ΑΝΩΤΑΤΟ ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΜΕΣΟΛΟΓΓΙΟΥ
ΠΑΡΑΡΤΗΜΑ ΝΑΥΠΑΚΤΟΥ
ΤΜΗΜΑ ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΔΙΚΤΥΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

"Δημιουργία Ασύρματης Δικτυακής Υποδομής Με Υποστήριξη Radius"

ΣΕΛΛΗΝΑ ΚΩΝΣΤΑΝΤΙΝΑ
ΑΜ: 497

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:

ΟΙΚΟΝΟΜΑΚΟΣ ΜΙΧΑΛΗΣ

[ΝΑΥΠΑΚΤΟΣ 2012]

Ευχαριστίες

Σε αυτό το σημείο, θα ήθελα να ευχαριστήσω όλους όσους συνέβαλαν με κάθε τρόπο στην επιτυχή εκπόνηση της πτυχιακής μου εργασίας. Καταρχήν θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου κ. Οικονομάκο Μιχάλη για την εμπιστοσύνη, την καθοδήγηση που μου προσέφερε καθώς και την επίβλεψη της παρούσας πτυχιακής εργασίας καθ’ όλη την διάρκεια του εξαμήνου. Στη συνέχεια, θα ήθελα να ευχαριστήσω τους φίλους μου και την οικογένειά μου για την βοήθεια και υποστήριξη που μου παρείχαν. Τέλος ένα μεγάλο ευχαριστώ στον Asmodeus, στην Kira και στην Hra.

Περίληψη

Τα ασύρματα δίκτυα hotspot είναι συχνό φαινόμενο στην καθημερινότητά μας και χρησιμοποιούνται για να προσφέρουν δικτυακές υπηρεσίες και πρόσβαση στο Internet στους ασύρματους πελάτες. Τα συναντούμε σε café, σε πανεπιστημιουπόλεις, σε αεροδρόμια κ.α. Κάποιες φορές είναι αναγκαίος ο έλεγχος πρόσβασης των ασύρματων χρηστών που συνδέονται σε υποδομές hotspot για λόγους ασφάλειας και καλύτερης διαχείρισης των δικτυακών πόρων ακόμα και για οικονομική εκμετάλλευση του δικτύου. Ένας Radius Server μπορεί να χρησιμοποιείται για να παρέχει λειτουργίες AAA (authentication, authorization, accounting), αυξάνοντας την ασφάλεια αυτών των δικτύων και εξασφαλίζοντας μια συγκεντρωτική διαχείριση του ελέγχου πρόσβασης των χρηστών.

Στην παρούσα πτυχιακή εργασία αναλύεται το θεωρητικό υπόβαθρο για την ανάπτυξη ενός hotspot. Επιπλέον περιγράφεται η διαδικασία της υλοποίησης αυτής της δικτυακής υποδομής καθώς και οι διαμορφώσεις του απαιτούμενου υλικού και λογισμικού.

Οι ασύρματοι χρήστες που συνδέονται σε αυτό το δίκτυο και επιθυμούν πρόσβαση στον Παγκόσμιο Ιστό, θα ανοίγουν τον browser τους και θα βλέπουν αμέσως μια σελίδα Login στην οποία θα πρέπει να εισάγουν τα προσωπικά τους στοιχεία (username, password) τα οποία πρέπει να έχουν παραλάβει από τον διαχειριστή του δικτύου. Έπειτα, ένας Radius Server εκτελεί την πιστοποίηση του κάθε χρήστη ανατρέχοντας σε καταλόγους προκειμένου να επιβεβαιώσει την καταχώρησή του. Μια θετική απάντηση του Radius Server οδηγεί σε επιτυχές Login και επιτρέπει στον χρήστη να ξεκινήσει την προήγηση στον Παγκόσμιο Ιστό, ενώ μια αρνητική απάντηση οδηγεί σε αποτυχία στο Login και ο χρήστης πρέπει να ξαναδοκιμάσει να εισάγει τα στοιχεία του απαγορεύοντας κάθε άλλη ενέργεια αναφορικά με το Web.

Περιεχόμενα

Πίνακας Εικόνων

Πίνακας Πινάκων

«Οι κινητοί ασύρματοι υπολογιστές είναι σαν τις φορητές τουαλέτες χωρίς αποχέτευση. Θα είναι συνηθισμένο φαινόμενο στα οχήματα, στις οικοδομές, και στις υπαίθριες συναυλίες. Η συμβουλή μου είναι να καλωδιώσετε το σπίτι σας και να μείνετε εκεί.»

Ο Bob Metcalfe (1995) ,

εφευρέτης του Ethernet[1]

«Τέσσερις ή πέντε υπολογιστές πρέπει να είναι αρκετοί για ολόκληρο τον κόσμο μέχρι το έτος 2000.»

T.J Watson (1945),

Πρόεδρος της IBM [1]

1 Εισαγωγή στα ασύρματα δίκτυα

1.1 Γενικά

Οι ψηφιακές ασύρματες επικοινωνίες και οι σχετικές με την κινητικότητα υπηρεσίες που παρέχουν είναι πλέον αναπόσπαστο κομμάτι της καθημερινότητάς μας. Παραδείγματα αυτών είναι τα ασύρματα τηλεπικοινωνιακά συστήματα όπως τα κυψελικά (*cellular*), τα ασύρματα και δορυφορικά τηλέφωνα αλλά και τα ασύρματα τοπικά δίκτυα (*Wireless Local Area Networks*, WLAN).
Ίσως πριν μερικά χρόνια να μην ήταν τόσο αποδεκτή η ιδέα της ασύρματης επικοινωνίας των υπολογιστών, όμως, σταδιακά, η τελευταία άρχισε να εξαπλώνεται με ραγδαίο ρυθμό καθιστώντας διαφορετικό τον τρόπο με τον οποίο εργάζονται οι άνθρωποι σε ηλεκτρονικούς υπολογιστές. Οι άνθρωποι αυτοί δεν περιορίζονται πλέον στα όρια ενός γραφείου αλλά έχουν την ανάγκη, ασχέτως του σημείου που βρίσκονται, να μπορούν εύκολα και γρήγορα να χρησιμοποιούν τον υπολογιστή τους, να συνδέονται με άλλες δικτυακές συσκευές καθώς και με το Internet για την παροχή υπηρεσιών και πληροφοριών.
Στα παραπάνω συνέβαλε η ανάπτυξη των φορητών συσκευών και υπολογιστών που έλυσε το πρόβλημα της φορητότητας των υπολογιστών και έκανε δυνατή τη παραγωγή συσκευών με πολύ μικρό κόστος και σε μεγάλες ποσότητες καθώς και οι διαρκώς αναπτυσσόμενες τεχνολογίες ασυρμάτων δικτύων έλυσαν το πρόβλημα της διασύνδεσης αυτών των υπολογιστών. Εγκαταστάσεις τοπικών ασύρματων δικτύων υπάρχουν πλέον σε πάρα πολλούς δημόσιους χώρους, καφετέριες, αεροδρόμια, αίθουσες συνεδρίων, κοινόχρηστους χώρους πανεπιστημίων και εταιρειών. Επιπλέον, ασύρματες συνδέσεις ενώνουν απομακρυσμένα δίκτυα (π.χ δύο κτίρια σε μια πόλη) δίνοντας λύσεις εκεί που τα καλώδια δεν μπορούν.

1.2 Ιστορικά στοιχεία

Η ασύρματη μετάδοση έχει ιστορία μεγαλύτερη από έναν αιώνα και τα τελευταία 15 με 20 χρόνια βρίσκει την άνθησή της στον τομέα τον τηλεπικοινωνιών.
Τα πρώτα βήματα της ασύρματης ψηφιακής μετάδοσης έγιναν από τον Ιταλό Φυσικό *Guglielmo Marconi*, όταν άρχισε κάποια πειράματα στα ραδιοκύματα. Το **1895** έκανε την πρώτη ασύρματη μετάδοση με χρήση ραδιοκυμάτων και κώδικα Morse μεταξύ του νησιού Wight και ενός ρυμουλκού πλοίου που βρισκόταν σε απόσταση 18 μιλίων. Το **1896**, ίδρυσε την εταιρεία *Wireless Telegraph and Signal Company*, την πρώτη εταιρεία στο είδος της εκείνη την εποχή παγκοσμίως. Λίγο αργότερα, το **1901**, μεταδόθηκε επιτυχώς ένα ραδιοφωνικό σήμα από την Κορνουάλλη της Βρετανίας στην άλλη άκρη του Ατλαντικού Ωκεανού, στο Newfoundland. Στη συνέχεια, η ασύρματη αυτή τεχνολογία άρχισε να χρησιμοποιείται ευρέως για στρατιωτικούς σκοπούς και ιδιαίτερα κατά τη διάρκεια του 2ου Παγκοσμίου Πολέμου. Οι πληροφορίες μεταδίδονταν κρυπτογραφημένες και ήταν εξαιρετικά δύσκολο να αποκρυπτογραφηθούν. Το πρώτο εμπορικό δίκτυο Ραδιοτηλεφωνίας έγινε διαθέσιμο στους πελάτες από την εταιρεία Bell Telephone Company στις αρχές της δεκαετίας του 50. Το πρόβλημα όμως με το δίκτυο αυτό ήταν ο περιορισμένος αριθμός χρηστών που θα μπορούσαν να είναι συνδεμένοι ταυτόχρονα. Το δίκτυο αυτό συνέχισε να αναπτύσσεται, έτσι ώστε να μπορεί να εξυπηρετεί περισσότερο κόσμο και να είναι πιο αξιόπιστο.
Το **1971**, οι ερευνητές του Πανεπιστημίου της Hawaii με επικεφαλή τον Norman Abramson, ανέπτυξαν το πρώτο ασύρματο σύστημα μεταφοράς δεδομένων στα πλαίσια του προγράμματος ALOHAnet. Η ανάγκη για αμφίδρομη επικοινωνία χωρίς χρήση τηλεφωνικών γραμμών λόγω ανεπαρκούς τηλεφωνικού δικτύου οδήγησε στην ανάπτυξη αυτού του προγράμματος. Έτσι το *ALOHA*, χρησιμοποιώντας τοπολογία αστέρα, αποτελούνταν από επτά υπολογιστές τοποθετημένους σε τέσσερα νησιά της Χαβάης, οι οποίοι επικοινωνούσαν με έναν κεντρικό υπολογιστή που βρισκόταν στο νησί Oahu

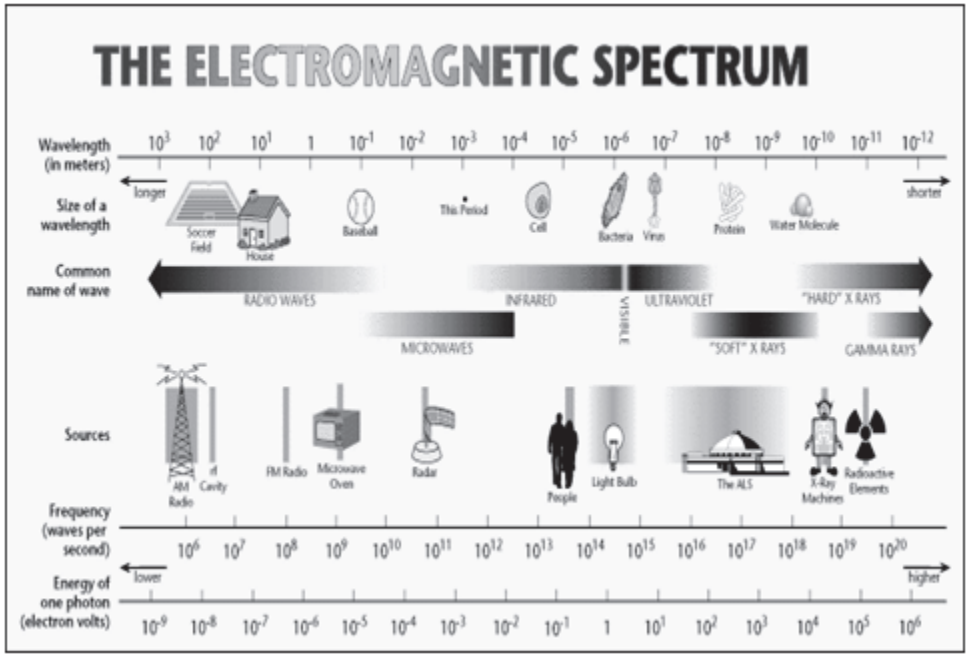
παίζοντας το ρόλο κομβικού σημείου (*hub*) χρησιμοποιώντας χαμηλού κόστους ερασιτεχνικά (*ham-like*) ραδιόφωνα.
Το **1979**, οι *F.R Gfeller* και *U. Baspst* δημοσίευσαν μία εργασία στα πρακτικά του IEEE παρουσιάζοντας ένα πρώιμο τοπικό ασύρματο δίκτυο, το οποίο βρισκόταν σε πειραματικό στάδιο και χρησιμοποιούσε για την επικοινωνία την υπέρυθρη ακτινοβολία (*Infrared* – IR) αλλά λόγω χαμηλού ρυθμού μετάδοσης (1Mbps) η προσπάθεια απέτυχε. Ακολούθησαν κι άλλες προσπάθειες με χρήση ραδιοκυμάτων στα 900 MHz (HP) και στα 1,73 GHz (Motorola), αλλά απέτυχαν λόγω της πολυπλοκότητας και της αδυναμίας εξασφάλισης μόνιμης άδειας χρήσης φάσματος. Το 1980, ο P. Ferrert υπέβαλε μία έκθεση σχετικά με μία πειραματική εφαρμογή για ασύρματη επικοινωνία μεταξύ τερματικών στο εθνικό συνέδριο τηλεπικοινωνιών του IEEE, που χρησιμοποιούσε την τεχνική της εξάπλωσης φάσματος (Spread Spectrum).
Το **1982**, οι προδιαγραφές AMPS (Advanced Mobile Phone Service) καθορίστηκαν ως το επίσημο πρότυπο της ραδιοτηλεφωνίας στις Ηνωμένες Πολιτείες. Παράλληλα, αρκετές άλλες χώρες άρχισαν να αναπτύσσουν κυψελωτά (*cellular*) δίκτυα, ορισμένα από τα οποία έκαναν χρήση των προτύπων των ΗΠΑ, ενώ άλλα χρησιμοποίησαν διαφορετικά πρότυπα. Τα δίκτυα GSM είναι τα πλέον διαδιδόμενα στα δίκτυα κυψελωτής τηλεφωνίας, κυρίως στη Βόρεια Αμερική.
Το **1984**, ο *Kaveh Pahlavan* παρουσίασε στο Συμπόσιο Δικτύων Υπολογιστών του IEEE μία σύγκριση ανάμεσα στα ασύρματα πληροφοριακά συστήματα δικτύων επικοινωνίας, που χρησιμοποιούν τις υπέρυθρες ακτινοβολίες και CDMA εξάπλωση φάσματος, η οποία αργότερα δημοσιεύτηκε στο περιοδικό Communication Society του IEEE.
Το **1985** η Ομοσπονδιακή Επιτροπή Τηλεπικοινωνιών (*Federal Communications Commission*, FCC) εξουσιοδότησε την δημόσια χρήση της Βιομηχανικής, Επιστημονικής, Ιατρικής ζώνης (*ISM bands*), για εμπορική εφαρμογή της τεχνολογίας Εξάπλωσης Φάσματος *(Spread Spectrum*), που περιλαμβάνει τις συχνότητες 902 MHz ως και 5.85GHz. Το γεγονός αυτό συνέβαλε σημαντικά στην αγορά των ασυρμάτων δικτύων, αφού στις περισσότερες χώρες του κόσμου δεν απαιτείται καμία ειδική άδεια για την εκπομπή στην περιοχή των ISM ζωνών, εκτός από περιορισμούς στην ισχύ εκπομπής που ποικίλλουν από χώρα σε χώρα. Έτσι πολλοί κατασκευαστές ασχολήθηκαν με την μαζική παράγωγη ασύρματων προϊόντων που οδήγησε στην αύξηση του αριθμού των WLANs. Αργότερα, ο *M. Kavehrad* δημοσίευσε μία έκθεση σχετικά με ένα πειραματικό ασύρματο PBX σύστημα, που χρησιμοποιούσε Πολλαπλή Πρόσβαση με Διαίρεση Κώδικα (CDMA). Αυτές οι προσπάθειες αποτέλεσαν το εναρκτήριο λάκτισμα για πολλές βιομηχανικές δραστηριότητες στην ανάπτυξη μιας νέας γενιάς ασύρματων τοπικών δικτύων και τον εμπλουτισμό και ανανέωση διαφόρων παλαιών θεμάτων σχετικών με τη φορητότητα και κινητικότητα.
Το **1991** πραγματοποιήθηκε συνέδριο για τα ασύρματα τοπικά δίκτυα του IEEE (IEEE Workshop) και η επιτροπή του IEEE 802.11 είχε μόλις αρχίσει τις δραστηριότητες της για την ανάπτυξη προτύπου για τα ασύρματα τοπικά δίκτυα κάνοντας και την εμφάνισή τους τα "πρόωρα" προϊόντα για τα ασύρματα τοπικά δίκτυα. Μέχρι το 1997, η τεχνολογία των ασύρματων τοπικών δικτύων είχε φτάσει σε ώριμο στάδιο, είχε καθοριστεί μία ποικιλία εφαρμογών και είχαν κατανοηθεί πλήρως οι τεχνολογίες που επέτρεπαν αυτές τις εφαρμογές.
Στις 21 Ιουλίου του **1999**, πρωτοεμφανίστηκε το *AirPort* στην πόλη της Νέας Υόρκης από τον *Steve Jobs*, ένα ασύρματο τοπικό δίκτυο που βασίζεται στο πρωτόκολλο του IEEE 802.11b. Αυτή ήταν η πρώτη φορά που τα ασύρματα τοπικά δίκτυα έγιναν δημόσια διαθέσιμα στους ιδιώτες καταναλωτές για προσωπική χρήση και βρήκαν μεγάλη απήχηση σε αυτούς αφού συνειδητοποίησαν την χρηστικότητα της μη ύπαρξης καλωδίων. Μέχρι τότε η ιδιωτική χρήση των WLANs ήταν πολύ ακριβή για τους καταναλωτές λόγω των ακριβών υλικών εγκατάστασης τους και αυτό είχε ως αποτέλεσμα την αποκλειστική τους χρήση σε εγκαταστάσεις μεγάλων εταιρειών ή ως εναλλακτική λύση του ενσύρματου, σε περιοχές όπου η καλωδίωση ήταν δύσκολη ή αδύνατη.
Αυτή τη στιγμή δύο είναι τα πρότυπα σε εξέλιξη όσον αναφορά τα ασύρματα τοπικά δίκτυα. Το, όχι και τόσο δημοφιλές, HIPERLAN (*High Performance European Radio LAN*) που αναπτύσσεται στην Ευρώπη από το ETSI (*European Telecommunications Standard Institute*) και το 802.11 WLAN που είναι το πιο διαδεδομένο σήμερα και αναπτύσσεται από

την IEEE (*Institute of Electrical and Electronics Engineers*). Πρωταγωνιστικό ρόλο παίζει και η τεχνολογία WiMax, που βασίζεται στο πρότυπο 802.16.

1.3 Ασύρματα δίκτυα

Ασύρματο δίκτυο αποτελεί κάθε δομημένο τηλεπικοινωνιακό δίκτυο που αποτελείται από δίκτυα και συσκευές υπολογιστών ή τηλεφωνίας και χρησιμοποιεί ως μέσο τον αέρα για την μετάδοση της πληροφορίας. Τα δεδομένα μεταφέρονται με ηλεκτρομαγνητικά κύματα (ραδιοκύματα ή υπέρυθρη ακτινοβολία), μέσω της διαδικασίας της διαμόρφωσης, με συχνότητα φέροντος η οποία εξαρτάται κάθε φορά από τον ρυθμό μετάδοσης δεδομένων που απαιτείται να υποστηρίζει το δίκτυο. Δεν αποτελούν ασύρματα δίκτυα το ραδιόφωνο και η τηλεόραση, όπως την ξέρουμε μέχρι στιγμής, αν και εντάσσονται στα ασύρματα τηλεπικοινωνιακά μέσα, αλλά η μετάδοση γίνεται προς κάθε κατεύθυνση χωρίς να υπάρχει κάποιο δομημένο δίκτυο τηλεπικοινωνιακών κόμβων.
Παραδείγματα ασύρματων δικτύων θεωρούνται τα εξής:

- Δίκτυα κινητής τηλεφωνίας
- Ασύρματα τηλέφωνα
- Δορυφορικές επικοινωνίες
- Ασύρματα δίκτυα ευρείας περιοχής (WWAN)
- Ασύρματα μητροπολιτικά δίκτυα (WMAN)
- Ασύρματα τοπικά δίκτυα (WLAN)
- Ασύρματα προσωπικά δίκτυα (WPAN)



Εικόνα 1 Στα ασύρματα δίκτυα τα δεδομένα μεταφέρονται με ηλεκτρομαγνητικά κύματα (ραδιοκύματα ή υπέρυθρη ακτινοβολία).

1.3.1 Ασύρματα συστήματα μεταφοράς δεδομένων

Τα ασύρματα συστήματα μεταφοράς δεδομένων είναι μια κατηγορία ασύρματων δικτύων που χρησιμοποιούνται για τη μεταφορά ψηφιακών δεδομένων. Τα τερματικά παραμένουν ανενεργά (*idle*) μέχρι να υπάρξει κάποιο πακέτο προς μετάδοση. Το πακέτο αυτό μεταδίδεται κατά ριπές (*bursts*).[3]
Για να επιτυγχάνεται η διασύνδεση, η επικοινωνία και η ανταλλαγή δεδομένων σε αυτά τα ασύρματα συστήματα έχουν θεσπιστεί κάποια πρότυπα λειτουργίας από τους παγκόσμιους οργανισμούς δημιουργίας προτύπων. Ακολουθούν τα ευρέως διαδεδομένα αυτά πρότυπα.

1.3.1.1 IEEE 802.11-Ασύρματα τοπικά δίκτυα (WLAN) ή Wi-Fi

Ασύρματο τοπικό δίκτυο είναι ένα μοιραζόμενο μέσο επικοινωνίας που διαβιβάζει πληροφορίες μέσα από ασύρματες διασυνδέσεις μεταξύ τερματικών που βρίσκονται εντός της εμβέλειάς του. Τα WLAN λειτουργούν με ένα από τα τρία ακόλουθα φυσικά μέσα: υπέρυθρες ακτίνες, μικροκύματα με διασπορά φάσματος, μικροκύματα με στενή ζώνη.
Η βασική μονάδα ενός ασύρματου τοπικού δικτύου είναι η *κυψέλη*. Η κυψέλη είναι η περιοχή όπου λαμβάνει χώρα η ασύρματη επικοινωνία. Η περιοχή κάλυψης μιας κυψέλης εξαρτάται από την ισχύ του μεταδιδόμενου σήματος και του τύπου και της κατασκευής των τοίχων, των χωρισμάτων και άλλων φυσικών χαρακτηριστικών του εσωτερικού χώρου. Οι χρήστες έχουν τη δυνατότητα να κινούνται μέσα στην περιοχή κάλυψης μένοντας συνδεδεμένοι στο δίκτυο. Η ακτίνα δράσης μπορεί να είναι αρκετά μέτρα επιτρέποντας την διασύνδεση ενός κτιρίου, γραφείου, ή πανεπιστημιούπολης.
Υπάρχουν αρκετά πρότυπα για τα ασύρματα τοπικά δίκτυα αλλά μόνο δύο χρησιμοποιούνται: το ευρωπαϊκό πρότυπο ασύρματων τοπικών δικτύων υψηλής ταχύτητας HIPERLAN και η οικογένεια προτύπων IEEE 802.11x (γνωστό και ως *Wireless Ethernet* ή *Wi-Fi*). Και τα δύο αυτά πρότυπα καλύπτουν μόνο τα δύο κατώτερα στρώματα του μοντέλου OSI: το *Medium Access Control* (MAC) και το *Physical Layer* (PHY).

OpenAir:
Είναι ένα ιδιόκτητο πρότυπο της εταιρείας Proxim, από τις μεγαλύτερες εταιρείες κατασκευαστών WLAN. Προσπαθεί να προωθήσει το OpenAir ως εναλλακτικό πρότυπο του 802.11. Χρησιμοποιεί την τεχνική μεταπήδησης συχνότητας (*Frequency Hopping*) με ρυθμούς δεδομένων 0.8 και 1.6 Mbps (χρησιμοποιώντας τεχνικές διαμόρφωσης 2FSK και 4FSK). Το OpenAir MAC πρωτόκολλο που χρησιμοποιείται είναι CSMA/CA και προαιρετικά βασίζεται στην ανταλλαγή RTS/CTS πακέτων.

HiperLAN:
Αποτελεί το ευρωπαϊκό πρότυπο ασύρματων τοπικών δικτύων υψηλής ταχύτητας HIPERLAN του Ευρωπαϊκού Ιδρύματος Προτύπων Τηλεπικοινωνιών (ETSI).
Το HiperLAN 1 πρότυπο καλύπτει φυσικό και MAC επίπεδο και λειτουργεί στην μπάντα από 5.1 έως 5.3 GHz του φάσματος ραδιοσυχνοτήτων και με ρυθμό μετάδοσης σηματοδοσίας (μετάδοσης δεδομένων) 2 έως 25 Mbps. Το πρωτόκολλο χρησιμοποιεί διαφορετική εκδοχή του CSMA/CA στο επίπεδο MAC και αναθέτει προτεραιότητες στα πακέτα πρόσβασης στο κανάλι με δυναμικό τρόπο λαμβάνοντας υπόψη την προτεραιότητα, την διάρκεια ζωής και τις αναμεταδόσεις πακέτων στο επίπεδο MAC εξασφαλίζοντας ποιότητα υπηρεσιών (QoS). Εφαρμόζεται σε ad-hoc και infrastructure δίκτυα.
Το HiperLAN 2 είναι ένα συνδεσιοστραφές σύστημα που έχει ως στόχο να προσφέρει πρόσβαση υψηλής ταχύτητας σε διάφορα δίκτυα και κυρίως σε δίκτυα ATM. Προσφέρει ταχύτητες δεδομένων μέχρι 54Mbps στο φυσικό επίπεδο στην ίδια ζώνη ραδιοσυχνοτήτων, καθώς και καλύτερη ποιότητα υπηρεσιών για να ικανοποιήσει τις ανάγκες για εφαρμογές πολυμέσων. Το ETSI συνεργάστηκε με το IEEE για την ανάπτυξη του.

<u>Εφαρμογές Ασύρματων τοπικών δικτύων</u>

Η χρήση καλωδίων είναι αρκετά δεσμευτική. Η χρήση τους μπορεί να είναι αρκετά ασύμφορη, είτε αντιαισθητική ακόμα και επικίνδυνη. Έτσι αρκετές φορές αναγκαία είναι η χρήση ασύρματης δικτύωσης.
Οι επιχειρήσεις χρησιμοποιούν WLANs, όπως τα αεροδρόμια, τα ξενοδοχεία, οι αλυσίδες café, γνωστά και ως hotspots, προσελκύοντας με αυτόν τον τρόπο αρκετούς πελάτες που θέλουν να είναι "online" ανελλιπώς. WLANs υπάρχουν επίσης και σε πανεπιστημιουπόλεις για να εξυπηρετούνται οι φοιτητές και το προσωπικό οποιαδήποτε στιγμή χρειαστούν πρόσβαση σε ηλεκτρονικά δεδομένα της σχολής ή στο Internet. Χρήσιμα είναι και σε συνέδρια για τον διαμοιρασμό της πληροφορίας μεταξύ τον συμμετεχόντων.
Θα μπορούσαμε να κατατάξουμε τις παραπάνω, καθώς και άλλες περιπτώσεις, σε τέσσερις βασικούς τομείς εφαρμογών των ασύρματων τοπικών δικτύων. Αυτοί είναι:

- **Ασύρματη επέκταση ενός υπάρχοντος ενσύρματου δικτύου:**
  Μέχρι τώρα οι επιχειρήσεις βασίζονται στα ενσύρματα τοπικά δίκτυα για ανταλλαγή δεδομένων μεταξύ των τερματικών συσκευών με καλώδια UTP Cat3 ή Cat5. Υπάρχουν όμως περιπτώσεις όπου χρειάζεται η επέκταση της δικτυακής υποδομής αλλά ο χώρος δεν είναι κατάλληλος για ενσύρματη δικτύωση ή δεν υπάρχει υφιστάμενη καλωδίωση. Έτσι η επέκταση πρέπει να γίνει ασύρματα με έναν κύριο κόμβο να συνδέεται μέσω Ethernet (UTP καλώδιο) με το LAN και να επικοινωνεί ασύρματα με άλλους σταθμούς.
- **Διασύνδεση LAN σε διαφορετικά κτίρια:**
  Είναι η διασύνδεση ενσύρματων τοπικών δικτύων, τα οποία βρίσκονται σε διαφορετικά γειτονικά κτίρια, μέσω μιας ασύρματης σύνδεσης. Η ασύρματη σύνδεση είναι τύπου *point-to-point* και ελέγχεται από δρομολογητές (*routers*) και γέφυρες (*bridges*) των ενσύρματων δικτύων. Με αυτόν τον τρόπο μια εταιρεία που θέλει να συνδέσει τα γραφεία της μπορεί να γλιτώσει αρκετό χρήμα και καλωδίωση που θα χρειαζόταν στην ενσύρματη δικτύωση.
- **Νομαδική πρόσβαση:**
  Είναι ασύρματη διασύνδεση μεταξύ φορητού τερματικού και ενός κομβικού σημείου LAN . Τέτοιου είδους ασύρματα δίκτυα βλέπουμε συχνά στην καθημερινότητά μας καθώς η μεταφορά δεδομένων από τον κεντρικό υπολογιστή του σπιτιού μας στο laptop μας και το αντίστροφο, ή η προσπέλαση πληροφοριών μέσω φορητών συσκευών από τους φοιτητές στην σχολή μας αποτελούν παραδείγματα νομαδικής πρόσβασης. Σε ένα τέτοιο δίκτυο αυξάνονται οι πιθανότητες εισβολής κακόβουλου λογισμικού στο σύστημά μας γι' αυτό πρέπει να λαμβάνουμε σοβαρά υπόψη ζητήματα ασφάλειας.
- **Αδόμητη δικτύωση (ad hoc) - απευθείας δικτύωση κινητών συσκευών:**
  Συνήθως δημιουργούνται προσωρινά για να ικανοποιήσουν άμεσα μία συγκεκριμένη ανάγκη και μετά καταργούνται. Είναι αποκεντρωμένο *peer to peer* δίκτυο το οποίο επιτρέπει σε μια ομάδα υπολογιστών, να μοιράζονται, τους πόρους τους ισοδύναμα έχοντας ίσα δικαιώματα. Οι υπολογιστές χρησιμοποιούνται ταυτόχρονα και ως πελάτες και ως εξυπηρετητές. Κάθε συσκευή όταν βρίσκεται εντός της εμβέλειας αυτού του δικτύου, ενσωματώνεται αυτόματα σε αυτό. Η τοπολογία τους δεν είναι σταθερή αλλά δυναμική αφού δεν απαιτούν κάποια προϋπάρχουσα υποδομή. Παράδειγμα ενός τέτοιου δικτύου μπορεί να αποτελέσει ένα έκτακτο ιατρικό συνέδριο στο οποίο στο οποίο οι συμμετέχοντες ιατροί θέλουν να ανταλλάξουν εύκολα και γρήγορα κάποια δεδομένα.

1.3.1.2 IEEE 802.15-Ασύρματα δίκτυα προσωπικής περιοχής (Wireless Personal Area Networks, WPANs)

Βρίσκονται ένα σκαλοπάτι πριν τα WLANs. Τα δίκτυα αυτά παρέχουν μικρότερη γεωγραφική κάλυψη από τα WLANs και είναι κατάλληλα για εφαρμογές διασύνδεσης και επικοινωνίας γειτονικών συσκευών που βρίσκονται εντός λίγων μέτρων. Κατά τη διάρκεια της καθημερινής δραστηριότητας, ο προσωπικός χώρος λειτουργίας του ατόμου (*Personal Operating Space*, POS) και των συσκευών του (κινητά τηλέφωνα, τα PDA's και οι Ultra Mobile υπολογιστές) αλλάζει. Έτσι κάθε φορά μπορεί να χρειαστούν διαφορετικές συσκευές που να του παρέχουν υπηρεσίες, όπως ανταλλαγή αρχείων ή διασύνδεση, και όλες μαζί να συμφωνούν σε ένα κοινό πρότυπο με το οποίο θα επικοινωνούν και θα ανταλλάσουν δεδομένα.
Οι πρώτες έρευνες για να καθοριστούν πρότυπα για δίκτυα προσωπικής περιοχής ξεκίνησαν το 1996 και η πρώτη προσπάθεια χρονολογείται το 1994 από ένα πρόγραμμα της Ericsson, γνωστό σε όλους ως *Bluetooth* (όνομα βασιλιά που ένωσε τις φυλές των Βίκινγκ), το οποίο αποσκοπούσε στην ασύρματη επικοινωνία μεταξύ κινητών τηλεφώνων και σχετικών εξαρτημάτων (*hands-free*). Σήμερα το πρότυπο αυτό χρησιμοποιείται από περισσότερες από 100 εταιρείες και σε αρκετές συσκευές στην αγορά όπως εκτυπωτές, φορητοί υπολογιστές, κινητά τηλέφωνα. Εκτός από το Bluetooth, έχουν σχηματιστεί κι άλλα πρότυπα για δίκτυα προσωπικής περιοχής όπως το *HomeRF* και το *Zigbee*.

