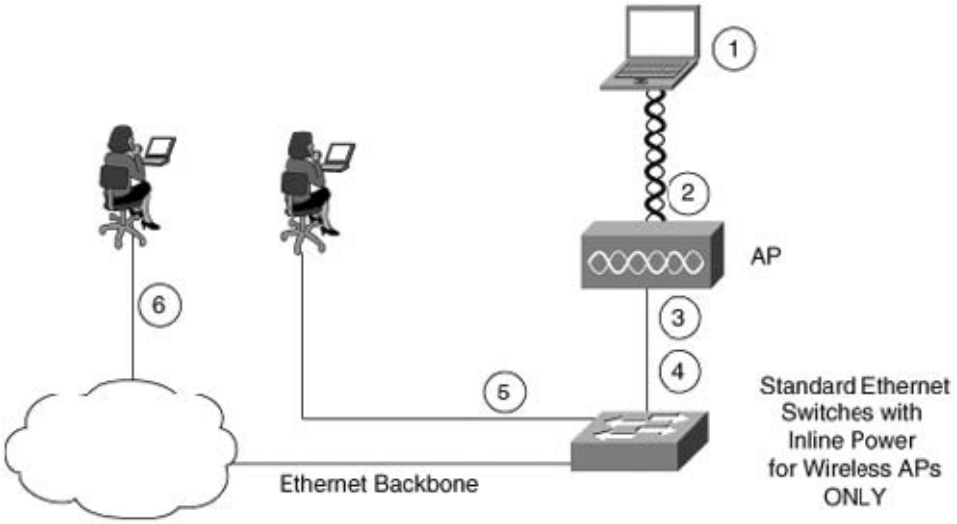
Η ακόλουθη κυκλοφοριακή ροή (συνήθης ακολουθία πακέτων) περιγράφει το σχήμα 5-4:

1. Ένα πακέτο ping (ICMP Echo Request) παράγεται από τον τερματικό σταθμό πελάτη.
2. Το πακέτο ταξιδεύει μέσω του αέρα πάνω σε ασύρματο δίκτυο 802.11b και φθάνει στο AP.
3. Το πακέτο γεφυρώνεται στο LAN Ethernet και κατευθύνεται προς τον ελεγκτή.
4. Το Ethernet switch λαμβάνει το πακέτο.
5. Το πακέτο αφήνει το Ethernet switch από τη θύρα του ελεγκτή.
6. Ο ελεγκτής λαμβάνει το πακέτο.
7. Ο ελεγκτής επεξεργάζεται το πακέτο (ταξινομεί, φιλτράρει, δημιουργεί ετικέτα και τα λοιπά).
8. Το πακέτο κατευθύνεται προς το δίκτυο κορμό μέσω της θύρας εξόδου.
9. Το switch του κορμού λαμβάνει το πακέτο.
10. Το πακέτο στέλνεται στη διεύθυνση IP στην οποία προορίστηκε.
11. Το PC προορισμός λαμβάνει το πακέτο.

Τώρα το πακέτο πρέπει να διασχίσει πίσω τα ίδια βήματα στην αντίστροφη σειρά για να παραληφθεί από το κατάλληλο AP και τον πελάτη. Δηλαδή πρέπει να κάνει συνολικά 22 βήματα για να κινηθεί από έναν ασύρματο πελάτη προς άλλο (ακόμα κι αν αυτοί οι πελάτες είναι στο ίδιο AP)! Ένα απλό ping ταξιδεύει μέσα από 22 διεπαφές. Εάν οι IP διευθύνσεις πηγής και προορισμού είναι σε διαφορετικά υποδίκτυα, τότε πρέπει να προστεθεί ένα hop στρώματος 3 στον ελεγκτή σε εκείνο το σύνολο.

Αντιπαραβάλετε το κεντρικοποιημένο σύστημα νοημοσύνης σε ένα διανεμημένο σύστημα νοημοσύνης όπου το AP παρέχει υπηρεσίες επικύρωσης και μπλοκαρίσματος θυρών, καθώς επίσης και τοπική κρυπτογράφηση.

Το σχήμα 2-15 παρουσιάζει τη ζωή ενός πακέτου σε ένα παχύ AP.



Εικόνα 2-15 Η ζωή ενός πακέτου σε σύστημα διανεμημένης νοημοσύνης

Η ακόλουθη κυκλοφοριακή ροή περιγράφει το σχήμα 5-5:

1. Το πακέτο ταξιδεύει μέσω του αέρα πάνω σε ασύρματο δίκτυο 802.11b και φθάνει στο AP.
2. Το πακέτο παραλαμβάνεται από το AP, η εσωτερική κεντρική μονάδα επεξεργασίας του AP επεξεργάζεται το πακέτο (ταξινομεί, φιλτράρει, δημιουργεί ετικέτα) και έπειτα το πακέτο γεφυρώνεται στο LAN Ethernet.
3. Το AP στέλνει το πακέτο.
4. Το Ethernet switch λαμβάνει το πακέτο.
5. Το πακέτο αφήνει το Ethernet switch προς το PC του πελάτη.
6. Το PC προορισμός λαμβάνει το πακέτο.

Εάν το πακέτο προορίζεται για μια άλλη ασύρματη συσκευή (σε ένα διαφορετικό AP), τότε αυτό ταξιδεύει απλά από το βήμα 5 στο άλλο AP και έπειτα στον πελάτη. Εάν η κυκλοφορία είναι μεταξύ δύο πελατών στο ίδιο AP, το πακέτο ταξιδεύει από τον πελάτη στο AP και έπειτα στον επόμενο πελάτη. Και στις δύο περιπτώσεις, ένα WLAN δίκτυο διανεμημένης νοημοσύνης οδηγεί σε πολύ λιγότερη συνολική κυκλοφορία από ότι ένα κεντρικοποιημένο σύστημα νοημοσύνης.

Η λύση κεντρικοποιημένων ελεγκτών διαπερνά σχεδόν διπλό αριθμό διεπαφών ανά πακέτο από ό,τι η διανεμημένη λύση. Η επίπτωση στην κυκλοφορία είναι σημαντική. Οι καθυστερήσεις μπορούν να εμφανιστούν σε πολλές περιοχές, συμπεριλαμβανομένων των εξής:

- RF θύρα στο AP
- Θύρα εξόδου στο AP
- Θύρα εισόδου στο Ethernet switch
- Θύρα εξόδου στο Ethernet switch
- Θύρα εισόδου στο controller
- Ο ίδιος ο ελεγκτής
- Θύρα εξόδου στον ελεγκτή
- Θύρα εισόδου στο δεύτερο Ethernet switch
- Θύρα εξόδου στο δεύτερο Ethernet switch

Οποιοδήποτε δεδομένο πακέτο μπορεί να υπόκειται σε καθυστέρηση διάδοσης και καθυστέρηση επεξεργασίας, και οι δύο από τις οποίες επηρεάζουν τη διακύμανση της

καθυστέρησης, που είναι γνωστή επίσης ως jitter. Η καθαρή επίδραση είναι ένα πιο αργό, λιγότερο προβλέψιμο δίκτυο. Αυτό είναι ιδιαίτερα μια ανησυχία για εφαρμογές όπως η φωνή πάνω σε IP (Voice over IP - VoIP), που είναι πολύ ευαίσθητες στο jitter.

Τεχνολογία Στοιχειοκεραιών

Οι στοιχειοκεραίες είναι σε θέση να επαναπροσανατολίσουν την ακτίνα της κεραίας με την ηλεκτρονική μετακίνηση ολόκληρης της δομής χωρίς οποιαδήποτε φυσική μετακίνηση.

Τα χαρακτηριστικά μιας στοιχειοκεραίας επιτρέπουν στο σήμα να είναι κατευθυντικό και λιγότερο ευαίσθητο στην ακτινοβολούσα παρεμβολή. Στον κόσμο των WLANs, χρησιμοποίηση στοιχειοκεραιών σημαίνει λιγότερη παρεμβολή από άλλες συσκευές λόγω των στενών κατευθυντικών ακτινών. Αυτό είναι ιδιαίτερα σημαντικό λόγω του μη αδειοδοτημένου και ελεύθερου φάσματος στο οποίο λειτουργεί. Υπάρχει στοιχειοκεραία, η οποία αποτελείται από 128 στοιχεία που λειτουργούν ομόφωνα για να διαβιβάσουν το 802.11 σήμα. Η ακτινοβολημένη δύναμη παρέχεται μόνο στις θέσεις όπου υπάρχουν χρήστες' συνεπώς, υπάρχει μια σημαντική μείωση της πιθανής παρεμβολής. Ως αποτέλεσμα του στενού πλάτους των ακτινών, οι χρήστες απολαμβάνουν μια ιδιαίτερη αύξηση στο κέρδος των κεραιών. Αυτή η αύξηση στο κέρδος παρέχει μια σημαντική βελτίωση στο εύρος κάλυψης. Επομένως, το εύρος ενός συστήματος στοιχειοκεραίας μπορεί να μετρηθεί σε χιλιόμετρα.

Η τεχνολογία αυτή συναντά, ωστόσο, προβλήματα. Όταν χρησιμοποιείται μια τεχνολογία οδήγησης των ακτινών, όπως η παρούσα, που χρησιμοποιεί ακτίνες πολύ στενής ακτινοβολίας, οι RF ανακλαστικές επιφάνειες μπορούν να αποτελέσουν ένα σημαντικό εμπόδιο. Στις περισσότερες περιπτώσεις, εάν υπάρχει οποιοσδήποτε τύπος μεταλλικής ή άλλης RF ανακλαστικής επιφάνειας στα πρώτα 15 έως 40 μέτρα επί της πορείας ακτινοβολίας της κεραίας, τότε η οδήγηση ακτινών διαστρεβλώνεται και η γενική απόδοση εκείνης της ακτίνας μειώνεται εντυπωσιακά. Αυτό περιορίζει σοβαρά τη χρήση του συστήματος σε ένα εσωτερικό περιβάλλον.

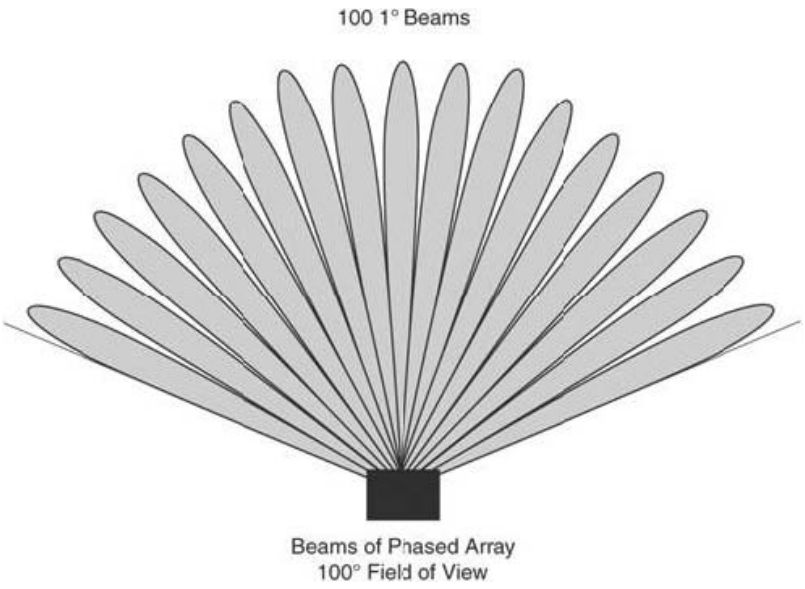
Το δεύτερο μειονέκτημα έχει να κάνει με την χωρητικότητα. Εάν, στην πραγματικότητα, το AP μπορεί να υποστηρίξει ένα ολόκληρο πάτωμα 250 ανθρώπων ως αποτέλεσμα της αυξημένης κάλυψής του, τι γίνεται με το εύρος ζώνης; Το AP παρέχει την κάλυψη χρησιμοποιώντας και τα τρία μη επικαλυπτόμενα κανάλια. Αυτό σημαίνει ότι όταν είναι βελτιστοποιημένο, η μέγιστη ρυθμαπόδοση και των τριών συνδυασμένων θα είναι περίπου 16 Mbps και αυτό θα μοιραστεί μεταξύ των 250 χρηστών. Για την αντιμετώπιση αυτού, πολλές βιομηχανίες, συμπεριλαμβανομένων των επιχειρήσεων, προσανατολίζονται προς μικρότερου μεγέθους κυψέλες, έτσι ώστε ο αριθμός των χρηστών ανά AP να είναι χαμηλότερος και το εύρος ζώνης ανά χρήστη να είναι υψηλότερο.

Δύο από τα μεγαλύτερα μειονεκτήματα σε αυτήν την τεχνολογία είναι μέγεθος και κόστος. Ένα χαρακτηριστικό εσωτερικό AP έχει μια τιμή καταλόγου μεγαλύτερη από $8000 και απαιτεί χώρο τοίχου από 1 ως 3 μέτρα.

Η στοιχειοκεραία επεκτείνει το εύρος κάλυψης

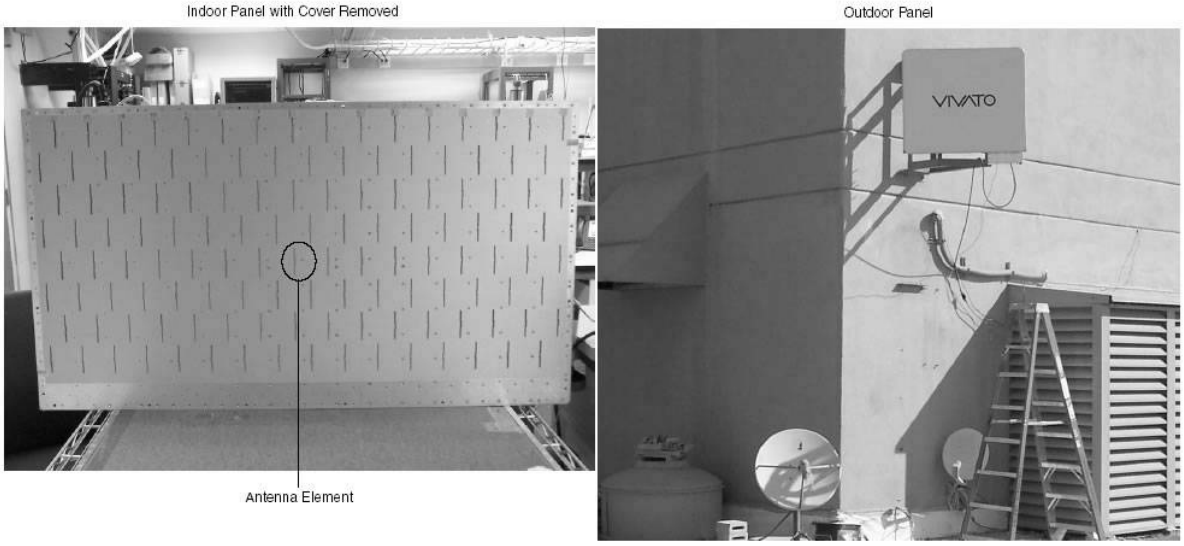
Υπάρχουν σήμερα ισχυρές στοιχειοκεραίες που συνδυάζονται με έναν κεντρικοποιημένο ευφυή ελεγκτή. Αυτός εμφανίζει ένα παρόμοιο διαχειριστικό πρότυπο με ένα Ethernet switch, αλλά λαμβάνει υπόψη και τις εξειδικευμένες πτυχές της διαχείρισης WLANs. Ο στόχος εδώ είναι οι μεγάλου εύρους ικανότητες αυτής της συσκευής να λύσουν τα ζητήματα της εγκατάστασης δωδεκάδων APs για την παροχή κάλυψης σε μια μεγάλη περιοχή.

Αντί να εκπέμπεται το σήμα 360, η στοιχειοκεραία έχει ένα διάγραμμα ακτινοβολίας 100 βαθμών και συνδέεται με οποιοδήποτε πελάτη μέσα σε αυτό το οπτικό πεδίο (βλ. σχήμα 2-16). Εκπέμπει σε μια συγκεκριμένη ακτίνα μόνο όταν ένας πελάτης είναι ενεργός, στέλνοντας μια στενή δέσμη ενέργειας άμεσα στον πελάτη. Η ισχυρή αυτή κεραία χρησιμοποιείται για να στείλει και να λάβει σε μια βάση από πακέτο σε πακέτο, επιτρέποντας φαινομενικά πολλαπλές συνομιλίες συγχρόνως. Στην πραγματικότητα, παρέχει μια πλατφόρμα με την οποία τρεις χρήστες μπορούν να επικοινωνήσουν μαζί σε οποιαδήποτε χρονική στιγμή (βασίζεται σε 802.11b ή 802.11g έχοντας μόνο τρία μη επικαλυπτόμενα κανάλια).



Εικόνα 2-16 Διάγραμμα ακτινοβολίας στοιχειοκεραίας

Επειδή ένα υπαίθριο switch εκτίθεται στα στοιχεία της φύσης, πρέπει να εσωκλειστεί σε ένα περιβάλλον ανθεκτικό στη σκόνη και την υγρασία και ελεγχόμενο ως προς τη θερμοκρασία. Αυτό επιτυγχάνεται με την ενσωμάτωση της συσκευής σε ένα NEMA 4 αξιολογημένο κουτί. Η στεγανή αυτή υλοποίηση είναι μια πλήρης συσκευασία που μπορεί εύκολα να τοποθετηθεί έξω από ένα κτήριο ή σε έναν πύργο (βλ. σχήμα 2-17).



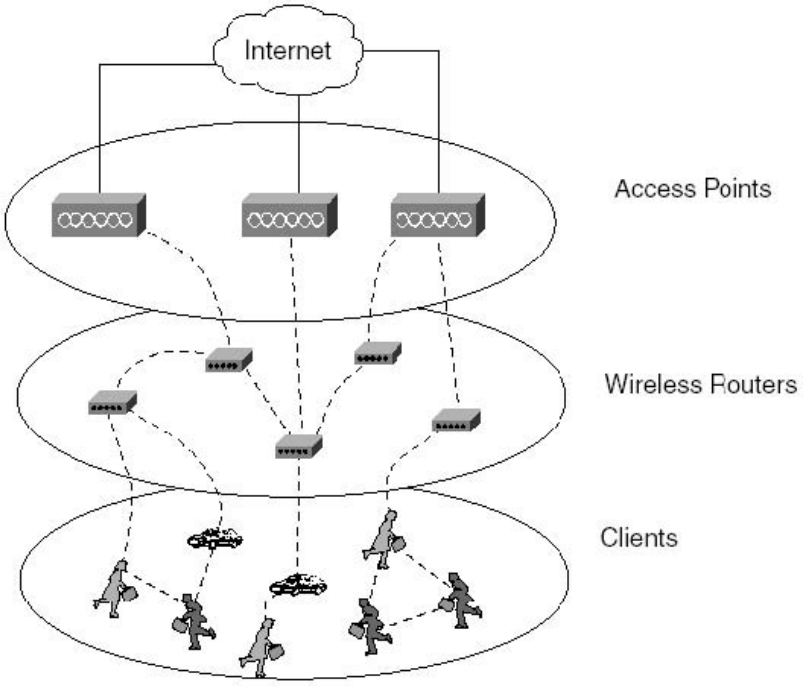
Εικόνα 2-17 Προϊόντα στοιχειοκεραιών

Δικτύωση Πλέγματος (Mesh)

Η δικτύωση πλέγματος (mesh) είναι μια ad hoc peer-to-peer τεχνολογία δρομολόγησης που υποστηρίζει τεχνικές δρομολόγησης αρχικά ανεπτυγμένες για το πεδίο της μάχης και άλλα προσωρινά συστήματα επικοινωνιών. Με την ώθηση της νοημοσύνης και της λήψης αποφάσεων

στο άκρο του δικτύου, είναι δυνατόν να χτιστούν ιδιαίτερα κινητά και εξελικτικά ευρυζωνικά δίκτυα με πολύ χαμηλό κόστος.

Μερικά συστήματα, όπως το σύστημα MeshNetworks, υποστηρίζουν και meshing υποδομής και meshing πελατών. Το meshing υποδομής δημιουργεί ένα εξελικτικό δίκτυο, ενώ το meshing πελατών επιτρέπει στους πελάτες να διαμορφώσουν αμέσως ένα ευρυζωνικό ασύρματο δίκτυο μεταξύ τους, με ή χωρίς υποδομή δικτύων. Χρησιμοποιώντας τη multihopping τεχνολογία δρομολόγησης MeshNetworks, είναι δυνατόν να χρησιμοποιηθεί κάθε συσκευή πελάτη ως δρομολογητής / επαναλήπτης, έτσι κάθε χρήστης στο σύστημα παίζει έναν ρόλο στην κάλυψη του δικτύου και τη ρυθμαπόδοση για άλλους χρήστες. Το σχήμα 2-18 απεικονίζει μια τοπολογία δικτύων mesh και τα σχέδια κυκλοφορίας RF.



Εικόνα 2-18 Αρχιτεκτονική δικτύου Mesh

Ένα ζήτημα σχετικό με την προσέγγιση των δικτύων πλέγματος, εκτός από την εφαρμογή ιδιαίτερα πολύπλοκων πρωτοκόλλων δρομολόγησης, είναι ασφάλεια. Το γεγονός ότι κάθε πελάτης μπορεί να γίνει επαναλήπτης για άλλες συσκευές σημαίνει ότι η κυκλοφορία άλλων πελατών διαπερνά συστήματα που μπορούν ή όχι να είναι πλήρως ασφαλή. Προσθέστε σε αυτό το γεγονός ότι μερικοί πελάτες μπορεί να σβήσουν ή να κινηθούν και η γενική σταθερότητα και απόδοση ενός τέτοιου δικτύου μπορούν να είναι αμφισβητήσιμες. Συνήθως, η δικτύωση πλέγματος γίνεται μόνο για προσωρινά και μη ασφαλή συστήματα.

Οπτική Ελευθέρου Χώρου (Laser)

Η οπτική ελεύθερου χώρου (Free-Space Optics - FSO) είναι μια τεχνολογία οπτικής επαφής που χρησιμοποιεί λέιζερ για να παρέχει οπτικές ευρυζωνκές συνδέσεις. Αυτήν την περίοδο, η FSO είναι ικανή για μέχρι 2,5 Gbps επικοινωνίες δεδομένων, φωνής και βίντεο μέσω του αέρα, που επιτρέπουν οπτική συνδεσιμότητα χωρίς την απαίτηση καλωδίου οπτικής ίνας ή εξασφάλιση άδειας φάσματος. Η FSO απαιτεί φως, το οποίο μπορεί να στραφεί με τη χρησιμοποίηση είτε διόδων εκπέμποντος φωτός (Light Emitting Diodes - LEDs) είτε λέιζερ (ενίσχυση φωτός από διεγερμένη εκπομπή ακτινοβολίας). Η χρήση των λέιζερ είναι μια απλή εργασία παρόμοια με τις οπτικές μεταδόσεις που χρησιμοποιούν τα καλώδια οπτικών ινών' η μόνη διαφορά είναι το μέσο. Τα φως

ταξιδεύει ταχύτερα μέσω του αέρα από ό,τι μέσω του γυαλιού, συνεπώς είναι δίκαιο να ταξινομηθεί η FSO ως οπτική επικοινωνία με την ταχύτητα του φωτός.

Η τεχνολογία FSO είναι σχετικά απλή (βλ. σχήμα 2-19). Είναι βασισμένη στη συνδεσιμότητα μεταξύ FSO μονάδων, κάθε μια αποτελούμενη από έναν οπτικό πομποδέκτη με ένα πομπό λέιζερ και ένα δέκτη για την παροχή πλήρους αμφίδρομης ικανότητας. Κάθε μονάδα FSO χρησιμοποιεί μια υψηλής ισχύος οπτική πηγή (δηλαδή λέιζερ), συν έναν φακό που εκπέμπει το φως μέσω της ατμόσφαιρας σε έναν άλλο φακό που λαμβάνει τις πληροφορίες. Ο λαμβάνων φακός συνδέεται με έναν δέκτη υψηλής ευαισθησίας μέσω οπτικής ίνας. Η FSO είναι εύκολα αναβαθμίσιμη και οι ανοικτές διεπαφές του υποστηρίζουν εξοπλισμό από ποικίλους προμηθευτές, κάτι που βοηθά τους παροχείς υπηρεσιών να προστατεύσουν την επένδυσή τους στις ενσωματωμένες τηλεπικοινωνιακές υποδομές.

Εικόνα 2-19 FSO

Τα συστήματα FSO χρησιμοποιούνται συνήθως σε συστήματα από σημείο σε σημείο που είναι σταθερά τοποθετημένα. Έχουν μια πολύ στενή δέσμη ακτινών και επομένως πρέπει να τοποθετηθούν σε μια ισχυρή δομή που εμφανίζει ελάχιστη μετακίνηση (λόγω του αέρα ή άλλων προβλημάτων δόνησης). Αν και μπορούν να παρέχουν πολύ υψηλά εύρη ζώνης, τα συστήματα FSO είναι σχετικά περιορισμένου εύρους συσκευές (από μερικές εκατοντάδες μέτρα μέχρι μερικά χιλιόμετρα).

Τα περισσότερα συστήματα FSO εγκαθίστανται με ένα εφεδρικό σύστημα RF σε περίπτωση που μερικές περιβαλλοντικές συνθήκες, όπως η ομίχλη, το βαρύ χιόνι ή βαριές θύελλες, παρεμποδίζουν το σήμα φωτός.

Υλοποιήσεις Υπαίθριων Γεφυρών

Συνδεσιμότητα από κτήριο σε κτήριο

Πρέπει να αναθεωρηθούν διάφορα βασικά ζητήματα κατά την επιλογή μιας τεχνολογίας γεφυρών για από κτήριο σε κτήριο συνδεσιμότητα. Όπως με τα WLANs, η πρώτη απαίτηση είναι το εύρος ζώνης. Πρέπει να καθοριστεί το ολικό εύρος ζώνης που θα απαιτηθεί μεταξύ των τοποθεσιών. Εάν οι γέφυρες θα χρησιμοποιηθούν και για τις ασύρματες γέφυρες και για την πρόσβαση WLAN, τότε αυτές πρέπει να ακολουθήσουν την κατάλληλη τεχνολογία για τις συσκευές πελατών. Εντούτοις, εάν η γέφυρα θα είναι αυστηρά για συνδεσιμότητα από κτήριο σε κτήριο, τότε μπορεί να χρησιμοποιηθεί οποιαδήποτε τεχνολογία γεφυρών, συμπεριλαμβανομένων των ιδιόκτητων συστημάτων.

Τα συστήματα γεφυρών έρχονται σε πολλούς τύπους και μεγέθη, με διαθέσιμες διάφορες ρυθμαποδόσεις. Τα 802.11b συστήματα μπορούν να παρέχουν ρυθμαποδόσεις μέχρι 6 Mbps ανά σύστημα και εύρη μέχρι 30 χιλιόμετρα (στα 6 Mbps) σε θέσεις όπου κεραίες υψηλού κέρδους επιτρέπονται. Γέφυρες βασισμένες στις τεχνολογίες 802.11g και 8021.11a παρέχουν συνήθως ρυθμαποδόσεις των 20 Mbps, αλλά σε μικρότερη απόσταση. Μερικοί γέφυρες βασισμένες στο 802.11α ή το 802.11g μπορούν να παρέχουν τη μέγιστη ρυθμαπόδοση σε περίπου 19 ή 24 χιλιόμετρα.

Για πολύ υψηλότερη ρυθμαπόδοση, πρέπει να αναθεωρηθούν μερικά ιδιόκτητα συστήματα. Πολλά διαφορετικά συστήματα είναι διαθέσιμα, συμπεριλαμβανομένων των οπτικών γεφυρών ελεύθερου χώρου, μέσω των οποίων οι ρυθμοί διέλευσης δεδομένων μπορούν να φθάσουν τα 155 Mbps ή υψηλότερα αλλά σε πολύ περιορισμένη απόσταση.