IEEE 802.15 WPAN		
802.15.1	Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs)	Καθορίζει τις προδιαγραφές του PHY και MAC στρώματος για ασύρματη σύνδεση σταθερών, φορητών ή κινητών συσκευών κατά τη διάρκεια εισόδου ή μέσα σε μια περιοχή προσωπικής λειτουργίας. Τα πρότυπα της 802.15.1-2005 καθορίζουν τους μηχανισμούς για να επιτρέψουν την καλύτερη συνύπαρξη με IEEE 802.11b™ κατηγορίες συσκευών.
802.15.2	Coexistence of Wireless Personal Area Networks with Other Wireless Devices Operating in Unlicensed Frequency Bands	Προτείνει τροποποιήσεις σε άλλα 802.15 πρότυπα και αναπτύσσει συνιστώμενες πρακτικές για συνύπαρξη 802.15 WPAN με άλλες επιλεγμένες ασύρματες συσκευές που λειτουργούν στις μη απαιτούμενης άδειας ζώνες συχνοτήτων. Διευκολύνει την συνύπαρξη 802.11 με 802.15 συσκευών που λειτουργούν στις μη απαιτούμενης άδειας ζώνες συχνοτήτων.
802.15.3 3b/3c	Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPANs)	Καθορίζονται οι PHY και MAC προδιαγραφές για υψηλό ρυθμό δεδομένων ασύρματης συνδεσιμότητας με σταθερές, φορητές και κινητές συσκευές κατά τη διάρκεια εισόδου ή μέσα σε ένα προσωπικό χώρο λειτουργίας. Πετυχαίνεται ένα επίπεδο διαλειτουργικότητας και συνύπαρξης με άλλα πρότυπα 802.15 και ασύρματες συσκευές.
802.15.4	Low-Rate WPAN	Ασχολείται με χαμηλού ρυθμού μετάδοσης δεδομένων αλλά μεγάλη διάρκεια ζωής της μπαταρίας που μπορεί να είναι μήνες ή χρόνια, καθώς και χαμηλή πολυπλοκότητα.
802.15.5	Mesh Topology Capability in Wireless Personal Area Networks (WPANs)	Αρχιτεκτονικό πλαίσιο που επιτρέπει σε συσκευές WPAN να προάγουν διαλειτουργικές, σταθερές, και εξελικτικές ασύρματες τοπολογίες πλέγματος (mesh) και, εάν χρειαστεί, να παρέχουν το κείμενο τροποποιήσεων στα τρέχοντα πρότυπα WPAN το οποίο απαιτείται για να εφαρμοστεί αυτή η συνιστώμενη πρακτική.
802.15.7	Short-Range Wireless Optical Communication Using Visible Light	Σφαιρικό πρότυπο για περιορισμένου φάσματος οπτικές ασύρματες επικοινωνία χρησιμοποιώντας το ορατό φώς. Πρόσβαση σε αρκετά THz από το μη απαιτούμενης άδειας φάσμα, ανεκτικότητα στις ηλεκτρομαγνητικές παρεμβολές, μη παρεμβολή με τα συστήματα ραδιοσυχνότητας (RF), πρόσθετη ασφάλεια με την άδεια του χρήστη

IEEE 802.15 WPAN		
		για να δει το κανάλι επικοινωνίας, αύξηση επικοινωνίας, συμπλήρωση των υπαρχουσών υπηρεσιών από τις υποδομές ορατού φωτός.

Πίνακας 1 Τα υποπρότυπα της οικογένειας IEEE 802.15.

Βασικές Τεχνολογίες WPAN

HomeRF:

Το πρότυπο αυτό ξεκίνησε το 1997 με μια ομάδα από εταιρείες, την HomeRF. Στόχος αυτής της ομάδας είναι να συνδυάσει ασύρματη δικτύωση φωνής και δεδομένων, διευρύνοντας την χρήση των WLANs μέσα στο σπίτι. Γι' αυτόν τον λόγο έχει αναπτύξει ένα νέο πρωτόκολλο με το όνομα SWAP (*Shared Wireless Access Protocol*).

Το SWAP επιτρέπει σε PCs, περιφερειακά, ασύρματα τηλέφωνα και άλλες συσκευές να επικοινωνούν ασύρματα για μετάδοση φωνής και δεδομένων. Χρησιμοποιεί το πρωτόκολλο CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) στο υπόστρωμα MAC, το οποίο συνδυάζει χαρακτηριστικά και λειτουργίες από το DECT (ένα πρότυπο της ETSI για ψηφιακά ασύρματα τηλέφωνα) και το 802.11 με μια επέκταση στην κίνηση φωνής. Το σύστημα SWAP μπορεί να λειτουργήσει είτε ως ad-hoc είτε ως infrastructure κάτω από τον έλεγχο ενός σημείου σύνδεσης. Σε ένα ad-hoc δίκτυο, όλοι οι σταθμοί είναι peers (όμοιοι), και ο έλεγχος διανέμεται μεταξύ των σταθμών και υποστηρίζει μόνο δεδομένα. Σε ένα δίκτυο infrastructure , απαιτείται ένα σημείο σύνδεσης έτσι ώστε να συντονίζει το σύστημα και παρέχει την πύλη (*gateway*) στο δημόσιο switched τηλεφωνικό δίκτυο (*PSTN*). Οι τοίχοι και τα πατώματα δεν προκαλούν προβλήματα στην λειτουργία του και παρέχεται ασφάλεια μέσω μοναδικών IDs δικτύου. Είναι γερό και αξιόπιστο, και ελαχιστοποιεί τον αντίκτυπο της ραδιοπαρεμβολής.

Η έκδοση 1.0 (1999) προσφέρει 4 συνδέσεις φωνής των 32 Kbps ρυθμού μετάδοσης μέχρι 1.6 Mbps χρησιμοποιώντας 2 *frequency-shift keying* (2FSK) διαμόρφωση και εμβέλεια 50 μέτρα. Η έκδοση 2.0 (2001) λειτουργεί με 8 κανάλια και ταχύτητες μετάδοσης μέχρι 10 Mbps χρησιμοποιώντας 4 FSK διαμόρφωση στην περιοχή συχνοτήτων 2.4GHz της ISM με τεχνική FHSS (50 hops per second), κατάλληλο για μετάδοση μουσικής, ήχου και βίντεο. Υποστηρίζει *Time Division Multiple Access* (TDMA) υπηρεσία για να παρέχει παράδοση διαδραστικής φωνής και CSMA/CA υπηρεσία για παράδοση υψηλής ταχύτητας πακέτων. Η ισχύς μετάδοσης είναι 100mW. Το δίκτυο είναι ικανό να υποστηρίζει μέχρι και 127 κόμβους.

Ωστόσο το Bluetooth υποστηρίζεται περισσότερο από τις βιομηχανίες απ' ότι το HomeRF. Το 1999 το IEEE αποφάσισε να συνεισφέρει στην τυποποίηση των WPANs με το σχηματισμό της ομάδας εργασίας 802.15. Επειδή τα πρότυπα Bluetooth και HomeRF προηγήθηκαν της πρωτοβουλίας του IEEE ένας στόχος της ομάδας 802.15 είναι να πετύχει την διαλειτουργικότητα αυτών των προτύπων στο φυσικό επίπεδο και στο επίπεδο πρόσβασης εμφανίζοντας μικρή πολυπλοκότητα και χαμηλή κατανάλωση ενέργειας.

Bluetooth (IEEE 802.15.1):

Αναπτύχθηκε από την ομάδα Bluetooth Special Interest Group (SIG). Το Bluetooth είναι μία εναλλακτική τεχνολογία ασύρματης σύνδεσης, και επικοινωνίας συσκευών μικρού μεγέθους όπως laptops, κινητά τηλέφωνα, ψηφιακές κάμερες, *personal digital assistants* (PDAs) με ελάχιστη έως καθόλου απαιτούμενη εργασία από τους χρήστες.

Η τεχνολογία αυτή χαρακτηρίζεται από υψηλή ταχύτητα, χαμηλή κατανάλωση ενέργειας και χαμηλό κόστος. Δεν απαιτείται οπτική επαφή (*line-of-sight*) των συμμετεχόντων συσκευών όπως απαιτούν οι υπέρυθρες. Αρκεί να βρεθούν οι Bluetooth-ενεργοποιημένες συσκευές εντός εμβέλειας για να ανταλλάξουν διευθύνσεις και εγκαθιστούν μικρά δίκτυα μεταξύ τους (*piconets*). Μπορεί να υποστηρίξει μέχρι οχτώ συσκευές (1 master, 7 slaves) εντός αυτού του μικρού δικτύου. Για την διασύνδεση των συσκευών και την μεταφορά πακέτων στο ασύρματο μέσο χρησιμοποιείται το κανάλι ραδιοεπικοινωνίας. Το κανάλι αυτό λειτουργεί στην περιοχή συχνοτήτων ISM των 2.4 GHz (δεν απαιτείται κάποια άδεια χρήσης) και χρησιμοποιεί διαμόρφωση διασποράς φάσματος μεταπήδησης συχνότητας

(*Frequency Hopping Spread Spectrum*, FHSS). Υποστηρίζει κανάλια φωνής των 64 Kbps και ασύγχρονα κανάλια δεδομένων με ταχύτητες που κυμαίνονται μέχρι 721 Kbps. Οι εμβέλειες που υποστηρίζουν είναι 10 μέτρα με ισχύ μετάδοσης 1mW και 100 μέτρα με ισχύ μετάδοσης 10 mW.
Το μειονέκτημα του Bluetooth είναι ότι παρουσιάζει παρεμβολές με WLANs που χρησιμοποιούν το πρωτόκολλο 802.11 καθώς και τα δύο χρησιμοποιούν την ίδια ραδιοσυχνότητα αλλά το πρώτο χρησιμοποιεί πολύ μικρότερη ισχύ και διαφορετικούς τρόπους πολυπλεξίας του σήματος. Στο θέμα ασφάλειας της επικοινωνίας χρησιμοποιούνται κρυπτογραφικές μέθοδοι και δυναμική δημιουργία κλειδιών για την προστασία των δεδομένων που διακινούνται. Οι εκδόσεις που υπάρχουν σήμερα είναι η 1.2 με ρυθμό μετάδοσης 1 Mbit/sec και η 2.0 με ρυθμό μετάδοσης 3 Mbit/sec.

Zigbee (IEEE 802.15.4 LR-WPAN):
Ονομάζεται έτσι από τον χορό που κάνουν οι μέλισσες όταν θέλουν να επικοινωνήσουν με τις άλλες μέλισσες της αποικίας για να τις πληροφορήσουν για τις καινούριες πηγές τροφής που βρήκαν. Είναι πιο απλή και φτηνή τεχνολογία σε σύγκριση με το Bluetooth. Το πεδίο εφαρμογής αυτού του προτύπου είναι η ραδιοεπικοινωνία συσκευών. Όπως και το Bluetooth, χαρακτηρίζεται από χαμηλή ισχύ και μικρό κόστος αλλά οι συσκευές απαιτούν το 50% του κώδικα απ' ότι οι συσκευές Bluetooth γεγονός που εξοικονομεί χώρο στην μνήμη. Παρέχει επίσης ευκολία στη εγκατάσταση και αξιόπιστη μεταφορά δεδομένων. Οι συχνότητες που χρησιμοποιεί είναι οι ίδιες με του Bluetooth.

<u>Εφαρμογές WPANs</u>

Διασύνδεση συστήματος:
Η διασύνδεση συστήματος αναφέρεται στην διασύνδεση των εξαρτημάτων ενός υπολογιστή όπως ποντίκια πληκτρολόγια χειριστήρια παιχνιδιών, με την χρήση ραδιοκυμάτων μικρής εμβέλειας, χωρίς να χρειάζονται ούτε καλώδια ούτε εγκατάσταση προγραμμάτων οδήγησης. Κλασσικό παράδειγμα αποτελεί το Bluetooth το οποίο επιτρέπει σε ψηφιακές κάμερες, εκτυπωτές, σαρωτές και άλλες συσκευές να συνδεθούν με έναν υπολογιστή απλώς και μόνο με την τοποθέτησή τους εντός της εμβέλειας του δικτύου. Στην απλούστερη μορφή τους τα δίκτυα διασύνδεσης συστήματος χρησιμοποιούν το μοντέλο *master-slave*. Η κεντρική μονάδα του συστήματος είναι συνήθως ο κύριος ο οποίος αναφέρεται στο εξάρτημα σαν υπηρέτη. Ο κύριος λέει στους υπηρέτες ποιές διευθύνσεις να χρησιμοποιούν, πότε μπορούν να εκπέμπουν, για πόσο χρόνο μπορούν να μεταδίδουν, ποιες συχνότητες μπορούν να χρησιμοποιούν.

Συγχρονισμός προσωπικών συσκευών: αυτόματος συγχρονισμός δεδομένων μεταξύ ασύρματων φορητών συσκευών οι οποίες εκτελούν παρόμοιες εφαρμογές.

Αδόμητη συνδεσιμότητα: μεταφορά αρχείων και άλλων πληροφοριών προς τη συσκευή PAN ενός άλλου χρήστη.

Πρόσβαση στο διαδίκτυο: λήψη email ή περιήγηση σε ιστοσελίδες.

Ασύρματος συγχρονισμός: Συγχρονισμός φορητών συσκευών με σταθερούς κεντρικούς υπολογιστές μέσω σημείων πρόσβασης για δίκτυα PAN.

Ασύρματη τηλεφωνία/ακουστικά: Ο χρήστης επιλέγει ένα όνομα επαφής από τη φορητή του συσκευή, η συσκευή αναζητά ασύρματα από κοντινό της κινητό τηλέφωνο να σχηματίσει τον αριθμό και ο ήχος από την κλήση διαβιβάζεται ασύρματα στα ακουστικά του χρήστη.

Αυτοματοποιημένο σπίτι: απρόσκοπτη μεταφορά εντολών στις οικιακές συσκευές PAN. Αυτόματο κλείδωμα της πόρτας κατά την άφιξη του χρήστη στο σπίτι του.

Ηλεκτρονικές αγορές/κρατήσεις: Οι συσκευές PAN είναι δυνατό να χρησιμοποιηθούν για την ηλεκτρονική κράτηση εισιτηρίων. Αποφεύγοντας τις μεγάλες ουρές ο χρήστης μπορεί να κάνει αίτηση για εισιτήριο όταν βρεθεί στο χώρο.

Κατάσταση έκτακτης ανάγκης: ιατρικές συσκευές με διασύνδεση PAN είναι δυνατό να χρησιμοποιηθούν για να αυξηθεί η ασφάλεια των ασθενών. Βηματοδότες που προγραμματίζονται ή ελέγχονται από μακριά μέσω διασύνδεσης PAN για να καλούν αμέσως ασθενοφόρο.

1.3.1.3 802.16 Worldwide Interoperability for Microwave Access (WiMAX) - Ασύρματα μητροπολιτικά δίκτυα (WMAN) Wireless MAN

Το WiMax είναι μια νέα τεχνολογία που έκανε την εμφάνισή της το 2001 και περιγράφεται από την οικογένεια προτύπων IEEE 802.16 τα οποία στοχεύουν στην ανάπτυξη της σταθερής ασύρματης ευρυζωνικής πρόσβασης καλύπτοντας τις ανάγκες επικοινωνίας στα ασύρματα μητροπολιτικά δίκτυα (*Wireless Metropolitan Area Networks*, WMANs). Τα δίκτυα αυτά διακρίνονται για τη αυξημένη ταχύτητα μετάδοσης δεδομένων (30 Mbps+) καθώς και για τη μεγάλη εμβέλεια (περίπου έως 50 Km) με δυνατότητες κάλυψης μεγάλων περιοχών όπως μια πόλη ή γραφεία μιας επιχείρησης σε γειτονικές πόλεις ή για την διασύνδεση διαφορετικών WLANs. Έχουν μεγαλύτερη εμβέλεια από τα WLANs και μικρότερη από τα WWANs (*Wireless Wide Area Networks*). Το πρότυπο αρχικά σχεδιάστηκε να λειτουργεί σε συχνότητες από 10 έως 66GHz αλλά στις πρόσφατες εκδόσεις του λειτουργεί από 2 έως 11 GHz.
Οι συνδέσεις είναι από σημείο-σε-σημείο (point-to-point) αλλά και από σημείο σε πολλά σημεία (point-to-multipoint,) είτε κυψελοειδείς όπως στα δίκτυα κινητής τηλεφωνίας. Το σήμα διαμορφώνεται συνήθως με ορθογωνική πολυπλεξία διαίρεσης συχνότητας OFDM, η οποία επιτρέπει μεγάλες ταχύτητες, και το διαθέσιμο εύρος ζώνης διαχωρίζεται με αμφίδρομη διαίρεση χρόνου (*Time Division Duplexing*) ή αμφίδρομη διαίρεση συχνότητας (*Frequency Division Duplexing*).
Για την ασύρματη διασύνδεση δύο απομακρυσμένων σημείων θα πρέπει πιθανώς να χρησιμοποιηθεί μια κατευθυντική κεραία υψηλής ισχύος ως σταθμός βάσης ώστε το σήμα να μην εξασθενεί και να μπορέσει να εστιάσει την ισχύ του στην απέναντι κεραία. Η οικογένεια προτύπων 802.11x μπορεί να χρησιμοποιηθεί σε ασύρματα μητροπολιτικά δίκτυα αρκεί να υπάρχει οπτική επαφή στην νοητή ευθεία ανάμεσα από τα σημεία που διασυνδέονται με χρήση κατάλληλων κεραιών και γεννητριών σήματος.
Ένα WMAN συνήθως ανήκει σε μια μοναδική οντότητα, όπως ένας πάροχος υπηρεσίας Internet (*Internet Service Provider*, ISP), κυβέρνηση, ή μεγάλος οργανισμός χρησιμοποιώντας την τεχνολογία WiMax για την συνδεσιμότητα "τελευταίου μιλίου" (*last-mile connectivity*)[1]. Η πρόσβαση σε ένα WMAN περιορίζεται σε εξουσιοδοτημένους συνδρομητές χρήστες και τα προϊόντα WiMax είναι μέχρι στιγμής ακριβότερα από τα Wi-Fi.
Τέλος αξίζει να αναφέρουμε ότι εκτός από το WiMax έχουν αναπτυχθεί και άλλα παρόμοια πρότυπα τα οποία είτε απορρίφθηκαν από την αγορά είτε ξεπεράστηκαν στην πορεία εξέλιξης των ασύρματων δικτύων. Παραδείγματα αυτών είναι το ευρωπαϊκό πρότυπο *HIPERACCESS* που αναπτύχθηκε από την επιτροπή προτυποποίησης ευρυζωνικών δικτύων ραδιοπρόσβασης (*Broadband Radio Access Networks*, BRAN), *WaveLAN* , το *FreePort* κ.α..

[1]Μια φράση που χρησιμοποιείται στις βιομηχανίες τηλεπικοινωνιών και τεχνολογίας για να περιγράψει τις τεχνολογίες και τις διαδικασίες που χρησιμοποιούνται για να συνδέσουν τον τελικό πελάτη με ένα δίκτυο του προμηθευτή επικοινωνιών (ISP).

IEEE 802.16		
IEEE Std 802.16-2009 (Revision of IEEE Std 802.16-2004)	Part 16: Air Interface for Broadband Wireless Access Systems	Διευκρινίζει τη διεπαφή αέρα, MAC και PHY στρώματος, συνδυάζοντας σταθερά και κινητά point-to-multipoint ευρυζωνικά ασύρματα συστήματα πρόσβασης (BWA) για παροχή πολλαπλάσιων υπηρεσιών. Το MAC στρώμα είναι δομημένο να υποστηρίξει τις πολλαπλές PHY προδιαγραφές, κάθε μια να ταιριάζει με κάθε ιδιαίτερο λειτουργικό περιβάλλον.
IEEE Std 802.16.2-2004 (Revision of IEEE Std 802.16.2-2001)	Coexistence of Fixed Broadband Wireless Access Systems	Αναθεωρεί το πρότυπο IEEE 802.16.2™-2001. Διευκρινίζει τις επεκτάσεις και τροποποιήσεις που εξετάζουν τη συνύπαρξη μεταξύ των πολυσημειακών (MP) και σημείο-προς-σημείο (PTP) συστημάτων στο φάσμα συχνοτήτων 10-66 Ghz και τη συνύπαρξη μεταξύ των συστημάτων FBWA(Fixed Broadband Wireless Access) τα οποία λειτουργούν στις εξουσιοδοτημένες ζώνες μέσα στο φάσμα συχνοτήτων 2-11 Ghz.
IEEE Std 802.16/conformance 04-2006	IEEE Standard for Conformance to IEEE 802.16 - Part 4: Protocol Implementation Conformance Statement (PICS) Proforma for Frequencies below 11 GHz	Αντιπροσωπεύει την αίτηση δήλωσης προσαρμογής και υλοποίησης πρωτοκόλλου (Protocol Implementation Conformance Statement, ανά ISO/IEC 9646-7 και ITU-τ X.296, για τον προσδιορισμό της προσαρμογής των σταθμών βάσης και των σταθμών των συνδρομητών, βασισμένων στη διεπαφή αέρα, που διευκρινίζεται στο IEEE Std 802.16 για τις συχνότητες κάτω από 11 Ghz.
IEEE Std 802.16k-2007 (Amendment to IEEE 802.1D)	IEEE Standard for Media Access Control (MAC) Bridges Amendment 5: Bridging of IEEE 802.16	Τροποποιεί το πρότυπο IEEE 802.1D, όπως προηγουμένως τροποποιείται από το IEEE 802.17a™-2004, για να υποστηρίξει το γεφύρωμα του IEEE 802.16 Medium Access Control.
IEEE Std 802.16j-2009 (Amendment to IEEE Std 802.16-2009)	Part 16: Air Interface for Broadband Wireless Access Systems Amendment 1: Multihop Relay Specification	Ενημερώνει και επεκτείνει το πρότυπο IEEE 802.16, διευκρινίζοντας το OFDMA φυσικό στρώμα και εμπλουτισμούς στο MAC στρώμα για τις εξουσιοδοτημένες ζώνες για να επιτρέψει τη λειτουργία των σταθμών αναμετάδοσης. Οι προδιαγραφές συνδρομητικών σταθμών δεν αλλάζουν. Η σύγχρονη εφαρμόσιμη έκδοση του IEEE 802.16 είναι το IEEE 802.16-2009, όπως τροποποιείται από IEEE 802.16j-2009.

IEEE 802.16		
IEEE Std 802.16h-2010	IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems Amendment 2: Improved Coexistence Mechanisms for License-Exempt Operation	Διευκρινίζει τους βελτιωμένους μηχανισμούς, ως πολιτικές και εμπλουτισμούς στο MAC, για να επιτρέψουν τη συνύπαρξη μεταξύ των απαλλαγμένων άδειας συστημάτων βασισμένων στο IEEE 802.16 και για να διευκολύνουν τη συνύπαρξη τέτοιων συστημάτων με τους αρχικούς χρήστες.
IEEE Std 802.16m-2011	IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems Amendment 3: Advanced Air Interface	Διευκρινίζει τη WMAN-προηγμένη διεπαφή αέρα, μια ενισχυμένη διεπαφή αέρα που χαρακτηρίζεται ως «IMT-Advanced» από τη διεθνή ένωση τηλεπικοινωνιών, Τομέα της ραδιοεπικοινωνίας (ITU-R). Η τροποποίηση είναι βασισμένη στη wirelessMAN-OFDMA προδιαγραφή και παρέχει τη συνεχή υποστήριξη στους κληροδοτημένους σταθμούς συνδρομητών.

Πίνακας 2 Τα υποπρότυπα της οικογένειας IEEE 802.16.

<u>Επιπλέον πρότυπα που αντικαταστάθηκαν, συγχωνεύτηκαν ή αποσύρθηκαν</u>

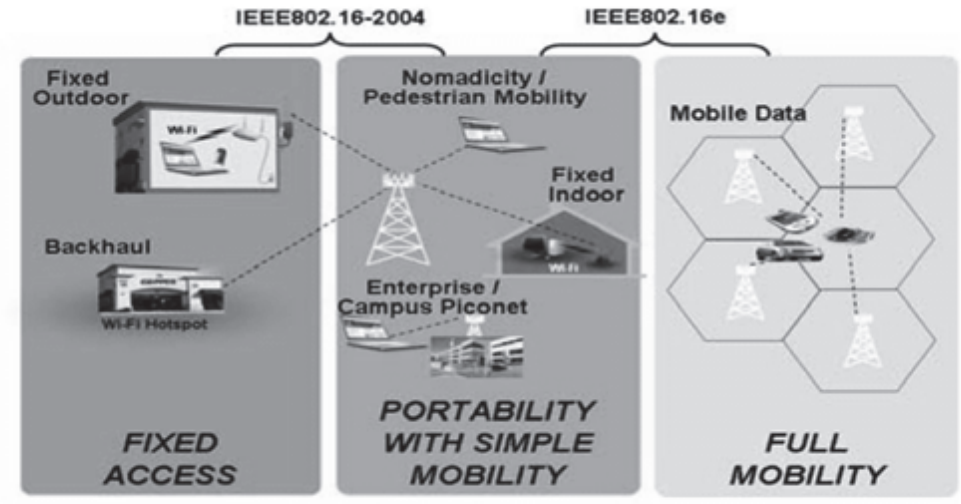
IEEE 802.16-2004
Προήλθε από συνένωση των προτύπων 802.16a, 802.16c, 802.16d. Προδιαγράφει την επικοινωνία των χρηστών οι οποίοι βρίσκονται μέσα σε μια κυψέλη (cell) και καλύπτονται από έναν σταθμό βάσης χωρίς οι χρήστες να έχουν την δυνατότητα να μετακινηθούν μεταξύ των κελιών. Λειτουργεί σε συχνότητες 2-66GHz και περιγράφει τα εξής επιμέρους υποπρότυπα:

- **IEEE 802.16a-2003**
  Physical layer and MAC definitions for 2–11 GHz
  Το υποπρότυπο IEEE 802.16 a επεκτάθηκε τον Ιανουάριο του 2003 προσφέροντας επικοινωνία μεταξύ σταθμών που δεν βρίσκονται σε οπτική επαφή. Λειτουργεί στις συχνότητες 2-11 GHz και ορίζει τρείς παραλλαγές φυσικού στρώματος (SC, 256 OFDM, 2048 OFDMA).
- **IEEE 802.11c**
  System profiles for 10–63 GHz
  Λειτουργεί, όπως και στην αρχική του έκδοση το πρότυπο IEEE 802.16, στην ζώνη συχνοτήτων 10-66 GHz. Η επίτευξη της επικοινωνίας πραγματοποιείται με οπτική επαφή των σταθμών.
- **IEEE 802.16d**
  Maintenance and System profiles for 2–11 GHz
  Το υποπρότυπο αυτό εξασφαλίζει ποιότητα υπηρεσίας στην επικοινωνία των ασύρματων δικτύων προκειμένου να διαχειριστεί την εκάστοτε πολυπλοκότητα και τις απαιτήσεις των εφαρμογών που διαδίδονται στα δίκτυα αυτά.

IEEE 802.16b
License-exempt frequencies
Δημιουργήθηκε με στόχο να λειτουργεί σε συχνότητες 5-6GHz εκτός νόμιμης (licensed) περιοχής, παρέχοντας ποιότητα υπηρεσίας καθώς εξασφαλίζει την προτεραιότητα σε εφαρμογές πραγματικού χρόνου και διαφορετικά επίπεδα υπηρεσίας σε άλλου είδους μετακίνηση δεδομένων.

IEEE 802.16-2004/Cor 1-2005
Corrections for fixed operations (co-published with 802.16e-2005)

- **IEEE 802.16 e**
  Mobile Broadband Wireless Access System
  Το υποπρότυπο IEEE 802.16e εγκρίθηκε το Δεκέμβριο του 2005 εισάγοντας και προδιαγράφοντας την κινητικότητα των χρηστών μεταξύ των κελιών, από έναν σταθμό βάσης σε άλλον χωρίς οπτική επαφή. Λειτουργεί στα 2-6 GHz και επιτρέπει την υψηλής ταχύτητας μεταπήδηση του σήματος μεταξύ των κελιών η οποία είναι απαραίτητη στην επικοινωνία των χρηστών που κινούνται με ταχύτητα οχήματος (περίπου 120 Km/h). [31][32][33][34]



Εικόνα 2 Το 802.16e εισάγει και προδιαγράφει την κινητικότητα των χρηστών μεταξύ των κελιών.

Εφαρμογές του WiMax

Όπως είδαμε η τεχνολογία WiMAX παρέχει κάλυψη μεγάλων αποστάσεων και ταυτόχρονα υψηλούς ρυθμούς μετάδοσης δεδομένων παρέχοντας έτσι πρακτική λύση σε προβλήματα που απασχολούν τις βιομηχανίες. Οι βασικές κατηγορίες εφαρμογών του WiMax χωρίζονται στις σταθερές εφαρμογές, που αφορούν την ευρυζωνική πρόσβαση σε σπίτια και σε επιχειρήσεις, και στις κινητές εφαρμογές, που αφορούν την πλήρη κινητικότητα των κυψελοειδών δικτύων στις αληθινές ευρυζωνικές ταχύτητες.
Ειδικότερα θα μπορούσαμε να διακρίνουμε τις παρακάτω εφαρμογές της τεχνολογίας WiMax:

- **Κυψελοειδής μετάδοση (*backhaul*)**
  Μπορεί να χρησιμοποιηθεί ως δίκτυο κορμού (*backbone*) στα κυψελωτά συστήματα κινητής τηλεφωνίας. Η τεχνολογία αυτή αποτελεί οικονομικότερη λύση για τις εταιρείες κινητής τηλεφωνίας όσον αφορά τα υλικά μέσα μετάδοσης συγκριτικά με τα υπάρχοντα δίκτυα κινητής τηλεφωνίας. Επίσης, δίνει την δυνατότητα στις εταιρείες παροχής υπηρεσιών Internet (ISP) να χρησιμοποιούν ασύρματες κυψέλες για να παρέχουν Internet στους χρήστες αποφεύγοντας έτσι την μίσθωση ενσύρματων γραμμών, εξασφαλίζοντας ταυτόχρονα αξιοπιστία και υψηλούς ρυθμούς μετάδοσης που απαιτούν τα συστήματα αυτά.
- **Broadband on Demand.**
  Χρήση της τεχνολογίας WiMax για εφαρμογές πραγματικού χρόνου (*real-time*) εξασφαλίζοντας ταχύτατους ρυθμούς μετάδοσης και καλύπτοντας μεγάλες αποστάσεις.

- **Άρση των περιορισμών των καλωδίων**
  Τα καλώδια, είτε αυτά είναι χαλκός είτε οπτική ίνα, συνεπάγονται περιορισμούς που εμποδίζουν τους πελάτες να συνδεθούν με το δίκτυο. Τέτοιοι περιορισμοί μπορεί να αφορούν
  - ✓ απομακρυσμένες περιοχές με λίγους χρήστες (όπως δυσπρόσιτα νησιά με λίγους κατοίκους) στα οποία η εγκατάσταση καλωδίων είναι δύσκολη και ζημιοφόρα
  - ✓ DSL συνδέσεις, οι οποίες έχουν μέγιστη απόσταση από τον κεντρικό δρομολογητή 3 μίλια με αποτέλεσμα να μην μπορούν να εξυπηρετήσουν προαστιακές
  - ✓ πολλά παλιά ενσύρματα δίκτυα τα οποία δεν έχουν κανάλι επιστροφής και η αναβάθμιση τους να είναι πολυδάπανη.
- **Επέκταση της ασύρματης ευρυζωνικότητας**
  Το WiMax προσφέρει εύκολη και ευέλικτη επεκτασιμότητα ταυτόχρονα με συμβατότητα και προσαρμοστικότητα με τα άλλα υπάρχοντα δίκτυα όπως τα 802.11 WLANs τα οποία μπορούν να γίνουν σταθμοί για ένα 802.16 WMAN. Το γεγονός αυτό εξυπηρετεί πολύ τις επιχειρήσεις αλλά και τους ιδιώτες χρήστες που επιθυμούν να έχουν πρόσβαση στο δίκτυο και στο Internet από οποιαδήποτε περιοχή χωρίς την ανάγκη για ενσύρματη υποδομή. Επιπλέον δίνεται το πλεονέκτημα διαμόρφωσης της σύνδεσης σε πιο αργή ή πιο γρήγορη χωρίς καμία επιπλέον εγκατάσταση.

1.4 Πλεονεκτήματα και μειονεκτήματα της χρήσης ασύρματων δικτύων

Αν και τα ενσύρματα δίκτυα έχουν προσφέρει αδιαμφισβήτητα πολλά πλεονεκτήματα, η απεξάρτηση από την Ethernet καλωδίωση έδωσε νέα ώθηση στους χρήστες και στις εφαρμογές τους.
Οι χρήστες έχουν τη δυνατότητα να χρησιμοποιούν τις δικτυακές εφαρμογές οπουδήποτε κι αν βρίσκονται αρκεί να μετακινούνται εντός της εμβέλειας του ασύρματου δικτύου. Σε αυτό συνέβαλε η τεχνολογική ανάπτυξη των φορητών συσκευών και των σταθμών πρόσβασης οι οποίοι μπορούν να προσφέρουν επαρκές και δυνατό σήμα έτσι ώστε οι χρήστες να διατηρούν την σύνδεσή τους και σε υψηλές ταχύτητες. Η κινητικότητα με την σειρά της έχει επιφέρει αλλαγές στον τρόπο εργασίας αφού οι εργαζόμενοι μπορούν να μετακινούνται μέσα στον εργασιακό τους χώρο και να εργάζονται με τις φορητές τους συσκευές ανάλογα με τις απαιτήσεις που υπάρχουν, αυξάνοντας έτσι την παραγωγικότητα. Σημαντική είναι η προσφορά της κινητικότητας και σε εφαρμογές πραγματικού χρόνου όπως η χρήση RFID με το οποίο ένα προϊόν που διαθέτει RFID tag σαρώνεται από έναν εργαζόμενο σε μια γραμμή παραγωγής και περνάει αυτόματα στην βάση δεδομένων του κεντρικού υπολογιστή της επιχείρησης για περεταίρω επεξεργασία.
Η εγκατάσταση των ασύρματων δικτύων είναι σχετικά απλή και απαιτεί ελάχιστη ως καθόλου τεχνική γνώση των χρηστών. Εφόσον οι φορητές συσκευές διαθέτουν τον κατάλληλο εξοπλισμό, μπορούν να συνδεθούν στο ασύρματο δίκτυο μέσω ενός σημείου πρόσβασης αρκεί να βρεθούν εντός της εμβέλειάς του. Με αυτόν τον τρόπο μπορούν να προστίθενται στο δίκτυο όλο και περισσότεροι χρήστες και να χρησιμοποιήσουν τις εφαρμογές και τις υπηρεσίες που αυτό προσφέρει διαμορφώνοντας διαφορετικές τοπολογίες δικτύου. Η εύκολη και γρήγορη εγκατάσταση των ασύρματων δικτύων έχει "λύσει τα χέρια" σε πολλές επιχειρήσεις που θέλουν να διασυνδέσουν τα απομακρυσμένα γραφεία τους ή να προσφέρουν επιπλέον υπηρεσίες στους πελάτες τους, όπως τα "hotspots"[2], και δεν θέλουν να χρησιμοποιήσουν καλώδια λόγω χρόνου, κόστους ή αδύνατης εγκατάστασης (για παράδειγμα παλαιά κτίρια) ή, σε εξαιρετικές περιπτώσεις, για να διατηρήσουν την καλαισθησία του χώρου.
Όσον αφορά το θέμα κόστους, τα ασύρματα δίκτυα έχουν από χαμηλό μέχρι υψηλό κόστος εγκατάστασης αναφορικά με την αγορά του εξοπλισμού, κυρίως αν αναφερόμαστε σε περιπτώσεις που χρειάζεται να καλύψουμε ασύρματα πολύ μεγάλες περιοχές.

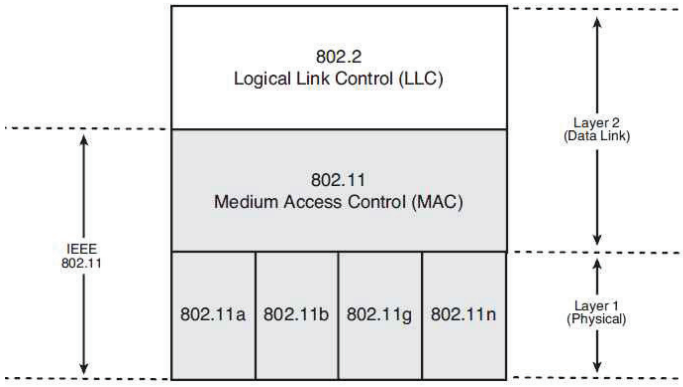
[2]Ο όρος **hotspot** αναφέρεται σε χώρους όπου υπάρχει ασύρματο δίκτυο (WLAN) το οποίο οργανώνεται από μια επιχείρηση ή ιδιώτη και παρέχει μια περιοχή κάλυψης σε ανθρώπους που επιθυμούν να συνδεθούν στο Internet ή σε ένα κοινοτικό δίκτυο.

Μακροπρόθεσμα όμως αποδεικνύονται αρκετά οικονομική λύση γιατί η υλοποίησή, η συντήρηση, η διαχείριση απαιτούν ελάχιστο κόστος συγκριτικά με τα ενσύρματα δίκτυα. Επιπλέον λόγω του ανταγωνισμού των κατασκευαστών, οι φορητές συσκευές που εμφανίζονται στην αγορά τείνουν να γίνονται οικονομικότερες και ποιοτικότερες με περισσότερες δυνατότητες.
Τέλος, τα ασύρματα δίκτυα διαθέτουν ευελιξία και συμβατότητα. Εμφανίζουν προσαρμοστικότητα στις εκάστοτε απαιτήσεις και αλλαγές του δικτύου και μπορούν να συνυπάρχουν και να επικοινωνούν με άλλου είδους δίκτυα ακόμα και να χρησιμοποιούνται σαν επέκταση ενός υπάρχοντος ενσύρματου δικτύου.
Όπως σε κάθε τεχνολογία εκτός, από τα πλεονεκτήματα υπάρχουν και τα μειονεκτήματα που αφορούν το φυσικό μέσο μετάδοσης των ασύρματων δικτύων.
Συγκριτικά με τα ενσύρματα δίκτυα, τα ασύρματα μειονεκτούν σε θέματα ταχύτητας, ασφάλειας και αξιοπιστίας. Επειδή δεν χρησιμοποιούνται καλώδια, δεν υπάρχει φυσικός περιορισμός των δεδομένων. Τα ραδιοκύματα και οι υπέρυθρες, που χρησιμοποιούνται για την μεταφορά των δεδομένων στα ασύρματα δίκτυα, είναι ευάλωτα σε παρεμβολές καθιστώντας προβλήματα στην επικοινωνία. Οποιοσδήποτε διαθέτει μια καλή κεραία μπορεί να λάβει ανεξέλεγκτα σήματα και να εισέλθει στο ασύρματο δίκτυο, να υποκλέψει πληροφορίες ή να επιτεθεί σε κάποιο σύστημα ακόμα και αν βρίσκεται σε πολύ μακρινή απόσταση. Γι’ αυτό πρέπει να λαμβάνονται πολιτικές ασφαλείας. Για την προστασία των WLANs χρησιμοποιήθηκαν αρχικά διάφορες μέθοδοι, όπως το WEP, η τεχνολογία WPA, το πρωτόκολλο IEEE 802.11i,οι οποίες έχουν μειώσει σημαντικά τους κινδύνους τέτοιων επιθέσεων. Επίσης, πολλά 802.11b και 802.11g δίκτυα ή το Bluetooth λειτουργούν στα 2.4 GHz χρησιμοποιώντας το ίδιο κανάλι, το οποίο οδηγεί σε συγκρούσεις στα κανάλια.

2 Οικογένεια Προτύπων IEEE 802.11

2.1 Γενικά

Από την δεκαετία του '90 έχει κυριαρχήσει το πρότυπο IEEE 802.11 για ασύρματα δίκτυα ή Wi-Fi hotspots. Από λογικής απόψεως, το πρότυπο 802.11 περιγράφει τις λειτουργίες που αφορούν τα δύο πρώτα επίπεδα του OSI μοντέλου. Το Layer 1, δηλαδή το φυσικό επίπεδο (*Physical layer,* PHY) και το Layer 2, δηλαδή το επίπεδο ζεύξης δεδομένων (*data link layer*). Συγκεκριμένα καθορίζει ένα κομμάτι του δεύτερου επιπέδου, το MAC (*medium access control*) υποεπίπεδο, το οποίο αλληλεπιδρά με το 802.2 επίπεδο ελέγχου λογικού συνδέσμου (*logical link control*, LLC). Η φιλοσοφία που ακολουθεί το πρότυπο 802.11 είναι η ύπαρξη ενός μόνο MAC που όμως υποστηρίζει περισσότερα του ενός φυσικά στρώματα. Υπάρχουν αρκετά 802.11 φυσικά επίπεδα όπως τα 802.11a, 802.11b 802.11g και 802.11n.
Η τεχνολογία 802.11 προσφέρει ευρυζωνική πρόσβαση σε χρήστες που διαθέτουν ασύρματο τερματικό εξοπλισμό (κατάλληλες κάρτες δικτύου - NICs). Πρόκειται λοιπόν κυρίως για τεχνολογία εσωτερικών χώρων (indoor) και πολλαπλής πρόσβασης (*point-to-multipoint*). Ένας σταθμός βάσης εκπέμπει στις συχνότητες 2,4 (*ISM band*) και 5 GHz (*UNII band*). Η δυνατότητα μετάδοσης εξαρτάται από το πρότυπο.
Η κύρια υπηρεσία του προτύπου αυτού είναι η μεταφορά των M-SDU (*MAC Service Data Unit*) μεταξύ ομότιμων στρωμάτων ζεύξης δεδομένων. Παράλληλα περιλαμβάνει βασικές υπηρεσίες όπως διασύνδεση με τα εξωτερικά δίκτυα, συσχέτιση ενός σταθμού με ένα σημείο πρόσβασης, επανασυσχέτιση ενός σταθμού σε περίπτωση μετακίνησης, τερματισμό της συσχέτισης, πιστοποίηση (*authentication*), ασφάλεια και διαχείριση ισχύος ενός τερματικού.

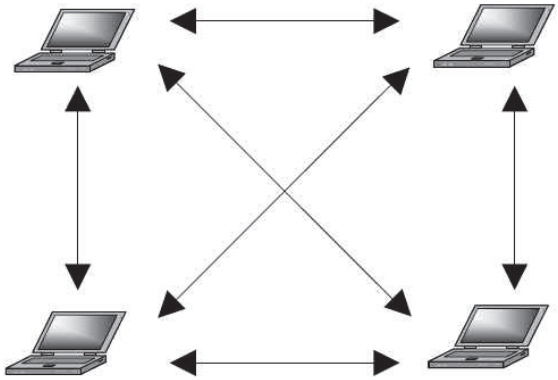


Εικόνα 3 Το 802.11 προσφέρει λειτουργίες φυσικού και MAC επιπέδου.

2.2 Αρχιτεκτονική και τοπολογίες του 802.11

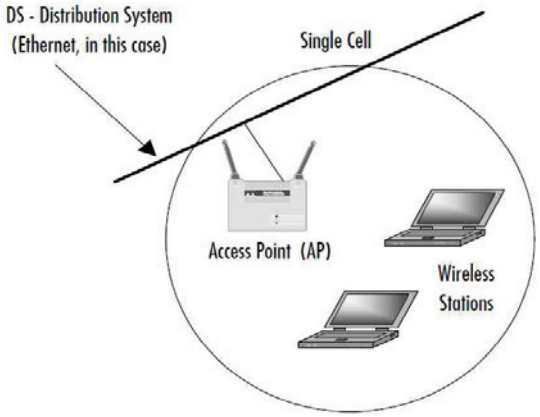
Τα ασύρματα δίκτυα επιτρέπουν σε ηλεκτρονικές συσκευές (από υπολογιστές μέχρι κινητά τηλέφωνα) να επικοινωνούν μεταξύ τους και να ανταλλάσσουν δεδομένα χωρίς την ύπαρξη καλωδίων, προϋποθέτοντας ή όχι την οπτική επαφή μεταξύ πομπού και δέκτη (ανάλογα με την υλοποίηση στο Layer 1 επίπεδο). Σε κάθε ασύρματο δίκτυο υπάρχουν δύο μέρη : η ασύρματη κάρτα δικτύου (*wireless LAN adapter*), η οποία επικοινωνεί είτε με άλλες συσκευές που έχουν ασύρματη κάρτα δικτύου, είτε με τον πομποδέκτη-κόμβο (*Access Point*) που λειτουργεί και ως γέφυρα με το ενσύρματο δίκτυο. Η κάρτα δικτύου μοιάζει με μια τυπική κάρτα δικτύου (ISA ή PCI διεπαφής για σταθερούς υπολογιστές, είτε PCMCIA για φορητούς) με μια μικρή κεραία, ενώ ο πομποδέκτης έχει τις διαστάσεις ενός βιβλίου και, εκτός από την κεραία, έχει και τις κατάλληλες διεπαφές για σύνδεση με το σταθερό δίκτυο. Όσον αφορά την ασφάλεια, τα πιο πολλά ασύρματα δίκτυα χρησιμοποιούν επίσης μεθόδους εξουσιοδότησης των συνδεόμενων και κρυπτογράφησης των δεδομένων. Αρκετά πρότυπα χρησιμοποιούν την τεχνική εναλλαγής συχνότητας

(*frequency hopping*) σύμφωνα με την οποία ο κάθε πομποδέκτης αλλάζει συχνότητα μετά την αποστολή / λήψη ενός πακέτου δεδομένων αποφεύγοντας έτσι τα παράσιτα.
Το πρότυπο IEEE 802.11 ορίζει δύο καταστάσεις λειτουργίας, την *ad hoc / IBSS* και *infrastructure*, οι οποίες υποστηρίζονται από την υλοποίηση του επιπέδου MAC.
Σε επίπεδο λογικής , ένας *ad hoc* σχηματισμός είναι ανάλογος με ένα δίκτυο *peer-to-peer* στο οποίο κανένας κόμβος δεν απαιτείται να λειτουργεί ως εξυπηρετητής (*server*). Η τοπολογία *IBSS* περιλαμβάνει έναν αριθμό κόμβων ή ασύρματων σταθμών οι οποίοι επικοινωνούν απευθείας με έναν άλλον σε *ad hoc*, *peer-to-peer* βάση, χτίζοντας μία *full-mesh* ή *partial-mesh* τοπολογία. Γενικά, οι ad hoc υλοποιήσεις καλύπτουν μια περιορισμένη περιοχή και δεν διαθέτουν διασύνδεση με εξωτερικά / ετερογενή δίκτυα.



Εικόνα 4 Ένα δίκτυο ad-hoc/IBSS.

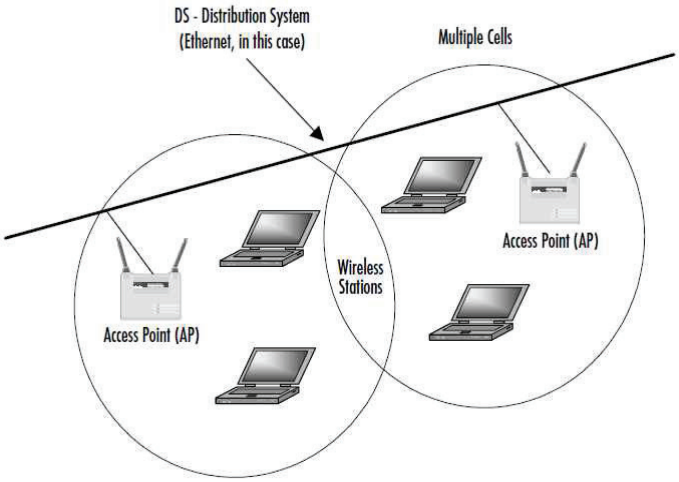
Στην κατάσταση *infrastructure*, το ασύρματο δίκτυο αποτελείται από τουλάχιστον ένα σταθμό πρόσβασης, ο οποίος συνδέεται σε μια υποδομή ενσύρματου δικτύου, και ένα σύνολο ασύρματων τελικών σταθμών. Η συγκεκριμένη τοπολογία καλείται *basic service set* (BSS). Δεδομένου ότι τα περισσότερα εταιρικά WLANs απαιτούν πρόσβαση στο ενσύρματο τοπικό LAN για υπηρεσίες (file servers, εκτυπωτές, και συνδέσεις Διαδικτύου), λειτουργούν στον τρόπο infrastructure και στηρίζονται σε ένα AP που ενεργεί ως λογικός server για ένα ενιαίο WLAN. Σε τέτοιου τύπου υλοποιήσεις, η επικοινωνία μεταξύ δύο κόμβων, Α και Β, πραγματοποιείται δια μέσου του AP, δηλαδή από τον κόμβο Α στο AP και έπειτα από το AP στον κόμβο Β. Το AP είναι απαραίτητο για τη γεφύρωση (bridging) και τη διασύνδεση πολλαπλών WLAN καθώς επίσης και να διασυνδέσει το ασύρματο με το ενσύρματο δίκτυο.



Εικόνα 5 BSS τοπολογία ασύρματου δικτύου.

Ένα *ESS* είναι ένα σύνολο δύο ή περισσότερου *BSSs* που διαμορφώνει ένα ενιαίο υποδίκτυο. Οι διαμορφώσεις ESS αποτελούνται από πολλαπλά BSS που μπορούν να συνδεθούν είτε με ενσύρματα είτε με ασύρματα δίκτυα κορμού. Το IEEE 802.11 υποστηρίζει τις διαμορφώσεις ESS στις οποίες τα πολλαπλά κύτταρα χρησιμοποιούν το ίδιο

κανάλι και χρησιμοποιούν διαφορετικά κανάλια για να ενισχύσουν τη συνολική ρυθμοαπόδοση.

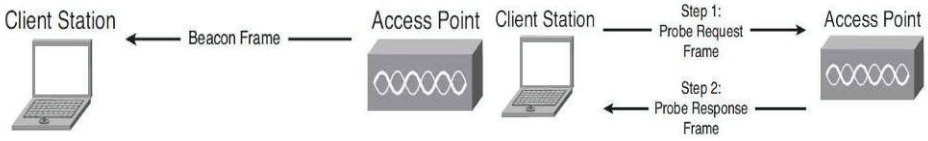


Εικόνα 6 ESS τοπολογία ασύρματου δικτύου.

2.3 Διασύνδεση

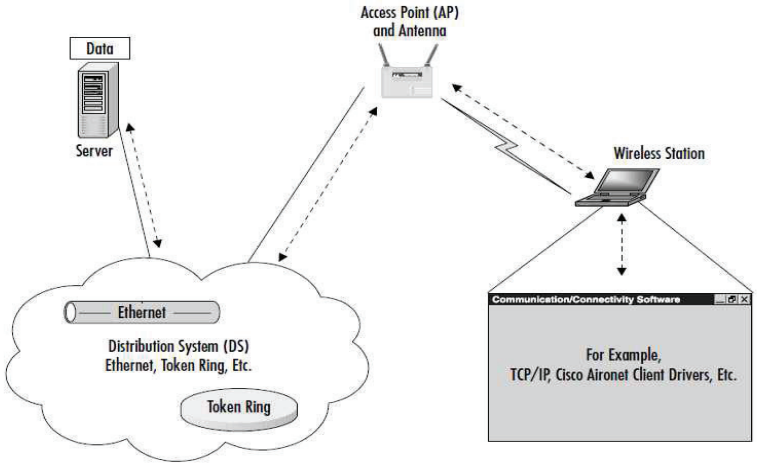
Στο 802.11 κάθε ασύρματος σταθμός πρέπει να συσχετιστεί με ένα σημείο πρόσβασης (*access point*, AP) προτού αρχίσει να μπορεί να στέλνει ή να δέχεται δεδομένα επιπέδου δικτύου. Ο διαχειριστής του δικτύου εγκαθιστά ένα AP και καταχωρεί σε αυτό ένα αναγνωριστικό συνόλου υπηρεσιών (*service set identifier*, SSID) μίας ή δύο λέξεων. Επιπλέον καταχωρεί και έναν αριθμό καναλιού.
Για να μπορέσει ένας φορητός υπολογιστής να αποκτήσει πρόσβαση στο Internet πρέπει να έχει μια κάρτα δικτύου η οποία στέλνει το δικό της ραδιοσήμα σε ένα ασύρματο δρομολογητή ο οποίος με την σειρά του συνδέεται στη πηγή παροχής Internet μέσω θύρας Ethernet, καλωδίου ή DSL modem και αναγνωρίζεται από τον φορητό υπολογιστή μόνο αν αυτός είναι εντός της εμβέλειάς του. Ο δρομολογητής μετατρέπει τα ψηφιακά σήματα σε υψηλής συχνότητας ραδιοσήματα.
Υπάρχει πολλές φορές το ενδεχόμενο της κατάστασης *Wi-Fi jungle*. Είναι μια φυσική τοποθεσία όπου ένας ασύρματος σταθμός δέχεται ένα αρκετά ισχυρό σήμα από δύο ή περισσότερα σημεία πρόσβασης που ανήκουν σε διαφορετικό υποδίκτυο και τους έχει εκχωρηθεί ανεξάρτητα ένα κανάλι. Για να συσχετιστεί (*associate*) ο ασύρματος σταθμός με ένα μόνο από αυτά, δημιουργεί ένα εικονικό κύκλωμα μεταξύ αυτού και του σημείου πρόσβασης. Έτσι το AP στέλνει πλαίσια δεδομένων στον ασύρματο σταθμό και ο σταθμός στέλνει πλαίσια προς το Διαδίκτυο μέσω του συσχετισμένου AP.
Το 802.11 πρότυπο απαιτεί ένα AP να στέλνει περιοδικά πλαίσια συγχρονισμού (*beacon frames*) το καθένα από τα οποία περιέχει το SSID και τη MAC διεύθυνση του AP. Ο ασύρματος σταθμός γνωρίζοντας ότι κάθε AP στέλνει πλαίσια σινιάλα, σαρώνει τα κανάλια ψάχνοντας για τέτοια πλαίσια από οποιοδήποτε AP βρίσκεται εκεί κοντά. Αφού μάθει ο σταθμός ποια είναι τα διαθέσιμα AP επιλέγει με ποιο από αυτά θα συσχετιστεί (ο χρήστης). Για την επιλογή αυτή δεν καθορίζεται αλγόριθμος αλλά αφήνεται στους σχεδιαστές του υλικού και λογισμικού της φορητής συσκευής και του 802.11 λογισμικού μέσα σε αυτή. Συνήθως συσχετίζεται με το AP του οποίου το beacon frame λαμβάνεται με την μεγαλύτερη ισχύ σήματος.
Η διεργασία σάρωσης των καναλιών και ακρόασης για beacon frames ονομάζεται παθητική σάρωση (*passive scanning*). Κατά το passive scanning ο σταθμός δεν εκπέμπει τίποτα, εξοικονομώντας έτσι ενέργεια. Ένας ασύρματος υπολογιστής μπορεί να κάνει επίσης ενεργή σάρωση (*active scanning*) εκπέμποντας περιοδικά σε όλα τα διαθέσιμα κανάλια *Probe Request* πλαίσια που περιέχουν και το SSID (ή network name) του δικτύου που ψάχνει. Για να εκπέμψει αυτό το πλαίσιο ο σταθμός πρέπει να αποκτήσει κανονικά πρόσβαση στο μέσο χρησιμοποιώντας τον αλγόριθμο DCF. Επίσης έχει προβλεφθεί κάποια διαδικασία ώστε να καταλαβαίνει ο σταθμός πότε ένα κανάλι είναι ανενεργό. Σε κάθε BSS

ένας σταθμός είναι υπεύθυνος για να απαντάει σε πλαίσια Probe Request. Σε infrastructure δίκτυα υπεύθυνο είναι το AP, ενώ σε IBSS υπεύθυνος είναι ο σταθμός που εξέπεμψε το τελευταίο πλαίσιο Beacon. Σε κάθε περίπτωση ο σταθμός που έστειλε το Probe Request θα λάβει ένα ή περισσότερα πλαίσια *Probe Response* αν υπάρχουν ασύρματα δίκτυα στην περιοχή του.



Εικόνα 7 Παθητική Σάρωση. **Εικόνα 8 Ενεργητική Σάρωση.**

Αφού επιλέξει με ποιο AP θα συνδεθεί, ο ασύρματος σταθμός στέλνει ένα πλαίσιο αίτησης συσχέτισης στο AP και το AP αποκρίνεται με ένα πλαίσιο απόκρισης συσχέτισης. Αφού συσχετιστεί με ένα AP ο ασύρματος σταθμός θα θέλει να συνδεθεί στο υποδίκτυο στο οποίο ανήκει το AP υπό την έννοια της διευθυνσιοδότησης IP. Στέλνει έτσι ένα μήνυμα ανακάλυψης DHCP στο υποδίκτυο, μέσω του AP ώστε να πάρει μια διεύθυνση στο υποδίκτυο. Στις περισσότερες περιπτώσεις για να δημιουργηθεί μια συσχέτιση με ένα συγκεκριμένο AP, η φορητή συσκευή απαιτείται να αυθεντικοποιηθεί στο AP. Το πρότυπο 802.11 παρέχει αρκετές εναλλακτικές μεθόδους για αυθεντικοποίηση και για πρόσβαση. Κάποιοι τρόποι αποδοχής της πρόσβασης μπορεί να είναι με βάση τη διεύθυνση MAC ενός σταθμού, ή με βάση το όνομα χρήστη και τον κωδικό πρόσβασης όπου το AP επικοινωνεί με έναν εξυπηρετητή αυθεντικοποίησης (*authentication server*) μεταφέροντας πληροφορίες ανάμεσα στον ασύρματο τερματικό σταθμό και στον εξυπηρετητή αυθεντικοποίησης χρησιμοποιώντας πρωτόκολλο όπως για παράδειγμα το RADIUS. Ένας τέτοιος εξυπηρετητής μπορεί να εξυπηρετεί πολλά AP κρατώντας χαμηλό το κόστος και την πολυπλοκότητα των AP.



Εικόνα 9 : Ένα ασύρματο δίκτυο με authentication server.

2.4 Κινητικότητα

Η κινητικότητα των ασύρματων σταθμών είναι ίσως το πιο σημαντικό χαρακτηριστικό των ασύρματων δικτύων. Το κύριο κίνητρο της ανάπτυξης ενός ασύρματου δικτύου είναι να επιτρέπει στους σταθμούς να μετακινούνται ελεύθερα από θέση σε θέση μέσα σε ένα συγκεκριμένο ασύρματο δίκτυο ή μεταξύ διαφορετικών τμημάτων ασύρματων δικτύων. Το κύριο πρόβλημα σε αυτές τις περιπτώσεις είναι το λεγόμενο *"handover"* το οποίο αναφέρεται στην διαδικασία αποσύνδεσης ενός ασύρματου χρήστη από ένα AP και στη σύνδεση με ένα άλλο. Κατά το handover ενός κινητού χρήστη, διακόπτονται οι οποιεσδήποτε ενεργές συνδέσεις του και όσα πακέτα φτάνουν στη συνέχεια στον προηγούμενο AP του χάνονται (η φυσική σύνδεση έχει κοπεί).

Για λόγους συμβατότητας, το 802.11 MAC πρέπει να εμφανίζεται στα ανώτερα στρώματα του δικτύου ως πρότυπο 802 LAN. Το 802.11 στρώμα MAC αναγκάζεται να χειριστεί την κινητικότητα των σταθμών με τρόπο ξεκάθαρο στα ανώτερα στρώματα της στοίβας 802 LAN. Είναι σημαντικό να εκτιμηθεί η διαφορά μεταξύ της αληθινής κινητικότητας και της απλώς φορητότητας. Η φορητότητα οδηγεί βεβαίως σε ένα καθαρό κέρδος παραγωγικότητας επειδή οι χρήστες μπορούν να έχουν πρόσβαση στις πηγές πληροφοριών οπουδήποτε είναι βολικό να γίνει. Στον πυρήνα, εντούτοις, η φορητότητα καταργεί μόνο τα φυσικά εμπόδια στη συνδεσιμότητα. Είναι εύκολο να μεταφερθεί ένα laptop μεταξύ διάφορων θέσεων, έτσι και οι άνθρωποι. Εντούτοις, η φορητότητα δεν αλλάζει το τελετουργικό της σύνδεσης με τα δίκτυα σε κάθε νέα θέση. Είναι ακόμα απαραίτητο να συνδεθεί φυσικά με το δίκτυο και να επανεγκατασταθούν οι συνδέσεις δικτύων, και οι συνδέσεις δικτύων δεν μπορούν να χρησιμοποιηθούν ενώ η συσκευή κινείται.
Η κινητικότητα καταργεί τα περαιτέρω εμπόδια, τα περισσότερα από τα οποία είναι βασισμένα στη λογική δικτυακή αρχιτεκτονική. Οι συνδέσεις δικτύων μένουν ενεργές ακόμη και ενώ η συσκευή είναι στην κίνηση. Αυτό είναι κρίσιμο για τους στόχους που απαιτούν οι επίμονες, μακρόβιες συνδέσεις, οι οποίες βρίσκονται στις εφαρμογές βάσεων δεδομένων.
Υπάρχουν δύο γενικά σενάρια κινητικότητας:

- Η περιπλάνηση (*roaming*) ενός κινητού σταθμού μεταξύ διαφορετικών BSS εντός των ορίων του ίδιου ESS (*Intra-Network Handover*), κατά το οποίο η IP παραμένει σταθερή. Εφ' όσον μένει ένας σταθμός στο ίδιο υποδίκτυο IP, μπορεί να κρατήσει τις συνδέσεις πρωτοκόλλου ελέγχου μετάδοσής (TCP) ανοικτές. Ο σταθμός για να συσχετιστεί στέλνει στο νέο AP ένα πλαίσιο *Reassociation Request*. Η μόνη διαφορά του πλαισίου αυτού από το πλαίσιο Association Request είναι ότι περιέχει τη διεύθυνση του προηγούμενου AP . Το νέο AP απαντάει με πλαίσιο *Reassociation Response*. Αν η διαδικασία ολοκληρωθεί χωρίς πρόβλημα το νέο AP πρέπει να επικοινωνήσει με το προηγούμενο AP και να του γνωστοποιήσει ότι ο ασύρματος σταθμός ανήκει πλέον στο δικό του BSS. Η επικοινωνία μεταξύ APs γίνεται μέσω ενός πρωτοκόλλου IAPP (*Inter Access Point Protocol*), γνωστό και σαν πρότυπο IEEE 802.11f. Η επικοινωνία αυτή γίνεται μέσω του ενσύρματου δικτύου (*Ethernet*) στο οποίο είναι συνδεδεμένα τα APs. Τελικά μετά το Reassociation το αρχικό AP στέλνει όσα αποθηκευμένα πλαίσια έχει και προορίζονται για τον ασύρματο σταθμό στο νέο AP και τερματίζει το association με τον σταθμό. Πλέον όλα τα πλαίσια από και προς τον σταθμό θα επεξεργάζονται από το νέο AP.
- Η περιπλάνηση ενός κινητού σταθμού μεταξύ BSS που ανήκουν σε διαφορετικά ESS (*Inter-Network Handover*) κατά την οποία η IP διεύθυνση ενός σταθμού μπορεί να αλλάξει κατά την αλλαγή AP και οι συνδέσεις χάνονται. Όσον αφορά το TCP/IP, απαιτείται το *Mobile IP* για να διατηρηθεί η ίδια IP διεύθυνση.

2.5 License-Free ασύρματες συχνότητες

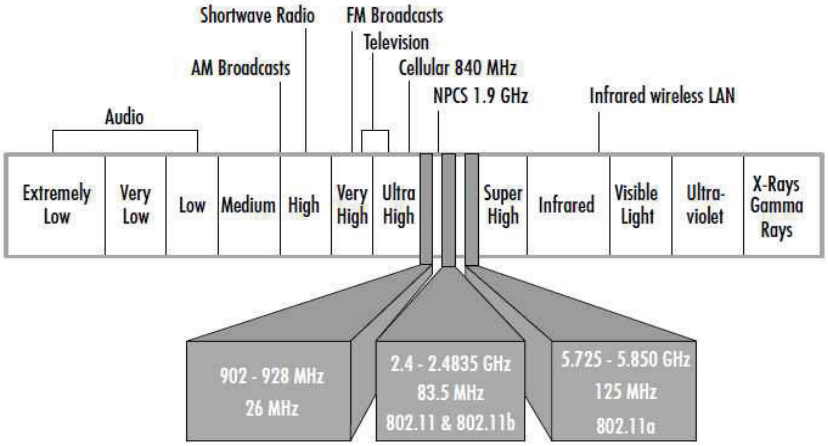
Το 1985, η Ομοσπονδιακή Επιτροπή Τηλεπικοινωνιών (Federal Communications Commission, FCC) ενέκρινε τη χρήση του ελεύθερου άδειας εξάπλωσης φάσματος ασύρματου εξοπλισμού στις ακόλουθες τρείς ISM μπάντες συχνοτήτων στις Ηνωμένες Πολιτείες:

900 έως 928 MHz (900 MHz εύρος)
2.4 έως 2.483 GHz (2.4 GHz εύρος)
5.725 έως 5.850 GHz (5 GHz εύρος)

Έπειτα, το 1997, η FCC ενέκρινε τη χρήση του ελεύθερου άδειας, χαμηλής ισχύος, χωρίς εξάπλωση φάσματος ασύρματου εξοπλισμού στις ακόλουθες τρεις ζώνες U-NII:

5.15 έως 5.25 GHz
5.25 έως 5.35 GHz

5.725 έως 5.825 GHz [46]



Εικόνα 10 ISM unlicensed ζώνες συχνοτήτων.