Σε όλες τις περιπτώσεις, η οπτική επαφή απαιτείται για τις μεγαλύτερες αποστάσεις, και συνήθως για ακόμη και τις μικρού μήκους συνδέσεις.

Οι περισσότερες γέφυρες θα παράσχουν μια σύνδεση που ενώνει δύο δίκτυα στο ίδιο υποδίκτυο. Εάν οι τοποθεσίες είναι σε χωριστά υποδίκτυα (συνήθως), οι γέφυρες πρέπει να συνδεθούν σε μια θύρα δρομολογητή για κατάλληλη κατάτμηση μεταξύ των δικτύων.

Ακόμα και τα ιδιόκτητα συστήματα δεν είναι ασφαλή επειδή η κυκλοφορία μπορεί "να παραληφθεί" από οποιονδήποτε που κατέχει μία συσκευή από την ίδια εταιρεία. Η ασφάλεια πρέπει να αναθεωρηθεί προσεκτικά και πρέπει να χρησιμοποιηθεί εφόσον κάποιος τύπος ευαίσθητων δεδομένων πρόκειται να σταλεί πάνω στη σύνδεση. Μερικές γέφυρες υποστηρίζουν την επικύρωση τύπου EAP, ενώ άλλες μπορούν μόνο να υποστηρίξουν το "εύκολο" WEP. Μια εναλλακτική λύση είναι να χρησιμοποιηθεί μια σήραγγα VPN μεταξύ των δρομολογητών σε κάθε πλευρά της σύνδεσης και να είναι οι γέφυρες συνδεμένες με αυτούς τους δρομολογητές. Αυτό παρέχει σε όλη την κυκλοφορία γεφυρών μια σήραγγα ασφάλειας VPN.

Κατανόηση των χαρακτηριστικών συστημάτων γεφυρών

Τα εύρη για τα συστήματα γεφυρών ποικίλλουν ως αποτέλεσμα της συχνότητας, της ισχύος εκπομπής και των διαθέσιμων κεραιών. Εύρη ορισμένων χιλιομέτρων ή λιγότερο καλύπτονται από τη μεγάλη πλειοψηφία των εγκαταστάσεων γεφυρών' εντούτοις, πιο μακρινά εύρη μπορούν να ενεργοποιηθούν με κατάλληλη επιλογή των κεραιών, καθαρή οπτική επαφή και εκκαθάριση της ζώνης Fresnel.

Η προδιαγραφή 802.11 βασίστηκε σε μια υπόθεση ότι μια σύνδεση επικοινωνίας WLAN (λαμβάνοντας υπόψη ότι αυτό καθορίζει ένα δίκτυο τοπικής περιοχής) θα ήταν όχι περισσότερα από 1000 πόδια. Επομένως, οι αποστάσεις για την επικοινωνία μεταξύ AP και πελάτη περιορίζονται σε πιο κοντινές αποστάσεις για ποιοτική απόδοση, ανεξάρτητα από την ισχύ εκπομπής, το χρησιμοποιούμενο καλώδιο και τους συνδυασμούς κεραιών. Αυτό συμβαίνει επειδή υπάρχουν περιορισμοί συγχρονισμού στο πρωτόκολλο 802.11, οι οποίοι συγχρονίζουν τις επικοινωνίες για την υποστήριξη καθυστερήσεων που εισάγονται από την απόσταση. Αν και αρκετές γέφυρες μπορεί να ακολουθήσουν τα πρωτόκολλα 802.11, δεν εμμένουν αυστηρά στις παραμέτρους συγχρονισμού ή έχουν τη δυνατότητα να αλλάξουν την ικανότητα συγχρονισμού (ή απόστασης).

Οι ικανότητες ρυθμού διέλευσης δεδομένων των γεφυρών επίσης ποικίλλουν. Εάν μια γέφυρα ακολουθήσει μια από τις προδιαγραφές 802.11, οι διαθέσιμα ρυθμοί δεδομένων θα

καθοριστούν από τις προδιαγραφές, και η ρυθμαπόδοση θα είναι παρόμοια με ένα WLAN χρησιμοποιώντας την ίδια τεχνολογία. Εντούτοις, μερικές γέφυρες χρησιμοποιούν ιδιόκτητη διαμόρφωση και, αν και να είναι στις ίδιες ζώνες συχνοτήτων με τα συστήματα 802.11, χρησιμοποιούν ιδιόκτητο σχηματισμό καναλιών, ο οποίος μπορεί να επιτρέψει υψηλότερους ρυθμούς διέλευσης δεδομένων και ρυθμαπόδοση.

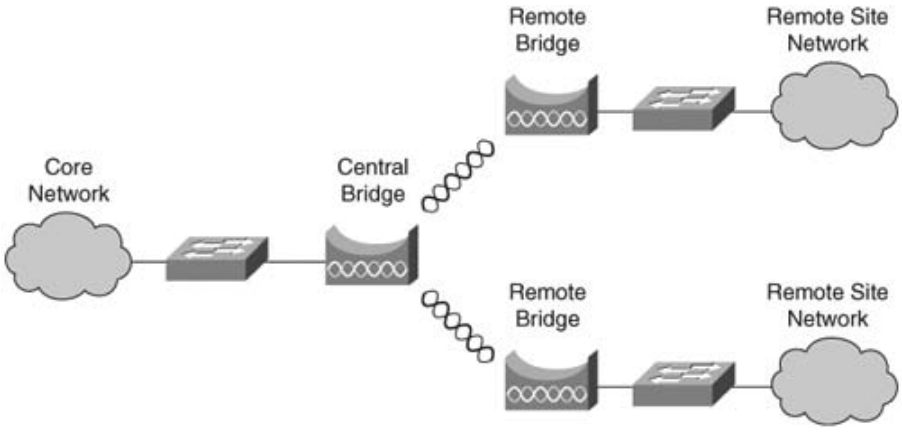
Πρέπει να ακολουθούνται οι διάφοροι κανονισμοί κατά την εγκατάσταση WLANs. Το ίδιο πράγμα ισχύει για το γεφύρωμα. Υπάρχουν διαφορετικοί περιορισμοί ενεργούς ισχύος ισοτροπικής ακτινοβολίας (Effective Isotropic Radiated Power - EIRP) για διαφορετικές χώρες, καθώς επίσης και διαφορές στα διαθέσιμα κανάλια και ακόμη και επιτρεπόμενα σχέδια διαμόρφωσης. Βλέπε αντίστοιχη υποενότητα του παραρτήματος Α για αυτούς τους κανονισμούς

Κατανόηση Τοπολογιών Γεφυρών

Δύο τύποι τοπολογιών γεφυρών υλοποιούνται συνήθως. Ένας μεγάλος αριθμός συστημάτων είναι από σημείο σε σημείο, συνδέοντας ακριβώς δύο τοποθεσίες. Το σχήμα 2-20 παρουσιάζει μια χαρακτηριστική τοπολογία γεφυρών για τα από σημείο σε σημείο συστήματα.

Εικόνα 2-20 Τοπολογία γεφυρών από σημείο προς σημείο

Σήμερα εγκαθίσταται ένας αυξανόμενος αριθμός πολυσημειακών συστημάτων. Στα περισσότερα συστήματα, μια γέφυρα ορίζεται συνήθως ως η κεντρική (root bridge) γέφυρα. Αυτό παρέχει το κεντρικό σημείο της ροής δεδομένων από τις μακρινές περιοχές (βλ. σχήμα 2-21).

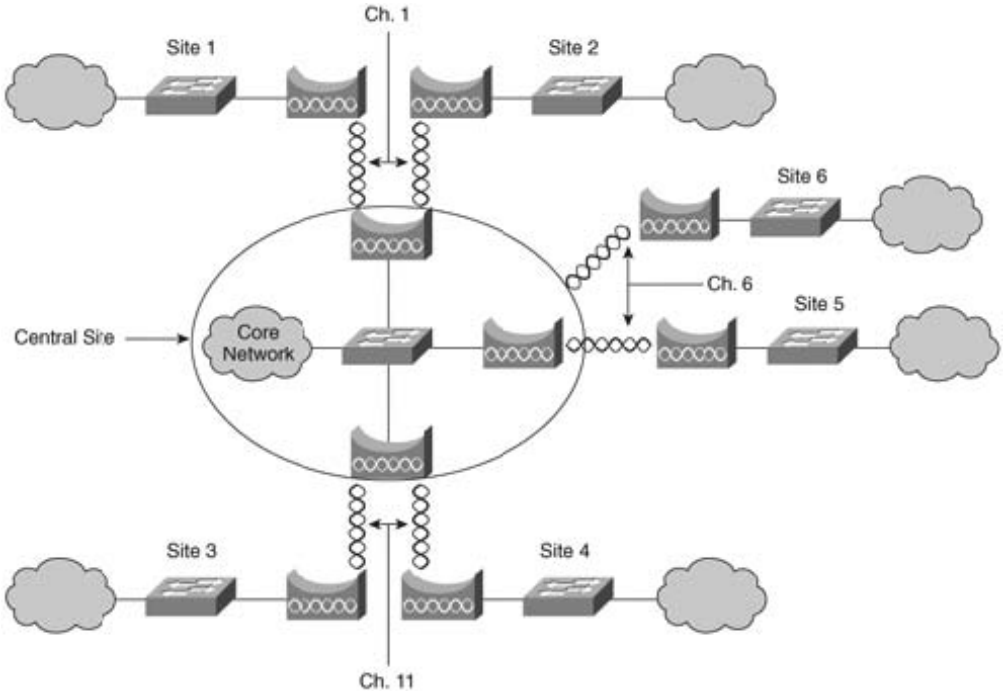


Εικόνα 2-21 Τοπολογία γεφυρών από σημείο προς πολλαπλά σημεία

Σε μερικές περιπτώσεις, οι γέφυρες δύνανται επίσης να ενεργήσουν ως AP επιτρέποντας σε μεμονωμένους ασύρματους πελάτες να συνδεθούν στη γέφυρα.

Ο αριθμός πιθανών μακρινών τοποθεσιών βασίζεται στον προμηθευτή, αλλά ο πραγματικός περιορισμός πρέπει να εξεταστεί από το ολικό εύρος ζώνης που απαιτείται από κάθε τελικό χρήστη. Η κύρια γέφυρα είναι το περιοριστικό σημείο. Σε μερικές περιπτώσεις, είναι επιθυμητό να υπάρχουν

πολλαπλές κύριες γέφυρες, που λειτουργούν σε χωριστές, μη επικαλυπτόμενες συχνότητες, όπως φαίνεται στο σχήμα 2-22.



Εικόνα 2-22 Τοπολογία γεφυρών από σημείο προς πολλαπλά σημεία

Οι περισσότερες γέφυρες λειτουργούν στο στρώμα 2 (στρώμα MAC). Εάν τα δίκτυα που συνδέονται είναι σε διαφορετικά υποδίκτυα, κάποιος τύπος δρομολογητή πρέπει να εγκατασταθεί τουλάχιστον σε μια τοποθεσία για να χωρίσει τα τμήματα και να δρομολογήσει την κυκλοφορία κατάλληλα. Πολλές εγκαταστάσεις χρησιμοποιούν δρομολογητές σε κάθε τοποθεσία, επιτρέποντας όχι μόνο την κατάτμηση, αλλά και τη χρήση εικονικών ιδιωτικών δικτυακών σηράγγων (VPN) πάνω στις RF συνδέσεις για ένα ασφαλέστερο σύστημα. Αυτό μπορεί επίσης να επιτρέψει μερικούς τύπους φιλτραρίσματος κυκλοφορίας για τη βελτίωση της ρυθμαπόδοσης της ασύρματης σύνδεσης.

Μελέτη σκοπιμότητας

Αυτή η ενότητα εξηγεί τι απαιτείται για να καθοριστεί εάν μια επιτυχής σύνδεση γεφυρών μπορεί να γίνει πραγματικότητα.

Κατά τον καθορισμό της δυνατότητας πραγματοποίησης μιας επιτυχούς σύνδεσης γεφυρών, πρέπει να καθοριστεί το πόσο μακριά η σύνδεση γεφυρών αναμένεται είναι, σε ποια συχνότητα και σε ποιους ρυθμούς διέλευσης δεδομένων. Οι πολύ κοντινές συνδέσεις γεφυρών (όπως 1 χιλιόμετρο ή λιγότερο) είναι αρκετά εύκολο να επιτευχθούν, υποθέτοντας ότι δεν υπάρχουν εμπόδια. Αυτό αναφέρεται ως καθαρή γραμμή θέας-οπτική επαφή (Line of Sight - LoS).

Κατά την προετοιμασία για την εγκατάσταση ενός συστήματος γεφυρών, πρέπει να εξεταστούν διάφοροι παράγοντες. Το LoS είναι εκ των ων ουκ άνευ για οποιαδήποτε υπαίθρια σύνδεση γεφυρών περισσότερων από 300m. Πρέπει επίσης να εξεταστούν δύο παράμετροι απόστασης: η ζώνη Fresnel και η καμπυλότητα της γης. Αυτοί οι δύο παράγοντες έχουν αντίκτυπο στην επιλογή ύψους των κεραιών. Οι περιβαλλοντικές συνθήκες όπως η βροχή, η ομίχλη και το χιόνι δεν έχουν μεγάλη επίδραση στις συνδέσεις των 2,4 ή 5 GHz.

Καθορισμός γραμμής θέας

Επειδή τα ραδιοκύματα, που χρησιμοποιούνται από τις γέφυρες των 2,4 και 5 GHz, είναι πολύ υψηλά σε συχνότητα, το μήκος κύματός τους είναι σχετικά μικρό. Κατά συνέπεια, τα

ραδιοκύματα δεν ταξιδεύουν τόσο μακριά (θεωρώντας το ίδιο ποσό ισχύος) όσο και τα ραδιοκύματα χαμηλότερων συχνοτήτων. Αυτό το γεγονός έχει επίσης ένα πλεονέκτημα: Κάνει τη γέφυρα ιδανική για χρήση χωρίς άδεια επειδή τα ραδιοκύματα δεν ταξιδεύουν μακριά, εκτός αν χρησιμοποιείται μια κεραία υψηλού κέρδους που μπορεί στενά να στρέψει τα ραδιοκύματα σε μια δεδομένη κατεύθυνση, μειώνοντας τις δυνατότητες παρέμβασης. Αυτό όχι μόνο παρέχει μεγαλύτερο εύρος αλλά παρέχει και μια πολύ μικρότερη εστίαση τόσο για την εκπομπή όσο και τη λήψη, μειώνοντας επίσης την πιθανότητα παρεμβολής σε άλλα συστήματα καθώς επίσης και από άλλα συστήματα. Αυτό με τη σειρά του σημαίνει επίσης ότι οι κεραίες αυτές είναι κρισιμότερες για την επίτευξη της κατάλληλης ευθυγράμμισης.

Όσο υψηλότερη είναι η χρησιμοποιούμενη συχνότητα, τόσο πιο εξαρτώμενο είναι ένα σύστημα από την οπτική επαφή. Επομένως, μεγαλύτερες αποστάσεις (περισσότερο ορισμένες εκατοντάδες μέτρα) που χρησιμοποιούν προϊόντα των 2,4 ή 5 GHz απαιτούν LoS για επιτυχή λειτουργία. Είναι πολύ δύσκολο να υλοποιηθεί μια καλή σύνδεση επικοινωνίας όταν επιχειρείται να μεταδοθούν ραδιοκύματα των 2,4 ή 5 GHz μέσω αντικειμένων όπως δέντρα, φύλλωμα, λόφοι ή άλλα κτήρια επειδή αυτά τα αντικείμενα μπορούν να απορροφήσουν ή να ανακλάσουν τα σήματα μακριά από τον προοριζόμενο στόχο.

Αποστάσεις μεγαλύτερες από 10 χιλιόμετρα απαιτούν γενικά ραδιοπύργους ή υψηλές θέσεις για να υπερνικήσουν την παρεμπόδιση LoS, που προκαλείται όχι μόνο από ενδιάμεσα εμπόδια αλλά και από την κυρτότητα της γης (βλ. σχήμα 2-23). Πιο συγκεκριμένα, η μέγιστη απόσταση πέραν από την το σφάλμα που εισάγεται στους υπολογισμούς εξ' αιτίας της καμπυλότητας της γης είναι σημαντικό δίνεται από τον τύπο $d = \frac{80}{f^{1/3}}$, όπου d σε km και f σε MHz. Συνεπώς προκύπτουν για τα δύο εύρη συχνοτήτων, που μας ενδιαφέρουν, $d_{2,4} = 5,975\text{km}$ και $d_{5,7} = 4,478\text{km}$. Για δύο κεραίες, που βρίσκονται σε ύψη h_1 και h_2, η μέγιστη απόσταση ζεύξης, ακολουθώντας τη γραμμή σκόπευσης, προκύπτει $d_m \cong \sqrt{2h_1\alpha} + \sqrt{2h_2\alpha}$, όπου $\alpha = 6370\text{km}$ είναι η μέση ακτίνα της γήινης επιφάνειας.

Εικόνα 2-23 Καμπυλότητα της γης

Καθώς η συχνότητα αυξάνεται, αυξάνονται και οι απώλειες του σήματος μέσω της ατμόσφαιρας. Αυτό είναι γνωστό ως απώλεια ελεύθερου χώρου ή απλά απώλεια διαδρομής. Καθώς το σήμα διαδίδεται από την κεραία, το επίπεδο ισχύος του μειώνεται με ρυθμό που είναι αντιστρόφως ανάλογος προς την απόσταση και ανάλογος προς το μήκος κύματος του σήματος. Η απώλεια μετάδοσης ελευθέρου χώρου L_s δίνεται από τον τύπο

$$L_s(\text{dB}) = 32,4 + 20\log_{10} d + 20\log_{10} f ,$$

όπου d η απόσταση πομπού-δέκτη σε km και f η συχνότητα σε MHz.

Η ισχύς του σήματος λήψης, που φτάνει στο άλλο άκρο του backbone link ή ζεύξης γεφυρώματος, θα δίνεται από τη γενική σχέση

$$W_R(\text{dBm}) = W_t(\text{dBm}) - L(\text{dB}),$$

$$\text{όπου } L(\text{dB}) = L_s - G_t - G_R + L_{c,t} + L_{c,R} + L_{con}$$

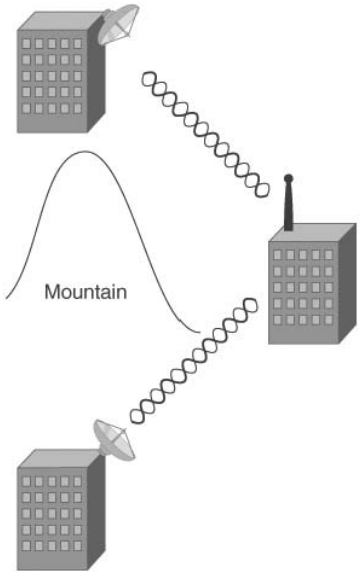
με L_s την προαναφερθείσα απώλεια μετάδοσης ελευθέρου χώρου, G_t και G_R τα κέρδη των κεραιών πομπού και δέκτη αντίστοιχα, $L_{c,t}$ και $L_{c,R}$ τις απώλειες των καλωδίων στον πομπό και το δέκτη αντίστοιχα και L_{con} τις απώλειες των μικροκυματικών βυσμάτων ή μετατροπέων.

Είναι δυνατόν, επομένως, να χρησιμοποιηθούν οι παραπάνω σχέσεις για να καθοριστεί η μέγιστη απόσταση, που μια σύνδεση γεφυρών μπορεί να φτάσει. Για τις συχνότητες, που μας ενδιαφέρουν, μπορεί να αποδειχθεί ότι κάθε αύξηση 6 dB (υψηλότερο κέρδος κεραιών, πιο σύντομα καλώδια) διπλασιάζει την απόσταση, ενώ με κάθε μείωση 6 dB (απώλεια από τα καλώδια ή χαμηλότερο κέρδος κεραιών) το εύρος πέφτει στο μισό.

Υπάρχουν εφαρμογές λογισμικού διαθέσιμες στον Ιστό που έχουν αναπτυχθεί για να βοηθήσουν σε αυτόν τον υπολογισμό. Μια τέτοια εφαρμογή είναι η "Cisco Outdoor Bridge Range Calculation Utility" διαθέσιμη στον ιστοχώρο της Cisco[1].

Αν και είναι δυνατόν να χρησιμοποιηθεί ένα σύστημα Global Positioning System (GPS) και τοπογραφικοί χάρτες για να καθοριστεί εάν οποιοιδήποτε λόφοι ή εμπόδια υπάρχουν ενδιάμεσα, είναι πάντα καλύτερο να πραγματοποιείται μία πρώτη επίσκεψη στην περιοχή και να καθοριστεί εάν οι τοποθεσίες που πρόκειται να συνδεθούν έχουν καθαρή οπτική επαφή. Μια επιτόπια αξιολόγηση μπορεί να απαντήσει σε πολλές ερωτήσεις, αλλά η πρόσβαση στη στέγη του κτηρίου ή η αναρρίχηση ενός πύργου μάλλον είναι απαραίτητη.

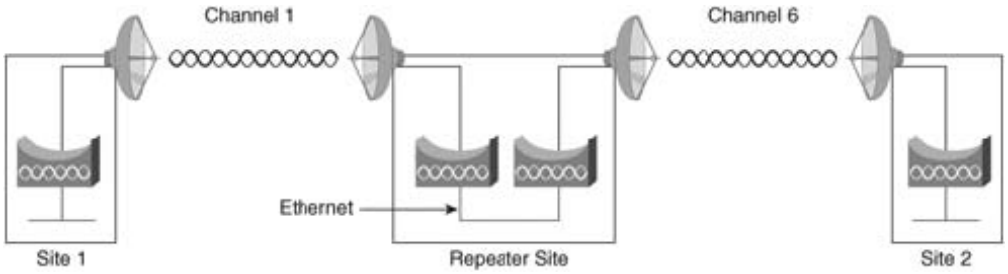
Εάν όλες οι τοποθεσίες έχουν οπτική σύνδεση με την τοποθεσία του κεντρικού κόμβου-γέφυρας, τότε η εγκατάσταση των συνδέσεων ίσως είναι ένα απλό θέμα καθορισμού των αποστάσεων και των επιθυμητών ρυθμών διέλευσης δεδομένων. Εάν τα κτήρια δεν έχουν οπτική επαφή άμεσα μεταξύ τους, τότε μία λύση είναι η εγκατάσταση ενός ραδιοπύργου ή η χρησιμοποίηση ενός κοντινού ραδιοπύργου ή ενός ιστού που να περνάει επάνω από το εμπόδιο. Μια άλλη πιθανή προσέγγιση είναι να βρεθεί μια θέση που και οι δύο περιοχές να μπορούν να δουν και να εγκατασταθεί εκεί ένας επαναλήπτης γεφυρών (βλ. σχήμα 2-24).



Εικόνα 2-24 Χρήση απομακρυσμένης τοποθεσίας για σύνδεση

Ένα μειονέκτημα με αυτόν τον τύπο λύσης είναι η μείωση της ρυθμαπόδοσης στο μισό, που εμφανίζεται κατά τη χρησιμοποίηση μιας ενιαίας ραδιοσυσκευής ως επαναλήπτης. Ένα εναλλακτικό σχέδιο, όπως φαίνεται στο σχήμα 2-25, χρησιμοποιεί δύο χωριστές συνδέσεις RF σε χωριστά κανάλια για να μειώσει αυτήν την υποβάθμιση της ρυθμαπόδοσης.

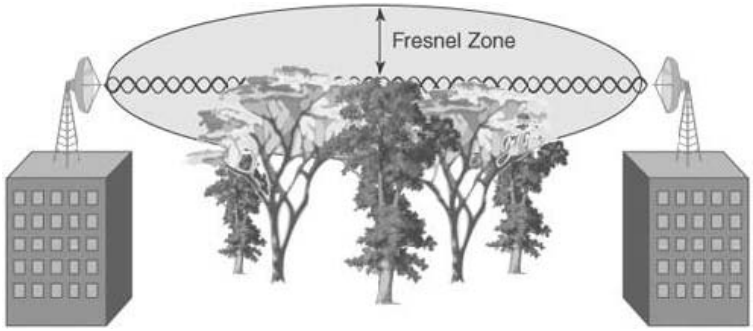
[1] http://www.cisco.com/en/US/products/hw/wireless/ps458/products_tech_note09186a008009459b.shtml



Εικόνα 2-25 Τοποθεσία επαναλήπτη με πλήρες εύρος ζώνης

Ζώνη Fresnel

Η ζώνη Fresnel είναι μια φανταστική έλλειψη γύρω από τη γραμμή οπτικής επαφής μεταξύ του πομπού και του δέκτη (βλ. σχήμα 2-26). Εάν τα ραδιοκύματα αντιμετωπίσουν μια παρεμπόδιση στην περιοχή Fresnel καθώς το σήμα ταξιδεύει μέσω του ελεύθερου χώρου στον προοριζόμενο στόχο, τότε το τελευταίο μπορεί να αποσβεσθεί, μερικές φορές σοβαρά. Η καλύτερη απόδοση και το καλύτερο εύρος επιτυγχάνονται όταν δεν υπάρχει καμία παρεμπόδιση αυτής της περιοχής Fresnel. Αν και αυτό είναι όχι πάντα απολύτως αναπόφευκτο, οι μηχανικοί πρέπει να προσπαθήσουν να διατηρήσουν μια καθαρή ζώνη για το 60% της περιοχής Fresnel. Επίσης πρέπει να ληφθεί υπόψη ότι μια ζώνη Fresnel είναι όχι μόνο κάθετη, αλλά πραγματικά περιβάλλει το σήμα σε μια ζώνη 360^{o}. Συνεπώς, πρέπει να διατηρηθεί η εκκαθάριση της ζώνης Fresnel σε όλες τις κατευθύνσεις.



Εικόνα 2-26 Fresnel Zone

Για να βελτιωθεί μια ζώνη Fresnel που εμποδίζεται από κάποια δομή είναι απαραίτητη η ανύψωση επάνω από ή μακριά από το εμπόδιο, η οποία απαιτεί συνήθως εγκατάσταση υψηλότερης κεραίας. Αυτό μπορεί να είναι απλό θέμα τοποθέτησης της κεραίας σε ένα άλλο σημείο στο κτήριο, όπως ένα δωμάτιο ανελκυστήρων ή άλλη δομή υψηλότερη στη στέγη του κτηρίου. Εντούτοις, μπορεί επίσης να σημαίνει τοποθέτηση μίας πιο ψηλής δομής.

Είναι δυνατό να υπολογιστεί η ακτίνα της πρώτης ζώνης Fresnel (σε μέτρα) σε οποιοδήποτε συγκεκριμένο σημείο κατά μήκος της γραμμής οπτικής επαφής χρησιμοποιώντας την ακόλουθη εξίσωση:

$$h_1 = \sqrt{\frac{c}{\left(\frac{1}{d_1} + \frac{1}{d_2}\right) \cdot f}}$$

όπου d_1 και d_2 οι αποστάσεις του προαναφερθέντος σημείου από τον πομπό και το δέκτη αντίστοιχα.

Εμπειρικά, όπως αναφέρθηκε παραπάνω, απαιτείται εκκαθάριση του 60% της πρώτης ζώνης Fresnel για μια καλή και σταθερή σύνδεση. Υπό αυτήν τη μορφή, μπορεί να τροποποιηθεί ο προηγούμενος τύπος ως εξής:

$$0,6 \cdot h_1 = \sqrt{\frac{3 \cdot 10^8}{\left(\frac{1}{d_1} + \frac{1}{d_2}\right) \cdot f}}$$

Η εφαρμογή "Cisco Outdoor Bridge Range Calculation Utility", που αναφέρθηκε προηγούμενα προσφέρει αυτόν τον υπολογισμό.