2.6 Το φυσικό στρώμα του 802.11

Το φυσικό επίπεδο ή στρώμα εξασφαλίζει την μετάδοση των bits μέσα από τα κανάλια επικοινωνίας. Αυτό περιλαμβάνει όλες τις απαραίτητες ενέργειες που απαιτούνται για να οριστεί ο φυσικός συνδυασμός των σημάτων που στέλνονται διαμέσου του ασύρματου δικτύου. Το φυσικό επίπεδο του 802.11 ορίζει τύπους διαμορφώσεων, συχνότητες και διαδικασίες συγχρονισμού των σημάτων και περιλαμβάνει διαφορετικές προδιαγραφές φυσικού επιπέδου. Όλα τα φυσικά επίπεδα μοιράζονται κοινές λειτουργίες του υποεπιπέδου MAC.
Όταν ένας υπολογιστής συνδέεται μέσω ενός δικτυακού καλωδίου σε ένα hub, switch ή router, προκειμένου να συνδεθεί με ένα δίκτυο ή στο Internet, η κάρτα διεπαφής δικτύου (*network interface card*, NIC) στέλνει μηδέν και ένα στο καλώδιο αλλάζοντας την τάση από 5 volts σε -5 volts, με προσχεδιασμένο ρυθμό. Το 802.11 δεν αλλάζει την τάση των καλωδίων αφού τα αντικαθιστά με μικρά, χαμηλής ενέργειας, ραδιοκύματα. Κωδικοποιεί τα δυαδικά μηδέν και ένα τοποθετώντας ένα εναλλασσόμενο ραδιοσήμα, πάνω από ένα σταθερό υπάρχον σήμα, με προκαθορισμένο ρυθμό.

2.6.1 PLCP και PMD

Η αρχιτεκτονική του 802.11 φυσικού επιπέδου αποτελείται από το physical layer *convergence procedure* (PLCP) υπόστρωμα και το *physical medium dependent* (PMD) υπόστρωμα. Το MAC στρώμα επικοινωνεί με το PLCP υπόστρωμα μέσω του *service access point* (SAP), όπως αναφέρεται στο πρότυπο. Μέσω του SAP το PLCP δέχεται μονάδες δεδομένων πρωτοκόλλου MAC (*MAC protocol data units*, MPDU) από το στρώμα MAC. Στο φυσικό επίπεδο, οι μονάδες MPDU ονομάζονται *PLCP service data units* (PSDU). Όταν το MAC επίπεδο δώσει οδηγίες, το PLCP ετοιμάζει ένα PSDU για μετάδοση προσαρτώντας πεδία γύρω από το PSDU. Οι πομποί και οι δέκτες χρειάζονται τις πληροφορίες που βρίσκονται σε αυτά τα πεδία για να εκτελέσουν τις προσδοκώμενες λειτουργίες τους. Το πρότυπο 802.11 αναφέρεται σε αυτό το σύνθετο πλαίσιο ως *PLCP protocol data unit* (PPDU). Η δομή του πλαισίου PPDU παρέχει ασύγχρονη μεταφορά των MPDU μεταξύ των σταθμών. Ως αποτέλεσμα, το φυσικό επίπεδο σταθμού λήψης πρέπει να συγχρονίσει τα κυκλώματά του για κάθε μοναδικό εισερχόμενο πλαίσιο. Το PLCP διανέμει επίσης τα εισερχόμενα πλαίσια από το ασύρματο μέσο στο στρώμα MAC.
Υπό την καθοδήγηση του PLCP, το *physical medium dependent* (PMD) υπόστρωμα παρέχει ακριβή μετάδοση και λήψη των 802.11 πλαισίων. Για να παρέχει αυτή την υπηρεσία, το PMD αλληλεπιδρά άμεσα με το ασύρματο μέσο, δηλαδή τον αέρα, και παρέχει διαμόρφωση και αποδιαμόρφωση στις μεταδόσεις των πλαισίων. Τα PLCP και PMD επικοινωνούν μεταξύ τους για να κατευθύνουν τις λειτουργίες μετάδοσης και λήψης.

2.6.2 Λειτουργίες 802.11 φυσικού επιπέδου

Το πρότυπο 802.11 υποστηρίζει τις παρακάτω επιτρεπόμενες τεχνικές μετάδοσης για το φυσικό επίπεδο. Η κάθε μία κάνει δυνατή τη μετάδοση ενός πλαισίου MAC από τον ένα σταθμό στον άλλο. Οι τεχνικές διαφέρουν στη χρησιμοποιούμενη τεχνολογία και στις ταχύτητες που επιτυγχάνουν. Οι τεχνικές αυτές είναι:

- Υπέρυθρες (*Infrared*)
- Εξάπλωση Φάσματος με Συνεχή Αλλαγή Συχνότητας (*Frequency-Hopping Spread Spectrum*, FHSS)
- Εξάπλωση Φάσματος Άμεσης Ακολουθίας (*Direct-Sequence Spread-Spectrum*, DSSS)
- Ορθογώνια Πολυπλεξία με Διαίρεση Συχνότητας (*Orthogonal Frequency-Division Multiplexing*, OFDM)(802.11a)
- Εξάπλωση Φάσματος Άμεσης Ακολουθίας Υψηλού Ρυθμού Μετάδοσης (*High-Rate Direct-Sequence Spread-Spectrum*, HR-DSSS)(802.11b)
- *Extended-Rate PHY* (802.11g)
- *High-Throughput PHY* (802.11n)

Υπέρυθρες (Infrared)

Η υπέρυθρη επιλογή χρησιμοποιεί διάχυτη μετάδοση στα 850 ή 950nm και επιτρέπονται δύο ταχύτητες: 1 Mbps και 2 Mbps. Για την λειτουργία των προϊόντων υπέρυθρης μετάδοσης χρησιμοποιούνται τρείς τεχνικές:

- *Διάχυτη εκπομπή* που πραγματοποιείται από έναν πανκατευθυντικό πομπό και το σήμα που παράγεται ακτινοβολείται σε όλες τις κατευθύνσεις παρέχοντας κάλυψη στους κόμβους του δικτύου.
- *Ανάκλαση του μεταδιδόμενου σήματος σε οροφή* όπου το σήμα στοχεύεται σε ένα σημείο μιας διάχυτα ανακλαστικής οροφής και λαμβάνεται με πανκατευθυντικό τρόπο από τους δέκτες.
- *Εστιασμένη μετάδοση* στην οποία η εμβέλεια μετάδοσης εξαρτάται από την ισχύ εκπομπής της ακτίνας και τον βαθμό εστίασής της.

Η ακτίνα λειτουργίας μπορεί να φτάσει περίπου τα 20 μέτρα, σε ελεύθερο φυσικά οπτικό πεδίο. Το υπέρυθρο φώς απορροφάται από τα σκοτεινά αντικείμενα και ανακλάται από τα φωτεινά. Έτσι, τα υπέρυθρα σήματα δεν μπορούν να διαπεράσουν τους τοίχους και οι κυψέλες που βρίσκονται σε διαφορετικά δωμάτια είναι καλά απομονωμένες η μία από την άλλη. Ωστόσο, λόγω του χαμηλού εύρους ζώνης και του γεγονότος ότι το φως του ήλιου εξαφανίζει τα υπέρυθρα σήματα, η επιλογή αυτή δεν είναι δημοφιλής.

Η σημασία της εξάπλωσης φάσματος ραδιοεπικοινωνίας (Spread Spectrum)

Μια από τις βασικές τεχνολογίες που κρύβονται κάτω από την οικογένεια IEEE 802.11 προτύπων είναι η ραδιοεπικοινωνία εξάπλωσης φάσματος. Αυτή η θεμελιώδης έννοια είναι η χρήση ενός ευρύτερου εύρους ζώνης συχνότητας από αυτό που απαιτείται για τις πληροφορίες που μεταδίδονται. Η χρησιμοποίηση του πρόσθετου εύρους ζώνης φαίνεται να είναι σπάταλη, αλλά οδηγεί πραγματικά σε διάφορα οφέλη, συμπεριλαμβανομένης της μειωμένης ευπάθειας στο μπλοκάρισμα (*jammin*g), της λιγότερης ευαισθησίας στις παρεμβολές, και τη συνύπαρξη με τις περιορισμένης ζώνης μεταδόσεις. Διάφορες τεχνικές εξάπλωσης φάσματος είναι διαθέσιμες όπως η χρονική μεταπήδηση (*time hopping*), η διαμόρφωση συχνότητας (*frequency modulation*), η *FHSS*, η *DSSS*, και τα υβρίδια αυτών.
Οι FHSS και DSSS δεν είναι τεχνικές διαμόρφωσης, αλλά μέθοδοι για να διανέμουν το ραδιοσήμα δια μέσω του εύρους ζώνης. Εκτός από τη διάδοση του σήματος δια μέσω μιας ζώνης συχνότητας, τα συστήματα εξάπλωσης φάσματος διαμορφώνουν το σήμα. Η διαμόρφωση είναι η παραλλαγή ενός ραδιοσήματος για να μεταβιβάσει τις πληροφορίες. Το βασικό σήμα καλείται φέρον. Η παραλλαγή μπορεί να βασιστεί στην ισχύ (διαμόρφωση εύρους, *amplitude modulation* [AM]), τη συχνότητα, ή τη φάση (συχνότητα που

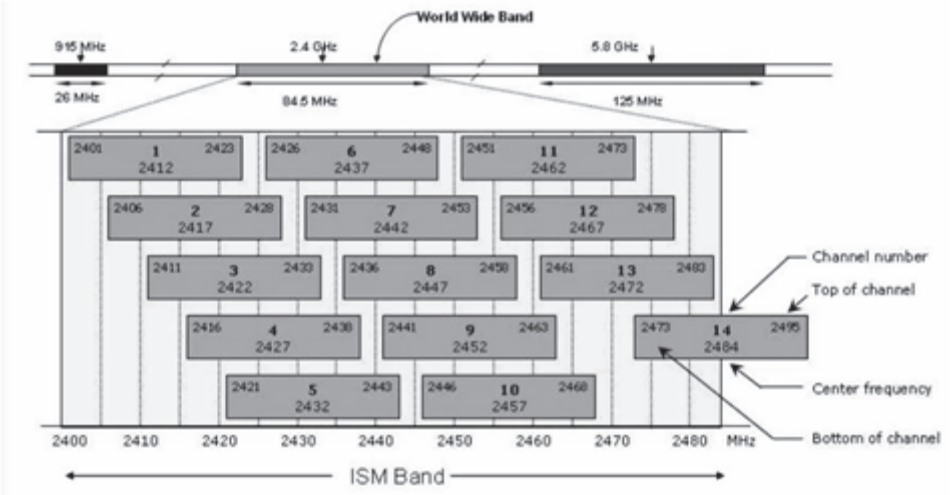
αντισταθμίζεται) του σήματος. Η τεχνική διαμόρφωσης έχει επιπτώσεις άμεσα στον ρυθμό δεδομένων. Οι υψηλότερου ρυθμού δεδομένων διαμορφώσεις είναι γενικά πιο σύνθετες και ακριβές να εφαρμόσουν αλλά συσκευάζουν περισσότερες πληροφορίες στο ίδιο εύρος ζώνης. Οι μικρές διασπάσεις στο σήμα προκαλούν την υποβάθμιση περισσότερων δεδομένων. Αυτό σημαίνει ότι το σήμα πρέπει να έχει μια υψηλότερη αναλογία σήματος προς θόρυβο (SNR) στο δέκτη ώστε να έχει αποτελεσματική επεξεργασία. Επειδή ένα ραδιοσήμα όσο πιο κοντά είναι στην πηγή τόσο πιο ισχυρό είναι, ο λόγος SNR μειώνεται με την απόσταση. Γι' αυτό τα συστήματα υψηλής ταχύτητας έχουν μικρότερο εύρος. Παραδείγματα των τεχνικών διαμόρφωσης που χρησιμοποιούνται στα πρότυπα IEEE 802.11 περιλαμβάνουν τη δυαδική διαμόρφωση μετατόπισης φάσης (*binary phase-shift keying,* BPSK), τη διαμόρφωση τετραγωνισμού μετατόπισης φάσης (*quadrature phase-shift keying,* QPSK), την διαμόρφωση γκαουσσιανής μετατόπισης συχνότητας (*Gaussian frequency-shift keying,* GFSK), και τη CCK (*Complementary Code Keying*).

Εξάπλωση Φάσματος με Συνεχή Αλλαγή Συχνότητας (Frequency-Hopping Spread Spectrum, FHSS)

Με τη χρήση αυτής της τεχνικής, το σήμα εκπέμπεται μέσω ενός φαινομενικά τυχαίου συνόλου καναλιών συχνότητας, μεταπηδώντας (*hopping*) από συχνότητα σε συχνότητα ανά τακτά χρονικά διαστήματα στις οποίες μεταβαίνουν διαδοχικά οι σταθμοί. Η χρονική διάρκεια (*dwell time*) στην οποία μένουν οι σταθμοί στη ίδια συχνότητα ονομάζεται *chip* και είναι μία ρυθμιζόμενη παράμετρος η οποία θα πρέπει να είναι μικρότερη από 400 msec. Ο δέκτης εκτελεί την ίδια ακολουθία μεταπήδησης ενώ διατηρείται σε συγχρονισμό με τον πομπό και έτσι λαμβάνει τα δεδομένα που μεταφέρονται. Όταν βρισκόμαστε σε ένα κανάλι, το πραγματικό μεταδιδόμενο σήμα είναι το αποτέλεσμα της διαμόρφωσης της κεντρικής συχνότητας του καναλιού με το αρχικό σήμα.
Το φυσικό στρώμα αυτό, διαιρεί την ISM μπάντα των 902 MHz σε κανάλια εύρους 0,5 MHz και την μπάντα των 2,4 GHz και 5,8 GHz σε κανάλια εύρους 1 MHz. Οι προδιαγραφές της ομάδας IEEE 802.11 για το φυσικό επίπεδο FHSS υπαγορεύουν τη χρήση γκαουσσιανής διαμόρφωσης μετατόπισης συχνότητας (*Gaussian Frequency Shift Keying*, GFSK) η οποία αλλάζει τη συχνότητα φέροντος για να αναπαριστά διαφορετικά δυαδικά σύμβολα για την μετάδοση δεδομένων με ταχύτητα 1 ή 2 Mbps στην ζώνη 2,4 GHz. Επιπλέον ορίζεται ότι περίπου το 99% της ενέργειας του εκπεμπόμενου σήματος πρέπει να βρίσκεται μέσα στο κανάλι. Διαφορετικά κανάλια είναι διαθέσιμα για χρήση σε διάφορες χώρες
Στις ΗΠΑ και στην Ευρώπη οι αρμόδιοι οργανισμοί έχουν θεσπίσει διαφορετικούς περιορισμούς για τα συστήματα Frequency Hopping. Για παράδειγμα, στις ΗΠΑ η FCC απαιτεί τουλάχιστον 75 διαφορετικά κανάλια (hopping channels) ενώ η Ευρωπαϊκή ETSI μόλις 20, περιορίζοντας όμως περισσότερο την ακτινοβολούμενη ισχύ. Τελικά, για να ικανοποιεί ένα προϊόν τις προδιαγραφές και της FCC και της ETSI πρέπει να ικανοποιεί τις αυστηρότερες από αυτές σε κάθε τομέα (στο παραπάνω παράδειγμα δηλαδή ένα σύστημα πρέπει να έχει τουλάχιστον 75 hopping channels και να ικανοποιεί και τους αυστηρούς περιορισμούς ισχύος της ETSI).
Όσο αναφορά την επίδοση του Frequency Hopping φυσικού στρώματος παρουσία θορύβου και παρεμβολών στενής ζώνης, αυτή είναι αρκετά καλή και μειώνεται γραμμικά όσο αυξάνονται οι παρεμβολές. Η παραγωγή της τυχαίας ακολουθίας παρέχει ένα δίκαιο τρόπο εκχώρησης του φάσματος καθώς επίσης και κάποια περιορισμένη ασφάλεια, αφού ένας εισβολέας που δεν γνωρίζει την ακολουθία συχνοτήτων ή το χρόνο παραμονής δεν μπορεί να υποκλέψει τις μεταδόσεις. Είναι επίσης ανθεκτική στις ραδιοκυματικές μεταβολές. Μεγάλες παρεμβολές σε ένα από τα χρησιμοποιούμενα κανάλια δεν προκαλεί σπουδαία ελάττωση της επίδοσης. Όσο όμως ο αριθμός των καναλιών που επηρεάζονται από τις παρεμβολές αυξάνει, η ελάττωση της επίδοσης αρχίζει να γίνεται πιο έντονη. Κύρια μειονεκτήματα αυτής της τεχνικής είναι το χαμηλό εύρος ζώνης και ότι σε μεγάλες αποστάσεις μπορεί να δημιουργήσει πρόβλημα η εξασθένηση των πολλαπλών διαδρομών.

Εξάπλωση Φάσματος Άμεσης Ακολουθίας (*Direct-Sequence Spread-Spectrum*, DSSS)

Τα συστήματα DSSS χρησιμοποιούν παρόμοια τεχνολογία με τα δορυφορικά συστήματα παγκόσμιας πλοήγησης (*Global Positioning System*, GPS) καθώς και με μερικούς τύπους κινητών τηλέφωνων.
Η βασική ιδέα της άμεσης ακολουθίας (*direct sequence*) είναι να εξαπλώσει ψηφιακά τα πλαίσια δεδομένων της βασικής μπάντας και στη συνέχεια να διαμορφώσει τα απλωμένα δεδομένα σε μια ειδική συχνότητα. Κάθε κομμάτι πληροφορίας (bit) συνδυάζεται στον πομπό με ένα μακρύτερο ψευδοτυχαίο αριθμητικό (*pseudorandom numerical*, PN) στη διαδικασία μετάδοσης. Αυτό έχει ως αποτέλεσμα ένα υψηλής ταχύτητας ψηφιακό ρεύμα (*stream*) το οποίο στη συνέχεια διαμορφώνεται σε μια συχνότητα φέροντος χρησιμοποιώντας διαφορική διαμόρφωση μετατόπισης φάσης (*differential phase-shift keying,* DPSK).
Για το φυσικό στρώμα αυτό ορίστηκαν 14 κανάλια (στην μπάντα των 2,4 GHz με εύρος 5 MHz το κάθε ένα) των οποίων 11 παρακείμενα κανάλια επικαλύπτουν μερικώς και τα υπόλοιπα 3 δεν επικαλύπτονται. Το κανάλι 1 έχει κεντρική συχνότητα τα 2,412 GHz τα υπόλοιπα ακολουθούν κάθε 5 MHz. Στην πράξη κάθε κανάλι καταλαμβάνει περίπου 22 MHz εύρος, γύρω από την κεντρική του συχνότητα. Αυτό σημαίνει ότι υποστηρίζει τρία μη επικαλυπτόμενα κανάλια για τη λειτουργία. Γίνεται χρήση RF φίλτρων για να καταπιέζονται οι πλευρικοί λοβοί έξω από τα 22 MHz. Ακόμα και έτσι, κανάλια που χρησιμοποιούνται σε διπλανές «κυψέλες» πρέπει να απέχουν μεταξύ τους 25 MHz (πέντε κανάλια των 5 MHz) για να αποφεύγονται οι παρεμβολές. Αυτό περιορίζει τον μέγιστο αριθμό καναλιών που μπορούν να χρησιμοποιηθούν. Σε κάθε χώρα επιτρέπεται η χρήση συγκεκριμένων καναλιών.



Εικόνα 11 Το 2,4 GHz κανάλι.

Τα δεδομένα στέλνονται διαμέσου ενός από αυτά τα κανάλια 22 MHz χωρίς μεταπήδηση σε άλλα κανάλια, προκαλώντας το θόρυβο στο δεδομένο κανάλι. Για να μειώσει τον αριθμό αναμεταδόσεων και θορύβου, χρησιμοποιείται διάσπαση για να μετατρέψει κάθε κομμάτι των δεδομένων χρηστών σε μια σειρά πλεοναζόντων bit, *chip*. Ο πλεονασμός κάθε *chip*, συνδυάζεται με τη διάδοση του σήματος πάνω στο κανάλι 22 MHz, παρέχοντας έλεγχο και διόρθωση λαθών για να ανακτήσει τα δεδομένα. Τα *chip* εκτείνονται από 11 bits σε εξαιρετικά επιμήκεις ακολουθίες. Η ταχύτητα με την οποία διαβιβάζονται καλείται *chipping rate*. Σε έναν παρατηρητή, αυτές οι ακολουθίες εμφανίζονται ως θόρυβος και καλούνται επίσης ψευδοτυχαίοι κώδικες θορύβου (*pseudorandom noise codes* , Pncodes). Οι Pncodes εισάγονται με διάφορες τεχνικές συμπεριλαμβανομένων των Barker κωδίκων, των Gold κωδίκων, των μ-ακολουθιών, και των κωδίκων Kasami. Ένα από τα πλεονεκτήματα τους είναι ότι ακόμα κι αν ένα ή περισσότερα από τα bit χαθούν κατά τη διάρκεια της μετάδοσης, οι ενσωματωμένες στατιστικές τεχνικές στην ραδιοσυχνότητα μπορούν να ανακτήσουν τα αρχικά δεδομένα χωρίς την ανάγκη για την αναμετάδοση. Στο δέκτη, ένα αντίστοιχο φίλτρο συσχέτισης χρησιμοποιείται για να αφαιρέσει την ακολουθία PN και να ανακτήσει το αρχικό ρεύμα δεδομένων.

Εξάπλωση Φάσματος Άμεσης Ακολουθίας Υψηλού Ρυθμού Μετάδοσης (High-*Rate Direct-Sequence Spread-Spectrum*, HR-DSSS)(802.11b)

Το 802.11b είναι το πρώτο πρότυπο που χρησιμοποιήθηκε ευρέως στα τοπικά ασύρματα δίκτυα. Μπορεί να θεωρηθεί σαν επέκταση του αρχικού DSSS φυσικού στρώματος που ορίστηκε στο 802.11 και μάλιστα χρησιμοποιεί τα ίδια κανάλια με αυτό, πετυχαίνοντας αρκετά μεγαλύτερους ρυθμούς μετάδοσης. Μόνο τρία IEEE 802.11b συστήματα DSSS μπορούν να συνδυαστούν.
Το IEEE 802.11 διευκρινίζει δύο τύπους διαμορφώσεων DPSK (*Differential Phase Shift Keying*) για τα συστήματα DSSS. Ο πρώτος είναι ο BPSK και ο δεύτερος είναι ο QPSK. Η διαμόρφωση μετατόπισης φάσης (*Phase-shift keying*, PSK), όπως το όνομα υπονοεί, ανιχνεύει τη φάση του ραδιοσήματος. Ο BPSK ανιχνεύει μια 180 μοιρών αντιστροφή του σήματος, που αντιπροσωπεύει ένα δυαδικό 0 ή 1. Αυτή η μέθοδος έχει ως αποτελεσματικό ρυθμό δεδομένων 1 Mbps. Ο QPSK ανιχνεύει τις 90 μοίρες μετατοπίσεις φάσης. Αυτό διπλασιάζει τον ρυθμό δεδομένων σε 2 Mbps. Το IEEE 802.11b προσθέτει τη CCK (*Co Complementary Code Keying*) και τη δυαδική συνελικτική κωδικοποίηση πακέτων (*packet binary convolutional coding*, PBCC). Υποστηρίζει ρυθμούς δεδομένων 1, 2, 5.5, ή 11 Mbps. Σε ενδοκτιριακές εφαρμογές πετυχαίνει κάλυψη ως 150 μέτρα.

Ορθογώνια Πολυπλεξία με Διαίρεση Συχνότητας (*Orthogonal Frequency-Division Multiplexing*, OFDM)(802.11a)

Το IEEE 802.11 φυσικό επίπεδο ορθογώνιας πολυπλεξίας με διαίρεση συχνότητας (OFDM) μεταφέρει 6 Mbps έως 54 Mbps ρυθμούς δεδομένων σε ζώνη UNII 5 GHz και αναφέρεται ως 802.11a. Η 802.11a τροποποίηση στο πρότυπο επικυρώθηκε το 1999, αλλά τα προϊόντα έγιναν διαθέσιμα το 2001 που ήταν αρκετό καιρό μετά τα δίκτυα 802.11b. Χρησιμοποιεί BPSK, QPSK, και QAM για να επιτύχει τους διάφορους ρυθμούς δεδομένων. Βασισμένο σε μια μαθηματική διαδικασία αποκαλούμενη γρήγορο μετασχηματισμό κατά Φουριέ (*Inverse FFT*), επιτρέπει σε 52 κανάλια να επικαλύπτονται παραμένοντας ξεχωριστά και ορθογώνια μεταξύ τους. Η επικάλυψη των καναλιών είναι μια αποδοτικότερη χρήση του φάσματος και επιτρέπει την αποτελεσματικότερη επεξεργασία του στον δέκτη. Οι συχνότητες λειτουργίας ποικίλλουν ανάλογα με την χώρα εφαρμογής του ασύρματου δικτύου. Το IEEE 802.11a OFDM δεν είναι είδος τεχνικής εξάπλωσης φάσματος. Αντιθέτως, διαιρεί τη συχνότητα φέροντος σε 52 χαμηλής ταχύτητας υποφέροντα που περιέχονται σε 20 MHz κανάλι. Σαράντα οκτώ (48) από αυτά χρησιμοποιούνται για τα δεδομένα και τέσσερα (4) χρησιμοποιούνται συγχρονισμό στο δέκτη.
Ένα από τα μεγαλύτερα πλεονεκτήματα της OFDM είναι η αντίστασή του στην παρέμβαση της πολυόδευσης και στην καθυστέρηση διάδοσης. Η πολυόδευση προκαλείται όταν τα ραδιοκύματα ανακλώνται και περνούν μέσω των αντικειμένων στο περιβάλλον. Τα ραδιοκύματα εξασθενούν ή αποδυναμώνονται σε ένα ευρύ φάσμα ανάλογα με το υλικό του αντικειμένου. Μερικά υλικά (όπως το μέταλλο) είναι αδιαφανή στις ραδιομεταδόσεις. Ένα περιβάλλον με πολλά εμπόδια είναι πολύ διαφορετικό από ένα ανοικτό περιβάλλον για τη μετάδοση και λήψη ραδιοκυμάτων. Αυτή η περιβαλλοντική μεταβλητότητα είναι ο λόγος που είναι τόσο δύσκολο να εκτιμηθεί ο ρυθμός δεδομένων και το εύρος ενός IEEE 802.11 συστήματος. Λόγω των αντανακλάσεων και της εξασθένησης, μια μοναδική μετάδοση μπορεί να έχει διαφορετική ισχύ σήματος από διαφορετικές κατευθύνσεις ανάλογα με τους τύπους υλικών που αντιμετωπίζει.
Η καθυστέρηση στην διάδοση συνδέεται με το φαινόμενο πολυόδευσης. Επειδή το σήμα ταξιδεύει μέσα από τις διαφορετικές πορείες μέχρι να καταλήξει στον δέκτη, το σήμα φθάνει σε διαφορετικούς χρόνους. Όσο ο ρυθμός μετάδοσης αυξάνεται τόσο αυξάνεται και η πιθανότητα της παρέμβασης από προηγούμενα μεταδοθέντα σήματα.
Η OFDM δεν είναι μια νέα τεχνική διαφέρει όμως από άλλες αναδυόμενες τεχνικές κωδικοποίησης όπως η πολλαπλή πρόσβαση με διαίρεση κώδικα (*Code Division Multiple Access* ,CDMA). Η CDMA χρησιμοποιεί τις σύνθετες μαθηματικές μετατροπές για να τοποθετήσει πολλές μεταδόσεις πάνω σε ένα μοναδικό φέρον. Η OFDM κωδικοποιεί μια

ενιαία μετάδοση σε πολλαπλά υποφέροντα κρύβοντας λιγότερα μαθηματικά από την CDMA. Οι συσκευές OFDM χρησιμοποιούν ένα ευρύ κανάλι συχνότητας και το σπάνε σε πολλαπλά υποκανάλια. Κάθε υποκανάλι χρησιμοποιείται για να διαβιβάσει τα δεδομένα. Όλα τα υποκανάλια πολυπλέκονται έπειτα και συνδιάζονται σε ένα κανάλι.[8]
Παρόλα αυτά οι υψηλότερες ραδιοσυχνότητες μειώνουν κατά πολύ την απόσταση κάλυψης καθώς και την διεισδυτική δύναμη του 802.11a , ειδικά σε εσωτερικούς χώρους. Εκεί που μια μετάδοση 802.11b θα περνούσε έναν τοίχο, μια μετάδοση 802.11a μπορεί να εμποδιστεί. Το γεγονός αυτό μπορεί να εμποδίσει την εγκατάσταση σε μεγάλη κλίμακα ενός δικτύου 802.11a καθώς απαιτούνται πιο πολλά Access Points για την κάλυψη του χώρου.

Channel Identifier	Frequency (in MHz)	Regulatory Domains			
		Americas	EMEA	Japan	Rest of World
34	5170	-	-	x	-
36	5180	x	x	-	x
38	5190	-	-	x	-
40	5200	x	x	-	x
42	5210	-	-	x	-
44	5220	x	x	-	x
46	5230	-	-	x	-
48	5240	x	x	-	x
52	5260	x	x	-	x
56	5280	x	x	-	x
60	5300	x	x	-	x
64	5320	x	x	-	x
100	5500	-	x	-	x
104	5520	-	x	-	x
108	5540	-	x	-	x
112	5560	-	x	-	x
116	5580	-	x	-	x
120	5600	-	x	-	x
124	5620	-	x	-	x
128	5640	-	x	-	x
132	5660	-	x	-	x
136	5680	-	x	-	x
140	5700	-	x	-	x
149	5745	x	-	-	x
153	5765	x	-	-	x
157	5785	x	-	-	x
161	5805	x	-	-	x

Εικόνα 12 Τα 802.11a κανάλια.

Extended-Rate PHY (802.11g)

Τον Ιούνιο του 2003 η ομάδα εργασίας IEEE ολοκλήρωσε τις εργασίες τις και εξέδωσε το πρότυπο 802.11g. Το 802.11g είναι ένας συνδυασμός των παραλλαγών 802.11a και 802.11b, δηλαδή επιτυγχάνονται υψηλοί ρυθμοί μετάδοσης της τάξης των 54 Mbps, διατηρώντας παράλληλα τη προς πίσω συμβατότητα με το διαδεδομένο 802.11b. Χρησιμοποιεί διαμόρφωση OFDM (όπως το 802.11a), καθώς και τη διαμόρφωση CCK ενώ λειτουργεί στη ζώνη συχνοτήτων ISM 2,4 Ghz (όπως το 802.11b).
Το 802.11g αντιμετωπίζει τους περιορισμούς σε bandwidth του 802.11b και παράλληλα προσφέρει την διεισδυτική δύναμη της μπάντας των μικροκυμάτων καθώς και την ικανότητα μετάδοσης σε μεγάλες αποστάσεις. Παρόλα αυτά δεν περιορίζει το πρόβλημα της συμφόρησης στην συγκεκριμένη μπάντα στην οποία λειτουργούνε πολλές συσκευές. Το 802.11g είναι επίσης περιορισμένο σε τρία μη αλληλοεπικαλυπτόμενα κανάλια όπως και ο προκάτοχος του, το 802.11b. Το 802.11g μπορεί να έχει τα ίδια προβλήματα απόδοσης όπως και το 802.11b λόγω της συμβατότητας προς τα πίσω που έχει. Εάν ένας σταθμός 802.11b είναι παρόν σε ένα δίκτυο 802.11g, όλοι οι σταθμοί θα πρέπει να χρησιμοποιήσουν την διαμόρφωση σήματος του 802.11b για συμβατότητα. Παρόλα αυτά σε ένα καθαρά 802.11g δίκτυο μπορεί κάποιος να εκμεταλλευτεί πλήρως τις ικανότητες της τεχνολογίας. Επίσης μια εξωτερική κεραία που λειτουργεί σε 802.11b δίκτυο μπορεί να λειτουργήσει και σε 802.11g μειώνοντας έτσι το κόστος αναβάθμισης.

Channel Identifier	Frequency (in MHz)	Regulatory Domains			
		Americas	EMEA	Japan	Rest of World
1	2412	x	x	x	x
2	2417	x	x	x	x
3	2422	x	x	x	x
4	2427	x	x	x	x
5	2432	x	x	x	x
6	2437	x	x	x	x
7	2442	x	x	x	x
8	2447	x	x	x	x
9	2452	x	x	x	x
10	2457	x	x	x	x
11	2462	x	x	x	x
12	2467	-	x	x	x
13	2472	-	x	x	x
14	2484	-	-	x	-

Εικόνα 13 Τα κανάλια 802.11b/g.