Ζητήματα περιβαλλοντικών συνθηκών

Η βροχή, το χιόνι, η ομίχλη και άλλες καιρικές συνθήκες υψηλής υγρασίας μπορούν να έχουν δυσμενείς επιπτώσεις στη γραμμή οπτικής επαφής, εισάγοντας μια μικρή απώλεια (μερικές φορές καλούμενη εξασθένιση βροχής ή περιθώριο εξασθένισης). Γενικά, αυτές οι καιρικές συνθήκες έχουν την ελάχιστη επίδραση στις συνδέσεις RF που υλοποιούνται σε συχνότητες κάτω από 10 GHz. Εάν έχει γίνει εγκατάσταση μια καλής και σταθερής σύνδεση, τέτοιος καιρός σχεδόν ποτέ δεν θα προκαλέσει πρόβλημα' εντούτοις, εάν η σύνδεση είναι εξ' αρχής "φτωχή", η κακοκαιρία δύναται να υποβιβάσει την απόδοση ή να προκαλέσει ακόμα και απώλεια της σύνδεσης.

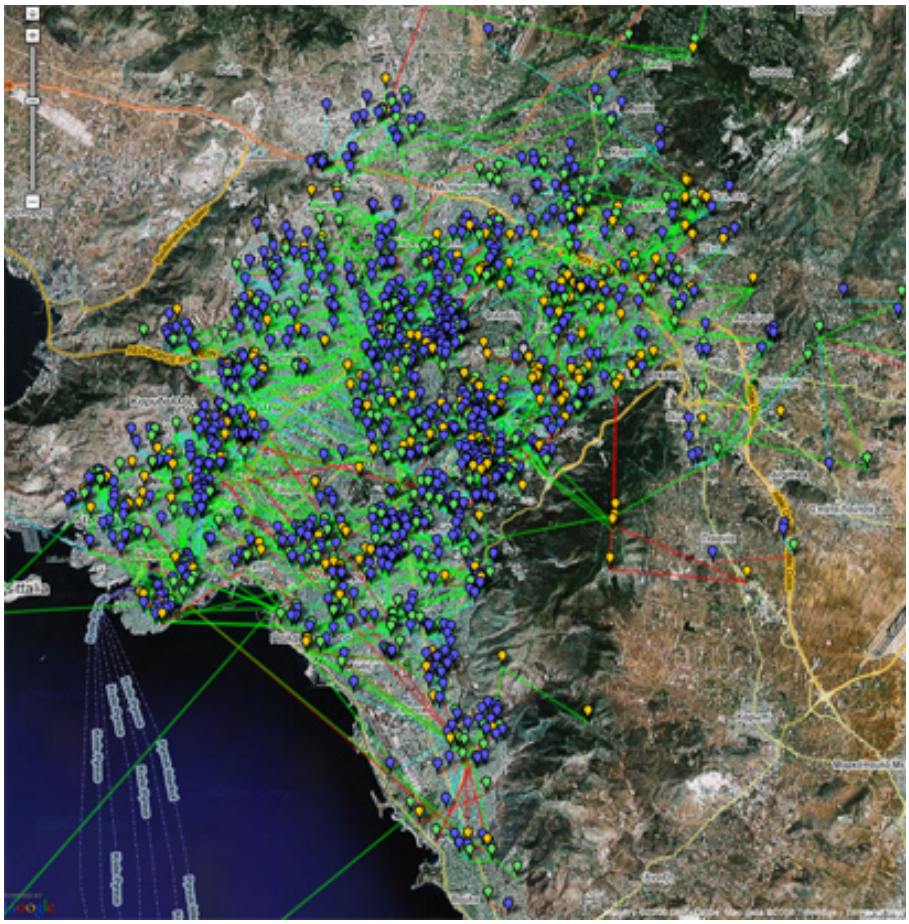
Για τον λόγο αυτό, οι περισσότεροι υπολογισμοί απωλειών διαδρομής πρέπει να περιλάβουν κάποιο περιθώριο εξασθένισης. Συνήθως 10 dB είναι ικανοποιητικά για τα δίκτυα δεδομένων στα 2,4 ή 5 GHz.

Μελέτη παρεμβολών

Αν και το μη αδειοδοτημένο φάσμα προσφέρει το όφελος της δωρεάν χρήσης αυτού, το αντιστάθμισμα προκύπτει από την άποψη της παρεμβολής. Δεν υπάρχει κανένας περιορισμός για τους τύπους των συσκευών που λειτουργούν σε αυτές τις ζώνες, υπό τον όρο ότι όλες αυτές προσαρμόζομαι σε ένα κοινό σύνολο κανόνων. Αν και σήμερα η ζώνη των 5 GHz είναι λιγότερο συσσωρευμένη από τη ζώνη των 2.4-GHz, με το πέρας του χρόνου θα γίνει πιθανώς η ζώνη των 5 GHz εξίσου συσσωρευμένη με όλο και περισσότερες παρεμβάλλουσες συσκευές.

Οι ISM συχνότητες (Industrial, Scientific, and Medical) μπορούν να περιέχουν εκπομπές από φούρνους μικροκυμάτων, θερμάστρες, ιατρικό εξοπλισμό και άλλες συσκευές. Αν και οι περισσότεροι από αυτούς τους τύπους συσκευών δεν αποτελούν συνήθως καμία απειλή παρεμβολής για τις συνδέσεις γεφυρών (επειδή είναι χαμηλής ισχύος, εσωτερικές συσκευές), ο μηχανικός πρέπει έχει υπόψη του τη πιθανότητα να υπάρχει κάποιο βιομηχανικό σύστημα υψηλής ισχύος που "ρίχνει" οποιαδήποτε αποπειραθείσα χρήση επικοινωνιών εκείνης της ζώνης.

Ραδιοερασιτέχνες επιτρέπεται επίσης να χρησιμοποιήσουν μέρη ζωνών, στις οποίες τα προϊόντα γεφυρών λειτουργούν. Μιλώντας συγκεκριμένα για την ευρύτερη περιοχή της Αττικής, είναι πολλές οι πλήρους απασχόλησης (στον αέρα συνεχώς) από σημείο σε σημείο ερασιτεχνικές συνδέσεις, που λειτουργούν στις ζώνες των 2,4 και 5 GHz (βλ. εικόνα 2-27).



Εικόνα 2-27 Χάρτης Ασύρματου Μητροπολιτικού Δικτύου Αθηνών

Επομένως είναι απαραίτητο να γίνει μια ανάλυση παρεμβολής χρησιμοποιώντας έναν αναλυτή φάσματος για να διαβεβαιωθεί ότι η μελλοντική ραδιοσύνδεση είναι ελεύθερη από παρεμβολές.

ΚΕΦΑΛΑΙΟ 3ο
Υλοποίηση

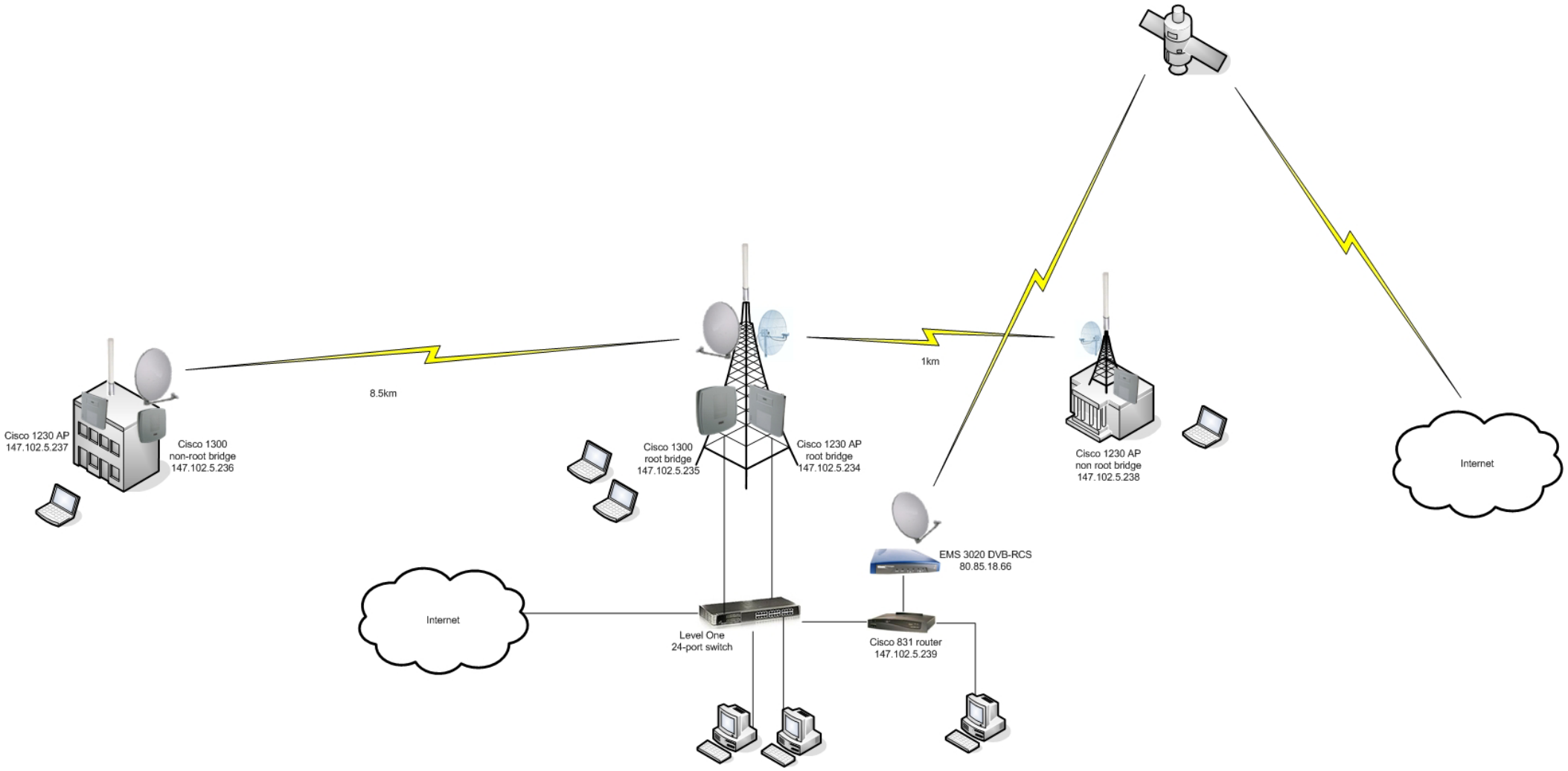
Εισαγωγή

Όπως έχει ήδη αναφερθεί στην εισαγωγή της παρούσας διπλωματικής εργασίας, σκοπός κατ' αρχάς αυτής ήταν η υλοποίηση ενός ασύρματου δικτύου κορμού (backbone ή backhaul) υψηλής ταχύτητας, που θα επεκτείνει το ενσύρματο δίκτυο του εργαστηρίου Μικροκυμάτων και Οπτικών Ινών του Εθνικού Μετσόβιου Πολυτεχνείου. Τα σημεία-χώροι, που επέλεξα για να αποτελέσουν όχι μόνο τα άκρα αυτού του κορμού αλλά και 802.11b/g σημεία πρόσβασης, είναι το Τμήμα Φυσικού του Εθνικού & Καποδιστριακού Πανεπιστημίου[2] και ένας ιδιωτικός χώρος (ταράτσα τετραώροφης πολυκατοικίας) στην περιοχή του Αμαρουσίου[3] μεταξύ των σταθμών ΗΣΑΠ Νερατζιώτισσα και Μαρούσι.

Επιπλέον στόχος ήταν να αποτελέσει πύλη προς το διαδίκτυο (gateway) του παραπάνω δικτύου όχι μόνο το ενσύρματο δίκτυο του Πολυτεχνείου αλλά και μια 512kbps DVB-RCS δορυφορική σύνδεση με το δορυφόρο Hellasat. Σίγουρα το εύρος ζώνης που προσφέρει η δορυφορική σύνδεση δεν μπορεί να συγκριθεί με εκείνη του Πολυτεχνείου, ωστόσο η υλοποίηση της δορυφορικής σύνδεσης κρίθηκε σημαντική στα πλαίσια εξάλειψης του "ψηφιακού χάσματος". Πιο συγκεκριμένα, πομποδέκτης DVB-RCS δύναται να αποτελέσει την διαδικτυακή πύλη ασύρματου τοπικού δικτύου, όπως αυτό που υλοποιήθηκε στην παρούσα διπλωματική, σε δύσβατη επαρχιακή τοποθεσία.

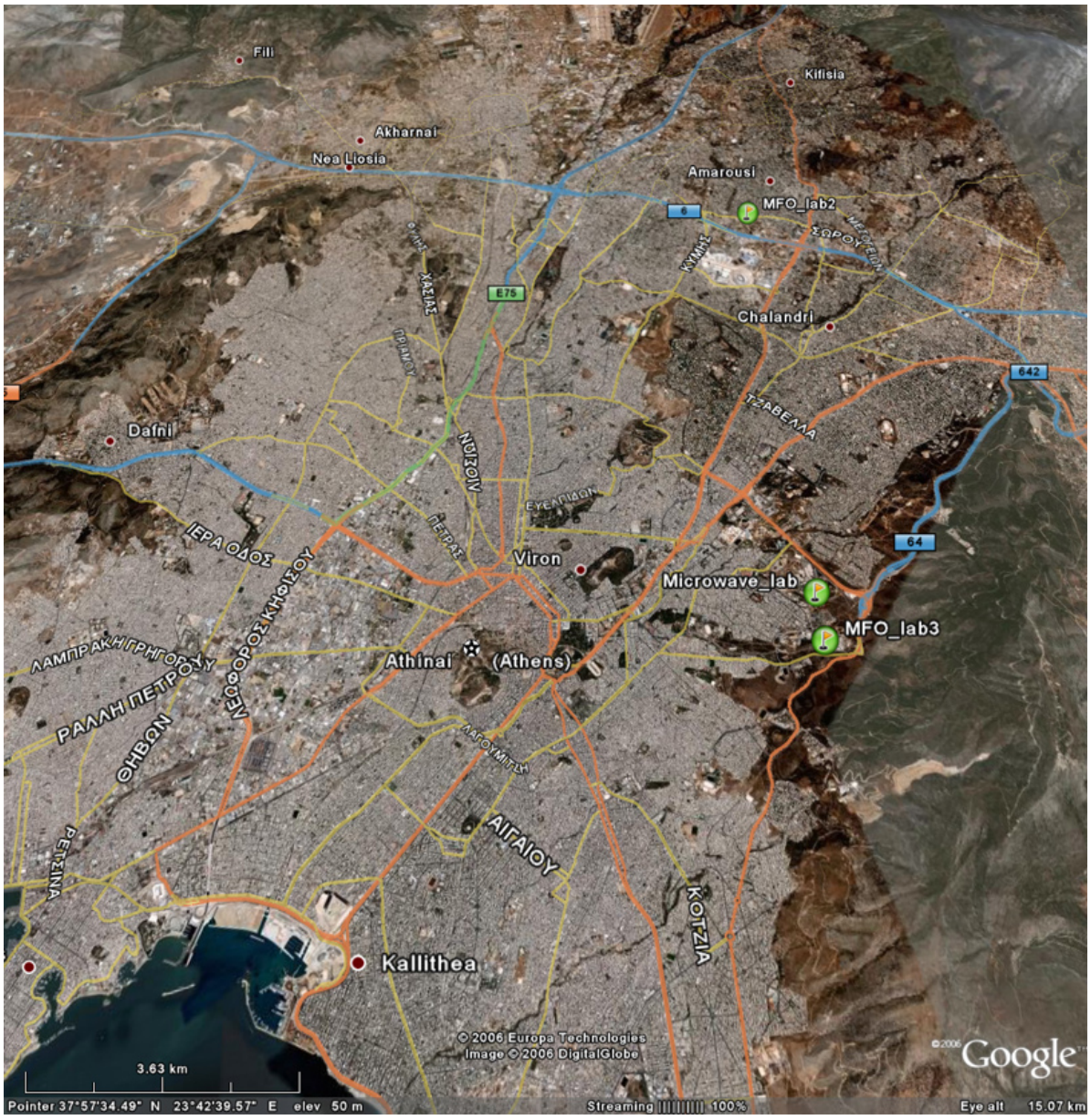
Πιο αναλυτικά, ακολουθεί παραστατικό διάγραμμα του ασύρματου δικτύου και των διαδικτυακών πυλών αυτού.

[2] Η απόσταση μεταξύ των bridges στο Πολυτεχνείου και το Τμήμα Φυσικού είναι 0,9 χιλιόμετρα.
[3] Η απόσταση μεταξύ των bridges στο Πολυτεχνείου και το την πολυκατοικία στο Μαρούσι είναι 8,5 χιλιόμετρα.



Εικόνα 3-1 Συνολικό διάγραμμα του υλοποιηθέντος ασύρματου δικτύου και των πυλών (gateways) αυτού

Ακολουθεί δορυφορική φωτογραφία, στα δεξιά της οποίας φαίνονται με ακρίβεια οι τοποθεσίες των εγκατεστημένων κόμβων με πράσινες βούλες.



Εικόνα 3-2 Δορυφορική φωτογραφία τοποθεσιών εγκατεστημένων κόμβων

Cisco® Aironet® 1230AG Series Access Point

Πριν ξεκινήσει η ανάλυση της υλοποίησης κάθε κόμβου χωριστά αξίζει να αναφερθεί ότι το υλοποιηθέν ασύρματο δίκτυο βασίστηκε κατά κύριο λόγο στα Cisco® Aironet® 1230AG Series Access Points. Αυτά τα a/b/g access points είναι σχεδιασμένα για απαιτητικό περιβάλλον ραδιοσυχνοτήτων. Διαθέτουν εξωτερικά βύσματα κεραιών τόσο για το b/g όσο και για το a δίκτυο προκειμένου να είναι δυνατό να επιτευχθεί εκτεταμένου εύρους κάλυψη. Σε αυτό, φυσικά συνεισφέρουν και η υψηλή ισχύς εκπομπής και ευαισθησία λήψης που χαρακτηρίζουν το ράδιο των 2,4 και 5 GHz.

Εικόνα 3-3 Cisco 1230 Access Point και Bridge

Στον τομέα της ασφάλειας υποστηρίζει 802.11i, WPA2 (Wi-Fi Protected Access 2), WPA και ένα μεγάλο αριθμό τύπων Extensible Authentication Protocol (EAP). Τα WPA και WPA2 αποτελούν τις πιστοποιήσεις του Wi-Fi Alliance για διαλειτουργική και προτυποποιημένη ασφάλεια ασυρμάτων δικτύων. Αυτές οι πιστοποιήσεις υποστηρίζουν την IEEE 802.1X για την επικύρωση της ταυτότητας των χρηστών. Το Temporal Key Integrity Protocol (TKIP) χρησιμοποιείται για την κρυπτογράφηση WPA και η Advanced Encryption Standard (AES) για την κρυπτογράφηση WPA2. Αυτές οι πιστοποιήσεις βοηθούν ώστε να εξασφαλιστεί διαλειτουργικότητα μεταξύ των επικυρωμένων ασύρματων συσκευών Wi-Fi, που προέρχονται από διαφορετικούς κατασκευαστές. Η πιστοποίηση IEEE 802.1X βοηθά να εξασφαλίσει ότι μόνο οι εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στο δίκτυο. Παρέχει επίσης συμβατότητα και υποστήριξη για συσκευές πελατών με WPA που τρέχουν TKIP και χρησιμοποιούν τον αλγόριθμο κρυπτογράφησης RC4. Για όλα τα παραπάνω υπάρχει αναφορά στο επόμενο κεφάλαιο.

Στον παρακάτω πίνακα φαίνονται τα χαρακτηριστικά γνωρίσματα του access point που χρησιμοποιήθηκε και επεξηγείται η χρησιμότητά του.

Χαρακτηριστικό	Όφελος
Διπλά 802.11a και 802.11g ράδιο	Παρέχει μέχρι και 108 Mbps χωρητικότητας για απαιτητικές εφαρμογές και συμβατότητα με παλαιότερες 802.11b συσκευές
Διπλοί RP-TNC κονέκτορες κεραιών και για τα δύο. 2.4 GHz και 5 GHz, ράδιο	Τα βύσματα των κεραιών επιτρέπουν σύνδεση με μεγάλη ποικιλία 2.4 GHz και 5 GHz κεραιών, ανάλογα με τις εκάστοτε ανάγκες κάλυψης
Ευελιξία στον ρόλο της σύνδεσης	Τα αυτόνομα access points μπορούν να λειτουργήσουν ως access point ή bridge (γέφυρα), όταν είναι ρυθμισμένα είτε σαν μονής είτε διπλής μπάντας πλατφόρμες, επιτρέποντας σε κάθε ράδιο να είναι ανεξάρτητα ρυθμισμένο σαν access point repeater, root bridge, non-root bridge ή workgroup bridge, δίνοντας τη δυνατότητα για ευρεία γκάμα εφαρμογών
Ενοποιημένο Cisco IDS/IPS	Αυτό το ενσωματωμένο χαρακτηριστικό λογισμικού είναι μέρος του Cisco Self-Defending Network και είναι η πρώτη βιομηχανικά ενσωματωμένη ενσύρματη και ασύρματη λύση ασφαλείας. Όταν ένας έμπιστο πελάτης δρα κακόβουλα, τότε το ενσύρματο IDS εντοπίζει την επίθεση και στέλνει αιτήσεις στους Cisco WLAN ελεγκτές, οι οποίοι θα προβούν στο disassociation με την συσκευή-πελάτη
Ασφάλεια	Authentication Πρότυπα ασφαλείας: · WPA · WPA2 (802.11i) · Cisco TKIP · Cisco message integrity check (MIC)

	· IEEE 802.11 WEP keys of 40 bits and 128 bits 802.1X EAP types: · EAP-Flexible Authentication via Secure Tunneling (EAP-FAST) · Protected EAP-Generic Token Card (PEAP-GTC) · PEAP-Microsoft Challenge Authentication Protocol Version 2 (PEAP-MSCHAP) · EAP-Transport Layer Security (EAP-TLS) · EAP-Tunneled TLS (EAP-TTLS) · EAP-Subscriber Identity Module (EAP-SIM) · Cisco LEAP Encryption: · AES-CCMP encryption (WPA2) · TKIP (WPA) · Cisco TKIP · WPA TKIP · IEEE 802.11 WEP keys of 40 bits and 128 bits
Υποστηρίζει 12 μη-επικαλυπτόμενα κανάλια, με δυνατότητα μέχρι και 23 κανάλια	Η το δυνατόν χαμηλότερη παρεμβολή με γειτονικά access points απλοποιεί τη λειτουργία. Λιγότερη λάθη εκπομπής μεγαλύτερη διέλευση
Ανθεκτικό μεταλλικό κάλυμμα	Ανθεκτικό μεταλλικό κάλυμμα και άλλα χαρακτηριστικά υποστηρίζουν τη χρησιμοποίηση σε εργοστάσια και σε εξωτερικό περιβάλλον (μέσα σε κατάλληλα κουτιά).
Κρυπτογράφηση AES υποβοηθούμενη από υλισμικό	Προσφέρει υψηλή ασφάλεια χωρίς υποβάθμιση των επιδόσεων
Αναβάθμιση του ασύρματου δικτύου	Επεκτείνει την ασφάλεια, την αξιοπιστία, την ευκολία της επέκτασης, και την διαχείριση του δικτύου
Λογισμικό Ios Cisco	Παραδίδει υψηλού επιπέδου υπηρεσίες κατηγορίας για τη συνδεσιμότητα, την εξελιξιμότητα, και τη διαθεσιμότητα του δικτύου
Εκτίμηση ολομέλειας UL 2043	Αντοχή σε υψηλές θερμοκρασίες

Στον επόμενο πίνακα εμφανίζονται όλα τα τεχνικά χαρακτηριστικά του σημείου πρόσβασης Aironet 1200

Λογισμικό	Cisco IOS Software Release 12.3(8) JA ή επόμενο	
Υποστηριζόμενοι ρυθμοί δεδομένων	802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps	
Ενσύρματη σύνδεση	Autosensing 802.3 10/100BASE-T Ethernet	
Υλισμική μορφή ράδιου	802.11a: CardBus (32-bit)	802.11b or 802.11g: Mini-PCI (32-bit)
Μπάντες συχνοτήτων και κανάλια λειτουργίας	ETSI 2.412 to 2.472 GHz; 13 κανάλια 5.15 to 5.35 GHz; 8 κανάλια 5.470 to 5.725 MHz; 11 κανάλια	
Μη επικαλυπτόμενα	802.11g: 3	

κανάλια			
Ασύρματη διαμόρφωση	802.11g: Direct sequence spread spectrum (DSSS); OFDM		
Ευαισθησία λήψης (τυπική)	802.11a: 6 Mbps: -87 dBm 9 Mbps: -87 dBm 12 Mbps: -85 dBm 18 Mbps: -84 dBm 24 Mbps: -81 dBm 36 Mbps: -78 dBm 48 Mbps: -73 dBm 54 Mbps: -72 dBm	802.11b: 1 Mbps: -94 dBm 2 Mbps: -91 dBm 5.5 Mbps: -89 dBm 11 Mbps: -85 dBm	802.11g: 6 Mbps: -90 dBm 9 Mbps: -84 dBm 12 Mbps: -82 dBm 18 Mbps: -80 dBm 24 Mbps: -77 dBm 36 Mbps: -73 dBm 48 Mbps: -72 dBm 54 Mbps: -72 dBm
Διαθέσιμες ρυθμίσεις ισχύος εκπομπής (η ρύθμιση για μέγιστη ισχύ εκπομπής μπορεί να διαφέρει ανά κανάλι και εξαρτάται από τους ισχύοντες κατά τόπους νόμους)	802.11a: OFDM: 17 dBm (50 mW) 15 dBm (30 mW) 14 dBm (25 mW) 11 dBm (12 mW) 8 dBm (6 mW) 5 dBm (3 mW) 2 dBm (2 mW) -1 dBm (1 mW)	802.11b CCK: 100 mW (20 dBm) 50 mW (17 dBm) 30 mW (15 dBm) 20 mW (13 dBm) 10 mW (10 dBm) 5 mW (7 dBm) 1 mW (0 dBm)	802.11g: OFDM: 30 mW (15 dBm) 20 mW (13 dBm) 10 mW (10 dBm) 5 mW (7 dBm) 1 mW (-1 dBm)
Συμβατότητα	Standards Safety UL 60950-1 CAN/CSA-C22.2 No. 60950-1 IEC 60950-1 EN 60950-1 UL 2043 FIPS 140-2 Pre-Validation List Common Criteria (Cisco IOS Software only) Radio Approvals FCC Part 15.247 RSS-210 (Canada) EN 300.328, EN 301.893 (Europe) ARIB-STD 33 (Japan) ARIB-STD 66 (Japan) ARIB-STD T71 (Japan) AS/NZS 4771, 4268.2 (Australia and New Zealand) EMI and Susceptibility (Class B) FCC Part 15.107 and 15.109 ICES-003 (Canada) VCCI (Japan) EN 301.489-1 and -17 (Europe) AS/NZS 3548 Security 802.11i, WPA2, WPA 802.1X AES, TKIP		

	Other IEEE 802.11g and IEEE 802.11a FCC Bulletin OET-65C RSS-102
Διαχείριση δικτύου	BootP, Secure Shell (SSH) Protocol, Secure HTTP (HTTPS), Trivial File Transfer Protocol (TFTP), FTP, Telnet, console port, Simple Network Management Protocol (SNMP) MIB I and MIB II, CiscoWorks Resource Manager Essentials (RME), CiscoWorks Software Image Manager (SWIM), CiscoWorks Campus Manager, CiscoWorks CiscoView, and CiscoWorks WLSE
Περίβλημα	Die-cast aluminum
Διαστάσεις (Υ x Π x Μ)	1.660 x 6.562 x 7.232 in. (4.22 x 16.67 x 18.37 cm); add 0.517 in. (1.31 cm) height for mounting bracket
Βάρος	1.725 lb (0.783 kg)
Περιβαλλοντικές ανοχές	Θερμοκρασία λειτουργίας: -4 to 122°F (-20 to 50°C) Υγρασία λειτουργίας: 10 ως 90% (non-condensing)
Μνήμη και επεξεργαστής	IBM PowerPC405 (200 MHz) 16 MB RAM; 8 MB Flash memory
Απαιτήσεις τροφοδοσίας	90 to 240 VAC ±10%(power supply) 48 VDC ±10%
Ισχύς	13W maximum
Πιστοποίηση Wi-Fi	Wi Fi CERTIFIED

Cisco® Aironet® 1300 Series Outdoor Bridge or Access Point

Εικόνα 3-4 Cisco 1300 Bridge και Access Point

Το Cisco® Aironet® 1300 Series Outdoor Access Point or Bridge (βλ. σχήμα 1) είναι ένα σημείο πρόσβασης και μια γέφυρα 802.11g που παρέχει ασύρματη συνδεσιμότητα υψηλής ταχύτητας μεταξύ πολλαπλών σταθερών ή κινητών δικτύων και πελατών. Το Cisco Aironet 1300 υποστηρίζει τους τυποποιημένους ρυθμούς διέλευσης δεδομένων 802.11g μέχρι 54 Mbps διατηρώντας πλήρη συμβατότητα προς τα πίσω με συσκευές 802.11b. Διατίθεται σε ένα συμπαγές και ισχυρό κάλυμμα για εγκατάσταση σε υπαίθριο περιβάλλον. Στα πλαίσια αυτής της διπλωματικής επιλέχθηκε η έκδοση του 1300 με βύσματα κεραιών που υποστηρίζουν μια μεγάλη ποικιλία κεραιών στη συχνότητα 2.4-GHz.