High-Throughput PHY (802.11n)

Στις αρχές του 2004, το IEEE ανακοίνωσε ότι σχημάτισε μια νέα ομάδα εργασίας, η οποία ονομάζεται Task Group n ή TGn. Η ομάδα αυτή ανέλαβε την δημιουργία μιας τροποποίησης του αρχικού προτύπου 802.11, με σκοπό την επίτευξη πραγματικού ρυθμού μεταφοράς τουλάχιστον 100 Mbps. Αυτό σημαίνει ότι ο θεωρητικός ρυθμός μεταφοράς θα πρέπει να είναι τουλάχιστον 600 Mbps. Ο μέγιστος ρυθμός δεδομένων εξαρτάται από τα ποιά χαρακτηριστικά 802.11n υποστηρίζονται μεταξύ των 802.11n συσκευών και από το τί υποστηρίζει το περιβάλλον. Για να επιτευχθούν τέτοιες ταχύτητες επιβάλλεται η μετάβαση σε νέες τεχνολογίες ασύρματης μετάδοσης και στη συγκεκριμένη περίπτωση, θα χρησιμοποιηθεί η τεχνολογία MIMO (*Multiple Input – Multiple Output*). Η ονομασία προήλθε από το γεγονός ότι η τεχνολογία αυτή χρησιμοποιεί πολλαπλές κεραίες για την αποστολή και λήψη δεδομένων και οι οποίες λειτουργούν ταυτόχρονα και ανεξάρτητα η κάθε μία. Αυτό το πρότυπο επικυρώθηκε το 2009 και λειτουργεί στις μπάντες συχνοτήτων 2,4 GHz και 5GHz και είναι προς τα πίσω συμβατό με το 802.11a και 802.11b/g. Το 802.11n δεσμεύει 2 κανάλια των 20 MHz σε ένα των 40 MHz.

Channel Identifier	Frequency (in MHz)	Regulatory Domains			
		Americas	EMEA	Japan	Rest of World
(36, 1) (40,-1)	5190	x	-	x	-
(44, 1) (48,-1)	5230	x	-	x	-
(52, 1) (56,-1)	5270	x	-	x	-
(60, 1) (64, -1)	5310	x	-	-	x
(100, 1) (104, -1)	5510	-	x	-	x
(108, 1) (112, -1)	5550	-	x	-	x
(116, 1) (120, -1)	5590	-	x	-	x
(124, 1) (128,-1)	5630	-	x	-	x
(132, 1) (136,-1)	5670	-	x	-	x
(149, 1) (153,-1)	5755	x	-	-	x
(157, 1) (161,-1)	5795	x	-	-	x

Εικόνα 14 Τα κανάλια 802.11n.

2.7 Το υπόστρωμα MAC του 802.11

Το 802.11 MAC είναι κοινό για όλα τα IEEE 802.11 PHY στρώματα και είναι αρμόδιο για τη διαχείριση της μεταφοράς δεδομένων από τις υψηλότερου επιπέδου λειτουργίες στα φυσικά μέσα. Εδρεύει εντός του επιπέδου κατάστασης συνδέσμων και επιτρέπει σε πολλαπλές συσκευές πελατών (αναφέρονται συνήθως ως σταθμοί) να μοιράζονται το κοινό μέσο μετάδοσης του αέρα μέσω ενός *carrier sense* πρωτόκολλου. Αυτό το πρωτόκολλο συντονίζει την πρόσβαση στο κοινό μέσο έτσι ώστε οι σταθμοί να μπορούν να μοιράζονται την ίδια συχνότητα και τον ίδιο χώρο στο ραδιοφάσμα. Οι λειτουργίες του MAC παρέχουν επίσης αξιόπιστη μετάδοση των δεδομένων πάνω από το αρκετά επιρρεπές, και σε μεγάλο βαθμό, σε σφάλματα ασύρματο μέσο. Για να γίνει πιο κατανοητό, θεωρούμε μια αίθουσα με ανθρώπους που λαμβάνουν μέρος στην ίδια συζήτηση. Κάθε άτομο μπορεί να ακούσει αν κάποιος μιλάει. Αυτό αντιπροσωπεύει μια ολοκληρωμένη τοπολογία bus όπου ο καθένας επικοινωνεί χρησιμοποιώντας την ίδια συχνότητα (φωνή) και τον ίδιο χώρο (την αίθουσα). Για να αποφύγουμε να μιλάνε ταυτόχρονα δύο άνθρωποι, όταν κάποιος θελήσει να πει κάτι, θα πρέπει να περιμένει μέχρι ένα άλλο άτομο σταματήσει να μιλάει. Αυτό το απλό πρωτόκολλο βεβαιώνει ότι μόνο ένα άτομο μιλάει σε δεδομένη χρονική στιγμή, προσφέροντας με αυτόν τον τρόπο μία διαμοιραζόμενη χρήση του κοινού μέσου επικοινωνίας.
Το 802.11 λειτουργεί με παρόμοιο τρόπο. Όταν ένας σταθμός θέλει να μεταδώσει δεδομένα, "ακούει" πρώτα το μέσο και αν είναι αδρανές (*idle*), δηλαδή δεν χρησιμοποιείται από κάποιον άλλον σταθμό, αρχίζει την μετάδοση των δεδομένων εξαρτώμενο από επιπρόσθετους κανόνες που ορίζει το πρότυπο. Αν το μέσο είναι απασχολημένο ο σταθμός αναβάλλει την μετάδοση. Αυτό το πρωτόκολλο αναφέρεται ως πολλαπλή πρόσβαση με ανίχνευση φέροντος (*carrier sense multiple access*, CSMA).
Το 802.11 ανταπεξέρχεται στον έλεγχο λαθών έχοντας σε κάθε σταθμό έλεγχο στα εισερχόμενα δεδομένα για αλλαγμένα bits. Αν ο σταθμός προορισμού δεν αντιληφθεί σφάλματα, στέλνει μια επιβεβαίωση πίσω στον σταθμό-πηγή. Σε αντίθετη περίπτωση, αν αντιληφθεί σφάλματα, το πρωτόκολλο data-link βεβαιώνει ότι ο σταθμός-πηγή θα ξαναστείλει το πακέτο. Λόγω καθυστερήσεων στην διάδοση, είναι πιθανό δύο ασύρματοι σταθμοί να ανιχνεύσουν ότι το μέσο δεν είναι απασχολημένο και να αρχίσουν και οι δύο να μεταδίδουν. Για να αποφύγει το 802.11 την πρόσκρουση αυτή, οι δύο σταθμοί σταματούν τη μετάδοση, περιμένουν για κάποιο χρονικό διάστημα και προσπαθούν ξανά.

2.7.1 Υπηρεσίες MAC στρώματος

Το MAC παρέχει εννέα λογικές υπηρεσίες: πιστοποίηση (A*uthentication*), τερματισμός πιστοποίησης (*Deauthentication)*, συσχέτιση (*Association)*, αποσύνδεση (*Disassociation)*, επανασυσχέτιση (*Reassociation*), διανομή (*Distribution*), ολοκλήρωση (*Integration)*, μυστικότητα (*Privacy*), και παράδοση στοιχείων (*MSDU Delivery)*. Ένα AP χρησιμοποιεί και τις εννέα υπηρεσίες. Ένα τελικό σημείο χρησιμοποιεί την επικύρωση, το deauthentication, τη μυστικότητα, και την παράδοση στοιχείων. Κάθε υπηρεσία χρησιμοποιεί ένα σύνολο μηνυμάτων με τα στοιχεία πληροφοριών που αρμόζουν στις υπηρεσίες.

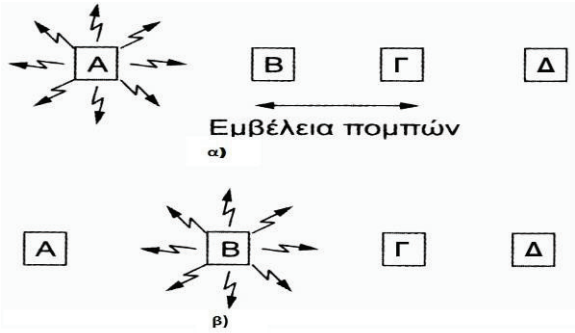
Distribution: Η υπηρεσία αυτή είναι απαραίτητη για την παράδοση ενός πλαισίου από το AP στον τελικό προορισμό του. Συνίσταται στον εντοπισμό του παραλήπτη, ώστε να γίνει εφικτή η τελική παράδοση του πλαισίου. Έτσι λαμβάνεται απόφαση αν ένα πλαίσιο πρέπει να σταλεί στο ίδιο BSS ή πρέπει να σταλεί στο DS προς παράδοση σε σταθμό συσχετιζόμενο με άλλο AP.
Integration: Η υπηρεσία αυτή παρέχεται από το σύστημα διανομής. Είναι υπεύθυνη για τη διασύνδεση του συστήματος διανομής DS σε ένα δίκτυο διαφορετικό του 802.11. Στην ουσία είναι υπεύθυνη για την μετάφραση των πλαισίων από τον ένα τύπο στον άλλο.
MSDU Delivery: Η παράδοση των πλαισίων MAC (*MAC Service Data Unit*) στον τελικό προορισμό τους.
Association: Απαραίτητη διαδικασία συσχετισμού ενός σταθμού με το AP, προκειμένου να είναι σε θέση να στείλει και να δεχτεί πλαίσια μέσω του ασυρμάτου δικτύου. Όταν ένας

σταθμός είναι συσχετισμένος με ένα AP, δημιουργείται τότε μια λογική σχέση μεταξύ τους, ώστε το DS να γνωρίζει που και πώς να παραδώσει δεδομένα σε έναν ασύρματο σταθμό.
Reassociation: Χρησιμοποιείται από τους κινητούς σταθμούς σε περίπτωση μετακίνησης από μία BSS σε μία άλλη. Είναι μέρος του μηχανισμού της διαπομπής.
Disassociation: Η διαδικασία αυτή αφαιρεί έναν σταθμό από το δίκτυο. Το MAC του 802.11 μπορεί να χειριστεί και σταθμούς που εγκαταλείπουν το δίκτυο χωρίς να κάνουν πρώτα disassociation.
Authentication: Αν απαιτείται από το διαχειριστή του δικτύου, πρέπει κάθε χρήστης να πιστοποιεί την ταυτότητά του πριν να προχωρήσει στη διαδικασία του association.
Deauthentication: Τερματισμός μιας ισχύουσας κατάστασης authentication. Τερματίζει επίσης και το association, εφόσον το authentication είναι προαπαιτούμενο αυτού.
Privacy: Λόγω του ασύρματου περιβάλλοντος μετάδοσης έχουν οριστεί από το 802.11 υπηρεσίες κρυπτογράφησης των δεδομένων.

2.7.2 Αρχιτεκτονική στρώματος MAC

Στα ασύρματα δίκτυα δύο είναι τα βασικά προβλήματα που πρέπει να αντιμετωπιστούν:

- Το πρόβλημα κρυφού σταθμού
- Το πρόβλημα εκτεθειμένου σταθμού



Εικόνα 15 α) πρόβλημα κρυφού σταθμού β) πρόβλημα εκτεθειμένου σταθμού

Πρόβλημα κρυφού σταθμού: Ο Α μεταδίδει στον Β. Αν ο Γ ανιχνεύσει το κανάλι, δεν θα ακούσει τον Α επειδή βρίσκεται εκτός εμβέλειας οπότε θα συμπεράνει λανθασμένα ότι μπορεί να μεταδώσει στον Β. Αν το κάνει, θα δημιουργήσει παρεμβολές στον Β εξαφανίζοντας το πλαίσιο από τον Α.

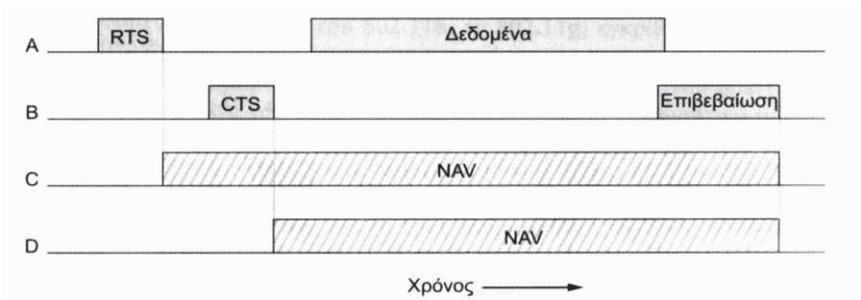
Πρόβλημα εκτεθειμένου σταθμού: Μεταδίδει ο Β στον Α. Αν ο Γ ανιχνεύσει το μέσο θα ακούσει μια μετάδοση σε εξέλιξη και θα συμπεράνει λανθασμένα ότι δεν μπορεί να στείλει στον Δ ενώ μια τέτοια μετάδοση θα οδηγούσε σε κακή λήψη μόνο μεταξύ του Β και Γ που όμως δεν βρίσκεται κανένας από τους επιθυμητούς παραλήπτες.

Τη λύση στα δύο αυτά προβλήματα προσφέρουν οι μηχανισμοί DCF και PCF που παρέχει το MAC επίπεδο για πρόσβαση στο μέσο.

<u>Κατανεμημένη Λειτουργία Συντονισμού DCF (*Distributed Coordination Function*)</u>

Αυτή η λειτουργία δεν εφαρμόζει κάποιο είδος κεντρικού ελέγχου και εφαρμόζει την μέθοδο της πολλαπλής πρόσβασης με ανίχνευση φέροντος για αποφυγή συγκρούσεων (CSMA/CA). Για να αποφευχθούν όσο το δυνατόν περισσότερο οι συγκρούσεις αντί για το μηχανισμό ανίχνευσης συγκρούσεων CD (*Collision Detection*) που χρησιμοποιείται στο 802.3 επιλέγηκε ο μηχανισμός αποφυγής συγκρούσεων CA (*Collision Avoidance*) επειδή ο δέκτης δεν μπορεί να αντιλαμβάνεται την κατάσταση του ασύρματου μέσου την χρονική στιγμή που μεταδίδει κάποια πληροφορία. Επομένως, το φαινόμενο της σύγκρουσης όταν δυο ή περισσότεροι σταθμοί μεταδίδουν την ίδια ακριβώς χρονική στιγμή, γίνεται

αντιληπτό από τους σταθμούς εργασίας μόνο με τη μη παράδοση των πακέτων πληροφορίας. Το CSMA/CA υποστηρίζει δύο μεθόδους λειτουργίας.
Στην πρώτη μέθοδο, ο σταθμός που επιθυμεί να μεταδώσει ανιχνεύει το κανάλι (τόσο το φυσικό όσο και το εικονικό) και αν είναι αδρανές αρχίζει την μετάδοση. Καθώς μεταδίδει δεν ανιχνεύει το κανάλι, αλλά στέλνει ολόκληρο το πλαίσιό του, το οποίο μπορεί να καταστραφεί στον παραλήπτη λόγω παρεμβολών. Σε αντίθετη περίπτωση, αν είναι απασχολημένο το κανάλι, ο αποστολέας δεν μεταδίδει μέχρι το κανάλι να αδρανοποιηθεί . Αν συμβεί μια σύγκρουση, οι σταθμοί που συγκρούστηκαν αναμένουν ένα τυχαίο χρονικό διάστημα και ξαναδοκιμάζουν αργότερα.
Στην δεύτερη μέθοδο, το CSMA/CA βασίζεται στο πρωτόκολλο MACAW (*multiple access with collision avoidance for wireless*) και χρησιμοποιεί ανίχνευση εικονικού καναλιού. Ο μηχανισμός αυτός χρησιμοποιεί δύο μικρά πλαίσια ελέγχου (frames), το RTS (*Ready To Send*) και το CTS (*Clear To Send*). Το RTS πακέτο στέλνεται από το σταθμό που θέλει να εκπέμψει στον παραλήπτη ζητώντας του έτσι την άδεια να καταλάβει το κανάλι και ο παραλήπτης αν είναι διαθέσιμος απαντά με το πλαίσιο CTS, το οποίο μόλις ο αποστολέας του RTS το λάβει έχει τη δυνατότητα να αρχίσει την εκπομπή των δεδομένων του, ενεργοποιώντας ταυτόχρονα ένα χρονόμετρο επιβεβαίωσης, χωρίς πιθανότητα σύγκρουσης καθώς οι υπόλοιποι κόμβοι, που άκουσαν το RTS ή το CTS, είναι ενήμεροι ότι το κανάλι είναι απασχολημένο και εισέρχονται σε κατάσταση αναμονής για κατάλληλο χρονικό διάστημα (*Network Allocation Vector-NAV*), το οποίο υπολογίζεται από τις πληροφορίες που μεταφέρουν τα πλαίσια ελέγχου. Με τη λήξη του διαστήματος αυτού, οι κόμβοι που έχουν πλαίσια για αποστολή ακολουθούν την ίδια διαδικασία για να καταλάβουν το κανάλι αλλά σε διαφορετικές χρονικές στιγμές ώστε να μειωθεί η πιθανότητα σύγκρουσης. Βέβαια, αν παρά ταύτα υπάρξει σύγκρουση μεταξύ δύο σταθμών, τίθενται σε κατάσταση αναμονής, περιμένοντας ένα τυχαίο χρονικό διάστημα, και προσπαθούν ξανά.



Εικόνα 16 Ανίχνευση εικονικού καναλιού με το CSMA/CA.

<u>Σημειακή Λειτουργία Συντονισμού PCF (*Point Coordination Function*)</u>

Αυτή η μέθοδος είναι προαιρετική και χρησιμοποιεί τον σταθμό βάσης για τον έλεγχο όλων των δραστηριοτήτων του στην αντίστοιχη κυψέλη του δίνοντας του τον ρόλο του κεντρικού διαχειριστή (*Point Coordinator*, PC) γι' αυτό και αυτή η μέθοδος χρησιμοποιείται μόνο στα *Infrastructure* δίκτυα. Η ενεργοποίηση της λειτουργίας PCF γίνεται αυτόματα για συγκεκριμένα διαστήματα όταν το access point το θεωρεί αναγκαίο ώστε να αποφευχθούν συγκρούσεις για κάποιο χρονικό διάστημα.
Σκοπός του PCF είναι να προσφέρει πρόσβαση στο μέσο χωρίς ανταγωνισμό μεταξύ των σταθμών (*contention-free medium access*). Υλοποιείται χρησιμοποιώντας την υποδομή του αλγορίθμου DCF και προσθέτοντας την επιπλέον λειτουργικότητα. Η χρήση του συνεπάγεται τη δημιουργία χρονικών περιόδων χωρίς ανταγωνισμό (contention - free periods), ενώ κατά τον υπόλοιπο χρόνο η πρόσβαση ελέγχεται κανονικά από τον DCF (*contention periods*). Υπάρχει δυνατότητα καθορισμού της σχέσης των δύο παραπάνω χρονικών περιόδων ανάλογα με τη χρήση του δικτύου. Αυτές οι περίοδοι επαναλαμβάνονται διαδοχικά, ενώ η διάρκειά τους κάθε φορά ονομάζεται *contention-free repetition interval*.
Πιο συγκεκριμένα, το access point, στην αρχή κάθε τέτοιου διαστήματος, χωρίς

ανταγωνισμό στέλνει ένα πλαίσιο συγχρονισμού (*beacon*) σε όλους τους κόμβους και έπειτα κάνει διαμερισμό του χρόνου σε θυρίδες και αναθέτει σε κάθε σταθμό μία θυρίδα κατά την οποία μόνο αυτός ο σταθμός μπορεί να εκπέμψει ή να λάβει δεδομένα. Η έναρξη κάθε θυρίδας σηματοδοτείται από την αποστολή ενός πλαισίου *Poll* από το access point στον κόμβο που ανήκει η τρέχουσα θυρίδα.

3 Ασφάλεια και Πιστοποίηση στα δίκτυα Wi-Fi

3.1 Διαδικασία σύνδεσης ενός σταθμού σε ένα BSS

Όπως είδαμε και προηγουμένως, όταν ένας σταθμός θέλει να συνδεθεί σε ένα BSS ακολουθεί την εξής διαδικασία:

1. Είτε είναι σε κατάσταση λειτουργίας (*power-up*), είτε σε κατάσταση αναμονής (*sleeping mode*) ή μόλις εισήλθε στην περιοχή του BSS, ο σταθμός χρειάζεται να λάβει πληροφορίες συγχρονισμού από το AP με ενεργή ή παθητική σάρωση (*active / passive scanning*).
2. Από την στιγμή που ο σταθμός έχει βρει ένα AP και αποφασίσει με ποιό BSS θα συνδεθεί, ακολουθεί η διαδικασία πιστοποίησης (*Authentication Process*), η οποία είναι η ανταλλαγή πληροφορίας μεταξύ του AP και του σταθμού όπου κάθε πλευρά αποδεικνύει την γνώση ενός δοσμένου κωδικού (*password*).
3. Αφού ο σταθμός πιστοποιηθεί, θα ακολουθήσει η διαδικασία *association* του σταθμού με το AP. Το association αφορά την ανταλλαγή πληροφορίας σχετικά με τις δυνατότητες των σταθμών και του BSS, η οποία επιτρέπει στα APs να γνωρίζουν την τρέχουσα τοποθεσία των σταθμών και να καθορίσουν μια πύλη εισόδου (λογική θύρα στο δίκτυο) για τους σταθμούς. Μόνο όταν ολοκληρωθεί και αυτή η διαδικασία ένας σταθμός είναι ικανός να μεταδώσει και να λάβει πακέτα δεδομένων (*data frames*) μέσω του AP. Ο ασύρματος σταθμός επικαλείται την υπηρεσία αυτή μόνο μία φορά, κατά την είσοδο του στο BSS. Κάθε σταθμός σχετίζεται μόνο με ένα AP αλλά ένα AP μπορεί να σχετιστεί με πολλούς σταθμούς. Περιοδικά ελέγχεται η σύνδεση αυτή.
   Η διαδικασία ξεκινά ως εξής: ο σταθμός στέλνει ένα αίτημα συσχέτισης (*association request*) στο AP με το οποίο πιστοποιείται. Εάν η απάντηση συσχέτισης είναι θετική, η σύνδεση δημιουργείται. Για να κινηθεί μεταξύ των σημείων πρόσβασης μέσα σε ένα ESS, ο σταθμός περιπλάνησης (*roaming station*) στέλνει ένα *reassociation request* στο νέο AP με σκοπό να ενωθεί στο νέο BSS και να αποσυνδεθεί από το προηγούμενο AP. Οποιοσδήποτε σταθμός μπορεί να ολοκληρώσει μια συσχέτιση με την αποστολή μιας ειδοποίησης αποσυσχέτισης. Σε ένα IBSS, κάθε σταθμός πρέπει να δημιουργήσει μια χωριστή συσχέτιση με κάθε έναν από τους άλλους σταθμούς μέσα στην ομάδα.

3.2 Προστασία ασύρματων δικτύων

Οι βασικές παράμετροι προστασίας για τα ασύρματα δίκτυα είναι οι εξής:

- ***Confidentiality ή εμπιστευτικότητα:*** είναι η ιδιότητα να μην αποκαλύπτεται η πληροφορία σε μη εξουσιοδοτημένα τμήματα. Πολλές φορές χρησιμοποιείται ο συνώνυμος όρος μυστικότητα (*secrecy*). Η εμπιστευτικότητα επιτυγχάνεται με την χρήση της κρυπτογράφησης. *Κρυπτογράφηση* (*encryption, συμβολίζεται με E*) καλείται η διαδικασία κατά την οποία τα δεδομένα αλλάζουν μορφή, μεταμφιέζονται, προκειμένου να επιτευχθεί η ασφαλής μετάδοση πληροφοριών. Τα δεδομένα πριν από την κρυπτογράφηση μεταφέρονται ως απλό κείμενο - *plaintext* (συμβολίζεται με P) ενώ τα δεδομένα μετά την κρυπτογράφηση μεταφέρονται ως κωδικοποιημένα - *cipher text* (συμβολίζεται με C). Η αντίστροφη διαδικασία μετατροπής ονομάζεται αποκρυπτογράφηση (*decryption*).
  Ο αλγόριθμος κρυπτογράφησης ή *cipher* είναι η μαθηματική ακολουθία που χρησιμοποιείται για την κωδικοποίηση / αποκωδικοποίηση των δεδομένων. Συνήθως οι αλγόριθμοι κρυπτογράφησης περιέχουν ακολουθίες κλειδιών για να τροποποιήσουν τα εξαγόμενά τους.
  Για να ικανοποιήσει τον αρχικό σκοπό της η κρυπτογράφηση, δηλαδή την επίτευξη της εμπιστευτικότητας, ο αλγόριθμος κρυπτογράφησης και ο τρόπος λειτουργίας αυτού θα πρέπει να σχεδιαστούν με τέτοιον τρόπο ώστε κάποιος μη εξουσιοδοτημένος να μην είναι δυνατό να ανακτήσει τα κλειδιά που

χρησιμοποιούνται στην κρυπτογράφηση ή να ανακτήσει το κείμενο ακόμα και με την βοήθεια των κλειδιών.

- ***Data Integrity ή Ακεραιότητα δεδομένων:*** είναι η ιδιότητα των δεδομένων να μην τροποποιηθούν τη στιγμή που δημιουργήθηκαν, μεταφέρθηκαν ή αποθηκεύτηκαν. Ως τροποποίηση εκλαμβάνεται κάθε είδους προσθήκη "ξένων" δεδομένων, διαγραφή έγκυρων δεδομένων ή αντικατάσταση έγκυρων με "ξένα" δεδομένα. Μηχανισμοί κρυπτογράφησης, όπως *message authentication codes* ή *digital signatures*, χρησιμοποιούνται για να ανιχνεύσουν εσκεμμένες και μη, τροποποιήσεις των πακέτων πληροφοριών. Οι εσκεμμένες τροποποιήσεις οφείλονται σε κάποιον επιτιθέμενο, ενώ οι μη εσκεμμένες τροποποιήσεις μπορεί να οφείλονται στην θορυβώδη μετάδοση ή σε σφάλματα της μνήμης του συστήματος. Συμπληρωματικά μπορούν να χρησιμοποιηθούν μη-κρυπτογραφικοί μηχανισμοί, οι οποίοι ανιχνεύουν κυρίως αλλοιώσεις δεδομένων που πραγματοποιήθηκαν κατά λάθος, ενώ δεν είναι αποτελεσματικοί στην εύρεση κακόβουλων αλλοιώσεων.
- ***Mutual Authentication ή Αμοιβαία πιστοποίηση:*** είναι η λειτουργία που χρησιμοποιείται για την επιβεβαίωση της ταυτότητας των οντοτήτων που συμμετέχουν στην επικοινωνία. Η αμοιβαία πιστοποίηση υλοποιείται με την χρήση *digital signatures* ή *message authentication codes*.
- ***Access control ή Έλεγχος πρόσβασης:*** είναι η δυνατότητα μίας οντότητας να καθορίζει ποιος χρήστης έχει το δικαίωμα πρόσβασης στις διάφορες πηγές.
- ***Non-repudiation ή Μη αποκήρυξη:*** είναι η ιδιότητα μίας οντότητας να μην μπορεί να αρνηθεί ότι προέβη σε ενέργειες που όντως πραγματοποίησε.
- ***Availability ή Διαθεσιμότητα:*** είναι η ιδιότητα συσκευών και χρηστών να μπορούν να προσπελάσουν το δίκτυο και τις πηγές του όποτε το επιθυμούν. Επίσης, η διαθεσιμότητα παρέχει προτεραιότητα στις πιο σημαντικές επικοινωνίες, όπως είναι οι κλήσεις πρώτης ανάγκης, και επιπλέον εξασφαλίζει δίκαιη διανομή του μέσου στους χρήστες που βρίσκονται στην ίδια περιοχή.

3.3 Μέθοδοι ασφάλειας στα hotspots

Υπάρχουν τρείς βασικές γενιές μεθόδων ασφαλείας για τα ασύρματα δίκτυα hotspots.
Σε χρονολογική σειρά εισαγωγής αυτές είναι:

- ✓ WEP
- ✓ WPA
- ✓ 802.11i/WPA2

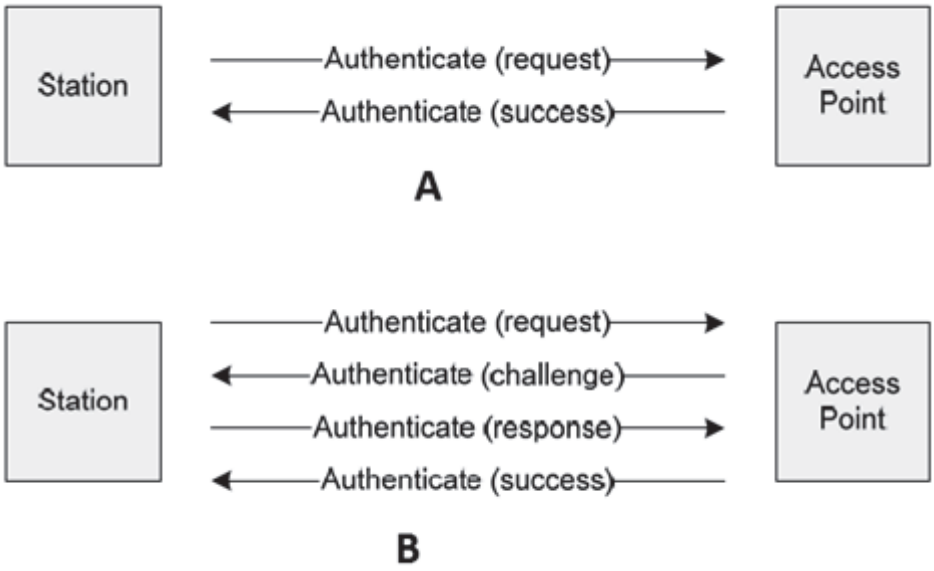
3.3.1 Pre-RSN Πιστοποίηση

Εάν ένας σταθμός λαμβάνει ένα αίτημα συσχέτισης (*association request*) από έναν σταθμό που δεν είναι πιστοποιημένος με αυτόν, στέλνει μια ειδοποίηση *deauthentication* στον αιτούντα. Η πιστοποίηση επιτυγχάνεται από μια ανταλλαγή των πακέτων διαχείρισης (*management packets*) τα οποία χρησιμοποιούνται για να υποστηρίξουν την πιστοποίηση, την συσχέτιση, και το συγχρονισμό. Το πρότυπο 802.11 υποστηρίζει διάφορους τύπους πιστοποίησης.

Τα αρχικά πρότυπα παρείχαν μόνο δύο μορφές πιστοποίησης: ανοικτού συστήματος και κοινού κλειδιού.

- Πιστοποίηση ανοικτού συστήματος (*Open system authentication*): Αυτή είναι η προκαθορισμένη μέθοδος πιστοποίησης του 802.11. Οποιοσδήποτε κόμβος, συμβατός με το πρότυπο, πιστοποιείται αυτόματα. Συγκεκριμένα, ο σταθμός που θέλει να χρησιμοποιήσει την υπηρεσία στέλνει ένα πλαίσιο ελέγχου με την ταυτότητα του αποστολέα και ο σταθμός που το λαμβάνει στέλνει ως απάντηση ένα πλαίσιο, με το οποίο αναγνωρίζει ή όχι την ταυτότητα του αποστολέα.

- Πιστοποίηση κοινού κλειδιού (*Shared key authentication*): Αυτός ο τύπος πιστοποίησης προϋποθέτει ότι όλοι οι σταθμοί έχουν λάβει μέσω ενός καναλιού (ανεξάρτητου από το 802.11 δίκτυο) ένα μυστικό κλειδί, με τη χρήση του οποίου λαμβάνει χώρα η πιστοποίηση. Για τη χρήση αυτής της μεθόδου εφαρμόζεται ο αλγόριθμος WEP (Wired Equivalent Privacy) και ο κόμβος πρέπει να αποδείξει ότι ξέρει ένα από τα κλειδιά WEP που λειτουργούν στο δίκτυο.



Εικόνα 17 A) Open System Authentication B) Shared Key Authentication.

Αυτές οι αρχικές μέθοδοι πιστοποίησης, που σχετίζονται με συστήματα pre-RSN (*pre-Robust Security Network)*, υποστηρίζονται ακόμα, αλλά η αναθεώρηση 802.11i πρόσθεσε επιπλέον βήματα για τα δίκτυα που χρησιμοποιούν νεώτερες μεθόδους κρυπτογράφησης. Για να αποφευχθούν οι σύνθετες αλλαγές στο αρχικό πρωτόκολλο, αυτές οι νεώτερες μέθοδοι πρώτα χρησιμοποιούν την παλαιότερη ανοικτού συστήματος πιστοποίηση, έπειτα δημιουργούν μια νέα συσχέτιση ασφάλειας μεταξύ των δύο κόμβων κατά τη διάρκεια της φάσης συσχέτισης που ακολουθεί αμέσως. *Η συσχέτιση ασφάλειας περικλείει και την πιστοποίηση και την κρυπτογράφηση* και μπορεί να αντιμετωπιστεί από έναν ξεχωριστό 802.1x εξυπηρετητή πιστοποίησης (*authentication server*), ή να βασίζεται στην επίδειξη της κατοχής του σωστού προ-κοινού κλειδιού (*Pre-Shared key, PSK*). Το πρότυπο υποστηρίζει επίσης ένα προαιρετικό μέτρο της προ-πιστοποίησης (*pre-authentication*) για roaming σε ένα ESS από τους σταθμούς που πιστοποιήθηκαν ήδη με το δίκτυο.