Το Cisco Aironet 1300 είναι διαθέσιμο είτε ως τμήμα του Cisco Unified Wireless Network είτε ως αυτόνομο σημείο πρόσβασης ή γέφυρα. Δεδομένου ότι η συσκευή θα χρησιμοποιούταν ως γέφυρα για μια μόνο ζεύξη κορμού επιλέχθηκε η έκδοσή του ως αυτόνομη συσκευή.

Στον πίνακα που ακολουθεί δείχνονται οι τρεις δυνατές διαφορετικές λειτουργίες του Cisco 1300.

Ρόλος	**Εφαρμογές**	**Ενοποιημένη ή αυτόνομη αρχιτεκτονική**	**Συμβατότητα**
Access Point	Κατασκευασμένο συγκεκριμένα για δύσκολα υπαίθρια περιβάλλοντα, αλλά και ικανό για εσωτερικές επεκτάσεις, το Cisco Aironet 1300 είναι ιδανικό για WLANs που απιτούν την υπαίθρια κάλυψη. Το Cisco Aironet 1300 είναι Wi-Fi πιστοποιημένο ως σημείο πρόσβασης.	ενοποιημένη ή αυτόνομη	• Συμβατό με οποιαδήποτε Wi-Fi πιστοποιημένη συσκευή πελάτη WPA ή WPA2 • Συμβατό με πελάτες Cisco Aironet και πελάτες συμβατούς με Cisco εξοπλισμό
Bridge	Το Cisco Aironet 1300 υποστηρίζει διαμορφώσεις είτε από σημείο σε σημείο είτε από σημείο σε πολλαπλά σημεία για να διασυνδέσει οικονομικά μακρινά, προσωρινά ή κινητά δίκτυα. Ενώ βρίσκεται σε λειτουργία γέφυρας, μπορεί επίσης να δεχτεί συνδέσεις από πελάτες παρέχοντας ταυτόχρονα την ικανότητα γέφυρας και σημείου πρόσβασης.	αυτόνομη	Συμβατό με γέφυρες σειρών Cisco Aironet 1300 και 350
Workgroup Bridge	Σαν γέφυρα ομάδας εργασίας, το Cisco Aironet 1300 συνδέει γρήγορα οποιαδήποτε συσκευή Ethernet, όπως ένα φορητό υπολογιστή, με ένα WLAN. Με την προσθήκη μιας τυποποιημένου Ethernet hub ή switch, είναι δυνατή η σύνδεση μέχρι 255 τέτοιων συσκευών.	αυτόνομη	Υποστηρίζει λειτουργία με σημεία πρόσβασης Cisco Aironet και γέφυρες Cisco

Το Cisco Aironet 1300 υποστηρίζει 802.11i, Wi-Fi Protected Access 2 (WPA2), WPA και πολυάριθμα πρωτόκολλα επεκτάσιμης επικύρωσης (Extensible Authentication Protocol - EAP). Τα WPA και WPA2 αποτελούν τις πιστοποιήσεις της συμμαχίας Wi-Fi για διαλειτουργική και προτυποποιημένη ασφάλεια WLAN. Αυτές οι πιστοποιήσεις υποστηρίζουν IEEE 802.1X για την επικύρωση χρηστών, TKIP (Temporal Key Integrity Protocol) για κρυπτογράφηση WPA και AES (Advanced Encryption Standard) για κρυπτογράφηση WPA2. Για όλα τα παραπάνω υπάρχει αναφορά στο επόμενο κεφάλαιο.

Ο παρακάτω πίνακας δείχνει τα πρωτόκολλα που υποστηρίζονται από τη σειρά Cisco Aironet 1300.

Προτυπα διεπαφής ράδιου	IEEE 802.11b or IEEE 802.11g
Ζώνη συχνοτήτων	• 2.412 to 2.462 GHz (FCC) • 2.412 to 2.472 GHz (ETSI) • 2.412 to 2.472 GHz (TELEC)
Ασύρματη διαμόρφωση	802.11b • Direct Sequence Spread Spectrum (DSSS): – Differential Binary Phase Shift Keying (DBPSK) at 1 Mbps – Differential Quadrature Phase Shift Keying (DQPSK) at 2 Mbps – Complementary Code Keying (CCK) at 5.5 and 11 Mbps 802.11g • Orthogonal Frequency Divisional Multiplexing (OFDM): – BPSK at 6 and 9 Mbps – QPSK at 12 and 18 Mbps – 16-quadrature amplitude modulation (QAM) at 24 and 36 Mbps – 64-QAM at 48 and 54 Mbps
Πρωτόκολλο πρόσβασης στο μέσο	Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA)
Κανάλια λειτουργίας	802.11b/g • ETSI: 13 • Americas: 11 • TELEC (Japan): 13
Μη επικαλυπτόμενα κανάλια	3
Ασφάλεια – Λειτουργία γέφυρας	Cisco Wireless Security Suite, including: Authentication • 802.1X support including LEAP to yield mutual authentication and dynamic per-user, per-session encryption keys Encryption • Cisco TKIP or WPA TKIP; key hashing (per-packet keying), Message Integrity Check (MIC) and broadcast key rotation • AES (802.11i)
Ασφάλεια – Λειτουργία σημείου πρόσβασης	Cisco Wireless Security Suite supporting WPA and WPA2, including: Authentication • Η προστασία πλαισίων διαχείρισης επιτρέπει την επικύρωση των πλαισίων διαχείρισης 802.11 από την ασύρματη δικτυακή υποδομή. Αυτό επιτρέπει στο δίκτυο να ανιχνεύσει πλαίσια από κακόβουλους χρήστες. Εάν ένα σημείο πρόσβασης ανιχνεύσει μια κακόβουλη επίθεση, ένα γεγονός θα παραχθεί από τα σημεία πρόσβασης και αναφορές θα μαζευτούν στον ελεγκτή Cisco του ασύρματου LAN. • 802.1X support including Cisco LEAP, Protected EAP-Generic Token Card (PEAP-GTC), PEAP-Microsoft Challenge Authentication Protocol Version 2 (MSCHAPv2), EAP Message Digest 5 (EAP MD5), EAP-Transport Layer Security (EAP-TLS), EAP-Tunneled TLS (EAP-TTLS), EAP-Subscriber Identity Module (EAP-SIM), and EAP-Flexible Authentication via Secure Tunneling (EAP-FAST) to yield mutual authentication and dynamic per-user, per-session encryption keys Encryption • WPA: Cisco TKIP or WPA TKIP; key hashing (per-packet keying), MIC and broadcast key rotation • WPA2: AES (802.11i)
Ασφάλεια – Λειτουργία γέφυρας ομάδας	Cisco Wireless Security Suite, including: Authentication

εργασίας	• 802.1X support including Cisco LEAP to yield mutual authentication και dynamic per-user, per-session encryption keys Encryption • Cisco TKIP or WPA TKIP; key hashing (per-packet keying), MIC και broadcast key rotation • AES (802.11i)
Συμβατότητα SNMP	Εκδόσεις 1 and 2
Πιστοποίηση Wi-Fi	Wi Fi CERTIFIED

Τοποθεσία Εθνικού Μετσόβιου Πολυτεχνείου

Εικόνα 3-5 Δορυφορική φωτογραφία τοποθεσίας Εθνικού Μετσόβιου Πολυτεχνείου

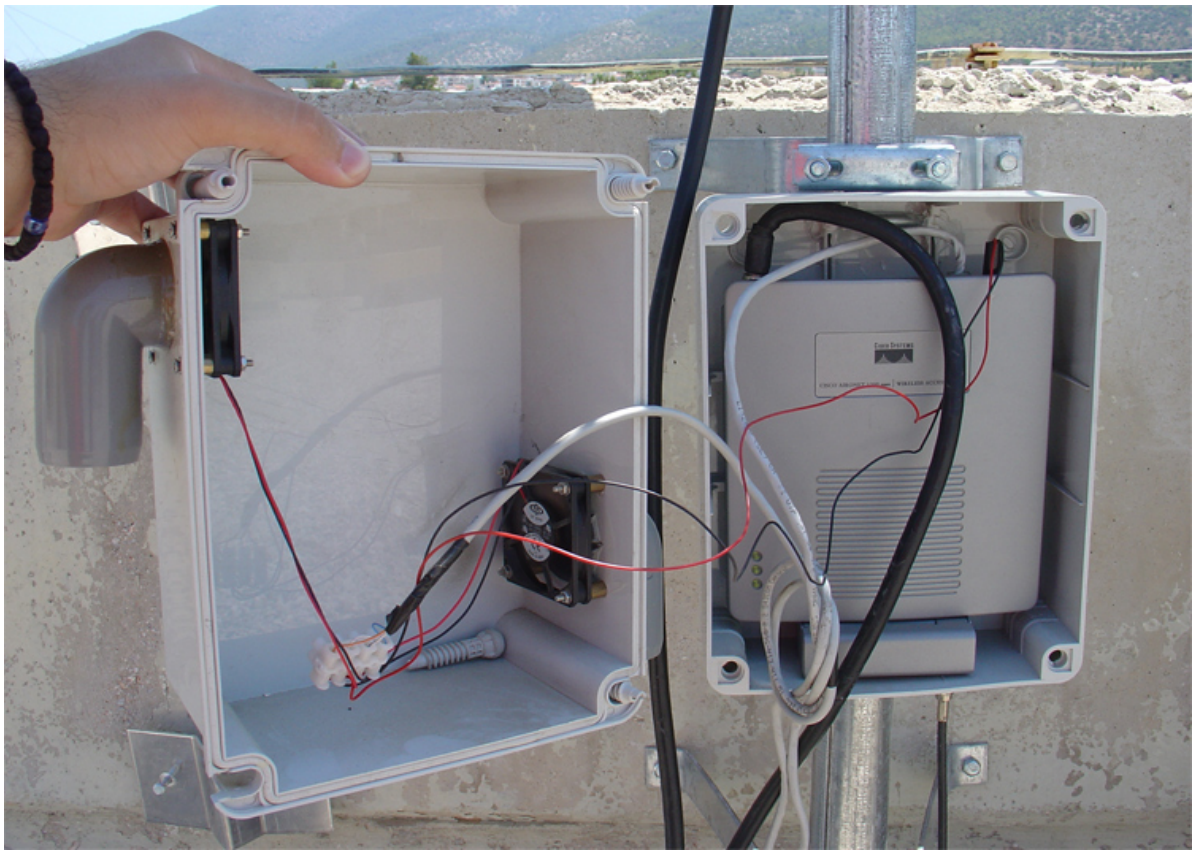
Με την πράσινη κουκίδα στην παραπάνω δορυφορική φωτογραφία δείχνεται το ακριβές σημείο τοποθέτησης του ασύρματου σημείου πρόσβασης – γέφυρας ρίζας (root bridge). Πρόκειται για την υψηλότερη ταράτσα του κτηρίου Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών στην Πολυτεχνειούπολη Ζωγράφου.

Ο κόμβος αυτός προσφέρει κατ' αρχάς ασύρματη πρόσβαση 802.11b/g. Το διαφημιζόμενο SSID του είναι το Microwave_lab, το οποίο μπορεί να εντοπίσει πελάτης σε ακτίνα 500m με απλή "αναζήτηση ασύρματων δικτύων" από το λειτουργικό του σύστημα. Αποτελέσματα επιπέδων λαμβανόμενης ισχύος σήματος δίνονται στην υποενότητα, που ακολουθεί. Για τη σύνδεση απαιτείται εισαγωγή WPA2 κλειδιού, που προσφέρει τη μέγιστη ασφάλεια σήμερα.

Επιπλέον, ο κόμβος αυτός λειτουργεί και σαν root bridge γεφυρώνοντας το ενσύρματο υποδίκτυο του εργαστηρίου Μικροκυμάτων & Οπτικών Ινών με τους εκατέρωθεν non-root bridge κόμβους στην Πανεπιστημιούπολη και το Μαρούσι. Η γεφύρωση αυτή επιτυγχάνεται στην πλευρά του Τμήματος Φυσικής με χρήση των λειτουργιών bridging του Cisco 1230. Όσον αφορά την πλευρά του Αμαρουσίου, δυσκολίες του εγχειρήματος, οδήγησαν στη χρήση "καθαρής" γέφυρας, όπως η Cisco 1300. Και για τις δύο ζεύξεις κορμού το χρησιμοποιούμενο SSID είναι το MFOL_backbone.

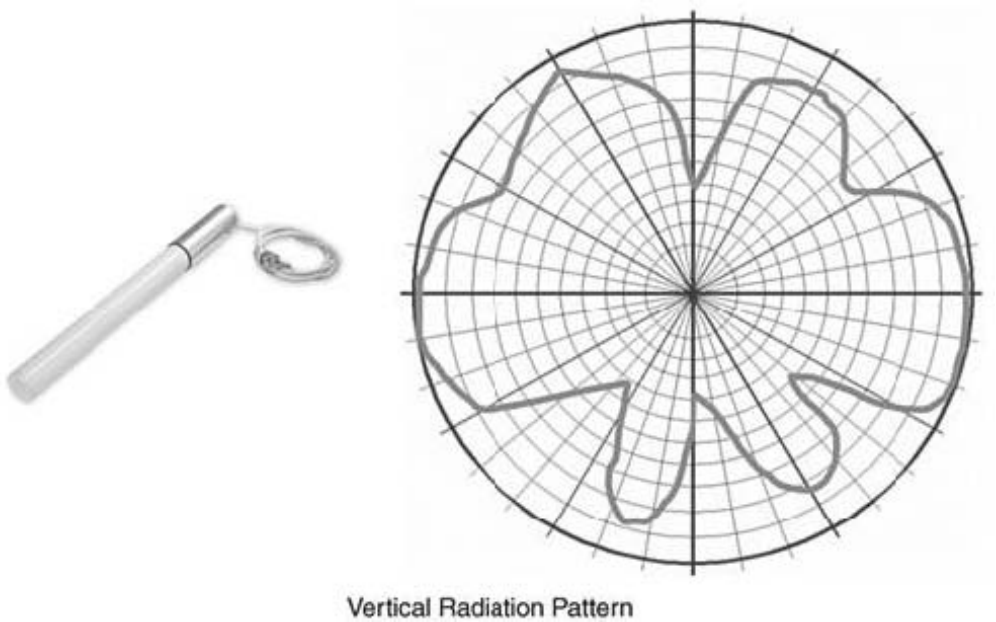
Εικόνες του κόμβου του Πολυτεχνείου δίνονται παρακάτω.

Εικόνα 3-6 Κόμβος στην τοποθεσία του Εθνικού Μετσόβιου Πολυτεχνείου



Εικόνα 3-7 Κουτί κόμβου στην τοποθεσία του Εθνικού Μετσόβιου Πολυτεχνείου

Στο υψηλότερο σημείο του ιστού διακρίνεται η 5.2-dBi ομοιοκατευθυντική κεραία κατασκευασμένη από την Cushcraft Corporation, η οποία συνδέεται με LMR-400 καλώδιο με το Cisco 1230 AP. Διάγραμμα ακτινοβολίας της κεραίας αυτής καθώς και πίνακας με τα χαρακτηριστικά της ακολουθούν.



Εικόνα 3-8 5.2-dBi ομοιοκατευθυντική κεραία

Παράμετρος	**Τιμή**
Εύρος συχνοτήτων	2,42 – 2,49 GHz
VSWR	2:1, 1.5:1 nominal
Κέρδος	5.2 dBi
Πόλωση	κάθετη
Αζιμούθιο (3-dB BW)	Ομοιοκατευθυντικό 360^{o}
Elevation (3-dB BW)	50^{o}
Διαστάσεις	13.5" * 1.25"

Δεδομένων των δύο βυσμάτων σε b/g, που διαθέτει το συγκεκριμένο access point, υπάρχει η δυνατότητα δοκιμής κάλυψης της περιοχής και με διαφορική εκπομπή και λήψη (diversity) συνδέοντας δύο πανομοιότυπες τέτοιες κεραίες σε μικρή μεταξύ τους απόσταση.

Λίγο χαμηλότερα διακρίνονται τα δύο κατευθυντικά interfaces των δύο 802.11a backbone links. Το δεξί πρόκειται για μία 27dB Ferimex FX 5G grid κεραία, η οποία είναι με ακρίβεια προσανατολισμένη προς την τοποθεσία του Τμήματος Φυσικής. Για τη σύνδεση αυτής με το αντίστοιχο βύσμα του access point χρησιμοποιήθηκε λεπτό καλώδιο RG-58, αφού από την πλευρά αυτή του κορμού δεν ήταν έντονη η απαίτηση για την το δυνατό μικρότερη απώλεια ισχύος του σήματος. Ακολουθούν εικόνα και πίνακας με τα χαρακτηριστικά της κεραίας αυτής.

Κατασκευαστής	Ferimex IT, spol. s r.o.
Εύρος συχνοτήτων	5470 ~ 5725 MHz
Κέρδος	27 ± 0,5 dBi
VSWR	< 1,3
Πλάτος δέσμης	9 ± 1 °
Βύσμα	N type Female 50 Ohms
Βάρος	4,1 kg

Εικόνα 3-9 Ferimex FX 5G 27dB grid κεραία

Το αριστερό πρόκειται για ένα παραβολικό κάτοπτρο διαστάσεων 90x100cm κέρδους 29 dB στου οποίου το lnb έχει τοποθετηθεί 8dB feeder Lanpoynt στα 2,4 GHz. Το feeder συνδέθηκε με το Cisco 1300 bridge με καλώδιο LMR400 για να εξασφαλιστούν οι το δυνατόν χαμηλότερες απώλειες ισχύος του σήματος. Δεδομένου ότι το κάτοπτρο είναι offset κατά περίπου 21^{o}, έχει φυσικά τοποθετηθεί, όπως φαίνεται και στη φωτογραφία, με κλίση προς τα κάτω. Χρήση ενός τέτοιου σχετικά μεγάλου κατόπτρου κρίθηκε οπωσδήποτε απαραίτητη δεδομένου το μακρινού link (8,5km) προς την τοποθεσία του Αμαρουσίου, που κλήθηκε να "σηκώσει".

Στο χαμηλότερο σημείο του ιστού φαίνεται κατ' αρχάς το κουτί μέσα στο οποίο φυλάσσεται το Cisco access point. Το κουτί, μετά από μηχανολογική παρέμβαση, δεν είναι μόνο αδιάβροχο αλλά φέρει και δύο ανεμιστήρες χαμηλής κατανάλωσης, οι οποίοι δημιουργούν ροή αέρα στο εσωτερικό και έτσι προστατεύουν τον σημείο πρόσβασης από τις υψηλές θερμοκρασίες που επικρατούν κατά τους θερμούς μήνες του καλοκαιριού. Η τροφοδότηση με ρεύμα τόσο του Cisco AP όσο και των ανεμιστήρων γίνεται μέσω δύο ζευγών κλώνων ενός και μόνο UTP καλωδίου, στο άλλο άκρο του οποίου βρίσκονται οι κατάλληλοι μετασχηματιστές. Το καλώδιο αυτό είναι μήκους 30m και, μετά από μετρήσεις, διαπιστώθηκε σχεδόν μηδενική πτώση τάσεως καθιστώντας το ιδανικό για την τροφοδότηση του κόμβου με ρεύμα. Στο ίδιο κουτί καταλήγει, φυσικά, και το UTP CAT5e crossover καλώδιο δεδομένων. Ομοίως, στο άλλο άκρο του ζεύγους κλώνων βρίσκεται ο κατάλληλος μετασχηματιστής.

Αριστερά διακρίνεται η γέφυρα Cisco 1300, στην οποία καταλήγει το προαναφερθέν παραβολικό κάτοπτρο. Δεδομένου του NEMA 4 εγκεκριμένου καλύμματος με το οποίο διατίθεται η γέφυρα αυτή, εγκαταστάθηκε η τελευταία άμεσα στον εξωτερικό χώρο. Η τροφοδότηση της γέφυρας με ρεύμα γίνεται μέσω ενός τρίτου ζεύγους κλώνων του ίδιου UTP καλωδίου, που τροφοδοτεί το Cisco 1230 και τους ανεμιστήρες του κουτιού του τελευταίου.

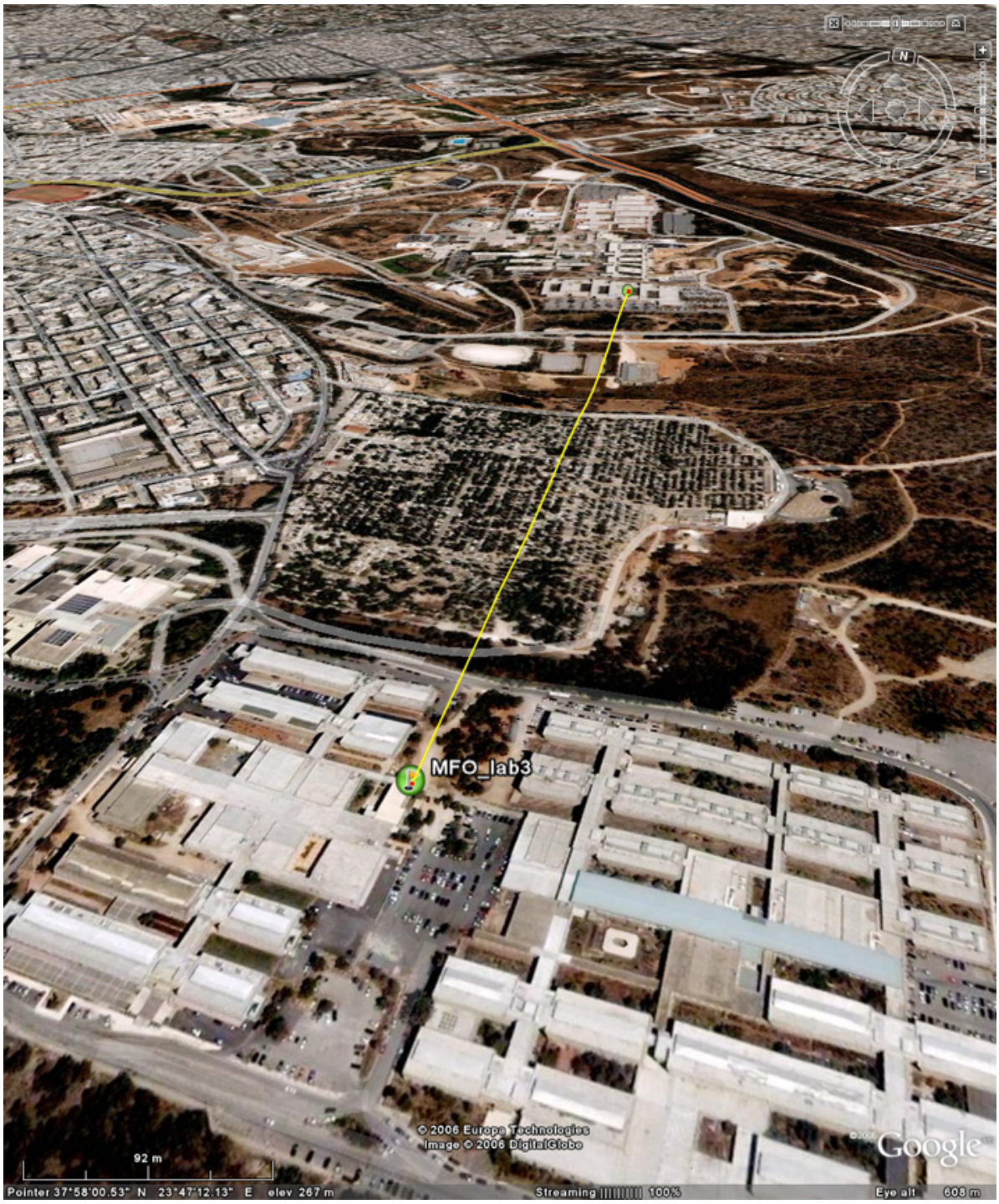
Τόσο το σημείο πρόσβασης 1230 όσο και η γέφυρα 1300 συνδέονται μέσω καλωδίων δεδομένων UTP σε δύο από τις 24 θύρες του Level One switch, που είναι εγκατεστημένο στο Εργαστήριο Μικροκυμάτων & Οπτικών Ινών. Το υποδίκτυο του εργαστηρίου είναι το 147.102.5.0 / 255.255.255.0 ή 24 με gateway 147.102.5.253 και DNS servers 147.102.222.220 και 147.102.222.210. Για τις ανάγκες του ασύρματου δικτύου δεσμεύθηκαν οι ip διευθύνσεις 147.102.5.234 ως 240. Η πρώτη από τις διευθύνσεις αυτές δόθηκε στο Cisco 1230 AP του Πολυτεχνείου, ενώ η 147.102.5.235 ανατέθηκε στη γέφυρα 1300.

Η ip διεύθυνση 147.102.5.239 δόθηκε στο εσωτερικό interface του Cisco 831 router, το οποίο συνδέεται με ετέρα θύρα του switch του εργαστηρίου. Ο δρομολογητής αυτός χρησιμοποιήθηκε κατά κύριο λόγο για να είναι δυνατή η δρομολόγηση της δικτυακής κίνησης από και προς το διαφορετικό υποδίκτυο (80.85.18.66 / 255.255.255.252 με gateway 80.85.18.65 και dns servers 80.85.16.6 και 80.85.16.7) του EMS 3020 DVB-RCS πομποδέκτη. Εικόνα του πομποδέκτη αυτού δίνεται παρακάτω

Εικόνα 3-10 Πομποδέκτης DVB-RCS EMS 3020

Η διαθέσιμη δορυφορική σύνδεση ήταν ρυθμού 512kbps, χορηγηθείσα από την Hellasat S.A.

Τοποθεσία Τμήματος Φυσικής



Εικόνα 3-11 Δορυφορική φωτογραφία τοποθεσίας Τμήματος Φυσικής

Με την πράσινη κουκίδα στην παραπάνω δορυφορική φωτογραφία δείχνεται το ακριβές σημείο τοποθέτησης του ασύρματου σημείου πρόσβασης – γέφυρας (non-root bridge). Πρόκειται για το εξωτερικό παράθυρο γραφείου του κτηρίου Τμήματος Φυσικής στην Πανεπιστημιούπολη Ζωγράφου και για αυτό το λόγο καταβλήθηκε προσπάθεια ο κόμβος αυτός συμπεριλαμβανομένων των κεραιών να είναι το δυνατόν πιο μικρός και συμπαγής.

Ο κόμβος αυτός έχει την 147.102.5.238 ip διεύθυνση και προσφέρει κατ' αρχάς ασύρματη πρόσβαση 802.11b/g. Το διαφημιζόμενο SSID του είναι το MFO_lab3. Για τη σύνδεση ενός πελάτη στον κόμβο αυτό απαιτείται εισαγωγή WPA2 κλειδιού. Επιπλέον, ο κόμβος αυτός λειτουργεί και σαν non-root bridge αποτελώντας "φύλλο" του 802.11a δένδρου, του οποίου ρίζα, όπως έχει προαναφερθεί, αποτελεί ο κόμβος στο Πολυτεχνείο. Δίνεται συνεπώς η δυνατότητα προσπέλασης, σε

κάθε συνδεδεμένο (associated) με αυτό το ασύρματο σημείο πρόσβασης πελάτη, στο ενσύρματο υποδίκτυο του εργαστηρίου Μικροκυμάτων & Οπτικών Ινών και κατ' επέκταση στο ασύρματο δίκτυο στο Μαρούσι καθώς και στο Διαδίκτυο.

Εικόνες αυτού του κόμβου δίνονται παρακάτω.

Εικόνα 3-12 Κόμβος Τμήματος Φυσικής

Εικόνα 3-13 Κόμβος Τμήματος Φυσικής

Κατ' αρχάς δεξιά και χαμηλά διακρίνεται η 5.2-dBi ομοιοκατευθυντική κεραία κατασκευασμένη από την Cushcraft Corporation, η οποία συνδέεται με RG-58 καλώδιο με το Cisco 1230 AP. Διάγραμμα ακτινοβολίας της κεραίας αυτής καθώς και πίνακας με τα χαρακτηριστικά της έχουν δοθεί παραπάνω.

Στο βάθος φαίνεται η κατευθυντική διεπαφή της ζεύξης κορμού 802.11a με το Πολυτεχνείο. Πρόκειται για μία 24dB Ferimex FX 5G grid κεραία. Για τη σύνδεση αυτής με το αντίστοιχο βύσμα του access point χρησιμοποιήθηκε καλώδιο RG-58. Ακολουθούν εικόνα και πίνακας με τα χαρακτηριστικά της κεραίας αυτής.

Κατασκευαστής	Ferimex IT, spol. s r.o.
Εύρος Συχνοτήτων	5470 ~ 5725 MHz
Κέρδος	24 ± 0,5 dBi
VSWR	< 1,3
Πλάτος δέσμης	11 ± 1 °
Βύσμα	N type Female 50 Ohms
Βάρος	3.1 kg

Εικόνα 3-14 Ferimex FX 5G 24dB grid κεραία

Αριστερά και χαμηλά φαίνεται το κουτί μέσα στο οποίο φυλάσσεται το Cisco access point. Το κουτί αυτό είναι επίσης αδιάβροχο αλλά δεν φέρει ανεμιστήρες, αφού κρίθηκε ότι στο σημείο αυτό, που βρίσκεται πάντα υπό σκιά, δεν αναπτύσσονται υψηλές θερμοκρασίες. Η τροφοδότηση τόσο του Cisco AP όσο και των ανεμιστήρων με ρεύμα γίνεται πάλι μέσω δύο ζευγών κλώνων ενός και μόνο UTP καλωδίου, στο άλλο άκρο του οποίου βρίσκονται οι κατάλληλοι μετασχηματιστές. Πέραν της τροφοδότησης με ρεύμα δεν υπάρχει καμία άλλη εξάρτηση του κόμβου αυτού από το κτήριο στο οποίο έχει εγκατασταθεί.

Μελέτη σκοπιμότητας

Ήδη από τη πρώτη επίσκεψη μου στις εκατέρωθεν προς σύνδεση τοποθεσίες, ήταν εμφανές ότι η υλοποίηση της ζεύξης αυτή κορμού μήκους ενός χιλιομέτρου (σύμφωνα με GPS δεδομένα) θα ήταν σχετικά απλή. Κατ' αρχάς οι ακριβείς θέσεις και των δύο κόμβων είναι υπερυψωμένες, εξασφαλίζοντας έτσι καθαρή οπτική επαφή μεταξύ τους. Και οι δύο χώροι επιλέχθηκαν έτσι ώστε να μην υπάρχει πάνω στη γραμμή θέας κανένα εμπόδιο.

Σύμφωνα, επίσης, με τους υπολογισμούς που ακολουθούν, το 100% (κι όχι μόνο το 60%) της πρώτης ζώνης Fresnel διατηρείται καθαρό. Πρώτα υπολογίζεται η ακτίνα του νοητού κυκλικού δίσκου με κέντρο το μέσο της απόστασης μεταξύ των δύο κόμβων, ο οποίος είναι κάθετος στη γραμμή οπτικής επαφής και εντός του οποίου δεν πρέπει να ευρίσκεται καμία δομή ή άλλο εμπόδιο.

$$h_{1,500m} = \sqrt{\frac{3\cdot 10^8}{\left(\frac{1}{500}+\frac{1}{500}\right)\cdot 5700\cdot 10^6}}\,m = 3,63m$$

Εν συνεχεία, υπολογίζεται η ακτίνα του νοητού κυκλικού δίσκου με κέντρο το σημείο που απέχει 20m από τον ένα εκ των δύο κόμβων, ο οποίος είναι κάθετος στη γραμμή οπτικής επαφής και εντός του οποίου δεν πρέπει να ευρίσκεται καμία δομή ή άλλο εμπόδιο.

$$h_{1,20m} = \sqrt{\frac{3\cdot 10^8}{\left(\frac{1}{20}+\frac{1}{980}\right)\cdot 5700\cdot 10^6}}\,m = 1,02m$$

Και στις δύο περιπτώσεις ο νοητός κυκλικός δίσκος διατηρήθηκε καθαρός.

Όσον αφορά την καμπυλότητα της γης, διαπιστώνεται ότι δεν υπάρχει κανένα πρόβλημα όχι μόνο από τη θεωρία (αφού $1km < 4,478km$, που απαιτείται για τη συχνότητα των 5 GHz) αλλά και από απλή παρατήρηση.

Τέλος, υπολογίζεται θεωρητικά η ισχύς του σήματος, που λαμβάνεται στο άλλο άκρο της ζεύξης κορμού. Δεδομένης της ευαισθησίας του χρησιμοποιούμενου δέκτη, που είναι ο ίδιος και για τις δύο πλευρές, για συγκεκριμένο ρυθμό διέλευσης δεδομένων, εκτιμάται το κατά πόσο επιτεύξιμο είναι το εγχείρημα εγκατάστασης της ζεύξης μεταξύ των δύο τοποθεσιών. Εν προκειμένω, η απώλεια μετάδοσης ελευθέρου χώρου L_s υπολογίζεται

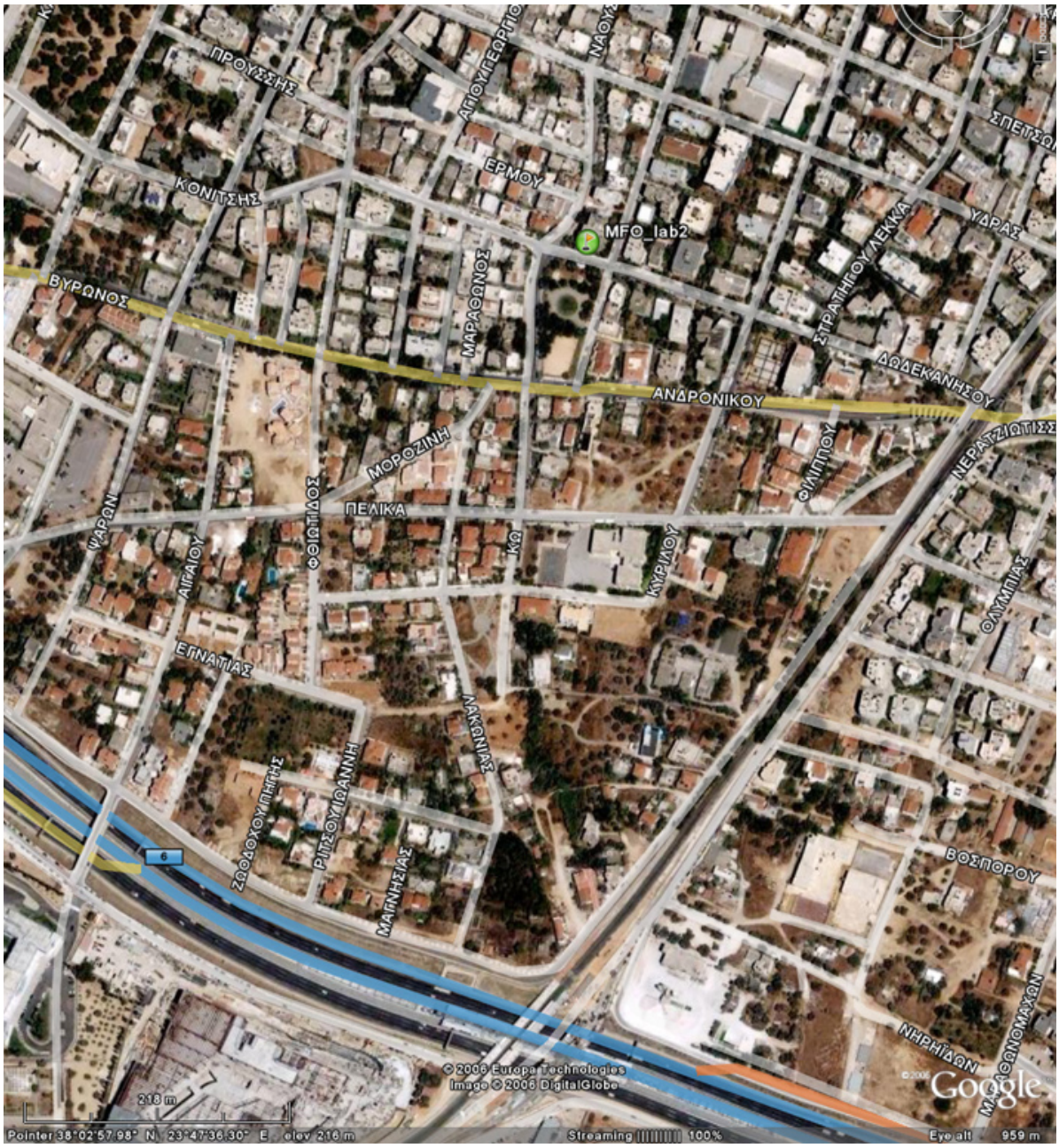
$$L_s(\text{dB}) = 32,4 + 20\log_{10} 1 + 20\log_{10} 5700 = 107,52\text{dB},$$

όπου d=1km η απόσταση πομπού-δέκτη και f=5700MHz η χρησιμοποιούμενη συχνότητα, στα πλαίσια της προδιαγραφής 802.11a. Η ισχύς του σήματος λήψης, που φτάνει στο άλλο άκρο της ζεύξης υπολογίζεται

$$W_R(\text{dBm}) = W_t(\text{dBm}) - L(\text{dB}) = W_t(\text{dBm}) - L_s + G_t + G_R - L_{c,t} - L_{c,R} - L_{con} =$$
$$= 3 - 107,52 + 27 + 24 - 2 - 2 - 4 = -61,52\text{dBm}$$

με L_s την παραπάνω υπολογισθείσα απώλεια μετάδοσης ελευθέρου χώρου, G_t και G_R τα κέρδη των κεραιών πομπού και δέκτη αντίστοιχα, $L_{c,t}$ και $L_{c,R}$ τις απώλειες των καλωδίων στον πομπό και το δέκτη αντίστοιχα και L_{con} τις απώλειες των μικροκυματικών βυσμάτων ή μετατροπέων. Θεωρώντας ισχύ εκπομπής από τη μία ραδιοσυσκευή ίση με 3dBm ή 2mW, αναμένεται η άλλη ραδιοσυσκευή να λαμβάνει ισχύ $-61,52\text{dBm}$, που είναι αρκούντως ικανοποιητική.

Τοποθεσία Αμαρουσίου



Εικόνα 3-15 Δορυφορική φωτογραφία τοποθεσίας Αμαρουσίου

Με την πράσινη κουκίδα στην παραπάνω δορυφορική φωτογραφία δείχνεται το ακριβές σημείο τοποθέτησης του ασύρματου σημείου πρόσβασης – γέφυρας (non-root bridge). Πρόκειται για την ταράτσα τετραώροφης πολυκατοικίας στην περιοχή του Αμαρουσίου μεταξύ των σταθμών ΗΣΑΠ "Νερατζιώτισσα" και "Μαρούσι".

Ο κόμβος αυτός προσφέρει κατ' αρχάς ασύρματη πρόσβαση 802.11b/g μέσω του Cisco 1230 AP, στο οποίο έχει ανατεθεί η ip διεύθυνση 147.102.5.237. Το διαφημιζόμενο SSID του είναι το MFO_lab2. Για τη σύνδεση ενός πελάτη στον κόμβο αυτό απαιτείται εισαγωγή WPA2 κλειδιού.

Επιπλέον, ο κόμβος αυτός λειτουργεί και σαν non-root bridge με χρήση της γέφυρας Cisco 1300. Αποτελεί, λοιπόν, κι αυτός "φύλλο" του δένδρου, του οποίου ρίζα αποτελεί ο κόμβος στο Πολυτεχνείο. Δίνεται συνεπώς σε κάθε συνδεδεμένο (associated) με το παραπάνω ασύρματο σημείο πρόσβασης πελάτη η δυνατότητα προσπέλασης στο ενσύρματο υποδίκτυο του εργαστηρίου Μικροκυμάτων & Οπτικών Ινών και κατ' επέκταση στο ασύρματο δίκτυο στο Τμήμα Φυσικής καθώς και στο Διαδίκτυο.

Εικόνα αυτού του κόμβου δίνεται παρακάτω.

Εικόνα 3-16 Κόμβος Αμαρουσίου

Κατ' αρχάς στο υψηλότερο σημείο του ιστού διακρίνεται η 5.2-dBi ομοιοκατευθυντική κεραία κατασκευασμένη από την Cushcraft Corporation, η οποία συνδέεται με RG-58 καλώδιο με το Cisco 1230 AP. Διάγραμμα ακτινοβολίας της κεραίας αυτής καθώς και πίνακας με τα χαρακτηριστικά της έχουν δοθεί παραπάνω.

Χαμηλότερα φαίνεται η κατευθυντική διεπαφή της ζεύξης κορμού 802.11g με το Πολυτεχνείο. Ακριβώς όπως ισχύει στην αντίστοιχη πλευρά του κόμβου του Πολυτεχνείου, πρόκειται για ένα παραβολικό κάτοπτρο διαστάσεων 90x100cm κέρδους 29 dB στου οποίου το lnb έχει τοποθετηθεί 8dB feeder Lanpoynt στα 2,4 GHz. Το feeder συνδέθηκε με το Cisco 1300 bridge με καλώδιο LMR400 για να εξασφαλιστούν οι το δυνατόν χαμηλότερες απώλειες ισχύος του σήματος.

Μέσα στο κουτί φυλάσσεται το Cisco access point. Το κουτί αυτό είναι επίσης αδιάβροχο και φέρει ανεμιστήρες για δημιουργία ροής αέρα εντός αυτού. Η τροφοδότηση τόσο του Cisco AP όσο και των ανεμιστήρων με ρεύμα γίνεται πάλι μέσω δύο ζευγών κλώνων ενός και μόνο UTP καλωδίου, στο άλλο άκρο του οποίου βρίσκονται οι κατάλληλοι μετασχηματιστές. Πέραν της τροφοδότησης με ρεύμα δεν υπάρχει καμία άλλη εξάρτηση του κόμβου αυτού από το κτήριο στο οποίο έχει εγκατασταθεί.

Μελέτη σκοπιμότητας

Μεγάλη δυσκολία που έπρεπε να αντιμετωπίσω για την υλοποίηση της ζεύξης αυτής ήταν η σχετικά μεγάλη απόσταση μεταξύ των κόμβων, που είναι ίση με 8,5km (σύμφωνα με GPS δεδομένα). Για το λόγο αυτό η μελέτη σκοπιμότητας εν προκειμένω κρίθηκε απολύτως απαραίτητη. Κατ' αρχάς ο χώρος στο Μαρούσι επιλέχθηκε έτσι ώστε να βρίσκεται σε υπερυψωμένο σημείο, όχι μόνο της γύρω περιοχής αλλά και του μέρους του λεκανοπεδίου της Αττικής μεταξύ των δύο κόμβων. Το ευτύχημα ήταν ότι η επιθυμητή αυτή τοποθεσία βρέθηκε και, σαν αποτέλεσμα, δεν υπάρχει κανένα εμπόδιο πάνω στη γραμμή οπτικής επαφής.

Σύμφωνα, επίσης, με τους υπολογισμούς που ακολουθούν, το 100% (κι όχι μόνο το 60%) της πρώτης ζώνης Fresnel διατηρείται καθαρό. Πρώτα υπολογίζεται η ακτίνα του νοητού κυκλικού δίσκου με κέντρο το μέσο της απόστασης μεταξύ των δύο κόμβων, ο οποίος είναι κάθετος στη γραμμή οπτικής επαφής και εντός του οποίου δεν πρέπει να ευρίσκεται καμία δομή ή άλλο εμπόδιο.

$$h_{1,4250m} = \sqrt{\frac{3\cdot 10^8}{\left(\frac{1}{4250}+\frac{1}{4250}\right)\cdot 2400\cdot 10^6}}\,m = 16,3m$$

Εν συνεχεία, υπολογίζεται η ακτίνα του νοητού κυκλικού δίσκου με κέντρο το σημείο που απέχει 20m από τον ένα εκ των δύο κόμβων, ο οποίος είναι κάθετος στη γραμμή οπτικής επαφής και εντός του οποίου δεν πρέπει να ευρίσκεται καμία δομή ή άλλο εμπόδιο.

$$h_{1,20m} = \sqrt{\frac{3\cdot 10^8}{\left(\frac{1}{20}+\frac{1}{8480}\right)\cdot 2400\cdot 10^6}}\,m = 1,58m$$

Και στις δύο περιπτώσεις ο νοητός κυκλικός δίσκος διατηρήθηκε καθαρός.

Όσον αφορά την καμπυλότητα της γης, αναμένεται θεωρητικά να υπάρχει πρόβλημα αν οι δύο κόμβοι δεν απέχουν από την επιφάνεια της γης αφού $8,5km > 5,975km$, που απαιτείται για τη συχνότητα των 2,4 GHz. Δεδομένων, όμως, των υψών $h_1 \cong h_2 \cong 20m$ των δύο κόμβων, η μέγιστη απόσταση ζεύξης, ακολουθώντας τη γραμμή σκόπευσης, προκύπτει $d_m \cong \sqrt{2h_1\alpha} + \sqrt{2h_2\alpha} = 2\cdot\sqrt{2\cdot 20\cdot 6370000} = 31,925km$, όπου $\alpha = 6370km$ είναι η μέση ακτίνα της γήινης επιφάνειας. Άρα, πάλι η καμπυλότητα της γης δεν προκαλεί κανένα πρόβλημα.

Υπολογίζεται, εν συνεχεία, η θεωρητική τιμή της ισχύος του σήματος, που λαμβάνεται στο άλλο άκρο της ζεύξης κορμού. Δεδομένης της ευαισθησίας του χρησιμοποιούμενου δέκτη, που είναι ο

ίδιος και για τις δύο πλευρές, για συγκεκριμένο ρυθμό διέλευσης δεδομένων, εκτιμάται το κατά πόσο επιτεύξιμο είναι το εγχείρημα εγκατάστασης της ζεύξης μεταξύ των δύο τοποθεσιών. Εν προκειμένω, η απώλεια μετάδοσης ελευθέρου χώρου L_s υπολογίζεται

$$L_s(\text{dB}) = 32,4 + 20\log_{10} 8,5 + 20\log_{10} 2400 = 118,59\text{dB},$$

όπου d=8,5km η απόσταση πομπού-δέκτη και f=2400MHz η χρησιμοποιούμενη συχνότητα, στα πλαίσια της προδιαγραφής 802.11b. Η ισχύς του σήματος λήψης, που φτάνει στο άλλο άκρο της ζεύξης υπολογίζεται

$$W_R(\text{dBm}) = W_t(\text{dBm}) - L(\text{dB}) = W_t(\text{dBm}) - L_s + G_t + G_R - L_{c,t} - L_{c,R} - L_{con} =$$
$$= 7 - 118,59 + 29 + 29 - 2 - 2 - 5 = -62,59\text{dBm}$$

με L_s την παραπάνω υπολογισθείσα απώλεια μετάδοσης ελευθέρου χώρου, G_t και G_R τα κέρδη των κεραιών πομπού και δέκτη αντίστοιχα, $L_{c,t}$ και $L_{c,R}$ τις απώλειες των καλωδίων στον πομπό και το δέκτη αντίστοιχα και L_{con} τις απώλειες των μικροκυματικών βυσμάτων ή μετατροπέων. Θεωρώντας ισχύ εκπομπής από τη μία ραδιοσυσκευή ίση με 7dBm ή 5,01mW, αναμένεται η άλλη ραδιοσυσκευή να λαμβάνει ισχύ $-62,59\text{dBm}$, που είναι ικανοποιητική λογαριάζοντας ένα περιθώριο εξασθένισης (κυρίως λόγω των περιβαλλοντικών συνθηκών) της τάξης των 10dBm.

Ειδικά για τη ζεύξη αυτή απαιτήθηκε να γίνει και μελέτη παρεμβολής. Ο λόγος είναι ότι, όπως φάνηκε σε δορυφορική φωτογραφία δραστηριότητας ραδιοερασιτεχνών, η ζώνη των 2.4 GHz στην περιοχή μεταξύ των κόμβων Αμαρουσίου και Πολυτεχνείου είναι ιδιαίτερα συσσωρευμένη. Ο μοναδικός ίσως τρόπος αντιμετώπισης της δυνητικής παρεμβολής είναι η χρήση εξαιρετικά κατευθυντικών κεραιών της τάξης των 28 dB, όπως και έγινε.

ΚΕΦΑΛΑΙΟ 4ο
Ασφάλεια

Επισκόπηση Ασφάλειας

Η εφαρμογή ισχυρών μηχανισμών ασύρματης ασφάλειας είναι το κλειδί για να εξασφαλιστεί ότι ένα ασύρματο δίκτυο προστατεύεται από μη εξουσιοδοτημένη πρόσβαση και υποκλοπή. Δυστυχώς, η ασύρματη ασφάλεια είναι τρωτή εάν εφαρμόζεται εσφαλμένα. Οι ακόλουθες ενότητες εξετάζουν μερικά από τα ζητήματα που αφορούν την ασύρματη ασφάλεια.

Επισκόπηση του WEP

Το πρώτο και βασικότερο επίπεδο ασφάλισης ενός ασύρματου LAN να ρυθμιστεί ένα κλειδί ισοδύναμης μυστικότητας με το ενσύρματο (Wired Equivalent Privacy - WEP). Πρόκειται για ένα τρόπο κρυπτογράφησης που κωδικοποιεί τις μεταδόσεις μεταξύ ενός σημείου πρόσβασης (AP) και ενός πελάτη. Αποτελεί έναν βασικό τρόπο ασφάλειας, αλλά δεν είναι ενδελεχής. Όταν ασύρματες συσκευές εισήχθησαν αρχικά, το WEP ήταν ένας γρήγορος και εύκολος τρόπος να παρασχεθεί ασφάλεια. Δυστυχώς, το WEP είναι εγγενώς εσφαλμένο' εντούτοις, δύναται να είναι η μόνη επιλογή εάν κάποιος εργάζεται με παλαιότερο λογισμικό ή εξοπλισμό πελάτη.

Εάν αρκετή κυκλοφορία διέρχεται πέρα δώθε μεταξύ του πελάτη και του AP, τα πακέτα μπορούν να παρεμποδιστούν και το κλειδί κρυπτογράφησης να συναχθεί. Αυτό δεν αποτελεί ίσως πρόβλημα για σπίτια και μικρά γραφεία, που αναπτύσσουν ελαφριά ασύρματη δραστηριότητα και εκπέμπουν δεδομένα χωρίς ενδιαφέρον. Εντούτοις, σε έναν οργανισμό ή εταιρία με μεγάλες ποσότητες ασύρματης κυκλοφορίας και κρίσιμων δεδομένων είναι εύκολο για έναν εισβολέα να σπάσει τον κώδικα.

Να σημειωθεί ότι οι σειρές γεφυρών και σημείων πρόσβασης Cisco Aironet 1100, 1200, 1300 και 1400, που τρέχουν Cisco IOS λογισμικό είναι ιδιαίτερα τρωτές, όταν χρησιμοποιούν WEP. Αυτό συμβαίνει επειδή στέλνουν οποιοδήποτε κλειδί WEP με καθαρό κείμενο στον SNMP server εάν η εντολή snmp-server enable traps wlan-wep επιτρέπεται.

Αδυναμίες του WEP

Το WEP είναι ευάλωτο σε επιθέσεις για διάφορους λόγους:

- Η διανομή των κλειδιών WEP με το χέρι είναι μια χρονοβόρα και επίπονη εργασία. Επειδή είναι κουραστικό να επανεισαχθεί με το χέρι ο κώδικας WEP, δεν είναι πιθανό τα κλειδιά να αλλάζουν συχνά. Επομένως, ένας επιτιθέμενος έχει πιθανώς αρκετό χρόνο να αποκρυπτογραφήσει το κλειδί.
- Όταν τα κλειδιά δεν αλλάζουν συχνά, οι επιτιθέμενοι μπορούν να συντάξουν τα αποκαλούμενα λεξικά αποκρυπτογράφησης. Αυτές είναι τεράστιες συλλογές πλαισίων, που κρυπτογραφούνται με το ίδιο κλειδί. Αυτά τα πλαίσια μπορούν έπειτα να αναλυθούν και να χρησιμοποιηθούν για την επίθεση.
- Οι τυποποιημένες εφαρμογές WEP χρησιμοποιούν κοινά κλειδιά των 64- ή 128-bit. Αν και κλειδιά των 128-bit ακούγονται υπερβολικά ανθεκτικά, είναι ακόμα δυνατό να σπάσει ένα κλειδί αυτού του μεγέθους μέσα σε ένα σύντομο χρονικό διάστημα με συνεχή κυκλοφορία.
- Το WEP χρησιμοποιεί το RC4 για κρυπτογράφηση. Από όλα τα πιθανά RC4 κλειδιά, οι στατιστικές για τις πρώτα λίγα bytes της εξόδου είναι μη τυχαίες, τα οποία μπορούν να παράσχουν πληροφορίες για το κλειδί.

Επικύρωση IEEE 802.1X

Το πρότυπο IEEE 802.1X αποτελεί μια βελτίωση των ικανοτήτων του WEP. Αν και το WEP παρέχει υπηρεσίες κρυπτογράφησης, το 802.1X παρέχει υπηρεσίες επικύρωσης. Το WEP προσφέρει ένα ορισμένο επίπεδο κρυπτογράφησης μεταξύ του AP και του πελάτη' εντούτοις, τα δεδομένα βρίσκονται ακόμα στον αέρα, εκτιθέμενα σε ανάλυση και εξέταση. Σε ένα ενσύρματο δίκτυο, μη εξουσιοδοτημένες συσκευές μπορούν να μπλοκαριστούν από το δίκτυο εάν απενεργοποιηθούν οι αχρησιμοποίητες RJ-45 θύρες και συσχετισθούν διευθύνσεις MAC με θύρες Ethernet switch.