3.3.2 Κρυπτογράφηση WEP (Wired Equivalent Privacy)

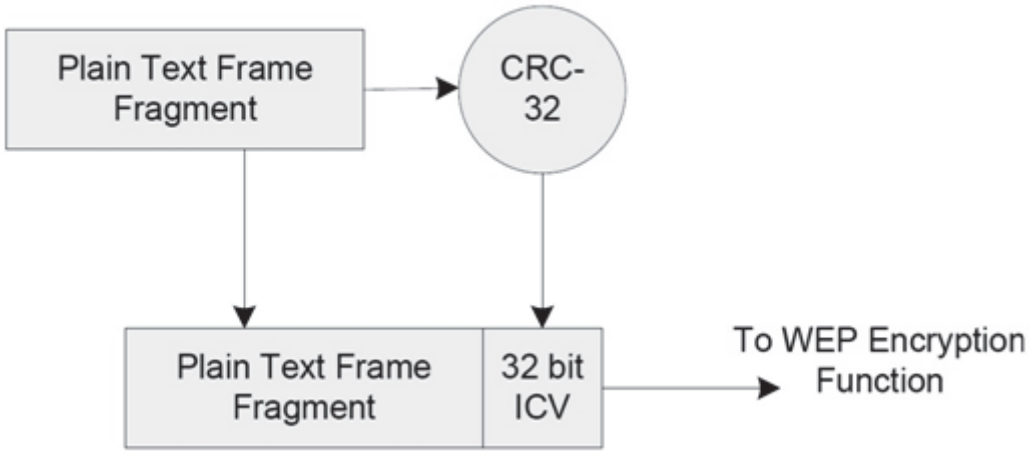
Η πιο γνωστή επιλογή παροχής ασφάλειας, που ορίστηκε για τα ασύρματα δίκτυα από το αρχικό πρότυπο 802.11, είναι το WEP. Με την επιλογή του WEP ένα κοινό κλειδί μοιράζεται ανάμεσα στο σημείο πρόσβασης και στους ασύρματους πελάτες του. Εάν επιθυμούμε εμπιστευτικότητα, μπορούμε να χρησιμοποιήσουμε την επιλογή του WEP και να κρυπτογραφήσουμε τα δεδομένα πριν αυτά σταλούν.
Το WEP χειρίζεται ταυτόχρονα τόσο την προστασία όσο και την ακεραιότητα των δεδομένων.

Κατακερματισμός
Το πακέτο δεδομένων, που μεταδίδεται, περιέχει τις κατάλληλες πληροφορίες για την αποστολή του και καλείται MSDU (*Mac Service Data Unit*). Το πακέτο αυτό χωρίζεται σε

μικρότερα κομμάτια, με τη διαδικασία του κατακερματισμού (*fragmentation*). Κάθε κομμάτι ακολουθεί τη δική του πορεία στην κρυπτογράφηση WEP. Επομένως το αρχικό πακέτο δεδομένων χωρίζεται σε μικρότερα μηνύματα, MPDU (Mac Protocol Data Unit) στα οποία προστίθενται και άλλα bytes. Έπειτα, τα δεδομένα καταφθάνουν στο επίπεδο MAC του προορισμού και σκοπός είναι να περάσουν στο λειτουργικό σύστημα και να μετατεθούν στην κατάλληλη εφαρμογή.

Εξασφάλιση Ακεραιότητας Δεδομένων

Η εξασφάλιση της ακεραιότητας του μηνύματος στο WEP βασίζεται στον αλγόριθμο *CRC-32*. Ο αλγόριθμος CRC-32 εφαρμόζεται στο απλό κείμενο και παράγει την τιμή ελέγχου ακεραιότητας (ICV - *Integrity Check Value*) μήκους 4 bytes (32bits) και συνεισφέρει στην αποφυγή της τροποποίησης του μηνύματος κατά τη μετάδοση. Η τιμή αυτή προστίθεται στο τέλος του πλαισίου πριν από την επεξεργασία για μετάδοση. Αυτή η πληροφορία αργότερα κρυπτογραφείται μαζί με το απλό κείμενο, με τον RC4 αλγόριθμο. Η κρυπτογράφηση του ICV μαζί με το απλό κείμενο κάνει δύσκολη την τροποποίηση των κρυπτογραφημένων δεδομένων και του ICV, με τέτοιο τρόπο ώστε το νέο ICV να ανταποκρίνεται στα τροποποιημένα δεδομένα. Αν αλλάξει έστω και ένα bit από το μήνυμα, ο παραλήπτης θα υπολογίσει διαφορετική τιμή του CRC από αυτή που μεταφέρει ο πομπός και επομένως θα απορρίψει το μήνυμα. Παρόλο που ο έλεγχος εντοπίζει τυχαία λάθη, δεν είναι δυνατόν να αναγνωρίσει σκόπιμα λάθη, καθώς ο εισβολέας είναι σε θέση να υπολογίσει τη νέα τιμή CRC και να αντικαταστήσει την αρχική. Ο αλγόριθμος CRC-32 περιγράφεται στο RFC 3309.



Εικόνα 18 Εξασφάλιση ακεραιότητας δεδομένων με τον αλγόριθμο CRC-32.

Αλγόριθμος Κρυπτογράφησης

Το WEP κάνει χρήση του αλγόριθμου κρυπτογράφησης RC4. Ο συγκεκριμένος αλγόριθμος είναι απλός στην υλοποίηση του και αρκετά ισχυρός. Οι αδυναμίες του WEP δεν οφείλονται στον ίδιο τον RC4 αλλά στον τρόπο χρήσης του μέσα στον WEP.

Ο RC4 είναι ένας συμμετρικός αλγόριθμος (χρησιμοποιεί το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση) και είναι αλγόριθμος συρμού *(stream cipher)*. Αυτό σημαίνει ότι το κλειδί θεωρείται ως ένας συρμός (*stream*) από bits και εφαρμόζεται στο απλό κείμενο (*Plain Text*) bit προς bit για να παραχθεί το κρυπτογραφημένο κείμενο (*Cipher Text*). Αυτό έχει το πλεονέκτημα ότι μπορεί να εφαρμοστεί σε κείμενο μεταβλητού μεγέθους, σε αντίθεση με τους *Block Ciphers* που εφαρμόζονται σε κομμάτια *(blocks)* κειμένου σταθερού μεγέθους (συνήθως 64 bits).

Ο RC4 περιλαμβάνει δύο φάσεις: Την παραγωγή του συρμού κλειδιού *(Key Stream)* και την κρυπτογράφηση του καθαρού κειμένου.

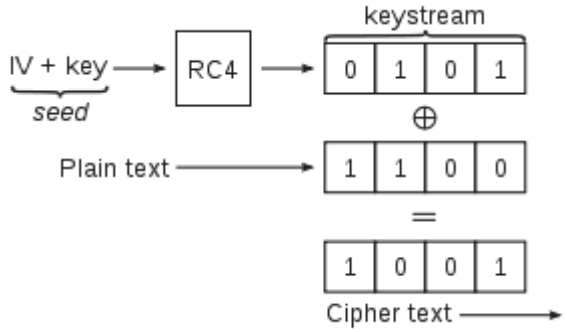
Για την παραγωγή του *keystream* ο RC4 δέχεται σαν είσοδο ένα *seed* και χρησιμοποιεί μια διαδικασία παραγωγής ψευδοτυχαίων αριθμών. Με βάση την ιδιότητα της XOR:

A (XOR) B= C, τότε C (XOR) B = A

Ο αλγόριθμος RC4 εκμεταλλεύεται την παραπάνω ιδιότητα ως εξής:

Κρυπτογράφηση: **plaintext (XOR) keystream = cipher text**
Αποκρυπτογράφηση: **cipher text (XOR) keystream = plaintext**

Η τυχαία ακολουθία κλειδιού ορίζεται από το IV και ονομάζεται ψευδοτυχαία διότι θα πρέπει να δείχνει τυχαία σε εισβολέα αλλά τα δυο άκρα της ζεύξης που επικοινωνούν θα πρέπει να παράγουν την ίδια τυχαία τιμή για κάθε byte που επεξεργάζονται.
Η πράξη XOR υλοποιείται πολύ εύκολα οπότε, το πιο δύσκολο κομμάτι αποτελεί ο υπολογισμός μιας καλής ψευδοτυχαίας ροής bytes. Ουσιαστικά χρειαζόμαστε ένα ψευδοτυχαίο byte για κάθε byte του μηνύματος προς κρυπτογράφηση.



Εικόνα 19 Παραγωγή του κρυπτογραφημένου κειμένου με τον αλγόριθμο RC4.

Seed και Μήκος Κλειδιού
Το WEP seed παράγεται βάση του IV (Initialization Vector) μήκους 24 bits και ενός κλειδιού 40 bits που παρέχεται από τον χρήστη. Ο συνδυασμός των δύο αυτών δίνει τον σπόρο μήκους 64 bits. Διάφορες υλοποιήσεις έχουν αυξήσει το μήκος του κλειδιού σε 104-bit, δίνοντας ένα μήκος σπόρου 128-bit.
Σημείωση: Ο RC4 μπορεί να χρησιμοποιήσει μήκη κλειδιών έως 256 bytes. Τα 24 bits είναι για το IV, αφήνοντας 232 πραγματικά bits για την προστασία. Όμως για το πρότυπο 802.11 επιλέχτηκε μήκος κλειδιού 40 bits εξαιτίας απαγορεύσεων εξαγωγής αλγορίθμων κρυπτογράφησης.

Τα κλειδιά που χρησιμοποιούνται στο WEP
Τα κλειδιά κρυπτογράφησης που χρησιμοποιούνται στο WEP έχουν τα ακόλουθα χαρακτηριστικά:

- **Σταθερό μήκος**: Συνήθως 40 ή 104 bits.
- **Στατικά:** Δεν μεταβάλλεται η τιμή του κλειδιού εφόσον δεν αλλάξουν οι ρυθμίσεις.
- **Διαμοιραζόμενα (shared):** Τόσο το σημείο πρόσβασης όσο και η κινητή συσκευή διαθέτουν αντίγραφο των ίδιων κλειδιών.
- **Συμμετρικά:** Χρήση του ίδιου κλειδιού για κρυπτογράφηση και αποκρυπτογράφηση των πληροφοριών.

Κάθε σταθμός μπορεί να έχει τέσσερα κλειδιά ταυτόχρονα και να χρησιμοποιεί ένα από αυτά σε κάθε αποστολή ή λήψη πλαισίου, για κρυπτογράφηση και αποκρυπτογράφηση. Το πιο κάθε φορά χρησιμοποιείται ορίζεται σε ένα πεδίο του κρυπτογραφημένου πλαισίου που λέγεται αριθμός κλειδιού (*KeyID*). Η αντιστοιχία και η αρίθμηση θα πρέπει να είναι η ίδια μεταξύ των σταθμών. Η δυνατότητα παράλληλης χρήσης περισσοτέρων κλειδιών αυξάνει την συνολική ασφάλεια της επικοινωνίας. Η καλύτερη δημόσια επίθεση ενάντια στο WEP μπορεί να ανακτήσει το κλειδί σε μερικά δευτερόλεπτα. Εφόσον γίνεται ήδη χρήση και των τεσσάρων κλειδιών, ο χρόνος που απαιτείται για την εύρεση αυτών με τη μέθοδο της εξαντλητικής αναζήτησης (*brute force*) τετραπλασιάζεται.

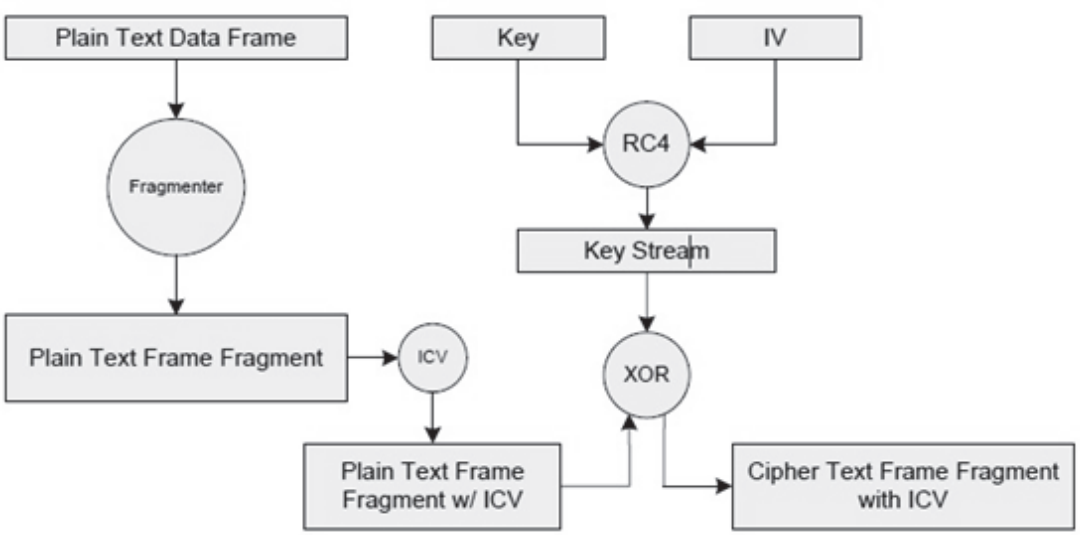
Παραγωγή του IV (Initialization Vector – Διάνυσμα Αρχικοποίησης)
Η ύπαρξη του IV είναι αναγκαία προκειμένου το ίδιο κλειδί με τα ίδια δεδομένα να μην παράγουν το ίδιο κρυπτογραφημένο κείμενο. Κάτι τέτοιο θα επέτρεπε την εφαρμογή ορισμένων στατιστικών μεθόδων προκειμένου να ανακαλυφθεί το απλό κείμενο (*residual effect*).
Το IV αλλάζει για κάθε πακέτο που αποστέλλεται και συνδυάζεται με το μυστικό κλειδί. Έτσι ακόμα και εάν τα αρχικά δεδομένα είναι ίδια, η κρυπτογραφημένη μορφή τους είναι πάντα διαφορετική. Το IV δεν είναι μυστικό, ενώ στέλνεται σε μη κρυπτογραφημένη μορφή σε κάθε μετάδοση ώστε ο παραλήπτης να είναι σε θέση να αποκρυπτογραφήσει την πληροφορία χρησιμοποιώντας την αντίστοιχη τιμή IV.

Διανομή κλειδιού
Το βασικότερο μειονέκτημα του WEP είναι πρόβλημα της διανομής του κλειδιού. Τα μυστικά κομμάτια του κλειδιού WEP πρέπει να μοιραστούν σε όλους τους σταθμούς που συμμετέχουν στο δίκτυο. Το 802.11 πρότυπο, δεν μας παρέχει ένα μηχανισμό παραγωγής κλειδιού έτσι ο καθένας πρέπει να δακτυλογραφεί το κλειδί στον οδηγό της συσκευής.
Οι δυσκολίες ενός τέτοιου πρωτοκόλλου είναι:

- Τα κλειδιά δεν είναι ουσιαστικά μυστικά, αφού εισάγονται στους οδηγούς software ή firmware στην ασύρματη κάρτα. Έτσι ένας τοπικός χρήστης μπορεί να έχει πρόσβαση στο μυστικό κλειδί.
- Εάν τα κλειδιά είναι προσιτά στους χρήστες, αυτά θα πρέπει να αλλάζουν συχνά. Η γνώση κλειδιών WEP επιτρέπει σε έναν χρήστη να φτιάξει έναν 802.11 σταθμό να ελέγχει παθητικά και να αποκρυπτογραφεί την κυκλοφορία χρησιμοποιώντας το μυστικό κλειδί.
- Οι επιχειρήσεις με μεγάλο αριθμό εξουσιοδοτημένων χρηστών πρέπει να δημοσιεύσουν το κλειδί στους χρήστες και έτσι δεν υφίσταται πλέον η μυστικότητα του κλειδιού.

Σύνθεση Πλαισίου
Ο αλγόριθμος RC4 παράγει βάση του σπόρου και του αρχικών δεδομένων, τα κρυπτογραφημένα δεδομένα, τα οποία μαζί με το IV και το Key ID τοποθετούνται στο πλαίσιο προς αποστολή. Πρέπει να τονιστεί ότι κρυπτογραφημένα είναι μόνο τα δεδομένα και το ICV, ενώ όλα τα υπόλοιπα στέλνονται χωρίς κρυπτογράφηση.

Η κρυπτογράφηση
1. Το μυστικό κλειδί συνδέεται με το *διάνυσμα έναρξης* (IV) και το αποτέλεσμα τους εισάγεται στον αλγόριθμο RC4. Ο αλγόριθμος RC4 παράγει μια ακολουθία κλειδιού *keystream.*
2. Για προστασία από αναρμόδια τροποποίηση δεδομένων, εφαρμόζεται ο αλγόριθμος ακεραιότητας επάνω στα δεδομένα και παράγεται το ICV.
3. Η κρυπτογράφηση ολοκληρώνεται με τη λογική πράξη του αποκλειστικού Η (XOR) μεταξύ της ακολουθίας κλειδιού και των δεδομένων που μετατράπηκαν σε ICV.

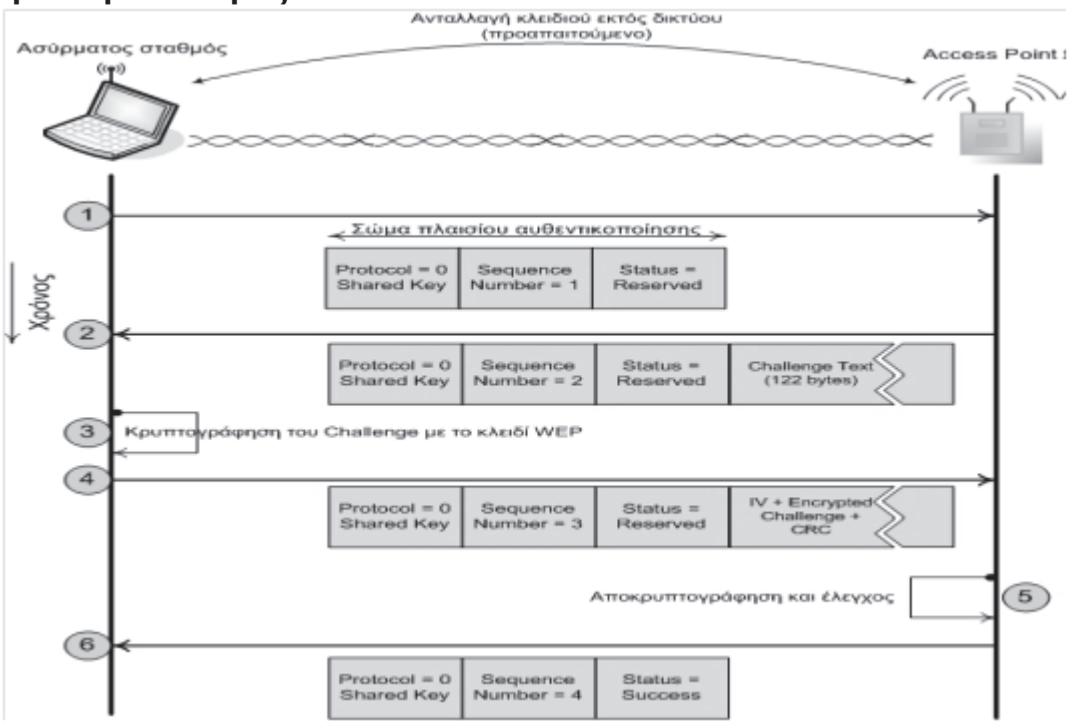


Εικόνα 20 Διαδικασία κρυπτογράφησης WEP.

Αποκρυπτογράφηση

Κατά την λήψη του πλαισίου ακολουθείται η αντίστροφη διαδικασία. Εντοπίζεται το κλειδί που χρησιμοποιήθηκε βάσει του πεδίου key ID, παράγεται το keystream και αποκρυπτογραφείται το περιεχόμενο του πλαισίου. Όταν ο παραλήπτης αποκρυπτογραφήσει το πακέτο υπολογίζει ξανά την τιμή ελέγχου ακεραιότητας ICV και τη συγκρίνει με αυτή που περιείχε το πακέτο που παρέλαβε. Αν οι δύο τιμές ταυτίζονται, τότε θεωρείται ότι το πακέτο είναι έγκυρο.

Επαλήθευση ταυτότητας



Εικόνα 21 Επαλήθευση ταυτότητας στο WEP.

Βήμα 1ο: Ο σταθμός που επιχειρεί να πιστοποιηθεί, στέλνει αίτημα πιστοποίησης στο AP (ή άλλο σταθμό εάν πρόκειται για ad-hoc δίκτυο).
Βήμα 2ο: Το AP απαντάει με μία τυχαία συμβολοσειρά (*Challenge Text*). Η τυχαία συμβολοσειρά αποσκοπεί στην αποφυγή της επίθεσης *Off-line Brute Force*.

Βήμα 3ο: Ο σταθμός κρυπτογραφεί την τυχαία συμβολοσειρά με το WEP κλειδί που διαθέτει.
Βήμα 4ο: Ο σταθμός αποστέλλει το κρυπτογραφημένο αποτέλεσμα στο AP.
Βήμα 5ο: Το AP αποκρυπτογραφεί την κρυπτογραφημένη τυχαία συμβολοσειρά με το δικό του WEP κλειδί. Αν η αποκρυπτογραφημένη τυχαία συμβολοσειρά είναι ίδια με την αρχική που είχε αποστείλει, συμπεραίνει ότι τα δύο κλειδιά είναι ίδια.
Βήμα 6ο: Αν στο βήμα 5 αποδείχτηκε ότι τα κλειδιά είναι ίδια, τότε το AP πιστοποιεί τον σταθμό.

Ωστόσο η μέθοδος αυτή αποτελεί πολύ μεγάλο πρόβλημα για την ασφάλεια της κρυπτογράφησης καθώς δίδει πληροφορίες σε κακόβουλους χρήστες, που παρακολουθούν την επικοινωνία τόσο της κρυπτογραφημένης αλλά και της μη κρυπτογραφημένης πληροφορίας.

Αδυναμίες του WEP
Παρακάτω αναφέρονται αναφορικά τα σημεία στα οποία εντοπίστηκαν αδυναμίες:

- Η επιλογή του IV καθώς και η έλλειψη μυστικότητάς του δίνει την ευκαιρία σε έναν εισβολέα να επιτεθεί σε ένα σχετικά αδύναμο κλειδί.
- Η μετάδοση του IV
- Η ύπαρξη αδύναμων IV
- Η ύπαρξη αδύναμων κλειδιών RC4
- Ο μηχανισμός CRC-32
- Η απουσία μηχανισμού αυτόματης διαμοίρασης των κλειδιών
- Η απουσία μηχανισμού αμοιβαίας πιστοποίησης μεταξύ των κόμβων. Το κλειδί που χρησιμοποιείται στη διαδικασία πιστοποίησης είναι το ίδιο με αυτό της κρυπτογράφησης, δίνοντας έτσι την ευκαιρία σε έναν επιτιθέμενο να αποκτήσει στοιχεία.

3.3.3 Wi-Fi Protected Access (WPA)

Για να διεκπεραιωθούν οι ευπάθειες του WEP, η IEEE εγκαθίδρυσε την ομάδα εργασίας 802.11 Working Group το 2001. Βασισμένη στα αρχικά σχέδια του Working Group, η *Wi-Fi Alliance Trade Group* εγκαθίδρυσε το WPA ως προσωρινή λύση που θα μπορούσε να επιτευχθεί με τον υπάρχοντα εξοπλισμό χρησιμοποιώντας μόνο ενημερώσεις λογισμικού και firmware. Το WPA εξασφαλίζεται σε όλες τις εκδόσεις 802.11. Ως υποσύνολο του 802.11i (γνωστού επίσης ως WPA2), το WPA είναι και προς τα εμπρός και προς τα πίσω συμβατό. Το WPA αυξάνει το επίπεδο προστασίας των δεδομένων που μεταδίδονται στον αέρα και τον έλεγχο πρόσβασης στα Wi-Fi δίκτυα. Παρέχει ισχυρή κρυπτογράφηση δεδομένων και προσθέτει την πιστοποίηση χρήστη που έλειπε κατά ένα μεγάλο μέρος από το WEP. Έτσι διαβεβαιώνει ότι τα δεδομένα στα δίκτυα Wi-Fi θα παραμείνουν προστατευμένα και ότι μόνο εξουσιοδοτημένοι χρήστες θα έχουν πρόσβαση στο δίκτυο.
Επιπλέον, προσφέρει καλύτερης κατηγορίας ασφάλεια στις επιχειρήσεις καθώς και στα δίκτυα μικρών γραφείων και σπιτιών (*small office / home office*, SOHO). Τα σημεία πρόσβασης (APs) απαιτούν βελτίωση λογισμικού. Οι τερματικοί σταθμοί πελατών απαιτούν βελτίωση λογισμικού στην NIC και μια πιθανή βελτίωση λογισμικού στο λειτουργικό σύστημα. Για τα δίκτυα επιχειρήσεων, η εφαρμογή του WPA περιλαμβάνει την ανάπτυξη μιας υποδομής 802.1x, δηλαδή:

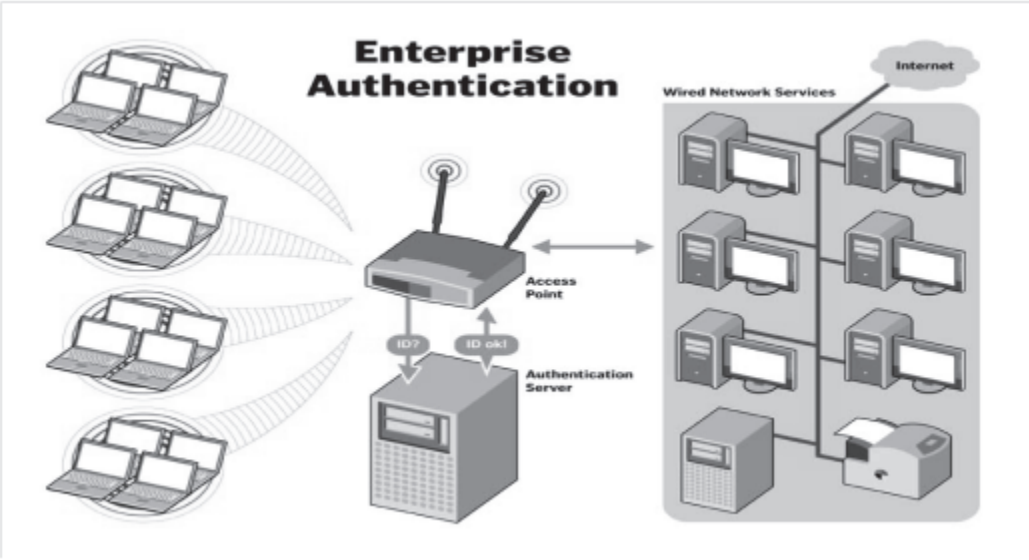
- Επιλογή των τύπων EAP που θα υποστηριχθούν στη NIC του πελάτη και στους εξυπηρετητές πιστοποίησης.
- Επιλογή και ανάπτυξη εξυπηρετητή πιστοποίησης, συνήθως έναν RADIUS server (*Remote Authentication Dial-In User Service*).
- Βελτίωση των APs με WPA ή της αγοράς νέων APs με WPA εγκατεστημένο.
- Βελτίωση της NIC του WLAN-πελάτη με WPA ή αγοράς νέας ασύρματης NIC με WPA εγκατεστημένο.

Το WPA εφοδιάζει τους χρήστες σπιτιού ή SOHO, που δεν έχουν διαθέσιμους τέτοιους εξυπηρετητές, με έναν ειδικό τρόπο που χρησιμοποιεί έναν κοινό κωδικό πρόσβασης που ενεργοποιεί την προστασία WPA.
Τα ενισχυμένα σχέδια κρυπτογράφησης και πιστοποίησης WPA είναι ιδανικά για δημόσια hotspots δεδομένου ότι παρέχουν ένα υψηλό επίπεδο ασφάλειας για τους φορείς παροχής υπηρεσιών και τους κινητούς χρήστες που δεν χρησιμοποιούν συνδέσεις VPN.

Μηχανισμός ασφάλειας στο WPA
Μια από τις κύριες αδυναμίες WEP είναι ότι χρησιμοποιεί ένα μικρό στατικό κλειδί για να αρχίσει την κρυπτογράφηση. Αυτό το 40bit κλειδί εισάγεται χειροκίνητα στο AP και σε όλους τους πελάτες που επικοινωνούν με το AP. Δεν αλλάζει εκτός αν ξαναεισαχθεί χειροκίνητα σε όλες τις συσκευές, μια τρομακτικά εντατική εργασία σε έναν μεγάλο οργανισμό.
Οι κρυπτογραφικές μελέτες έχουν δείξει ότι ένας εισβολέας που συλλέγει αρκετά δεδομένα μπορεί να απειλήσει ένα δίκτυο WEP με τρεις τρόπους: με την παρεμπόδιση και την αποκρυπτογράφηση των δεδομένων που μεταδίδονται στον αέρα, με την αλλαγή των δεδομένων που επικοινωνούν, και με πρόβλεψη του κλειδιού WEP αποκτώντας μη εξουσιοδοτημένη πρόσβαση σε υπηρεσίες του δικτύου και Διαδικτύου. Αυτό θα μπορούσε να ολοκληρωθεί σε ζήτημα ωρών σε ένα πολυάσχολο, εταιρικό WLAN.
Επίσης, το WEP στερείται την πιστοποίηση για να εξασφαλίσει ότι μόνο εκείνοι που πρέπει να είναι στο δίκτυο έχουν την άδεια να έχουν πρόσβαση σε αυτό.
Το WPA εξετάζει αυτά τα ελαττώματα και φέρνει πρόσθετα μέτρα προστασίας στην ασφάλεια WI-Fi. Χρησιμοποιεί ένα πολύ ενισχυμένο σχέδιο κρυπτογράφησης, το πρωτόκολλο TKIP (*Temporal Key Integrity Protocol*). Μαζί με την πιστοποίηση 802.1x/EAP, το TKIP υιοθετεί μια ιεραρχία κλειδιού που ενισχύει πολύ την προστασία. Προσθέτει επίσης έναν έλεγχο ακεραιότητας μηνυμάτων (Message Integrity Check, MIC, μερικές φορές ο αποκαλούμενος «Michael») για προστασία από τις παραποιήσεις πακέτων.

Κρυπτογράφηση και ακεραιότητα μηνυμάτων
Το TKIP αυξάνει το μέγεθος του κλειδιού από τα 40 στα 128 bit και αντικαθιστά το μοναδικό στατικό κλειδί του WEP με κλειδιά που παράγονται δυναμικά και διανέμονται από τον εξυπηρετητή πιστοποίησης (*authentication server*). Το TKIP χρησιμοποιεί μια ιεραρχία κλειδιού και μια μεθοδολογία διαχείρισης κλειδιού που αφαιρεί την προβλεψιμότητα επάνω στην οποία στηρίζονται οι εισβολείς για να εκμεταλλευτούν το κλειδί WEP.
Για να το κάνει αυτό, το TKIP ισχυροποιεί τη δομή 802.1x/EAP. Ο εξυπηρετητής πιστοποίησης, αφού αποδεχτεί τα πιστοποιητικά ενός χρήστη, χρησιμοποιεί τη δομή 802.1x για να παράγει έναν μοναδικό κύριο (*master*), ή «*pair-wise*» κλειδί για αυτή την σύνοδο υπολογισμού. Το TKIP διανέμει αυτό το κλειδί στον πελάτη και στο AP και εγκαθιστά μια ιεραρχία κλειδιού και ένα σύστημα διαχείρισης, χρησιμοποιώντας το pair-wise κλειδί για να παράγει δυναμικά τα μοναδικά κλειδιά κρυπτογράφησης δεδομένων για να κρυπτογραφήσει το κάθε πακέτο δεδομένων που επικοινωνεί ασύρματα κατά τη διάρκεια της συνόδου εκείνου του χρήστη. Η ιεραρχία του κλειδιού του TKIP ανταλλάσει το μοναδικό στατικό κλειδί του WEP για 500 τρισεκατομμύρια περίπου πιθανά κλειδιά που μπορούν να χρησιμοποιηθούν σε ένα πακέτο δεδομένων.
Ο έλεγχος ακεραιότητας μηνυμάτων (*Message Integrity Check*, MIC) έχει ως σκοπό να αποτρέψει έναν επιτιθέμενο από την σύλληψη των πακέτων δεδομένων, την αλλαγή τους και την εκ νέου αποστολή τους. Ο MIC παρέχει μια ισχυρή μαθηματική συνάρτηση με την οποία ο αποστολέας και λήπτης υπολογίζει ξεχωριστά και στη συνέχεια συγκρίνουν το MIC. Εάν δεν ταιριάζουν, τα δεδομένα υποτίθεται ότι έχουν πειραχτεί και το πακέτο απορρίπτεται.
Με την μεγάλη επέκταση του μεγέθους των κλειδιών, τον αριθμό των κλειδιών σε χρήση και τη δημιουργία μηχανισμού ελέγχου, το TKIP ενισχύει την πολυπλοκότητα και τη δυσκολία στην αποκωδικοποίηση δεδομένων όσον αφορά ένα δίκτυο WI-Fi. Το TKIP αυξάνει πολύ τη δύναμη και πολυπλοκότητα της ασύρματης κρυπτογράφησης, που κάνει δύσκολο σε έναν εν δυνάμει εισβολέα να σπάσει ένα δίκτυο WI-Fi.
Σχεδιασμένο για να επεκταθεί με τις υπάρχουσες επικυρωμένες συσκευές WI-Fi, το TKIP περιλαμβάνεται και στα WPA2 πρότυπα.