Διαχείριση θυρών πρόσβασης

Τα WLANs μπορούν να περιλάβουν ή να αποκλείσουν συσκευές με βάση τις διευθύνσεις MAC χρησιμοποιώντας καταλόγους ελέγχου πρόσβασης (Access Control Lists - ACLs). Αν και αυτός ο τύπος του ACL είναι εύκολο να εφαρμοστεί και να το διαχειριστεί κανείς σε μικρά δίκτυα, η διαχείρισή του σε μεγάλα και δυναμικά δίκτυα είναι ιδιαίτερα δύσκολη επειδή μεμονωμένες διευθύνσεις MAC πρέπει να εισαχθούν με το χέρι για κάθε εξουσιοδοτημένη συσκευή. Προφανώς, αυτό είναι επίπονο.

Επίθεση με MAC

Επειδή οι ACLs χρησιμοποιούν διευθύνσεις MAC είναι επίσης επιρρεπείς σε επιθέσεις. Ένας εισβολέας μπορεί να βρεθεί κοντά και να πάρει την κυκλοφορία μεταξύ του AP και των εξουσιοδοτημένων του πελατών. Αν και το περιεχόμενο μιας συνομιλίας WEP κρυπτογραφείται, η διεύθυνση MAC δεν είναι κρυπτογραφημένη. Κατά συνέπεια, ένας επιτιθέμενος μπορεί να κάνει ένα από τα εξής δύο:

- Ο υπομονετικός επιτιθέμενος μπορεί να περιμένει έως ότου αποσυνδεθεί ο παρακολουθούμενος πελάτης από το δίκτυο και έπειτα απλά επαναρυθμίζει την κάρτα διεπαφής δικτύου για να εκπέμψει την υποκλεμμένη διεύθυνση MAC.

- Ο ανυπόμονος επιτιθέμενος μπορεί απλά να στείλει ένα αίτημα αποσύνδεσης στο AP, πετώντας έξω τον νόμιμο πελάτη από το WLAN. Προτού να μπορέσει να επανασυνδεθεί ο νόμιμος σταθμός, ο επιτιθέμενος μπορεί να συνδεθεί με την υποκλεμμένη διεύθυνση MAC.

Τα πρωτόκολλα 802.1X

Το 802.1X μπορεί να θεωρηθεί ως ένας έλεγχος μέσα στα Ethernet switches και τα APs. Ο έλεγχος ξεκινά από τη θέση OFF. Εξετάζει τα αιτήματα 802.1X και εάν αποφασίζει να χορηγήσει πρόσβαση, ο έλεγχος κινείται προς τη θέση ON. Μετά από μια χρονική περίοδο, η χρονική διάρκεια πρόσβασης, που έχει δοθεί στον σταθμό, λήγει ή ο τελευταίος αποσυνδέεται, μεταφέροντας τον έλεγχο πίσω στη θέση OFF.

Αν και η αξιοπιστία WEP έχει κλονισθεί, δεν είναι απολύτως έξω από το παιχνίδι της ασφάλειας ενός WLAN. Το WEP αποτελεί ένα απαραίτητο μέρος μιας υλοποίησης 802.1X. Το WEP, που χρησιμοποιείται από κοινού με το 802.1X, είναι πολύ ασφαλέστερο από όταν χρησιμοποιείται μόνο του. Ένας ακόμα πιο ισχυρός μηχανισμός ασφάλειας, η προστατευμένη πρόσβαση Wi-Fi (Wi-Fi Protected Access - WPA), συζητείται αργότερα σε αυτό το κεφάλαιο.

Υπάρχουν αρκετά πρωτόκολλα που χρησιμοποιούνται με το πρότυπο 802.1X για τον έλεγχο πρόσβασης σε θύρες του LAN. Μέσα στα πλαίσια του 802.1X, ένας σταθμός του LAN δεν επιτρέπεται να περάσει κυκλοφορία μέσω μιας συσκευής Ethernet ή ενός AP WLAN εφόσον δεν έχει ο ίδιος επικυρωθεί επιτυχώς. Αφότου έχει επικυρωθεί, ο πελάτης μπορεί να περάσει κυκλοφορία στο LAN.

Υπάρχουν 43 πρωτόκολλα που λειτουργούν στα πλαίσια της επικύρωσης 802.1X. Μερικά από τα πιο δημοφιλή πρωτόκολλα, που χρησιμοποιεί η ασύρματη δικτύωση Cisco, καλύπτονται στη συνέχεια.

Πρωτόκολλο Επεκτάσιμης Επικύρωσης (Extensible Authentication Protocol)

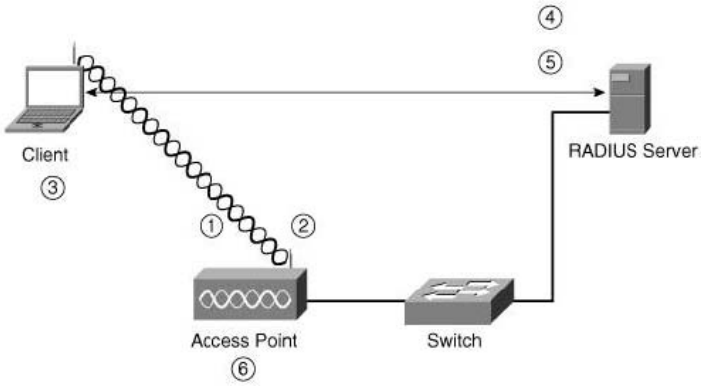
Το EAP αποτελεί ένα πλαίσιο που υποστηρίζει πολλαπλές μεθόδους επικύρωσης. Στην ουσία, το EAP διαχειρίζεται την επικύρωση αλλά η χρησιμοποιούμενη παραλλαγή EAP υπαγορεύει πώς οι πελάτες επικυρώνονται. Μερικές μέθοδοι επικύρωσης είναι:

- Κάρτες Token
- Kerberos
- Επικύρωση δημόσιου κλειδιού
- Πιστοποιητικά
- Έξυπνες κάρτες
- Συνθηματικά μίας χρήσης (One-time passwords - OTP)

Διάφορες παραλλαγές σε EAP είναι δυνατές. Ανάλογα με τις ανάγκη κάθε υλοποίησης, το EAP επιτρέπει διαφορετικούς τύπους επικύρωσης.

Όπως δείχνει το σχήμα 4-1, η επικύρωση EAP είναι μια διαδικασία πολλών βημάτων:

1. Ο πελάτης συνδέεται με το AP.
2. Το AP εμποδίζει τον πελάτη να έχει πρόσβαση στο δίκτυο.
3. Ο πελάτης παρέχει πληροφορίες εισόδου (login).
4. Ένας εξυπηρετητής απομακρυσμένης επικύρωσης εισόδου υπηρεσιών χρηστών (Remote Authentication Dial-In User Service - RADIUS) και ο πελάτης επικυρώνουν ο ένας τον άλλο.
5. Ο RADIUS server και ο πελάτης συμφωνούν σχετικά με ένα κλειδί WEP.
6. Η επικύρωση έχει ολοκληρωθεί.



Εικόνα 4-1 Η διαδικασία επικύρωσης EAP

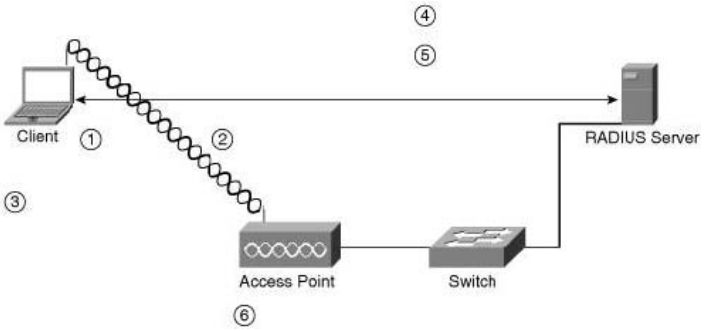
Αυτό είναι το βασικό πλαίσιο για το πώς λειτουργεί το EAP. Εντούτοις, μεμονωμένες μέθοδοι επικύρωσης μπορούν να καταστήσουν τη διαδικασία ελαφρώς διαφορετική.

EAP-TLS

Το EAP με ασφάλεια στρώματος μεταφοράς (EAP with Transport Layer Security - EAP-TLS) απαιτεί και ο σταθμός και ο εξυπηρετητής RADIUS να επικυρώνονται χρησιμοποιώντας κρυπτογραφία δημόσιου κλειδιού, όπως έξυπνες κάρτες ή ψηφιακά πιστοποιητικά.

Αυτή η συνομιλία προστατεύεται με μια κρυπτογραφημένη σήραγγα TLS. Δηλαδή μόνο η επικύρωση κρυπτογραφείται. Αφότου αυτό ολοκληρωθεί, τότε το WEP, το WPA ή το WPA2 παρέχει την κρυπτογράφηση των δεδομένων του χρήστη. Αν και αυτό καθιστά το EAP-TLS ανθεκτικό στο λεξικό αποκρυπτογράφησης και στις επιθέσεις ατόμου-στη-μέση (man-in-the-middle - MitM), η ταυτότητα του σταθμού (και το όνομα που δεσμεύεται στο πιστοποιητικό) μπορεί ακόμα να υποκλαπεί από επιτιθεμένους.

Το EAP-TLS είναι δημοφιλές επειδή είναι προεπιλεγμένο στα Windows XP, Windows 2000 και Windows Server 2003. Το σχήμα 4-2 παρουσιάζει το EAP-TLS εν δράση.



Εικόνα 4-2 Η διαδικασία επικύρωσης EAP-TLS

Η διαδικασία επικύρωσης EAP-TLS έχει ως εξής:

1. Ο πελάτης συνδέεται με το AP.
2. Το AP εμποδίζει τον πελάτη να έχει πρόσβαση στο δίκτυο.
3. Ο πελάτης επικυρώνει τον κεντρικό υπολογιστή RADIUS με ένα πιστοποιητικό.
4. Ο εξυπηρετητής RADIUS επικυρώνει τον πελάτη με ένα πιστοποιητικό.

5. Ο RADIUS server και ο πελάτης συμφωνούν σχετικά με ένα κλειδί WEP.
6. Μια ασφαλής σήραγγα εγκαθίσταται μεταξύ του πελάτη και του κεντρικού υπολογιστή.

Το μειονέκτημα σε αυτήν την μέθοδο είναι ότι η διανομή ψηφιακών πιστοποιητικών σε κάθε σταθμό είναι χρονοβόρα και οι περισσότερες οργανώσεις προτιμούν να χρησιμοποιήσουν ονόματα χρήστη και κωδικούς πρόσβασης για την ασύρματη επικύρωση. Το προστατευμένο EAP (Protected EAP - PEAP), που συζητείται αργότερα σε αυτό το κεφάλαιο, είναι καλό υποκατάστατο του EAP-TLS.

Cisco Wireless EAP

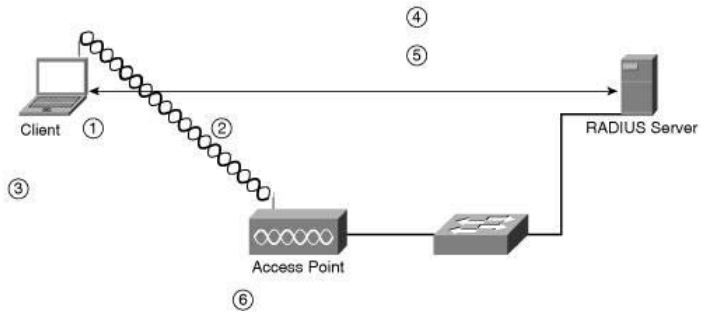
Το ιδιόκτητο EAP της Cisco είναι γνωστό ως ασύρματο Cisco EAP (ή Lightweight EAP - LEAP).

Το Cisco Wireless EAP παρέχει επικύρωση βασισμένη στο όνομα χρήστη και στον κωδικό πρόσβασης μεταξύ ενός ασύρματου πελάτη και ενός AP, μέσω ενός κεντρικού υπολογιστή επικύρωσης.

Ο server Cisco Wireless EAP και ο πελάτης παράγουν ένα κλειδί συνόδου, έτσι ώστε μελλοντικά πλαίσια να μπορούν να κρυπτογραφηθούν με ένα κλειδί διαφορετικό από τα κλειδιά που χρησιμοποιήθηκαν από άλλες συνόδους, παρέχοντας κατά συνέπεια ισχυρότερη ασφάλεια. Επιπλέον, νέα κλειδιά παράγονται κάθε φορά που ο πελάτης περιπλανάται σε ένα νέο AP.

Τα δυναμικά κλειδιά, ένα χαρακτηριστικό σε όλες τις εφαρμογές EAP, αντιμετωπίζουν μια τεράστια τρωτότητα έμφυτη με τα στατικά κλειδιά κρυπτογράφησης. Τα στατικά κλειδιά μοιράζονται μεταξύ όλων των σταθμών στο WLAN. Εάν ένας επιτιθέμενος μπορεί να σπάσει το κοινό στατικό κλειδί, τότε μπορεί να υποκλέψει όλη την κυκλοφορία του WLAN. Τα δυναμικά κλειδιά συνόδου καθιστούν την υποκλοπή δυσκολότερη για τον επιτιθέμενο επειδή υπάρχει λιγότερη κυκλοφορία προς ανάλυση. Επιπλέον, εάν ο επιτιθέμενος είναι σε θέση να σπάσει το κλειδί, η σύνοδος μπορεί να έχει ήδη τελειώσει.

Όταν χρησιμοποιείται το Cisco Wireless EAP, δυναμικά ανά χρήστη και ανά σύνοδο WEP κλειδιά παράγεται κάθε φορά που ο χρήστης επικυρώνεται στο WLAN. Είναι δυνατόν να ενισχυθεί ακόμα περαιτέρω η ασφάλεια με την απαίτηση χρονικής διάρκειας ισχύος του κλειδιού WEP, η οποία αναγκάζει την επαναεπικύρωση. Έτσι, παράγεται ένα νέο κλειδί WEP, ακόμη και για τις υπάρχουσες συνόδους. Το σχήμα 4-3 παρουσιάζει τη διαδικασία Cisco Wireless EAP.



Εικόνα 4-3 Η διαδικασία επικύρωσης Cisco Wireless EAP

Η διαδικασία επικύρωσης Cisco Wireless EAP έχει ως εξής:

1. Ο πελάτης συνδέεται με το AP.
2. Το AP εμποδίζει τον πελάτη να έχει πρόσβαση στο δίκτυο.
3. Ο πελάτης παρέχει πιστοποιητικά εισόδου στον κεντρικό υπολογιστή RADIUS.
4. Ο εξυπηρετητής RADIUS και ο πελάτης επικυρώνουν ο ένας τον άλλο.
5. Ο εξυπηρετητής RADIUS και ο πελάτης παράγουν ένα κλειδί συνόδου.
6. Ασφαλής επικοινωνία καθιερώνεται μεταξύ του πελάτη και του server.

PEAP

Το PEAP αναπτύχθηκε από τη Cisco, τη Microsoft και την ασφάλεια RSA. Το PEAP επιτρέπει την επικύρωση πελατών του WLAN χωρίς να απαιτεί πιστοποιητικά. Αυτό το πρωτόκολλο απλοποιεί την αρχιτεκτονική της ασφάλειας του WLAN.

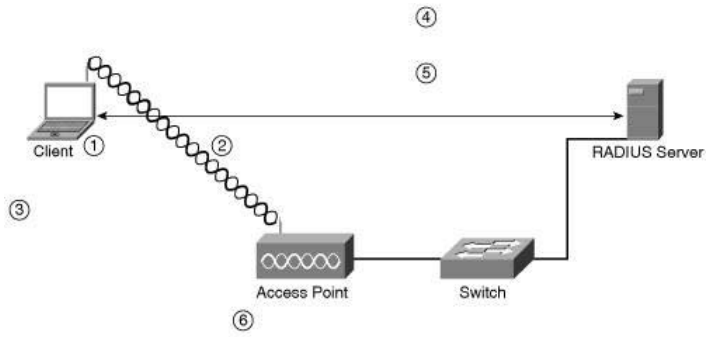
Επισκόπηση PEAP

Το PEAP, όπως και το ανταγωνιστικό TTLS (Tunneled Transport Layer Security), χρησιμοποιεί ασφάλεια στρώματος μεταφοράς (Transport Layer Security - TLS). Μπορεί να θεωρηθεί ως ισχυρότερη έκδοση του SSL, του πρωτοκόλλου που χρησιμοποιείται για να προστατεύσει τις συνόδους HTTP. Το TLS καθιερώνει μια απ' άκρη σε άκρη σήραγγα για να μεταδώσει τα πιστοποιητικά του πελάτη. Ένα πιστοποιητικό είναι απαιτούμενο στον κεντρικό υπολογιστή.

Υπάρχουν δύο φάσεις κατά τη λειτουργία του PEAP:

- Φάση 1η: Ξεκινά η επικύρωση TLS από την πλευρά του server και δημιουργείται μια κρυπτογραφημένη σήραγγα. Αυτό δημιουργεί ένα σύστημα επικύρωσης από την πλευρά του server, όπως το είδος που χρησιμοποιείται για την επικύρωση με χρήση της SSL. Όταν αυτή η φάση ολοκληρώνεται, όλο τα δεδομένα επικύρωσης κρυπτογραφούνται.
- Φάση 2η: Ο πελάτης επικυρώνεται χρησιμοποιώντας είτε το MS-CHAP Version 2 είτε άλλα σχήματα επικύρωσης, όπως εξηγείται στην επόμενη υποενότητα.

Το σχήμα 4-4 επιδεικνύει πως λειτουργεί το PEAP.



Εικόνα 4-4 Η διαδικασία επικύρωσης PEAP

Η διαδικασία επικύρωσης PEAP είναι η ακόλουθη:

1. Ο πελάτης συνδέεται με το AP.
2. Το AP εμποδίζει τον πελάτη να έχει πρόσβαση στο δίκτυο.
3. Ο πελάτης ελέγχει το πιστοποιητικό του κεντρικού υπολογιστή RADIUS.
4. Ο εξυπηρετητής RADIUS επικυρώνει τον πελάτη χρησιμοποιώντας το MS-CHAP ή άλλα μέσα, όπως ένα OTP.
5. Ο RADIUS server και ο πελάτης συμφωνούν σχετικά με το κλειδί WEP.
6. Μια ασφαλής σήραγγα εγκαθίσταται μεταξύ του πελάτη και του κεντρικού υπολογιστή.

Μια οργάνωση μπορεί να χρησιμοποιήσει κωδικούς πρόσβασης των Windows εάν δεν έχει διανεμημένα πιστοποιητικά σε κάθε σταθμό. Οι κεντρικοί υπολογιστές RADIUS που υποστηρίζουν EAP-TTLS και PEAP μπορούν να ελέγξουν τα αιτήματα πρόσβασης στο τοπικό δίκτυο με ελεγκτές περιοχών Windows, ενεργούς καταλόγους και άλλες υπάρχουσες βάσεις δεδομένων χρηστών.

Έκδοση PEAP 0 και 1

Υπάρχουν δύο εκδόσεις PEAP:

- Έκδοση PEAP 0 (επίσης γνωστό ως Microsoft PEAP)
- Έκδοση PEAP 1 (επίσης γνωστό ως Cisco PEAP)

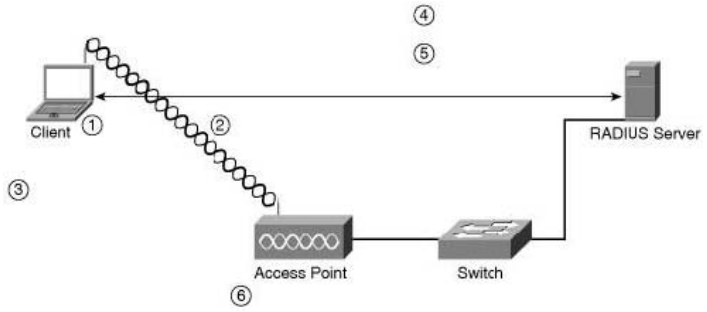
Κάθε έκδοση υποστηρίζει μια διαφορετική μέθοδο επικύρωσης πελατών μέσω της δικής της σήραγγας TLS. Η έκδοση 0 επικυρώνει τους πελάτες χρησιμοποιώντας MS-CHAP Version 2. Αυτό περιορίζει τις βάσεις δεδομένων χρηστών σε εκείνες που υποστηρίζουν MS-CHAP Version 2, όπως ο ενεργός κατάλογος (Active Directory).

Η έκδοση 1 (Cisco PEAP) επικυρώνει τους πελάτες χρησιμοποιώντας OTPs και κωδικούς πρόσβασης. Επιπλέον, η έκδοση 1 επιτρέπει στους χρήστες να κρύψουν τις ταυτότητές τους έως ότου δημιουργηθεί η σήραγγα TLS. Αυτό εξασφαλίζει ότι τα ονόματα χρήστη (usernames) δεν εκπέμπονται κατά τη διάρκεια της φάσης επικύρωσης.

EAP-FAST

Το EAP-FAST είναι σαν το EAP-TLS δεδομένου ότι χρησιμοποιεί ένα αρχείο πιστοποιητικών προστατευμένης πρόσβασης (Protected Access Credential - PAC) για την επικύρωση και επικυρώνει το σταθμό χρησιμοποιώντας ένα όνομα χρήστη και έναν κωδικό πρόσβασης μέσω μιας κρυπτογραφημένης σήραγγας TLS. Το EAP-FAST είναι μοναδικό υπό την έννοια ότι έχει σχεδιαστεί να επιταχύνει την επαναεπικύρωση καθώς οι σταθμοί περιπλανιόνται μεταξύ των APs. Τα EAP-TLS και PEAP απαιτούν ανταλλαγές μεγάλων μηνυμάτων μεταξύ του σταθμού και του κεντρικού υπολογιστή με αποτέλεσμα να χρειάζονται αρκετά δευτερόλεπτα για την επαναεπικύρωση. Οι εφαρμογές που είναι ευαίσθητες στην καθυστέρηση (όπως το VoIP) υποφέρουν εάν η επαναεπικύρωση διαρκεί περισσότερο από μερικά χιλιοστά του δευτερολέπτου.

Το EAP-FAST χρησιμοποιεί κοινά μυστικά κλειδιά για να επιταχύνει τη διαδικασία επαναεπικύρωσης. Τα δημόσια κλειδιά είναι βολικά επειδή ο σταθμός και το AP μπορούν να επικυρώσουν ο ένας τον άλλον χωρίς να πρέπει να είναι γνωστοί μεταξύ τους εκ των προτέρων. Τα μυστικά κλειδιά είναι γρηγορότερα, αλλά απαιτούν και ο σταθμός και το AP να έχουν ήδη το μυστικό κλειδί. Το σχήμα 4-5 επιδεικνύει πως λειτουργεί το EAP-FAST.



Εικόνα 4-5 Η διαδικασία επικύρωσης EAP-FAST

Η διαδικασία επικύρωσης EAP-FAST είναι η ακόλουθη:

1. Ο πελάτης συνδέεται με το AP.
2. Το AP εμποδίζει τον πελάτη να έχει πρόσβαση στο δίκτυο.
3. Ο πελάτης ελέγχει τα πιστοποιητικά του κεντρικού υπολογιστή RADIUS με το κοινό μυστικό κλειδί.
4. Ο εξυπηρετητής RADIUS επικυρώνει τον πελάτη με το κοινό μυστικό κλειδί.
5. Ο RADIUS server και ο πελάτης συμφωνούν σχετικά με ένα κλειδί WEP.

6. Ασφαλής επικοινωνία καθιερώνεται μεταξύ του πελάτη και του server.

Σύγκριση των Μεθόδων Επικύρωσης 802.1X

Υπάρχουν πολλές διαφορές μεταξύ των PEAP, Cisco Wireless EAP, EAP-TLS και EAP-FAST. Ο παρακάτω πίνακας συγκρίνει τα διάφορα χαρακτηριστικά αυτών των διαφορετικών μεθόδων επικύρωσης.

Χαρακτηρι-στικά	**EAP-TLS**	**Cisco Wireless EAP**	**PEAP Version 1 (with Generic Token Card)**	**PEAP Version 0 (with MS-CHAP Version 2)**	**EAP-FAST**
Εξυπηρετητής και Βάση Δεδομένων Επικύρωσης Χρηστών	OTP LDAP Novell NDS Windows NT Domains Active Directory	Windows NT Domains Active Directory	OTP LDAP Novell NDS Windows NT Domains Active Directory	Windows NT Domains Active Directory	Windows NT Domains Active Directory LDAP
Απαιτούνται πιστοποιητικά εξυπηρετητή;	Ναι	Όχι	Ναι	Ναι	Όχι
Απαιτούνται πιστοποιητικά πελάτη;	Ναι	Όχι	Όχι	Όχι	Όχι
Λειτουργικά Συστήματα	Windows XP/2000/CE Υποστηρίζονται άλλα ΛΣ με λογισμικό τρίτων	Windows 98/2000/NT/ME/XP/CE Mac OS Linux DOS	Windows XP/2000/CE Υποστηρίζονται άλλα ΛΣ με λογισμικό τρίτων	Windows XP/2000/CE Υποστηρίζονται άλλα ΛΣ με λογισμικό τρίτων	Windows XP/2000/CE Υποστηρίζονται άλλα ΛΣ με λογισμικό τρίτων
Χρησιμοποιού-μενα διαπιστευτήρια	Ψηφιακό πιστοποιητικό	Κωδικός πρόσβασης Windows	Πελάτες: Κωδικός πρόσβασης Windows, Novell NDS, LDAP και OTP ή token. Εξυπηρετητής: Ψηφιακό πιστοποιητικό	Πελάτες: Κωδικός πρόσβασης Windows Εξυπηρετητής: Ψηφιακό πιστοποιητικό	Κωδικός πρόσβασης Windows, LDAP όνομα χρήστη και κωδικός πρόσβασης PAC
Απλή εγγραφή χρησιμοποιώντας Windows Login?	Ναι	Ναι	Όχι	Ναι	Ναι
Λήξη ισχύος κωδικού πρόσβασης και		Όχι	Όχι	Ναι	Ναι

αλλαγή;					
Συμβατό με γρήγορη και ασφαλή διαπομπή;	Όχι	Ναι	Όχι	Όχι	Ναι
Συμβατό με WPA;	Ναι	Ναι	Ναι	Ναι	Ναι

Wi-Fi Protected Access (WPA)

Ένα άλλο μέσο ασφάλειας WLAN έρχεται υπό τη μορφή της προστατευμένης πρόσβασης Wi-Fi (Wi-Fi Protected Access - WPA). Το WPA εισήχθη το 2003 από τη συμμαχία Wi-Fi, που αναφέρθηκε στο πρώτο κεφάλαιο. Υπάρχουν δύο εκδόσεις WPA: το WPA και το WPA2. Περιγράφονται στα τμήματα που ακολουθούν.

WPA

Το WPA σχεδιάστηκε ως αντικατάστατο του WEP. Το πρωτόκολλο TKIP (Temporal Key Integrity Protocol) είναι μια βελτίωση του WEP. Αναγκάζει τα κλειδιά να αλλάζουν αυτόματα και, όταν χρησιμοποιείται από κοινού με ένα μεγαλύτερο διάνυσμα αρχικοποίησης (Initialization Vector - IV) [4], κάνει την ανακάλυψη των κλειδιών ιδιαίτερα δύσκολη.