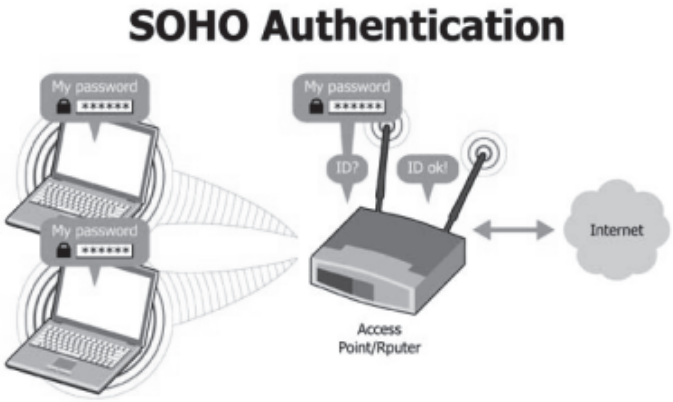
Πιστοποίηση
Το WPA χρησιμοποιεί πιστοποίηση 802.1x με ένα από τα πρωτόκολλα EAP που είναι διαθέσιμα σήμερα. Το 802.1x είναι μια μέθοδος ελέγχου πρόσβασης στο δίκτυο, βασισμένη σε θύρες (*port-based*), τόσο για ενσύρματα όσο και για ασύρματα δίκτυα. Υιοθετήθηκε ως πρότυπο από την IEEE τον Αύγουστο του 2001.
Το EAP χειρίζεται την παρουσίαση των πιστοποιητικών των χρηστών υπό μορφή ψηφιακών πιστοποιητικών, μοναδικών ονομάτων χρηστών (*usernames*) και κωδικών πρόσβασης (*passwords*), έξυπνων καρτών, ασφαλών IDs, ή οποιοδήποτε άλλο πιστοποιητικό ταυτότητας αναπτύξει ο διαχειριστής δικτύου.
Το WPA είναι ευέλικτο και στον τύπο πιστοποιητικών που χρησιμοποιούνται και στην επιλογή του τύπου EAP. Ένας ευρύς αριθμός, βασισμένων στο πρότυπο, εφαρμογών EAP είναι διαθέσιμος για χρήση. Με το EAP, το 802.1x δημιουργεί μια δομή στην οποία οι τερματικοί σταθμοί πελατών πιστοποιούνται αμοιβαία με τον εξυπηρετητή πιστοποίησης. Αυτή η αμοιβαία πιστοποίηση αποτρέπει τους χρήστες από τυχαία σύνδεση με ένα *rogue* ή μη εξουσιοδοτημένο AP στο δίκτυο Wi-Fi και επίσης εξασφαλίζει ότι οι χρήστες που έχουν πρόσβαση στο δίκτυο είναι αυτοί που θα έπρεπε να είναι εκεί. Όταν ένας χρήστης ζητά πρόσβαση στο δίκτυο, ο πελάτης στέλνει τα πιστοποιητικά του χρήστη στον εξυπηρετητή πιστοποίησης μέσω του AP. Εάν ο server δέχεται τα πιστοποιητικά του χρήστη, το κύριο κλειδί (*master key*) TKIP στέλνεται και στον πελάτη και στο AP. Η χειραψία τεσσάρων καταστάσεων (*four-way handshake*), αποτελεί μια διαδικασία στην οποία ο πελάτης και το AP αναγνωρίζουν ο ένας τον άλλον και εγκαθιστούν τα κλειδιά, ολοκληρώνοντας έτσι τη διαδικασία.



Εικόνα 22 Μηχανισμός WPA πιστοποίησης σε επιχειρησιακό περιβάλλον.

Ασφάλεια σπιτιών και μικρών γραφείων (Small Office, Home Office **- SOHO)**
Οι χρήστες σε περιβάλλοντα μικρών γραφείων και γραφείων σπιτιών στερούνται προϋπολογισμό και προσωπικό για να εγκαταστήσουν και να διατηρήσουν RADIUS servers. Το WPA προσφέρει σε αυτούς τους χρήστες τα οφέλη της ασφάλειάς του μέσω της χρήσης προ-μοιραζόμενου κλειδιού (*pre-shared key*, PSK) ή κωδικού πρόσβασης.
Το PSK παρέχει σε SOHO περιβάλλοντα την ίδια ισχυρή κρυπτογράφηση TKIP, κατασκευή κλειδιού για κάθε πακέτο (*per-packet*), και διαχείριση κλειδιού που παρέχει το WPA στην επιχείρηση.
Η διαφορά είναι ότι εδώ, ένας προσωπικός κωδικός πληκτρολογείται με το χέρι στις συσκευές πελατών και στο AP ή την ασύρματη πύλη (*gateway*) και χρησιμοποιείται για πιστοποίηση. Το PSK παρέχει μια χρήσιμη εναλλακτική λύση για τα μικρότερα δίκτυα αν και δεν αποτελεί ισχυρή διαδικασία πιστοποίησης όπως τα RADIUS, EAP και 802.1x.
Η αναβάθμιση του WPA στο σπίτι και τα μικρά περιβάλλοντα γραφείων είναι απλή.
Τα βήματα είναι:

- Αναβάθμιση APs με το λογισμικό WPA.
- Αναβάθμιση των NICs των WLAN με WPA λογισμικό.
- Διαμόρφωση του PSK, ή του κύριου κωδικού πρόσβασης, στο AP.
- Διαμόρφωση του PSK στους τερματικούς σταθμούς πελατών.



Εικόνα 23 Μηχανισμός WPA πιστοποίησης σε σπίτι ή γραφείο.

3.3.4 Wi-Fi Protected Access Version 2 (WPA2)

Η *Wi-Fi Alliance* αναφέρεται στην εφαρμογή πιο γερών χαρακτηριστικών ασφαλείας που καθορίζονται στο έγγραφο 802.11i-2004, το οποίο εισήγαγε την έννοια *Robust Security Network Association* (RSNA), ως WPA2. Η πιο ισχυρή κρυπτογράφηση απαιτεί ανάπτυξη του υλικού καθώς δεν υποστηρίζεται από παλαιότερο εξοπλισμό.
Το WPA2 είναι η σημερινή παραγωγή ασφάλειας στα δίκτυα Wi-Fi. Θεμελιώνεται με δύο βασικούς μηχανισμούς:

1) AES (*Advanced Encryption Standard*): το πρωτόκολλο κρυπτογράφησης που χρησιμοποιείται από τις Ηνωμένες Πολιτείες και άλλες κυβερνήσεις, για να προστατεύουν εμπιστευτικές και απόρρητες πληροφορίες, και από τις επιχειρήσεις για να παρέχουν ασφάλεια στα WLANs.
2) IEEE 802.1x: ένα ευρέως χρησιμοποιημένο πρότυπο στα εταιρικά δίκτυα για να παρέχει γερή επικύρωση και περίπλοκα χαρακτηριστικά γνωρίσματα ελέγχου προσπέλασης δικτύων.

Το WPA2 παρέχει 128-bit AES block cipher[3] κρυπτογράφηση με βάση το πρωτόκολλο CCMP (*Message Authentication Code Protocol*). Παρέχει επίσης αμοιβαία πιστοποίηση με προ-μοιραζόμενο κλειδί (PSK στον Personal τρόπο) και με IEEE 802.1x/EAP (στον Enterprise τρόπο).

<u>Τεχνολογική επισκόπηση του WPA2</u>

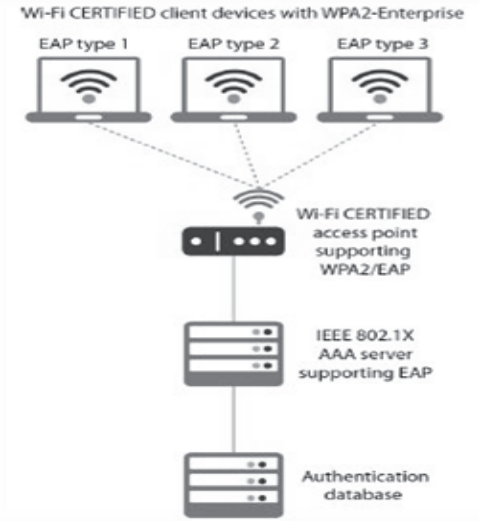
1 Αμοιβαία πιστοποίηση (*Mutual Authentication*): Το WPA2 χρησιμοποιεί IEEE 802.1x (*WPA2-Enterprise*) και PSK (*WPA2-Personal*) για να παρέχει αμοιβαία πιστοποίηση. Με τη μονόδρομη πιστοποίηση, η συσκευή πελάτη στέλνει τα πιστοποιητικά της και, εάν η πρόσβαση εξουσιοδοτείται, η συσκευή πελάτη συνδέεται με το δίκτυο. Η αμοιβαία πιστοποίηση απαιτεί η συσκευή πελάτη να επαληθεύσει το πιστοποιητικό δικτύου προτού εγκαταστήσει τη σύνδεση, για να αποτρέψει το χρήστη από τη σύνδεση με μη εξουσιοδοτημένα σημεία πρόσβασης.

[3]**Block cipher** είναι ένας ντετερμινιστικός αλγόριθμος που λειτουργεί στις καθορισμένου μήκους ομάδες bits, αποκαλούμενες blocks, με έναν αμετάβλητο μετασχηματισμό που διευκρινίζεται από ένα συμμετρικό κλειδί και αποτελούν σημαντικά στοιχειώδη συστατικά στον σχεδιασμό πολλών κρυπτογραφικών πρωτοκόλλων, και χρησιμοποιούνται ευρέως για να εφαρμόσουν την κρυπτογράφηση μαζικών δεδομένων.

2 Ισχυρή κρυπτογράφηση (*Strong Encryption*): Ο AES ορίζεται ως ένα ομοσπονδιακό πρότυπο επεξεργασίας πληροφοριών (*Federal Information Processing Standard*, FIPS Publication 197) και είναι ο πρώτος δημόσια διαθέσιμος μηχανισμός κρυπτογράφησης που καλύπτει τις απαιτήσεις της Αμερικανικής κυβέρνησης για την προστασία ευαίσθητων και ταξινομημένων πληροφοριών. Μέχρι σήμερα, ο AES έχει αποδειχθεί εξαιρετικά ανθεκτικός παρά το μεγάλο αριθμό των δημοσιευμένων επιθέσεων που προκαλούνται από την ευρεία υιοθέτηση του. Τα δεδομένα που ταξιδεύουν μέσω ενός WPA2 δικτύου κρυπτογραφούνται χρησιμοποιώντας τον αλγόριθμο CCMP με AES, τα οποία παρέχουν μαζί προηγμένη μέθοδο κρυπτογράφησης δεδομένων που είναι διαθέσιμη. Η υποστήριξη AES απαιτείται από πολλά πρωτόκολλα και εφαρμογές που χρησιμοποιούνται παγκοσμίως στα δίκτυα επιχειρήσεων.
3 Διαλειτουργικότητα (*Interportability*): Το WPA2 είναι μια λύση, βασισμένη στο πρότυπο, που υποστηρίζεται από όλο τον Wi-Fi επικυρωμένο εξοπλισμό που έχει υποβληθεί σε εξέταση από το 2006. Το WPA2 μπορεί να ενεργοποιηθεί μέσα σε οποιαδήποτε σύνοδο στην οποία το σημείο πρόσβασης και η συσκευή πελάτη το υποστηρίζουν, ανεξάρτητα από τα εμπορικά ονόματα (*brands*) του εξοπλισμού που εμπλέκονται. Αυτό επεκτείνει πολύ τη διαθεσιμότητα του WPA2 και δίνει την σιγουριά στους διαχειριστές δικτύου και στους χρήστες ότι τα δίκτυα τους, οι συσκευές, και οι ροές δεδομένων τους μπορούν να προστατευθούν παντού.
4 Ευκολία στη χρήση (*Ease of use*): Το WPA2 είναι όχι μόνο ένα ισχυρό εργαλείο για να προστατεύσει τους χρήστες Wi-Fi, αλλά και εύκολο να ενεργοποιηθεί. Το 2007 η Wi-Fi Alliance εισήγαγε ένα χωριστό πρόγραμμα πιστοποίησης, το *Wi-Fi Protected Setup*, για να απλοποιήσει τη διαμόρφωση του WPA2 και για να επιταχύνει την υιοθέτησή του στα οικιακά δίκτυα.

WPA2-Enterprise και WPA2-Personal

Το WPA2 λειτουργεί σε δύο τρόπους, *Enterprise* και *Personal*, ανάλογα με τις απαιτήσεις του δικτύου. Η υποστήριξη για WPA2-Personal είναι υποχρεωτική σε όλες τις επικυρωμένες συσκευές Wi-Fi και τα σημεία πρόσβασης των πελατών. Η υποστήριξη για WPA2-Enterprise είναι προαιρετική, αλλά συστήνεται για συσκευές που λειτουργούν σε μεγάλης κλίμακας δίκτυα. Οι συγκεκριμένες απαιτήσεις ασφάλειας υπαγορεύουν ποιος τρόπος χρησιμοποιείται μέσα σε ένα δίκτυο.
Τα οικιακά και μικρά δίκτυα γραφείων χρησιμοποιούν τυπικά *WPA2-Personal*, επειδή δεν απαιτείται οποιοσδήποτε εξοπλισμός πέρα από ένα *Wi-Fi Certified* σημείο πρόσβασης και μια συσκευή. Στο WPA2-Personal, το κλειδί παράγεται από το καθορισμένο SSID (Service Set Identifier) και μία φράση εισόδου (*passphrase*) που εισάγονται από το χρήστη. Απαιτείται η επιλογή ενός ισχυρού passphrase προκειμένου να εκμεταλλευθεί πλήρως την προστασία WPA2. Τα μακριά, σύνθετα, και τυχαία pass phrases , όπως και οι συχνές αλλαγές passphrase, είναι κρίσιμα για την καλή ασφάλεια.
Τα δίκτυα επιχειρήσεων με IEEE 802.1x AAA (*Authentication, Authorization, Accounting*) εξυπηρετητές μπορούν να ωφεληθούν από την περιπλοκότερη λειτουργία που διατίθεται από το *WPA2-Enterprise*, το οποίο περιλαμβάνει τη δυνατότητα να ελέγξει και να διαχειριστεί την κυκλοφορία, να καθορίσει τα ειδικού χρήστη επίπεδα πιστοποίησης, και να προσφέρει πρόσβαση στους φιλοξενούμενους. Το WPA2-Enterprise επιτρέπει επίσης στην ασύρματη πρόσβαση να ενσωματώνεται με γενικό έλεγχο προσπέλασης δικτύου που επιτυγχάνεται με καταμερισμό των υπαρχόντων βάσεων δεδομένων χρηστών.

WPA2-Enterprise	WPA2-Personal
Κάθε χρήστης ορίζει τα δικά του μοναδικά πιστοποιητικά	Η πιστοποίηση με χρήση PSK επιτρέπει την χρήση μιας passphrase η οποία εισάγεται χειροκίνητα και συνήθως μοιράζεται από τους χρήστες του δικτύου
Απαιτείται IEEE 802.1X server με υποστήριξη EAP και authentication database	Δεν απαιτείται authentication server
Τα κλειδιά ασφάλειας δεδομένων είναι μοναδικά για κάθε σύνοδο	Τα κλειδιά ασφάλειας δεδομένων είναι μοναδικά για κάθε σύνοδο
	

Πίνακας 3 Μηχανισμός πιστοποίησης σε WPA2-Enterprise και WPA2-Personal.

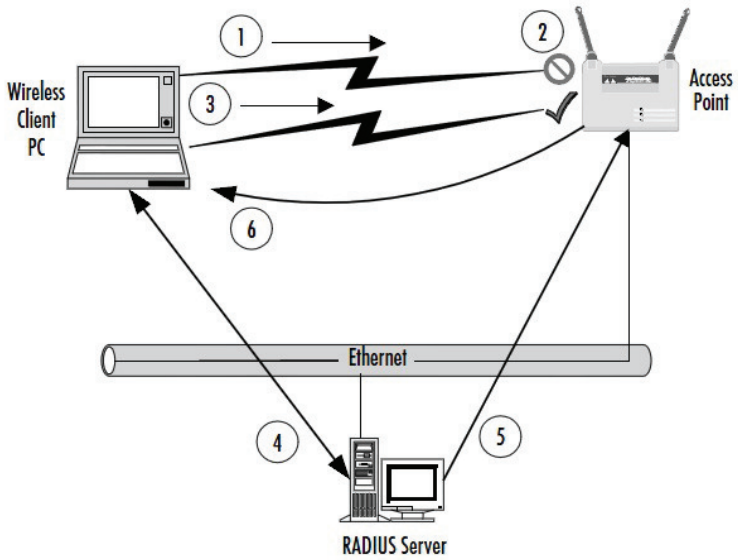
3.4 Προηγμένη ασφάλεια με 802.1x και EAP

Το 802.1x παρέχει μια δομή πιστοποίησης (network port authentication) στα WLANs, επιτρέποντας σε έναν χρήστη να επικυρώνεται από μια κεντρική αρχή.
Η δομή αυτή αποτελείται από τρία συστατικά μέρη:

1 *Supplicant* (συνήθως το λογισμικό πελατών)
2 *Authenticator* (συνήθως το AP) συνδέεται με το δίκτυο του τοπικού LAN
3 Εξυπηρετητής Πιστοποίησης/AS, *Authentication Server* – AS (συνήθως ένας RADIUS server)

Το 802.1x χρησιμοποιεί το EAP , ένα υπάρχον πρωτόκολλο (RFC 2284) που λειτουργεί σε Ethernet, token ring, ή WLANs για την ανταλλαγή μηνυμάτων κατά τη διάρκεια της διαδικασίας πιστοποίησης.
Δύο κύρια στοιχεία περιλαμβάνονται στη χρησιμοποίηση αυτών των προτύπων:
Το EAP επιτρέπει σε όλους στους ασύρματους adapters πελατών να επικοινωνούν με διαφορετικούς εξυπηρετητές πιστοποίησης, όπως RADIUS servers, που βρίσκονται στο δίκτυο. Επίσης υλοποιείται το πρότυπο IEEE 802.1x για έλεγχο πρόσβασης στο δίκτυο το οποίο βασίζεται σε θύρες (ports) για το φιλτράρισμα MAC.
Όταν αυτά τα χαρακτηριστικά γνωρίσματα επεκτείνονται μαζί, οι ασύρματοι πελάτες που συνδέονται με τα APs δεν θα είναι σε θέση να αποκτήσουν πρόσβαση στο δίκτυο μέχρις ότου ο χρήστης να εκτελέσει μια σύνδεση logon στο δίκτυο.
Ο χρήστης θα πρέπει να πληκτρολογήσει ένα όνομα χρήστη και έναν προσωπικό κωδικό για το logon δικτύου. Μετά ο πελάτης και ο RADIUS server θα εκτελέσουν την επικύρωση, ενδεχομένως οδηγώντας τον πελάτη σε πιστοποίηση, που παρέχεται από το όνομα χρήστη και τον κωδικό πρόσβασης. Έτσι ο πελάτης αποκτάει πρόσβαση στο δίκτυο και στους πόρους. Αυτό συμβαίνει επειδή ο RADIUS server και η συσκευή του πελάτη θα λάβουν ένα

συγκεκριμένου-πελάτη WEP κλειδί που χρησιμοποιείται από τον πελάτη για εκείνη την συγκεκριμένη σύνοδο σύνδεσης (*logon*). Για ένα πρόσθετο βαθμό ασφάλειας, ο κωδικός πρόσβασης του χρήστη και το κλειδί συνόδου δεν διαβιβάζεται ποτέ πάνω στην ασύρματη σύνδεση.



Εικόνα 24 Πιστοποίηση βασισμένη στο πρότυπο 802.1x/EAP.

Παρακάτω είναι τα βήματα που ακολουθούνται κατά τη φάση πιστοποίησης καθώς και πώς διαβιβάζεται το κλειδί WEP:

1. Ο ασύρματος πελάτης αιτείται να συνδεθεί με ένα AP που βρίσκεται στο ασύρματο δίκτυο με την αποστολή ενός μηνύματος έναρξης (*EAPOL-start*).
2. Το AP ανιχνεύει τον πελάτη και καθιστά τη θύρα (*port*) του πελάτη σε μια μη εξουσιοδοτημένη κατάσταση , έτσι ώστε μόνο 802.1x/EAP μηνύματα να διαβιβάζονται. Εμποδίζει όλες τις άλλες προσπάθειες που γίνονται από εκείνο τον πελάτη για να κερδίσει πρόσβαση στο δίκτυο μέχρι ο πελάτης να συνδεθεί (*log on*) στο δίκτυο.
3. Ο πελάτης στέλνει έπειτα ένα μήνυμα έναρξης *EAP-Start*. Το AP στηρίζεται σε ένα μήνυμα *EAP-Request/Identity* για να λάβει την ταυτότητα του πελάτη. Ο πελάτης απαντάει με ένα πακέτο *EAP-Response/Identity* και παρέχει ένα όνομα χρήστη και έναν κωδικό πρόσβασης για τη σύνδεση στο δίκτυο.
4. Χρησιμοποιώντας το πρότυπο 802.1x και το EAP, ο ασύρματος πελάτης και ένας RADIUS server θα εκτελέσουν την πιστοποίηση δια μέσου του AP όπως φαίνεται στο βήμα 5 της παραπάνω εικόνας. Τα μηνύματα EAP που χρησιμοποιούνται για την πιστοποίηση περνούν άμεσα στον εξυπηρετητή πιστοποίησης. Στην πραγματικότητα, κατά τη διάρκεια αυτής της φάσης ο *supplican*t και ο *server* μιλούν απευθείας. Κατά τη διάρκεια της διαδικασίας πιστοποίησης, ο *authenticator* ρίχνει μια γρήγορη ματιά σε κάθε μήνυμα EAP που περνά μεταξύ του supplicant και του εξυπηρετητή πιστοποίησης. Προσέχει για ορισμένα μηνύματα που καταλαβαίνει. Ειδικότερα, ψάχνει ένα *EAP-Success* ή ένα *EAP-Failure*. Πρέπει να περιμένει έως ότου ο εξυπηρετητής πιστοποίησης δηλώσει εάν ο supplicant έχει γίνει αποδεκτός ή έχει απορριφθεί. Ένα μήνυμα *RADIUS* παρέχει την ένδειξη όταν χρησιμοποιείται RADIUS. Ο πελάτης έπειτα θα χρησιμοποιήσει one-way hash[4] του, παρεχόμενου από τον χρήστη, κωδικού πρόσβασης ως απάντηση στην πρόκληση, και αυτό θα σταλεί στον *RADIUS server*. Ο RADIUS server θα ανατρέξει στον δικό του πίνακα χρηστών και θα συγκρίνει εκείνον με την απάντηση του πελάτη. Εάν υπάρχει αντιστοιχία, ο RADIUS server πιστοποιεί τον πελάτη, και η διαδικασία θα

[4]**One-way hash**: είναι ένας αλγόριθμος που μετατρέπει ένα μήνυμα ή κείμενο σε μια σταθερή ψηφίων, συνήθως για λόγους ασφάλειας ή διαχείρισης δεδομένων. "One way" σημαίνει ότι είναι σχεδόν αδύνατο να αντληθεί το αρχικό κείμενο.

επαναληφθεί, αλλά στην αντιστροφή. Αυτό επιτρέπει στον πελάτη να πιστοποιήσει τον RADIUS server.

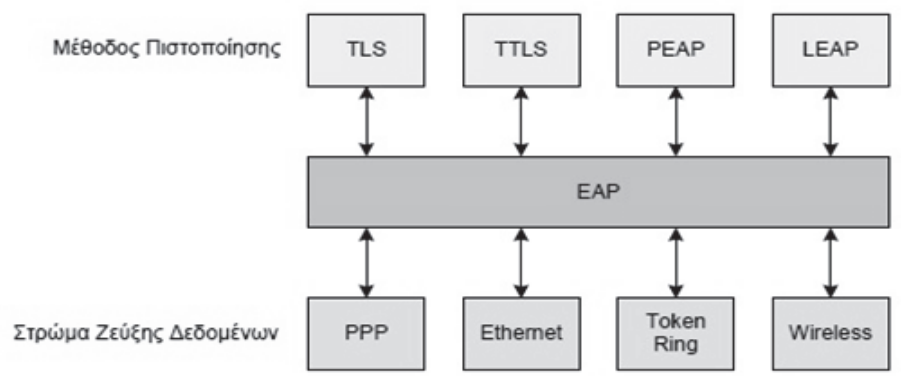
5. Ανάλογα με την απάντηση του AP, μια θετική απάντηση πιστοποίησης θα ενεργοποιήσει την θύρα (port) και η αρνητική απάντηση πιστοποίησης θα έχει ως αποτέλεσμα η θύρα να παραμείνει μπλοκαρισμένη.

Αφότου ολοκληρωθεί επιτυχώς η πιστοποίηση, πραγματοποιούνται τα ακόλουθα βήματα:

1 Ο RADIUS server και ο πελάτης καθορίζουν ένα κλειδί WEP που είναι μοναδικό για τον πελάτη και εκείνη την σύνοδο.
2 Ο RADIUS server διαβιβάζει αυτό το κλειδί WEP (επίσης γνωστό ως κλειδί συνόδου), πέρα από το ενσύρματο LAN στο AP.
3 Το AP θα κρυπτογραφήσει το κλειδί ασύρματης μετάδοσης και το κλειδί συνόδου έτσι ώστε να μπορεί κατόπιν να στείλει το νέο κρυπτογραφημένο κλειδί στον πελάτη. Ο πελάτης θα χρησιμοποιήσει έπειτα το κλειδί συνόδου για να το αποκρυπτογραφήσει.
4 Ο πελάτης και το AP ενεργοποιούν έπειτα το WEP. Τα APs και οι πελάτες έπειτα θα χρησιμοποιήσουν τα κλειδιά συνόδου και ασύρματης μετάδοσης WEP για όλες τις επικοινωνίες που συμβαίνουν κατά τη διάρκεια της συνόδου.
5 Για ενισχυμένη ασφάλεια, το κλειδί συνόδου και το κλειδί ασύρματης μετάδοσης αλλάζουν συνέχεια σε συχνές περιόδους που διαμορφώνονται στον RADIUS server.

Extensible Authentication Protocol (EAP)

Το EAP είναι ένα ευέλικτο πρωτόκολλο μεταφοράς πληροφοριών πιστοποίησης. Αρχικά αναπτύχθηκε για πιστοποίηση ταυτότητας σε συνδέσεις μέσω τηλεφωνικών γραμμών (*dial-up*) δηλαδή για την παροχή υπηρεσιών αυθεντικοποίησης στο πρωτόκολλο PPP (Point-to-Point Protocol). Το EAP έχει δύο βασικά και χρήσιμα χαρακτηριστικά. Πρώτον, διαχωρίζει την ανταλλαγή των μηνυμάτων πιστοποίησης, παρέχοντας ένα ανεξάρτητο στρώμα, από την διαδικασία της πιστοποίησης. Αυτό οδηγεί στο δεύτερο χαρακτηριστικό, την επεκτασιμότητα. Η μέθοδος πιστοποίησης μπορεί να αλλάζει με κάποια άλλη, πιθανώς νεότερη, για μεγαλύτερη ασφάλεια χωρίς αντίκτυπο στον τρόπο μεταφοράς μηνυμάτων, δηλαδή το στρώμα EAP. Το περιεχόμενο αυτών των συγκεκριμένων μεθόδων πιστοποίησης δεν καθορίζεται στο EAP. Οι μέθοδοι πιστοποίησης ανώτερου-στρώματος περιλαμβάνουν μεθόδους όπως η SSL, TLS, και Kerberos V5.



Εικόνα 25 Η μέθοδος πιστοποίησης αλλάζει χωρίς αντίκτυπο στο στρώμα EAP.

Το RFC2284 (EAP) είναι ένα πολύ σύντομο έγγραφο που διευκρινίζει ότι τέσσερις τύποι μηνυμάτων μπορούν να σταλούν:

- Αίτημα (*Request*): Χρησιμοποιείται για να στείλει τα μηνύματα από τον authenticator στον supplicant.
- Απάντηση (*Response*): Χρησιμοποιείται για να στείλει τα μηνύματα από τον supplicant στον authenticator.

- Επιτυχία (*Success*): Στέλνεται από τον authenticator για να δείξει ότι επιτρέπεται η πρόσβαση.
- Αποτυχία (*Failure*): Στέλνεται από τον authenticator για να δείξει ότι πρόσβαση απορρίπτεται.

Αυτά τα μηνύματα περιγράφονται από την πλευρά του authenticator. Εντούτοις, στο IEEE 802.1x σενάριο, ο authenticator διαβιβάζει τα μηνύματα στον εξυπηρετητή πιστοποίησης (RADIUS server). Σε αυτήν την περίπτωση ο εξυπηρετητής πιστοποίησης παράγει μηνύματα αιτήματος, επιτυχίας, ή/και μηνύματα αποτυχίας και ο authenticator απλώς τα αναμεταδίδει στον supplicant. Τα μηνύματα αιτήματος και απάντησης υποδιαιρούνται περαιτέρω χρησιμοποιώντας το πεδίο EAP Type. Το πεδίο Type προσδιορίζει ποιες πληροφορίες μεταφέρονται στο μήνυμα EAP. Ο σημαντικότερος προκαθορισμένος τύπος είναι η ταυτότητα (*Identity*) (τύπος τιμής 1).
Χαρακτηριστικά, αυτός ο τύπος χρησιμοποιείται ως τμήμα της φάσης εισαγωγής EAP όπως είδαμε και παραπάνω: το μήνυμα *EAP-Request/Identity* στέλνεται από το authenticator σε έναν νέο supplicant. Ο supplicant απαντάει με μήνυμα EAP-Response/Identity που περιέχει το δικό του όνομα χρήστη και μερικά άλλα αναγνωριστικά τα οποία θα γίνουν κατανοητά στον εξυπηρετητή πιστοποίησης.
Οι πρώτοι έξι τύποι μηνυμάτων καθορίζονται στο πρότυπο, όλοι οι άλλοι είναι για συγκεκριμένες μεθόδους πιστοποίησης και εκδίδονται (μεμονωμένα) από τον IANA (*Internet Assigned Numbers Authority*) για κάθε νέα μέθοδο πιστοποίησης που εισάγεται. Όταν ο αριθμός Type του TLS, παραδείγματος χάριν, είναι 13, σημαίνει ότι όλα τα μηνύματα EAP-Request και EAP-Response με αυτό το πεδίο Type περιέχουν τις πληροφορίες που είναι συγκεκριμένες για τη μέθοδο πιστοποίησης ανώτερου-στρώματος TLS.
Σε μερικές περιπτώσεις, το πεδίο *Type* καθορίζει ένα ειδικού σκοπού μήνυμα. Παραδείγματος χάριν, ένα μήνυμα με μια τιμή *Type 2* καλείται μήνυμα ανακοίνωσης και χρησιμοποιείται για να στείλει κάποιο εμφανές στον χρήστη κείμενο. Αυτό θα μπορούσε να είναι «παρακαλώ πληκτρολογείστε τον προσωπικό κωδικό σας». Το μήνυμα προορίζεται να εμφανιστεί στην οθόνη του συστήματος του χρήστη (αν και λίγα συστήματα υποστηρίζουν στην πραγματικότητα αυτό). Ένα μήνυμα με μια τιμή Type 3 καλείται NAK και χρησιμοποιείται όταν υποβάλλεται ένα αίτημα για μια μέθοδο πιστοποίησης που δεν υποστηρίζεται. Εάν ένα αίτημα EAP με τύπο TLS στέλνεται σε έναν peer που δεν υποστηρίζει TLS, μπορεί να αποκριθεί με ένα πεδίου τύπου NAK.

Διαμόρφωση Μηνύματος EAP
Όλα τα μηνύματα EAP έχουν παρόμοια βασική διαμόρφωση. Ο κώδικας (Code) είναι 1 byte υποδεικνύοντας τον τύπο του μηνύματος:
Request (01)
Response (02)
Success (03)
Failure (04)

Εικόνα 26 Μορφή μηνύματος EAP.