Πέραν των βελτιώσεων επικύρωσης και κρυπτογράφησης, το WPA προστατεύει το ωφέλιμο φορτίο (δεδομένα) καλύτερα από το WEP. Το WEP χρησιμοποιεί ελέγχους κυκλικού πλεονασμού (Cyclic Redundancy Checks - CRC) για να εξασφαλίσει την ακεραιότητα των πακέτων. Εντούτοις, είναι δυνατό να αλλοιωθεί το ωφέλιμο φορτίο και να ενημερωθεί το το μήνυμα CRC χωρίς γνώση του κλειδιού WEP επειδή το CRC δεν κρυπτογραφείται. Το WPA χρησιμοποιεί ελέγχους ακεραιότητας μηνυμάτων (Message Integrity Checks - MIC) για να εξασφαλίσει την ακεραιότητα των πακέτων. Τα MICs χρησιμοποιούν επίσης έναν μετρητή πλαισίων, ο οποίος αποτρέπει τις επιθέσεις επανάληψης. Οι τελευταίες εμφανίζονται όταν ένας επιτιθέμενος παρεμποδίζει μια μετάδοση και έπειτα επαναμεταδίδει εκείνη τη μετάδοση λίγο αργότερα. Παραδείγματος χάριν, εάν έχει υποκλαπεί ένας κωδικός πρόσβασης, ο επιτιθέμενος δεν χρειάζεται να ξέρει πως να διαβάσει το μήνυμα' μπορεί απλά να το επαναμεταδώσει αργότερα και έπειτα να αποκτήσει πρόσβαση χρησιμοποιώντας τα διαπιστευτήρια του θύματος.

WPA2

Το WPA2 είναι προφανώς η δεύτερη και πιο πρόσφατη έκδοση του WPA. Η σημαντικότερη διαφορά μεταξύ των δύο είναι η μέθοδος κρυπτογράφησης. Το WPA χρησιμοποιεί για μέθοδο κρυπτογράφησης το RC4, ενώ το WPA2 χρησιμοποιεί το AES. Όχι μόνο είναι η μέθοδος κρυπτογράφησης AES πολύ ισχυρότερη, αλλά και απαίτηση από ορισμένες κυβερνήσεις και βιομηχανίες. Το AES αναλύεται στην επόμενη ενότητα.

Το WPA2 είναι προς τα πίσω συμβατό με το WPA, και πολλά WPA-πιστοποιημένα προϊόντα μπορούν να αναβαθμιστούν με λογισμικό στο WPA2. Εντούτοις, μερικά προϊόντα ενδέχεται να απαιτήσουν βελτιώσεις υλικού. Το WPA σχεδιάστηκε να είναι μια βελτίωση λογισμικού του WEP. Το WPA2, όμως, δεν είχε έναν τέτοιο στόχο. Υπό αυτήν την έννοια, σε πολλές περιπτώσεις μια βελτίωση υλικού θα είναι απαραίτητη για αναβάθμιση σε WPA2.

[4] Να σημειωθεί ότι ένα IV είναι ένα τμήμα των bits που προστίθεται στον πρώτο τμήμα των δεδομένων ενός κρυπτογραφημένου τμήματος. Αυτό το τμήμα ενισχύει την ασφάλεια επειδή οι ίδιες μεταδόσεις με το ίδιο κλειδί παράγουν την ίδια έξοδο. Κατά συνέπεια, οι επιτιθέμενοι μπορούν να παρατηρήσουν τις ομοιότητες και να παραγάγουν και τα μηνύματα και τα κλειδιά που χρησιμοποιούνται.

Κρυπτογράφηση

Scrambling a WLAN's data as it leaves the AP, and then unscrambling it when it arrives at the client, requires an encryption method. The popular RC4 has already been discussed, but sturdier, stronger encryption methods are out there and in use in WLAN systems, as described next.

Data Encryption Standard (DES)

Το πρότυπο κρυπτογράφησης δεδομένων (Data Encryption Standard - DES) είναι μια μέθοδος κρυπτογράφησης που χρησιμοποιεί ένα μυστικό κλειδί. Είναι τόσο δύσκολο να σπαστεί (παρέχει 72 πεντάκις εκατομμύρια πιθανά κλειδιά) που η κυβέρνηση των Η.Π.Α. απαγορεύει την εξαγωγή της σε άλλες χώρες. Είναι δύσκολο να σπάσει επειδή το κλειδί επιλέγεται τυχαία από μια τεράστια "δεξαμενή".

Το DES εφαρμόζει ένα κλειδί των 56 bitς σε κάθε 64 bits δεδομένων. Αυτό θεωρείται ισχυρή κρυπτογράφηση. Πολλές οργανώσεις υιοθετούν τριπλό DES, το οποίο εφαρμόζει τρία κλειδιά σε διαδοχή.

Advanced Encryption Standard (AES)

Το πρότυπο προηγμένης κρυπτογράφησης (Advanced Encryption Standard - AES) τείνει να γίνει το de facto πρότυπο κρυπτογράφησης. Το AES εφαρμόζει κλειδιά των 128, 192 ή 256 bits σε τμήματα δεδομένων των 128, 192 ή 256 bits.

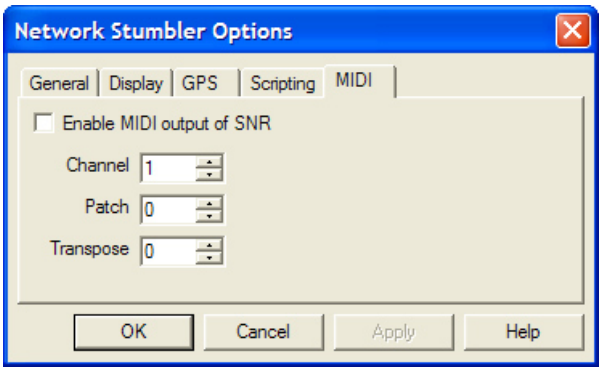
Από το 2004, δεν έχει υπάρξει ακόμα κανένα αναφερθέν σπάσιμο του AES και είναι την πρώτη φορά που η NSA (U.S. Government's National Security Agency) ενέκρινε ένα εργαλείο κρυπτογράφησης για τη μετάδοση άκρως απόρρητων πληροφοριών.

ΚΕΦΑΛΑΙΟ 5ο
Υπηρεσίες - Μετρήσεις

Ανακάλυψη Ασυρμάτων Δικτύων με χρήση του NetStumbler

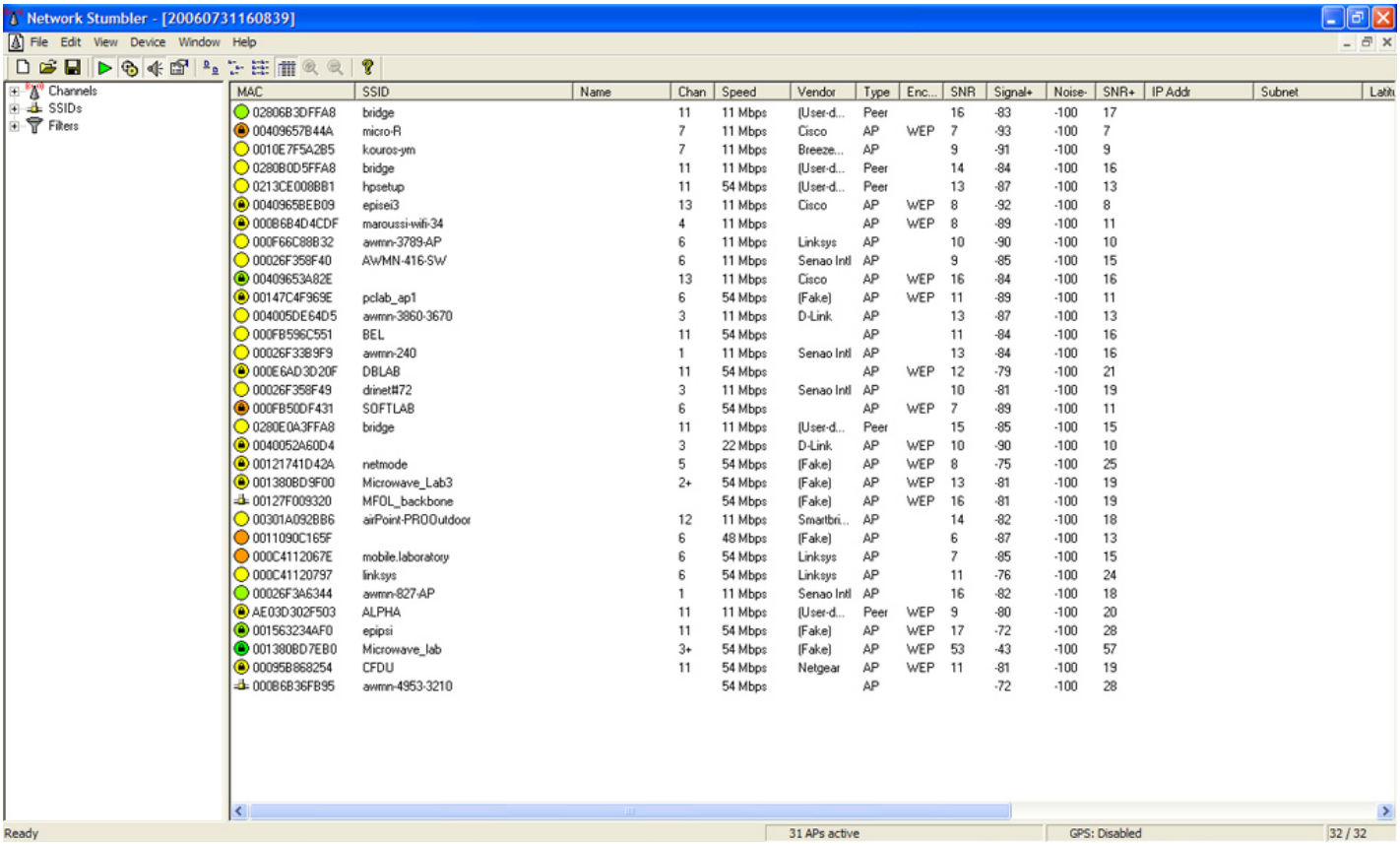
Το NetStumbler (http://www.netstumbler.com/downloads/) αποτελεί μια άριστη και δωρεάν εφαρμογή λογισμικού (πρόγραμμα), το οποίο έχει την ικανότητα να δίνει πολλές λεπτομέρειες για όλα τα ασύρματα δίκτυα στη γύρω περιοχή, συμπεριλαμβανομένου του ESSID τους, εάν χρησιμοποιούν WEP, τα κανάλια που χρησιμοποιούν και άλλα. Η τρέχουσα έκδοση είναι η 0,4. Η εγκατάσταση είναι εύκολη και γρήγορη και για όλα όσα το NetStumbler προσφέρει, το πακέτο λογισμικού είναι εντυπωσιακά μικρό.

Το NetStumbler δεν υποστηρίζει όλες τις κάρτες ασύρματων δικτύων. Υποστηριζόμενες κάρτες είναι εκείνες που χρησιμοποιούν το chipset Hermes (κάρτες Lucent, Orinoco, Avaya, Agere, Proxim). Από την έκδοση 0.30, το λογισμικό υποστηρίζει επίσης τους εγγενείς οδηγούς NDIS 5.1 του Windows XP, επιτρέποντας την υποστήριξη των Cisco Aironet και μερικών καρτών βασισμένων σε chipset Prism.



Εικόνα 5-1 Επιλογές εξόδου MIDI

Υποθέτοντας ότι η ασύρματη κάρτα είναι ήδη εγκατεστημένη, το NetStumbler αρχίζει αμέσως. Με μια ματιά φαίνονται όλα τα ασύρματα δίκτυα που το NetStumbler έχει βρει, μαζί με την ισχύ σήματος, το SNR και το θόρυβο.



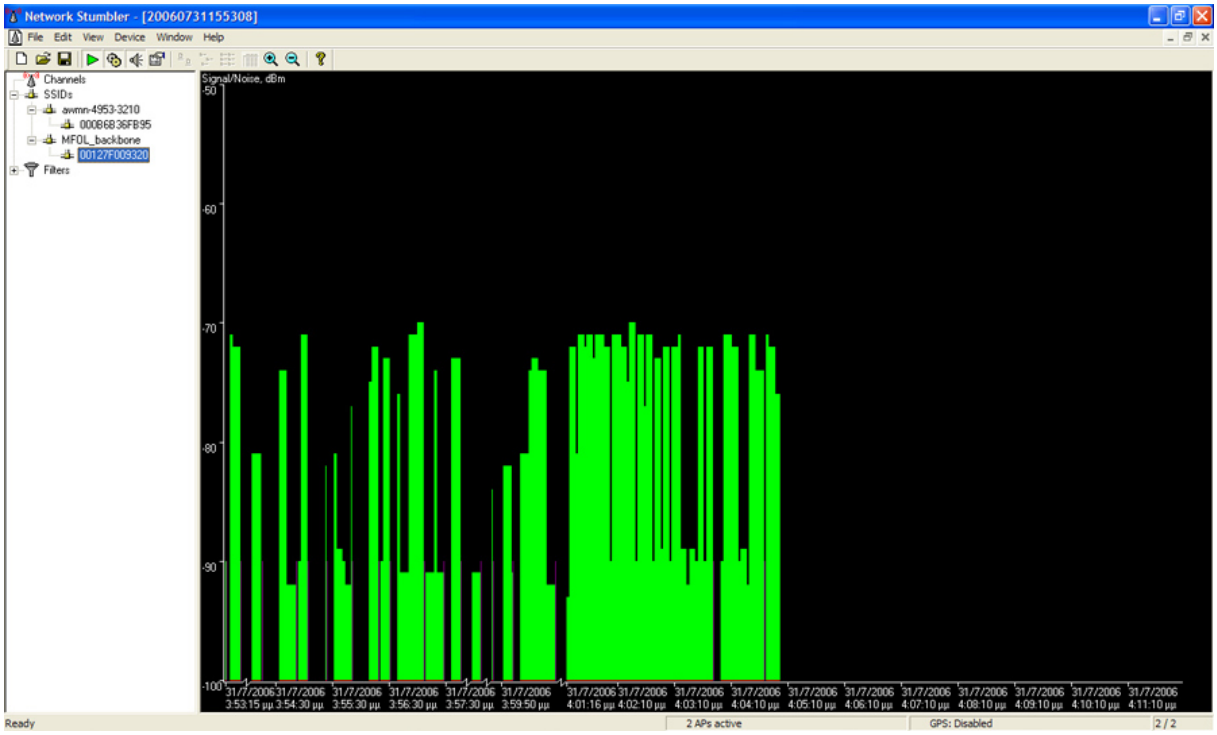
Εικόνα 5-2 Το NetStumbler καθώς δείχνει πολλά εντοπισμένα δίκτυα

Το NetStumbler παρουσιάζει τις πιο ενεργές συνδέσεις με χρώμα. Το πράσινο δείχνει ένα ισχυρό σήμα, το κίτρινο ένα οριακό και το κόκκινο ένα σχεδόν άχρηστο. Το γκρι σημαίνει ότι το ασύρματο δίκτυο δεν είναι προσιτό. Το σύμβολο της κλειδαριάς, όπου αυτό εμφανίζεται, δείχνει ότι το συγκεκριμένο δίκτυο χρησιμοποιεί WEP ή άλλο πρωτόκολλο ασφαλείας.

Ένα από τα πιο ενδιαφέροντα χαρακτηριστικά του NetStumbler είναι η δυνατότητα της αναπαραγωγής MIDI με βάση την ισχύ του λαμβανόμενου σήματος. Αυτό αποτελεί μεγάλη ευκολία κατά την εύρεση του καλύτερου δυνατού σήματος μεταξύ δύο τοποθεσιών, όπως όταν επιχειρείται ευθυγράμμιση κεραιών σε μεγάλη απόσταση. Όταν η ισχύς του σήματος αυξάνεται, τότε ο τόνος που

αναπαράγει το NetStumbler είναι πιο ψηλός. Συνεπώς, το μόνο που απαιτείται να γίνει είναι να κινηθεί η κεραία γύρω τόσο οριζόντια όσο και κατακόρυφα έως ότου ακουστεί ο υψηλότερος τόνος.

Μια δεύτερη επιλογή για την απεικόνιση της ισχύος των σημάτων είναι διαθέσιμη μέσω του μενού πλοήγησης στην αριστερή πλευρά της οθόνης του προγράμματος. Θα εμφανιστεί κάτι παρόμοιο με το σχήμα 5-3 με ένα κλικ στο σταυρό δίπλα στο επιθυμητό SSID. Δείχνονται όλες οι διευθύνσεις MAC που συσχετίζονται με εκείνο το SSID. Με ένα κλικ στη διεύθυνση MAC δείχνεται μια γραφική αναπαράσταση της ισχύος του σήματος σε αυτό το ασύρματο δίκτυο.



Εικόνα 5-3 Όψη δικτύων ανά SSID

Το NetStumbler παρέχει και διεπαφή για σύνδεση με σύστημα GPS. Μετά τη σύνδεση της μονάδας GPS, η κύρια οθόνη όχι μόνο παρουσιάζει λεπτομέρειες του ασύρματου δικτύου, αλλά παρουσιάζει και το γεωγραφικό πλάτος και γεωγραφικό μήκος του ασύρματου δικτύου.

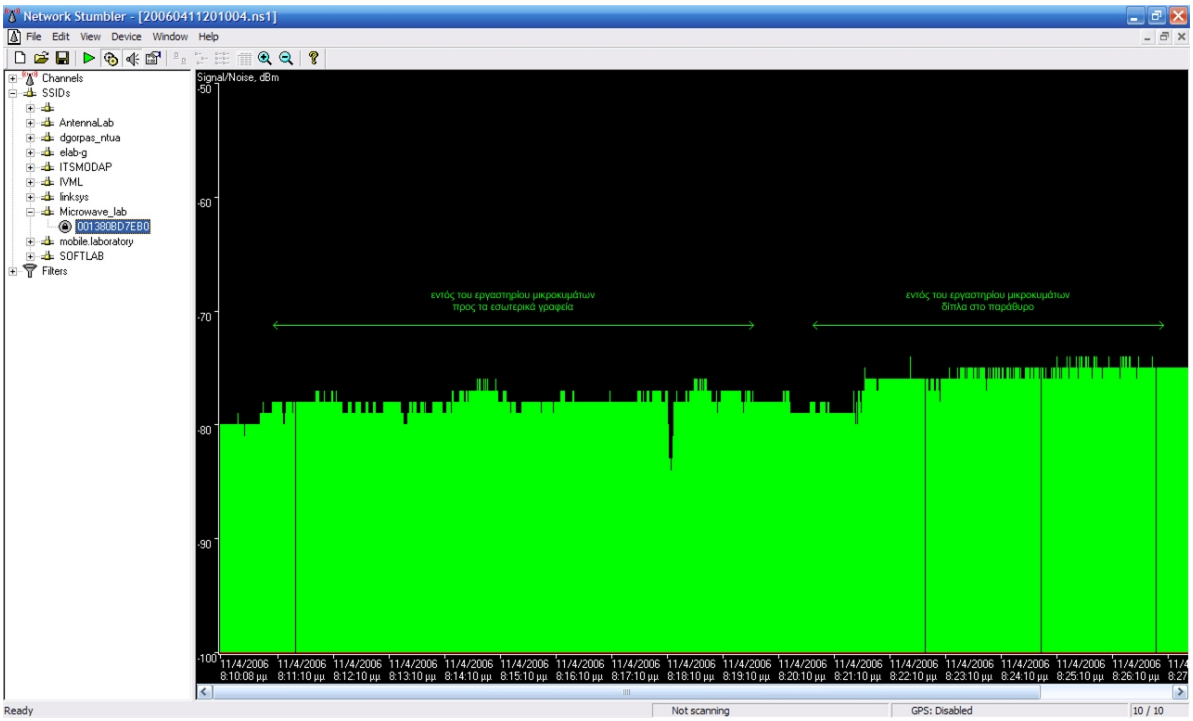
Το NetStumbler είναι ένας ενεργός ανιχνευτής δικτύων, που στέλνει αιτήματα ανίχνευσης και παρακολουθεί για αποκρίσεις στα αιτήματα αυτά. Συνεπώς, δεν θα ανιχνεύσει τα αποκαλούμενα "κλειστά" δίκτυα, τα οποία δεν διαφημίζουν το SSID τους. Για να επιτευχθεί αυτό, απαιτείται ένα παθητικό εργαλείο ελέγχου όπως τα Kismet ή KisMAC.

Στις υποενότητες, που ακολουθούν, δίνονται αποτελέσματα μετρήσεων ισχύος σημάτων στις τρεις τοποθεσίες των κόμβων, που εγκαταστάθηκαν στα πλαίσια της παρούσας διπλωματικής.

Τοποθεσία Εθνικού Μετσόβιου Πολυτεχνείου

Στην υποενότητα αυτή δίνονται δύο γραφικές αναπαραστάσεις της ισχύος του λαμβανόμενου σήματος 2,4 GHz, που εκπέμπεται από την ομοιοκατευθυντική κεραία, τη συνδεδεμένη με το Cisco 1230 AP. Με άλλα λόγια, πρόκειται για την ισχύ του σήματος που λαμβάνει ένας πελάτης από το σημείο πρόσβασης με SSID Microwave_lab.

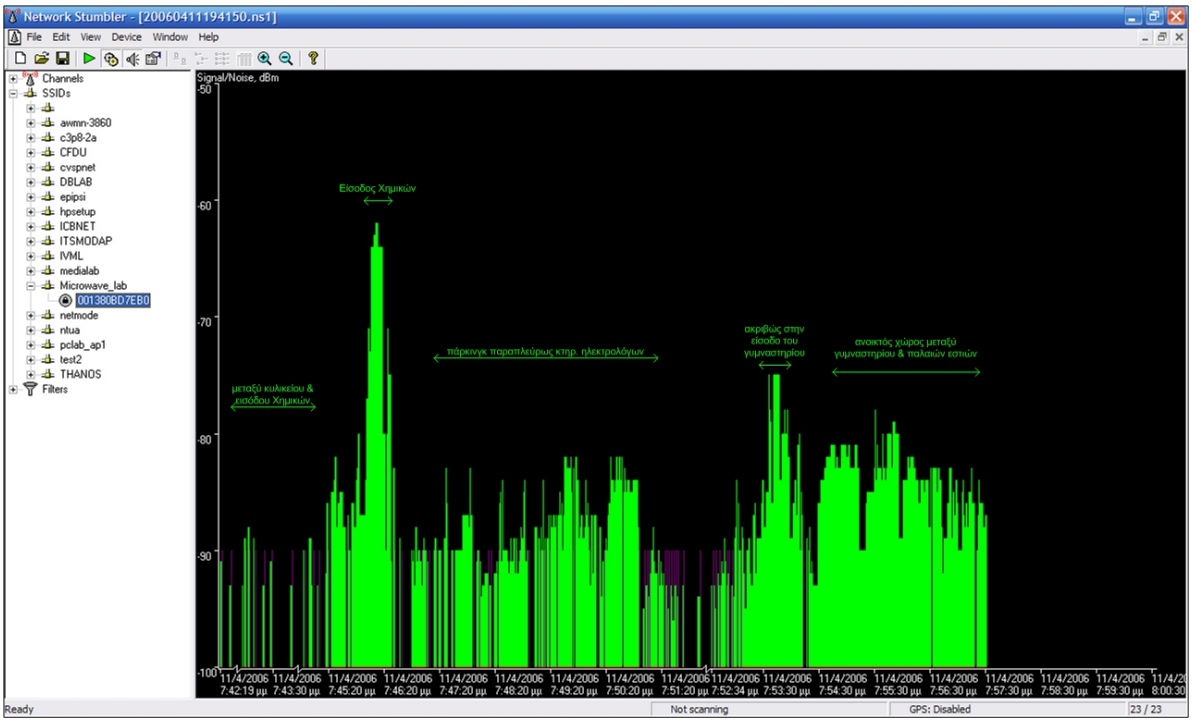
Πρώτα δείχνονται τα επίπεδα ισχύος του σήματος εντός του εργαστηρίου Μικροκυμάτων & Οπτικών Ινών στο δεύτερο όροφο του κτηρίου Ηλεκτρολόγων Μηχ. & Μηχ. Υπολογιστών.



Εικόνα 5-4 Η ισχύς του λαμβανόμενου σήματος εντός του εργαστηρίου Μικροκυμάτων & Οπτικών Ινών

Στο αριστερό τμήμα των μετρήσεων φαίνεται η ισχύς που μετρήθηκε στο βάθος των γραφείων, μακριά από το παράθυρο. Πρόκειται για τη χειρότερη περίπτωση λήψης εντός του εργαστηρίου. Στην περίπτωση αυτή η ισχύς κυμαίνεται στα -80 ως -76dBm. Τα επίπεδα αυτά ισχύος μπορεί μεν να μην παρέχουν το μέγιστο ρυθμό διέλευσης δεδομένων αλλά προσφέρουν συνδεσιμότητα με τουλάχιστον 11Mbps, για 802.11g κάρτα πελάτη. Στο δεξί τμήμα των μετρήσεων φαίνεται η ισχύς που μετρήθηκε κοντά στο παράθυρο. Στην περίπτωση αυτή η ισχύς κυμαίνεται στα -76 ως -73dBm. Στα επίπεδα αυτά ισχύος είναι δυνατό να επιτευχθεί ο μέγιστος ρυθμός διέλευσης δεδομένων στα 54Mbps, για 802.11g κάρτα πελάτη.

Η δεύτερη μέτρηση έγινε ακριβώς έξω από το κτήριο των Ηλεκτρολόγων Μηχ. & Μηχ. Υπολογιστών στην Πολυτεχνειούπολη και, μάλιστα, εν κινήσει με χρήστη φορητού υπολογιστή. Η διαδρομή είχε ως εξής: σκαλοπάτια προς κυλικείο γενικών εδρών, είσοδος κτηρίου Χημικών μηχανικών, παράπλευρος χώρος στάθμευσης κτηρίου Ηλεκτρολόγων, είσοδος γυμναστηρίου πίσω από το κτήριο Ηλεκτρολόγων και ανοικτός χώρος μεταξύ γυμναστηρίου και παλαιών εστιών.

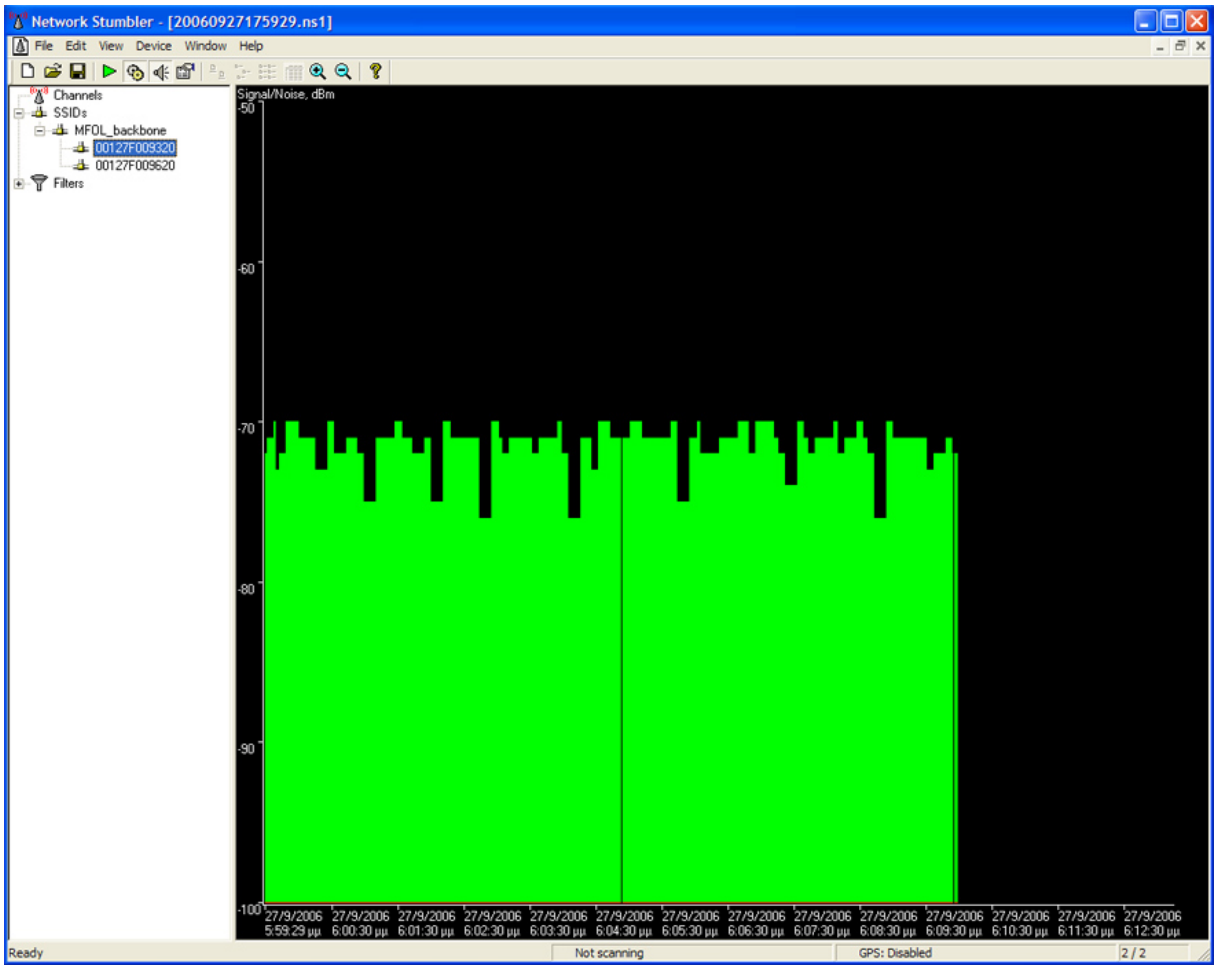


Εικόνα 5-5 Η ισχύς του λαμβανόμενου σήματος εκτός του κτηρίου των Ηλεκτρολόγων

Η μεγάλη διακύμανση της ισχύος, που φαίνεται παραπάνω, οφείλεται κυρίως στην κίνηση του φορητού υπολογιστή. Πολύ καλή υπήρξε η τιμή ισχύος του σήματος στην είσοδο του κτηρίου Χημικών, που μπορεί να παρέχει και τον υψηλότερο ρυθμό διέλευσης δεδομένων. Ενθαρρυντικό ήταν και το σταθερό σήμα των -75dBm στην είσοδο του γυμναστηρίου, σε απόσταση 350m από την εκπέμπουσα ομοιοκατευθυντική κεραία του σημείου πρόσβασης.

Τοποθεσία Τμήματος Φυσικής

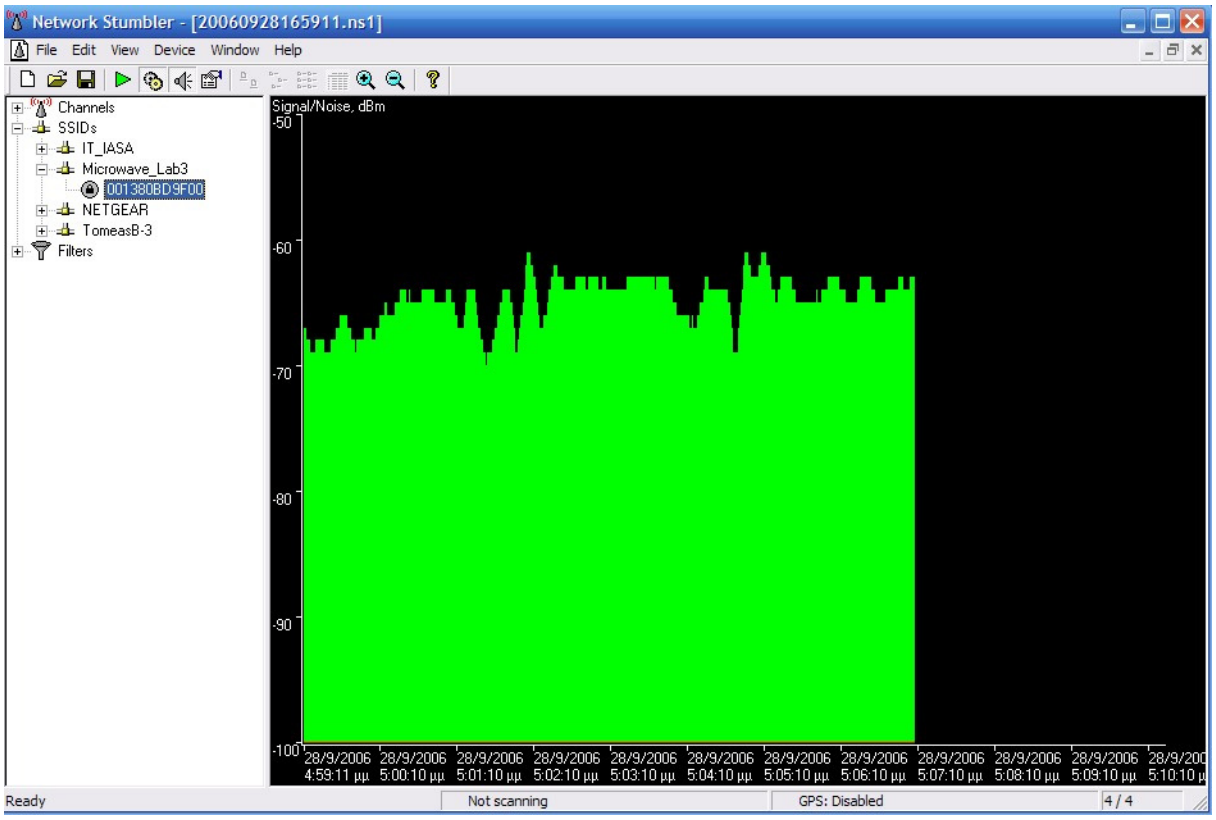
Κατ' αρχάς δίνεται η γραφική αναπαράσταση της ισχύος του σήματος (στα 5,4 GHz) της ζεύξης κορμού 802.11a με τον κόμβο του Πολυτεχνείου.



Εικόνα 5-6 Η ισχύς του σήματος ζεύξης κορμού μεταξύ Τμήματος Φυσικής και Πολυτεχνείου

Όπως αναμενόταν τα επίπεδα ισχύος αυτής της ζεύξης κορμού είναι αρκετά ικανοποιητικά χωρίς η εκπεμπόμενη ισχύος εκατέρωθεν να είναι υψηλή. Σαν αποτέλεσμα, οι ρυθμοί διέλευσης δεδομένων φτάνουν τα πρακτικά μέγιστα επίπεδα.

Τέλος, ακολουθεί γραφική αναπαράσταση της ισχύος του σήματος που λαμβάνει ένας πελάτης σε απόσταση περίπου 50 μέτρα με καθαρή οπτική επαφή από το 802.11b/g σημείο πρόσβασης με SSID MFO_lab3.

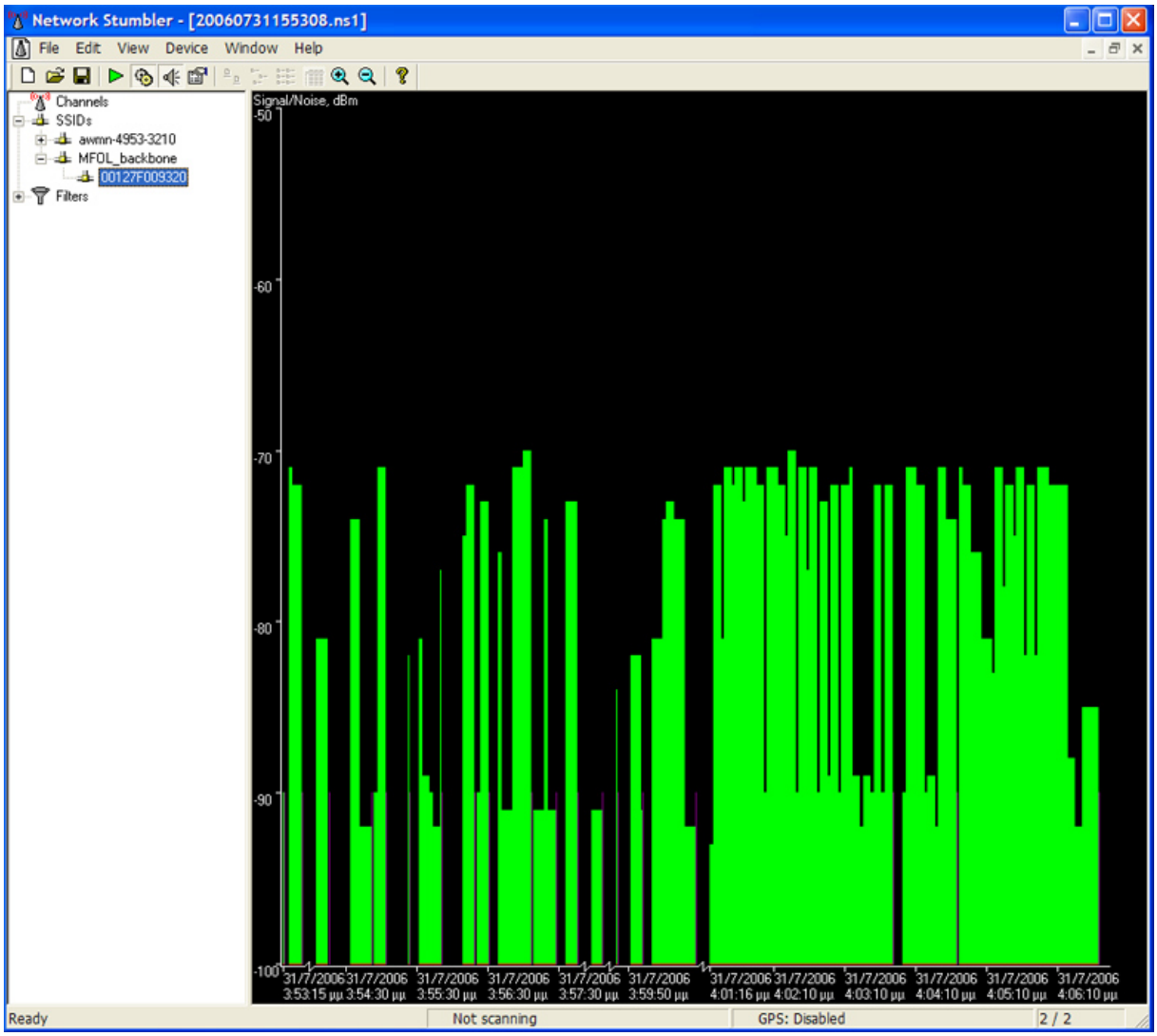


Εικόνα 5-0-7 Η ισχύς του σήματος που λαμβάνει ένας πελάτης του σημείου πρόσβασης MFO_lab3

Τα παραπάνω επίπεδα ισχύος εξασφαλίζουν φυσικά απόλυτη αξιοποιήση του διατιθέμενου εύρους ζώνης.

Τοποθεσία Αμαρουσίου

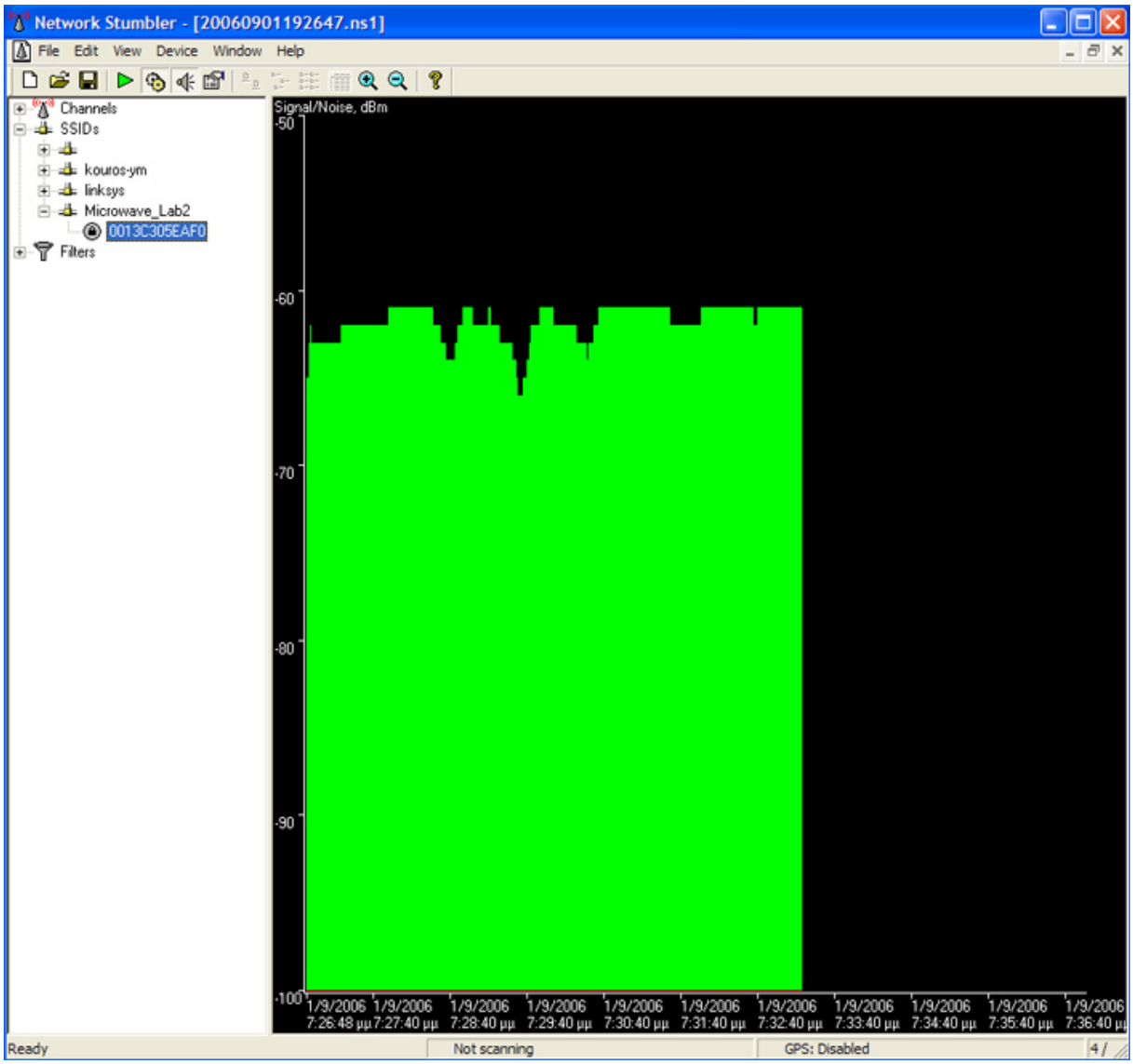
Δίνεται πρώτα η γραφική αναπαράσταση της ισχύος του σήματος (στα 2,4 GHz) της ζεύξης κορμού 802.11b με τον κόμβο του Πολυτεχνείου.



Εικόνα 5-8 Η ισχύς του σήματος ζεύξης κορμού μεταξύ Αμαρουσίου και Πολυτεχνείου

Τα επίπεδα ισχύος, που δείχνονται, δεν είναι σταθερά για τον απλό λόγο ότι η παραπάνω μέτρηση ελήφθη κατά τη διάρκεια κεντραρίσματος (pointing) του πιάτου. Σταθερότερη κατάσταση εμφανίζεται στα δεξιά της εικόνας όπου τα επίπεδα ισχύος είναι τα καλύτερα που μπορούν να ληφθούν από τη γέφυρα (bridge) του Τμήματος Φυσικής μετά από βέλτιστο προσανατολισμό των δύο κατευθυντικών κεραιών στις εκατέρωθεν τοποθεσίες.

Ακολουθεί γραφική αναπαράσταση της ισχύος του σήματος που λαμβάνει ένας πελάτης από το 802.11b/g σημείο πρόσβασης με SSID MFO_lab2 εντός του απέναντι πάρκου του δήμου.



Εικόνα 5-9 Η ισχύς του σήματος που λαμβάνει ένας πελάτης του σημείου πρόσβασης MFO_lab2

Όπως εύκολα διακρίνεται, τα επίπεδα ισχύος που λαμβάνει ο πελάτης είναι παραπάνω από ικανοποιητικά.

Διαμοιρασμός και κατέβασμα Αρχείων

FTP

Το FTP ή το πρωτόκολλο μεταφοράς αρχείων (File Transfer Protocol) είναι ένα συχνά χρησιμοποιημένο πρωτόκολλο για ανταλλαγή αρχείων σε ένα οποιοδήποτε δίκτυο, που υποστηρίζει το πρωτόκολλο TCP/IP (όπως το Διαδίκτυο ή ένα εσωτερικό δίκτυο). Υπάρχουν δύο υπολογιστές που περιλαμβάνονται σε μια μεταφορά FTP: ένας εξυπηρετητής και ένας πελάτης. Ο εξυπηρετητής FTP, που τρέχει λογισμικό server FTP, ακούει στο δίκτυο για αιτήματα σύνδεσης από άλλους υπολογιστές. Ο υπολογιστής πελάτη, τρέχοντας λογισμικό πελάτη FTP, αρχίζει μια σύνδεση στον κεντρικό υπολογιστή. Μόλις συνδεθεί, ο πελάτης μπορεί να κάνει διάφορες διαδικασίες χειρισμού αρχείων

όπως φόρτωμα αρχείων στον κεντρικό υπολογιστή, κατέβασμα αρχείων από τον κεντρικό υπολογιστή, μετονομασία ή διαγραφή αρχείων στον κεντρικό υπολογιστή και άλλα.

Στα πλαίσια της διπλωματικής αυτή έγινε απλά δοκιμή κατεβάσματος μεγάλου μεγέθους αρχείων, κατ' αρχάς από το δικτυακό τόπο ftp.ntua.gr του Πολυτεχνείου. Για το σκοπό αυτό επιλέχθηκαν μεγάλα ISO αρχεία διαφόρων διανομών του λειτουργικού συστήματος Linux να ζητηθούν προς κατέβασμα από ένα πελάτη του κόμβου προσπέλασης MFO_lab2 στο Τμήμα Φυσικής στην Πανεπιστημιούπολη. Η ισχύς του λαμβανόμενου σήματος στον πελάτη ήταν άνω των -65dBm, η ημέρα που έγινε η δοκιμή δεν ήταν εργάσιμη (Μ. Πέμπτη απόγευμα) ώστε να υπάρχει φόρτος στο δίκτυο και, συνεπώς, επετεύχθη εύκολα ρυθμός διέλευσης δεδομένων της τάξης των 1900kBps ή 15,2Mbps, τιμή διόλου ευκαταφρόνητη.

Διαμοιρασμός αρχείων μεταξύ πελατών

Διαμοιρασμός αρχείων μεταξύ πελατών του ίδιου ή διαφορετικού εκ των τριών σημείου πρόσβασης αλλά και μεταξύ ενός τέτοιου πελάτη και ενσύρματου υπολογιστή, ευρισκόμενου στο χώρο του εργαστηρίου Μικροκυμάτων & Οπτικών Ινών, εννοείται ότι είναι δυνατός. Αυτό ισχύει ανεξάρτητα του λειτουργικού συστήματος, που χρησιμοποιεί κάθε πελάτης. Μάλιστα, στην περίπτωση αυτή είναι δυνατή η επίτευξη του μέγιστου δυνατού ρυθμού διέλευσης δεδομένων, αφού τα hops μεταξύ των σταθμών εργασίας είναι ελάχιστα και εφόσον εκείνη τη χρονική διάρκεια δεν υπάρχει μεγάλος φόρτος από άλλες εφαρμογές στο δίκτυο.

Voice over IP (VoIP)

Η φωνή πάνω από το πρωτόκολλο Διαδικτύου (IP), αποκαλούμενο επίσης VoIP (Voice over Internet Protocol), τηλεφωνία IP η τηλεφωνία Διαδικτύου, είναι η δρομολόγηση των φωνητικών συνομιλιών στο Διαδίκτυο ή σε οποιοδήποτε άλλο δίκτυο, βασισμένο στο IP. Τα πρωτόκολλα που χρησιμοποιούνται για να μεταφέρουν τα σήματα φωνής πάνω στο δίκτυο IP αναφέρονται συνήθως ως πρωτόκολλα VoIP. Μπορούν κανείς να πει ότι αυτά αποτελούν εμπορικές υλοποιήσεις του πειραματικού πρωτοκόλλου φωνής δικτύων (Network Voice Protocol - 1973) που εφευρέθη για το ARPANET.

Οι περισσότερες και πιο επιτυχημένες λύσεις στο χώρο χρησιμοποιούν είτε το H.323 είτε το πρωτόκολλο έναρξης συνόδου (Session Initiation Protocol - SIP). Συνήθη χρησιμοποιούμενα codecs για την κυκλοφορία VoIP αποτελούν τα G.711, G.723.1 και G.729 , όλα διαμορφωμένα από την ITU-T.

Το VoIP μπορεί να υλοποιηθεί σε οποιοδήποτε δίκτυο IP, συμπεριλαμβανομένων εκείνων που στερούνται μια σύνδεση στο Διαδίκτυο, όπως παραδείγματος χάριν σε ένα ασύρματο δίκτυο τοπικής περιοχής.

Ειδικά στα πλαίσια αυτής της διπλωματικής εργασίας, η υλοποίηση μίας υπηρεσίας VoIP προσφέρει δύο σημαντικά πλεονεκτήματα. Πρώτον η υπηρεσία φωνής μέσω VoIP δεν κοστίζει τίποτα. Με άλλα λόγια πελάτες των σημείων πρόσβασης στο Μαρούσι ή την Πανεπιστημιούπολη μπορούν να μιλούν, καθώς και να ανταλλάζουν μηνύματα δωρεάν με άλλους εντός ή εκτός του εργαστηρίου Μικροκυμάτων & Οπτικών Ινών. Δεύτερον, οι εισερχόμενες κλήσεις μπορούν να δρομολογηθούν αυτόματα στο τηλέφωνο VoIP του καλούμενου, ανεξάρτητα από που ο τελευταίος έχει συνδεθεί με το δίκτυο. Δηλαδή, ένας εγγεγραμμένος στην υπηρεσία VoIP χρήστης μπορεί να δεχτεί κλήσεις στον ίδιο VoIP αριθμό είτε βρίσκεται στην περιοχή κάλυψης του σημείου πρόσβασης του Αμαρουσίου είτε εκείνη του Ζωγράφου είτε εκείνη του Πολυτεχνείου.

Ωστόσο, οι VoIP υλοποιήσεις αντιμετωπίζουν και δυσκολίες, όπως η καθυστέρηση, η απώλεια πακέτων κυρίως λόγω συμφόρησης σε ενδιάμεσους κόμβους, η διακύμανση στη καθυστέρηση (jitter) και η ηχώ. Εφόσον δεν ικανοποιούνται κάποιες προϋποθέσεις, όπως QoS, επαρκές εύρος ζώνης κλπ., τα προβλήματα αυτά είναι ικανά να καταστήσουν την υπηρεσία VoIP αναξιόπιστη. Ευτυχώς, στο νεοϋλοποιηθέν ασύρματο δίκτυο που εγκαταστάθηκε ο πολύ χαμηλός κυκλοφοριακός φόρτος σε συνδυασμό με τη δυνατότητα διάθεσης πολλαπλού ρυθμού διέλευσης

δεδομένων από το απαιτούμενο επέτρεψαν όλες οι συνομιλίες να πραγματοποιηθούν όχι μόνο απρόσκοπτα αλλά με καλή ποιότητα.

Για την πραγματοποίηση των προαναφερθέντων συνομιλιών επιλέχθηκε να εγκατασταθεί σε σταθερό υπολογιστή, που συνδέεται άμεσα με το switch του δικτύου στο εργαστήριο Μικροκυμάτων με ip διεύθυνση 147.102.5.242, ένας Asterisk server με τις προεπιλεγμένες ρυθμίσεις (dialplans, πρωτόκολλα VoIP κλπ.). Το Asterisk αποτελεί μια τηλεπικοινωνιακή πλατφόρμα ανοικτού κώδικα, σχεδιασμένη να επιτρέπει σε διαφορετικούς τύπους υλικού, υλικολογισμικού και λογισμικού τηλεφωνίας IP να διασυνδέονται ο ένας με τον άλλον με συνέπεια. Παρέχει πολλαπλά στρώματα, διαχείριση και TDM και πακέτων φωνής σε χαμηλότερα στρώματα ενώ ταυτόχρονα προσφέρει και μια ιδιαίτερα εύκαμπτη πλατφόρμα για PBX (Private Branch eXchange – ιδιόκτητο τηλεφωνικό δίκτυο) και εφαρμογές τηλεφωνίας. Το Asterisk μπορεί να γεφυρώσει και να μεταφράσει διαφορετικούς τύπους πρωτοκόλλων VoIP όπως τη SIP και H.323. Συγχρόνως μπορεί να παρέχει μια πλήρη πλατφόρμα κεντρικού υπολογιστή για μακρινά και κεντρικά PBX και για συνδιάσκεψη.

Στα αρχεία ρύθμισης του Asterisk server, μεταξύ άλλων, έχουν ανατεθεί αριθμοί VoIP σε εκ των προτέρων γνωστούς πελάτες και έχει ορισθεί ένα όνομα χρήστη και συνθηματικό (password) για κάθε πελάτη. Οι πελάτες συνδέονται με τον Asterisk με χρήση του προγράμματος X-Lite της X-Ten, ενός λογισμικού τηλεφώνου (soft phone). Ακολουθεί εικόνα αυτής της εφαρμογής.

Εικόνα 5-10 X-Lite 3.0 soft phone

Αξίζει να αναφερθεί ότι, μεταξύ πολλών άλλων λειτουργιών, η εφαρμογή αυτή επιτρέπει και βιντεοκλήσεις εφόσον στον εξοπλισμό του κάθε πελάτη περιλαμβάνεται και κάμερα.

Βιβλιογραφία - Αναφορές

Pejman Roshan, Jonathan Leary, "*802.11 Wireless LAN Fundamentals*", Cisco Press, 2004

Toby J. Velte - Ph.D., Anthony T. Velte, "*Cisco 802.11 Wireless Networking Quick Reference*", Cisco Press, 2005

Matthew Gast, "*802.11 Wireless Networks The Definitive Guide*", O'Reilly, 2005

Bruce E. Alexander, "*802.11 Wireless Network Site Surveying and Installation*", Cisco Press, 2004

Creative Commons Attribution-ShareAlike 2.5 license, "*Wireless Networking in the Developing World*", Limehouse Book Sprint Team, 2006

Rob Flickenger, "*Building Wireless Community Networks*", O'Reilly, 2003

Rob Flickenger, "*Wireless Hacks*", O'Reilly, 2003

Ι. Δ. Κανελλόπουλος, "*Διάδοση ηλεκτρομαγνητικών κυμάτων σε γήινο περιβάλλον*", Εκδ. Τζιόλα, 2003

Joseph Davies, "*Deploying Secure 802.11 Wireless Networks with Microsoft Windows*", Microsoft Press, 2004

Eric Ouellet, Robert Padjen, Arthur Pfund, "*Building A Cisco Wireless LAN*", Syngress, 2002

Ian F. Akyildiz, Xudong Wang & Weilin Wang, "*Wireless mesh networks: a survey*", Computer Networks 47 (2005) 445–487