Το προσδιοριστικό (*Identifier*) λαμβάνει τιμές από 0 ως255 και το IEEE 802.1x υποδεικνύει ότι πρέπει να αυξάνεται για κάθε μήνυμα που στέλνεται. Όταν στέλνεται μια απάντηση, το προσδιοριστικό τίθεται ίσο με αυτό στο αίτημα. Αυτό βοηθά για τον έλεγχο ποια απάντηση πηγαίνει με ποιό αίτημα. Το μήκος (*Length*) είναι ο συνολικός αριθμός των bytes στο μήνυμα EAP (συμπεριλαμβανομένου του κώδικα και ούτω καθεξής). Είναι μια τιμή 16 bit. Τέλος, το Data είναι τα πραγματικά δεδομένα αιτήματος ή απάντησης που στέλνονται.
Τα πακέτα *Success/Failure* είναι μικρά και δεν περιέχουν δεδομένα. Ένα από αυτά τα μηνύματα χρησιμοποιείται στο τέλος της διαδικασίας πιστοποίησης για να επισημάνει το αποτέλεσμα. Επειδή τα μηνύματα Success και Failure είναι κοινά σε όλα τα πρωτόκολλα πιστοποίησης, οι ενδιάμεσες συσκευές (όπως το σημείο πρόσβασης) μπορούν να

ανιχνεύσουν πότε ολοκληρώνεται μια πιστοποίηση χωρίς κατανόηση όλων των λεπτομερειών της μεθόδου πιστοποίησης. Το σημείο πρόσβασης πρέπει να περιμένει το *RADIUS accept* μήνυμα προτού λάβει οποιαδήποτε απόφαση για τα δικαιώματα πρόσβασης.
Οι λεπτομέρειες της μεθόδου πιστοποίησης στέλνονται στα μηνύματα *Request* και *Response*. Αυτά έχουν ένα επιπλέον πεδίο ονομαζόμενο Type.

Εικόνα 27 Request/Response μορφή μηνύματος EAP.

EAPOL
Στην πραγματικότητα το EAP δεν είναι ένα LAN πρωτόκολλο επειδή σχεδιάστηκε για χρήση με dial-up πιστοποίηση μέσω modem. Έτσι εάν πηγαίναμε να λάβουμε μηνύματα EAP που περνούν στο δίκτυο, θα έπρεπε να βρούμε ένα τρόπο να ενθυλακώσουμε μηνύματα EAP κατά τη διάρκεια του ταξιδιού τους. Το IEEE 802.1x καθορίζει ένα πρωτόκολλο αποκαλούμενο EAP over LAN (EAPOL) για να λάβει τα μηνύματα EAP που περνούν μεταξύ supplicant και του authenticator.
Το IEEE 802.1x παρέχει την περιγραφή για το EAPOL. Περιγράφει τις μορφές πλαισίων για Ethernet (IEEE 802.3) και token ring LANs αλλά όχι για το IEEE 802.11.
Οι πέντε τύποι μηνυμάτων EAPOL είναι:

- EAPOL-Start
- EAPOL-Key
- EAPOL-Packet
- EAPOL-Logoff
- EAPOL-Encapsulated-ASF-Alert

Άλλες μέθοδοι EAP
Μερικές από τις διαδεδομένες μεθόδους EAP περιγράφονται παρακάτω:

- EAP-PSK: Πιστοποίηση βασισμένη στο προ-μοιρασμένο κλειδί (*pre-shared key*).
- EAP-MD5: Μια λιτή μέθοδος πιστοποίησης που βασίζεται σε μια MD5 λειτουργία αναδιάταξης (*hash*). Η πιστοποίηση δεν είναι αμοιβαία αφού μόνο η πιστοποίηση του πελάτη εκτελείται. Είναι ευπαθές στο λεξικό και στις επιθέσεις *man-in-the-middle*. Επιπλέον, είναι ακατάλληλο για την παραγωγή κλειδιών.
- EAP-MSCHAPv2: Το CHAP της Microsoft, έκδοση 2, είναι ένα πρωτόκολλο για πιστοποίηση με χειραψία διεκδίκησης. Ενώ η έκδοση 1 ήταν ένας μηχανισμός πιστοποίησης του πελάτη μόνο, η έκδοση 2 επιτρέπει και στον πελάτη και στον εξυπηρετητή να πιστοποιούνται.
- EAP-LEAP: *Light EAP*, είναι ένα ιδιόκτητο πρωτόκολλο EAP από τη Cisco. Το EAP-LEAP παρέχει αμοιβαία πιστοποίηση βασισμένη στην διεκδίκηση-απάντηση κωδικού πρόσβασης.
- EAP-PEAP: *Protected EAP*, είναι ένα ιδιόκτητο πρωτόκολλο που συναναπτύχθηκε από την Microsoft, Cisco, και RSA Security. Το PEAP παρέχει ασφαλή αμοιβαία πιστοποίηση από τον πελάτη και τον server.
- EAP-TLS: *Transport Layer Security*, είναι βασισμένη στην αμοιβαία επικύρωση πιστοποιητικών. Τα πιστοποιητικά και από τον πελάτη και από τον κεντρικό υπολογιστή ανταλλάσσονται.
- EAP-TTLS: *Tunneled Transport Layer Security*, TTLS, είναι μια επέκταση του TLS. Οι πελάτες πιστοποιούνται από τον κωδικό πρόσβασης, αλλά η πιστοποίηση των εξυπηρετητών βασίζεται στο πιστοποιητικό.

3.4.1 RADIUS (Remote Access Dial-In User Service)

Ο όρος RADIUS καθορίζει δύο πράγματα. Κατ' αρχάς, καθορίζει ένα σύνολο λειτουργιών που πρέπει να είναι κοινό στους εξυπηρετητές πιστοποίησης. Δεύτερον, καθορίζει ένα πρωτόκολλο που επιτρέπει σε άλλες συσκευές να έχουν πρόσβαση σε αυτές τις δυνατότητες. Όταν μιλάμε για έναν RADIUS server, μιλάμε για εκείνο τον υποτομέα του authentication server που υποστηρίζει τι δυνατότητες RADIUS και όταν μιλάμε για RADIUS, αναφερόμαστε γενικά στο πρωτόκολλο που χρησιμοποιείται για να μιλήσει στον server.
Αν και ο RADIUS δεν είναι συγκεκριμένα μέρος του προτύπου IEEE 802.11i, πολλές εταιρικές εφαρμογές το χρησιμοποιούν για να επικοινωνήσουν μεταξύ του σημείου πρόσβασης και του εξυπηρετητή πιστοποίησης. Οι μικρές εγκαταστάσεις γραφείων ή σπιτιών είναι σχεδόν απίθανο να χρησιμοποιήσουν RADIUS επειδή ο εξυπηρετητής πιστοποίησης είναι πιθανώς μέσα στο σημείο πρόσβασης.
Οι RADIUS servers εκτελούν τις λειτουργίες AAA (*Authentication, Authorization, Accounting*) για κάθε αίτηση πρόσβασης ενός νέου πελάτη και μπορεί να συνυπάρχουν με άλλα συστατικά (όπως ελεγκτές περιοχών και κατάλογοι LDAP) για να παρέχουν μια συγκεντρωμένη διαχείριση των αποφάσεων ελέγχου προσπέλασης. Ένα ολοκληρωμένο σύστημα AAA περιγράφει τον τρόπο που γίνεται η πιστοποίηση των χρηστών, η εξουσιοδότησή τους στους πόρους του δικτύου και την καταγραφή των δραστηριοτήτων τους καθώς και ένα πρωτόκολλο επικοινωνίας μεταξύ των πιστοποιητών και του εξυπηρετητή πιστοποίησης. Οι RADIUS servers συγκεντρώνουν επίσης τις λειτουργίες δημόσιου κλειδιού που χρησιμοποιούνται από το PEAP και το TTLS, αποδεσμεύοντας τα APs από τις αποφάσεις ελέγχου προσπέλασης, χαμηλώνοντας τις δαπάνες επέκτασης και διαχείρισης. Το πρωτόκολλο RADIUS παρέχει αύξηση της ασφάλειας WLAN ενώ ο RADIUS server ενεργεί ως «κεντρικός κριτής» λαμβάνοντας αποφάσεις πιστοποίησης και ασφάλειας πρόσβασης. Η ανάπτυξη ενός RADIUS AAA σε hotspots είναι πολύ σημαντική αφού εμπλέκονται πολλοί χρήστες που πρόκειται μετακινηθούν μεταξύ ποικίλων δικτύων και λειτουργιών.
Ο RADIUS ορίστηκε από την IETF (Internet Engineering Task Force) και σχεδιάστηκε για τη χρήση σε δίκτυα TCP/IP. Δηλαδή οι συσκευές χρησιμοποιούν ένα δίκτυο IP για να μιλήσουν σε έναν RADIUS server. Ο RADIUS έχει υποστεί διάφορες προσθήκες κατά τη διάρκεια των ετών. Παραδείγματος χάριν, το EAP over RADIUS (RFC 2869) απαιτείται για την ασφάλεια IEEE 802.11i RSN, αλλά δεν περιλήφθηκε στην αρχική προδιαγραφή RADIUS (RFC 2865).
Τα πρότυπα, σχετικά με WPA/RSN είναι:

RFC 2865: Remote Authentication Dial-In User Service (RADIUS)
RFC 2866: RADIUS Accounting
RFC 2867: RADIUS Accounting for Tunneling
RFC 2868: RADIUS Authentication for Tunneling
RFC 2869: RADIUS Extensions (EAP over RADIUS)
RFC 3162: RADIUS over IP6
RFC 2548: Microsoft Vendor-Specific RADIUS Attributes

Το κίνητρο για τον RADIUS είναι να υπάρχει ένας authentication server που να γνωρίζει όλους τους πελάτες και να επιτρέπει στους modem pool servers να διαβιβάζουν τις πληροφορίες πιστοποίησης στην κεντρική περιοχή για έλεγχο. Στον όρο RADIUS, ο modem pool server είναι ένας server πρόσβασης στο δίκτυο (Network Access Server, NAS) και ο εξυπηρετητής πιστοποίησης (authentication server, AS) είναι ο RADIUS server. Η αναλογία με το τοπικό LAN WI-Fi είναι σαφής. Στην περίπτωσή μας το σημείο πρόσβασης (AP) είναι όπως ο NAS. Μπορεί να υπάρχουν πολλοί διάσπαρτοι, και δεν θέλουμε ο καθένας να γνωρίζει τη βάση δεδομένων πιστοποίησης. Μπορούμε να χρησιμοποιήσουμε τον RADIUS server για να παρέχει συγκέντρωση των αποφάσεων πιστοποίησης.

Χαρακτηριστικά του RADIUS

Ακολουθούν τα βασικά χαρακτηριστικά RADIUS :

1. *Client/server* μοντέλο: Ένας *Network Access Server* (NAS) λειτουργεί ως πελάτης του RADIUS. Ο πελάτης είναι αρμόδιος για τη διαβίβαση των πληροφοριών χρηστών στους οριζόμενους RADIUS servers και έπειτα να ενεργεί στην απάντηση που επιστρέφεται. Οι RADIUS servers είναι αρμόδιοι για τη λήψη των αιτημάτων σύνδεσης των χρηστών, να πιστοποιούν τον χρήστη, και έπειτα να επιστρέφουν όλες τις πληροφορίες διαμόρφωσης, που είναι απαραίτητες για τον πελάτη, για να παραδώσει υπηρεσίες στο χρήστη. Ένας RADIUS server μπορεί να ενεργήσει ως proxy πελάτης σε άλλους RADIUS servers ή άλλων ειδών servers.
2. Ασφάλεια Δικτύου: Οι συναλλαγές μεταξύ του πελάτη και του RADIUS server πιστοποιούνται μέσω της χρήσης ενός κοινού μυστικού, το οποίο δεν στέλνεται ποτέ πέρα από το δίκτυο. Επιπλέον, οποιοιδήποτε κωδικοί πρόσβασης χρηστών στέλνονται κρυπτογραφημένοι μεταξύ του πελάτη και του RADIUS server για να αποβάλουν τη πιθανότητα κάποιος που κατασκοπεύει ένα ακάλυπτο δίκτυο να μπορεί να καθορίσει τον κωδικό πρόσβασης ενός χρήστη.
3. Ευέλικτος Μηχανισμός Πιστοποίησης: Ο RADIUS server μπορεί να υποστηρίξει ποικίλες μεθόδους πιστοποίησης για έναν χρήστη. Όταν παρέχεται μαζί το όνομα χρήστη και τον αρχικό κωδικό πρόσβασης που δίνονται από το χρήστη, μπορεί να υποστηρίξει PPP PAP ή CHAP, σύνδεση (login) UNIX, και άλλους μηχανισμούς πιστοποίησης.
4. Εκτεταμένο Πρωτόκολλο: Νέες τιμές ιδιοτήτων μπορούν να προστεθούν χωρίς διατάραξη των υπαρχουσών εφαρμογών του πρωτοκόλλου.

Ο μηχανισμός του RADIUS

Παρακάτω φαίνεται πώς δουλεύει ο RADIUS σε επίπεδο πρωτοκόλλου.
Ένα πακέτο RADIUS ενθυλακώνεται στο UDP Data πεδίο όπου το UDP Destination Port πεδίο είναι 1812. Όταν δημιουργείται μία απάντηση, οι θύρες (*ports*) πηγής και προορισμού δεσμεύονται.

Μορφή μηνυμάτων πυρήνα και Ιδιότητες

Κάθε μήνυμα RADIUS έχει την ίδια βασική μορφή, όπως φαίνεται στο σχήμα.

Εικόνα 28 Μορφή πακέτου RADIUS.

Το ***Code***, ενός byte, δηλώνει τον τύπο του μηνύματος:
1 Access-Request: (NAS→AS) για κάθε νέα προσπάθεια εισόδου στο δίκτυο
2 Access-Accept: (NAS← AS) ως απάντηση στο Access-Request ότι πιστοποιήθηκε και εξουσιοδοτήθηκε η προσπάθεια εισόδου στο δίκτυο
3 Access-Reject: (NAS ← AS) ως απάντηση στο Access-Request fότι απορρίφθηκε η προσπάθεια εισόδου στο δίκτυο λόγω μη έγκυρων διαπιστευτηρίων
11 Access-Challenge: (NAS← AS) ως απάντηση στο Access-Request με σκοπό να εξακριβώσει την ταυτότητα του πελάτη
4 Accounting-Request: από NAS περιέχοντας πληροφορίες για τη χρήση του δικτύου
5 Accounting-Response: από τον AS ως απάντηση σε Accounting-Request ότι το μήνυμα λήφθηκε με επιτυχία
12 Status-server (experimental)
13 Status-client (experimental)
255 Reserved

Για τα μηνύματα πιστοποίησης οι τιμές είναι 1,2,3,11.
Όταν ληφθεί ένα πακέτο με μη έγκυρο πεδίο Code, τότε απορρίπτεται.

Το ***Identifier*** είναι ένας αυθαίρετος αριθμός που χρησιμοποιείται για να ταιριάξει τα αιτήματα και τις απαντήσεις και η λέξη **Length** δηλώνει το συνολικό αριθμό από bytes στο μήνυμα.

Το ***Authenticator*** είναι περισσότερο ενδιαφέρον επειδή έχει σχέση με την ασφάλεια. Είναι μήκους 16 bytes (128 bits) και η χρήση του εξαρτάται από τον τύπο του μηνύματος.

- Στο μήνυμα Access-Request, το authenticator περιέχει μια 16 bit μοναδική τιμή (*nonce*) και αυτή η τιμή δεν χρησιμοποιείται ποτέ δύο φορές σε δύο διαφορετικά αιτήματα. Αυτό χρησιμοποιείται στο RADIUS για δύο λόγους. Κατ' αρχάς, εάν το μήνυμα Access-Request στέλνει μια τιμή κωδικού πρόσβασης σε μια ιδιότητα, η τιμή κωδικού πρόσβασης κρυπτογραφείται χρησιμοποιώντας έναν συνδυασμό μυστικού κλειδιού και αυτής της μοναδικής τιμής. Δεύτερον, τα μηνύματα απάντησης χρησιμοποιούν την τιμή αυτής της μοναδικής τιμής στον προσδιορισμό μιας τιμής ελέγχου ακεραιότητας.
- Το ένα από τρία μηνύματα- Access-Accept, Access-Reject, και Access-Challenge - στέλνεται σε απάντηση σε ένα μήνυμα Access-Request. Είναι σημαντικό να ελεγχθεί ότι η απάντηση προήλθε από τον γνήσιο RADIUS server και δεν έχει τροποποιηθεί κατά τη μεταφορά. Για να ολοκληρωθεί αυτό, υπολογίζεται μια τιμή ελέγχου ακεραιότητας 16 bit (integrity check) και παρεμβάλλεται στο τμήμα authenticator της απάντησης. Ο NAS και ο RADIUS server μοιράζονται ένα μυστικό κλειδί μεταξύ τους. Για να δημιουργήσει την τιμή ελέγχου, ο RADIUS server συνδυάζει ολόκληρο το μήνυμα απάντησης με το μυστικό κλειδί. Πριν από τον υπολογισμό, εισάγει το nonce από το μήνυμα αιτήματος στη θέση authenticator του μηνύματος απάντησης και όταν υπολογιστεί η τιμή ελέγχου ακεραιότητας, επικαλύπτει το nonce για να διαμορφώσει μια νέα τιμή authenticator.

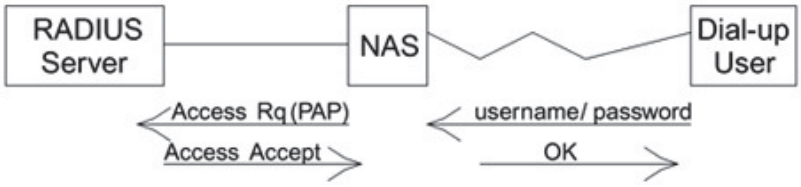
Ιδιότητες (*Attributes*)

Αν και ουσιαστικά μόνο τέσσερα μηνύματα χρησιμοποιούνται για την πιστοποίηση μέσω RADIUS, η έννοια των μηνυμάτων μπορεί να αλλάξει εκτενώς μέσω διαφορετικών ιδιοτήτων (Attributes) των μηνυμάτων. Τα PAP/CHAP επιδεικνύουν πώς το μήνυμα Access-Request μπορεί να σημάνει τρία διαφορετικά πράγματα σε διαφορετικές στιγμές. Οι ιδιότητες που φέρνει το μήνυμα είναι διαφορετικές σε κάθε περίπτωση. Το κύριο σώμα του μηνύματος RADIUS αποτελείται από μια σειρά ιδιοτήτων και κάθε μια είναι ένα ανεξάρτητο πακέτο χρήσιμων πληροφοριών που έχει σημασία και στα δύο επικοινωνούντα συμβαλλόμενα μέρη που επικοινωνούν.
Η δυνατότητα του RADIUS να επεκταθεί εξαρτάται από τη δυνατότητα να καθοριστούν και να υποστηριχθούν νέες ιδιότητες. Για να είναι χρήσιμος ένας RADIUS server, πρέπει να υποστηρίζει τις ιδιότητες που χρειάζονται ανάλογα με τις εφαρμογές (και οι υπηρεσίες που προσεγγίζονται μέσω των ιδιοτήτων).
Κάθε attribute έχει την ίδια μορφή:
Type τμήμα για να αναγνωρίσει την ιδιότητα
Length τμήμα που δηλώνει τον αριθμό των bytes σε όλη την ιδιότητα
Ιδιαίτερα δεδομένα ιδιότητας (εάν υπάρχουν)

Πιστοποίηση με PAP και CHAP

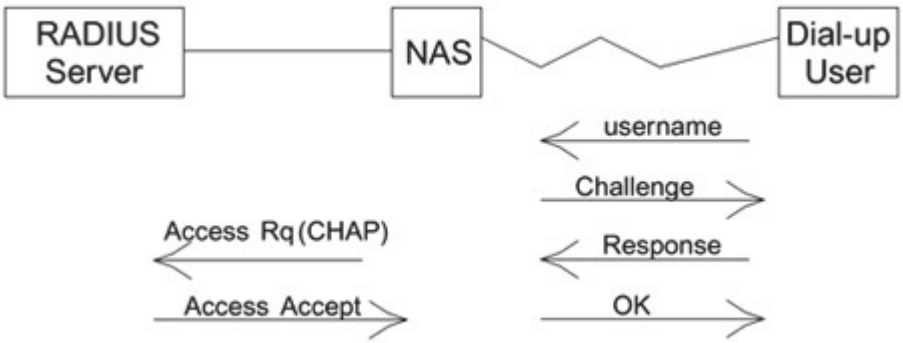
Ο RADIUS σχεδιάστηκε συγκεκριμένα με δύο PPP σενάρια πιστοποίησης: απλού αιτήματος κωδικού πρόσβασης PAP και απάντησης πρόκλησης CHAP.
Το PAP είναι μια απλή προσέγγιση ονόματος/κωδικού πρόσβασης χρηστών. Το CHAP απαιτεί ο server να στέλνει τυχαία στοιχεία αποκαλούμενα πρόκληση (*challenge*), τα οποία το σύστημα dial-in πρέπει να κρυπτογραφήσει και να τα επιστρέψει για τον έλεγχο.
Στην PAP (*Password Authentication Protocol*) υλοποίηση, ο χρήστης καλεί και ο NAS απαντάει και δηλώνει ότι χρησιμοποιεί την PAP πιστοποίηση. Το σύστημα του χρήστη αποκρίνεται έπειτα με την αποστολή του ονόματος χρήστη και του κωδικού πρόσβασης για τον λογαριασμό. Ο NAS στέλνει τώρα ένα μήνυμα *Access-Request* στον RADIUS server που περιέχει τις πληροφορίες ονόματος χρήστη και κωδικού πρόσβασης . Ο RADIUS server αποκρίνεται είτε με *Access-Accept* είτε με *Access-Reject* και ο NAS πράττει αναλόγως. Αυτό είναι μια πολύ απλή προσέγγιση και, φυσικά, υπόκειται σε ένα ευρύ

φάσμα επιθέσεων. Το χειρότερο μέρος είναι ότι ο κωδικός πρόσβασης στέλνεται χωρίς κρυπτογράφηση πέρα από την τηλεφωνική σύνδεση έτσι οποιοσδήποτε που ελέγχει τη σύνδεση μπορεί να τον αντιγράψει.



Εικόνα 29 Πιστοποίηση με PAP.

Το CHAP (*Challenge-Handshake Authentication Protocol*) είναι λίγο καλύτερο, και κάνει μια προσπάθεια για ασφαλή πιστοποίηση. Αντί να στείλει τον κωδικό πρόσβασης αποκρυπτογραφημένο πέρα από την τηλεφωνική σύνδεση, ο χρήστης στέλνει μόνο το όνομα χρήστη του στο NAS. Ο NAS πρέπει τώρα να αποκριθεί με μια πρόκληση (*challenge*). Για να πάρει τα στοιχεία πρόκλησης, ο NAS θα μπορούσε να στείλει το όνομα χρήστη στον server χρησιμοποιώντας ένα *Access-Request*, κατόπιν του οποίου ο server θα έστελνε τα στοιχεία πρόκλησης χρησιμοποιώντας την *Access-Challenge*. Εντούτοις, στις περισσότερες εφαρμογές ο NAS αποφεύγει να ενοχλήσει τον server και παράγει την πρόκληση μόνος του όπως φαίνεται στο παρακάτω σχήμα. Η πρόκληση περνάει πίσω στον *dial-in* σύστημα του χρήστη, το οποίο απαιτείται να κρυπτογραφήσει την πρόκληση με τον κωδικό πρόσβασης και να την στείλει πίσω. Τελικά ο NAS είναι σε θέση να στείλει την πρόκληση, την απάντηση και την ταυτότητα στο authentication server, δηλώνοντας ότι χρησιμοποιεί το CHAP.

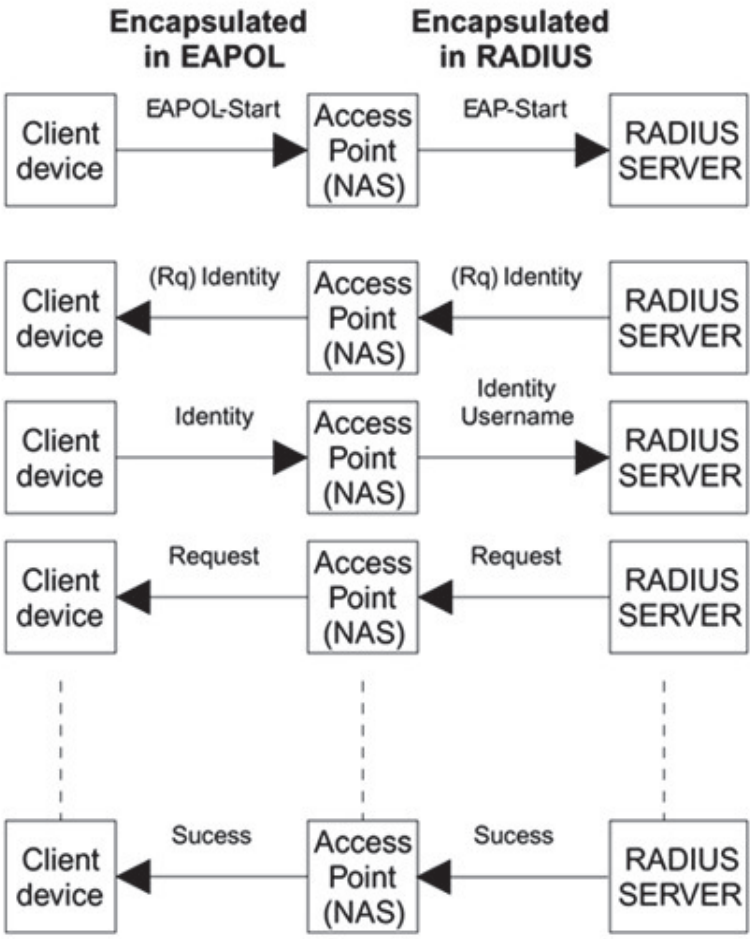


Εικόνα 30 Πιστοποίηση με CHAP.

Αυτή η προσέγγιση σημαίνει ότι ο κωδικός πρόσβασης δεν στέλνεται χωρίς κρυπτογράφηση και η πρόκληση αλλάζει σε κάθε προσπάθεια πρόσβασης. Εντούτοις, υπόκειται ακόμα στην επίθεση λεξικών επειδή και οι κρυπτογραφημένες και οι μη κρυπτογραφημένες εκδόσεις προκλήσεων είναι προσβάσιμες σε ένα επιτιθέμενο.
Λόγω της αδυναμίας σε επίθεσης λεξικών, η Microsoft εφάρμοσε μια τροποποιημένη έκδοση αποκαλούμενη MS-CHAP. Στο WPA/RSN, πρέπει να χρησιμοποιήσουμε RADIUS από κοινού με ένα πρωτόκολλο ασφάλειας με τεχνική ανώτερου επίπεδου, πολύ πιο σύνθετη και ασφαλής από τις απλές PAP και CHAP μεθόδους. Για να το κάνουμε αυτό, πρέπει να αλλάξουμε το σκοπό μερικών από τα μηνύματα στο RADIUS. Παραδείγματος χάριν, για να υποστηρίξουμε EAP θα χρησιμοποιήσουμε τη μέθοδο πρόσβαση-πρόκλησης (*access-challenge*), όχι ως πρόκληση, αλλά ως έναν τρόπο να σταλούν τα αιτήματα και οι απαντήσεις EAP. Ο RADIUS είναι αρκετά ευέλικτος να προσαρμοστεί σε αυτές τις αλλαγές.

EAP over RADIUS

1. Η νέα συσκευή στέλνει ένα *EAPOL-Start* στο σημείο πρόσβασης (AP) *authenticator* για να τον δραστηριοποιήσει. Το RFC2 869 καθορίζει ένα παρόμοιο μήνυμα αποκαλούμενο *EAP-Start*, το οποίο είναι μια ιδιότητα EAP 2 bytes χωρίς δεδομένα. Το AP περιέχει έναν IEEE802.1x authenticator, ο οποίος μιλάει EAP στον καινούριο πελάτη (*supplicant*). Τα μηνύματα EAP τα οποία θέλει ο IEEE 802.1x authenticator να περάσει πίσω στον authentication server, συσκευάζονται σε RADIUS και στέλνονται στον RADIUS server.
2. Εάν το AP ξέρει ότι ο RADIUS server υποστηρίζει EAP, μπορεί να προχωρήσει και να διανείμει το μήνυμα EAP-Request/Identity στη συσκευή πελάτη και να στείλει την απάντηση στον server άμεσα.
3. Εάν, εντούτοις, είναι αβέβαιο για την ικανότητα του server, μπορεί να ζητήσει από τον RADIUS server να ξεκινήσει την ανταλλαγή EAP στέλνοντας στον RADIUS server ένα μήνυμα EAP-Start σε ένα μήνυμα Access-Request που περιέχει ιδιότητες όπως το όνομα του χρήστη, τον κωδικό πρόσβασης του χρήστη, την ταυτότητα ID του πελάτη, και την port ID που ο χρήστης έχει πρόσβαση. Όταν ένας κωδικός πρόσβασης είναι παρών, είναι κρυμμένος χρησιμοποιώντας μια μέθοδο βασισμένη στον αλγόριθμο MD-5 (*RSA Message Digest*). Εάν ο server επιτρέπει το EAP, στέλνει το μήνυμα EAP-Request/Identity σε ένα μήνυμα RADIUS Access-Challenge. Αυτή η μέθοδος επικύρωσης είναι γνωστή ως TLS. Στο τέλος της ανταλλαγής, ένα EAP-Success ή EAP-Fail δηλώνει το αποτέλεσμα
4. Εάν ο πελάτης είναι εξακριβωμένος, ο RADIUS server συμβουλεύεται μια βάση δεδομένων των χρηστών για να βρει το χρήστη του οποίου το όνομα ταιριάζει με το αίτημα. Η καταχώρηση χρήστη στη βάση δεδομένων περιέχει έναν κατάλογο απαιτήσεων που καλύπτονται προτού να χορηγηθεί στο χρήστη η πρόσβαση. Περιλαμβάνει πάντα την επαλήθευση του κωδικού πρόσβασης, αλλά μπορεί επίσης να διευκρινίσει τον πελάτη ή την θύρα που ο χρήστης έχει την άδεια πρόσβασης. Ο RADIUS server μπορεί να υποβάλει αιτήματα σε άλλους servers προκειμένου να ικανοποιήσει το αίτημα, οπότε σ' αυτή την περίπτωση ενεργεί ως πελάτης.
5. Εάν ο server δεν υποστηρίζει EAP, επαναλαμβάνει με ένα μήνυμα απόρριψης Access-Reject. Εάν επιθυμεί, ο server μπορεί να περιλαμβάνει ένα μήνυμα κειμένου στο access-reject που εμφανίζεται από τον πελάτη στο χρήστη. Καμία άλλη ιδιότητα δεν επιτρέπεται σε ένα access-reject.
   Σημείωση:
   Εάν ο πελάτης λάβει μια access-challenge και υποστηρίζει μια challenge/response, μπορεί να επιδείξει το μήνυμα κειμένου στο χρήστη και να υποβάλει έπειτα το χρήστη για μια απάντηση. Ο πελάτης έπειτα υποβάλλει εκ νέου το αρχικό access-request του με μια νέα αίτηση ID, με τις ιδιότητες user-password που αντικαθίστανται από την απάντηση (που κρυπτογραφείται), και συμπεριλαμβανομένων των ιδιοτήτων κατάστασης από την access-challenge. Μόνο μηδενική ή μια περίπτωση ιδιοτήτων κατάστασης πρέπει να είναι παρούσα σε ένα αίτημα. Ο server μπορεί να αποκριθεί σε αυτό το νέο access-request με access-accept, access-reject ή μια άλλη access-challenge.
   Εάν όλοι οι όροι ικανοποιούνται, ο κατάλογος τιμών διαμόρφωσης για το χρήστη τοποθετείται μέσα σε μια access-accept απάντηση. Αυτές οι τιμές περιλαμβάνουν τον τύπο υπηρεσίας (όπως SLIP, PPP, και το login χρήστη) και όλες τις απαραίτητες τιμές για να παραδώσουν την επιθυμητή υπηρεσία. Για το SLIP και PPP, αυτό μπορεί να περιλαμβάνει τιμές όπως η διεύθυνση IP, η μάσκα υποδικτύου, η μέγιστη μονάδα μετάδοσης (Maximum Transmission Unit ,MTU), η επιθυμητή συμπίεση.



Εικόνα 31 Ανταλλαγή πιστοποίησης χρησιμοποιώντας EAP over Radius.

4 Υλοποιήσεις RADIUS server

4.1 FreeRADIUS

Ο FreeRADIUS ξεκίνησε τον Αύγουστο του 1999 από το Alan DeKok και τον Miquel van Smoorenburg. Ο FreeRADIUS δημιούργησε έναν νέο RADIUS server, χρησιμοποιώντας ένα σχέδιο αποτελούμενο από υπομονάδες (modules) που θα ενθάρρυνε περισσότερη ενεργή κοινοτική συμμετοχή.
Τα modules, τα οποία περιλαμβάνονται με τον πυρήνα του server, υποστηρίζουν LDAP, MySQL, PostgreSQL, Oracle, και πολλές άλλες βάσεις δεδομένων. Υποστηρίζει όλους τους δημοφιλείς τύπους πιστοποίησης EAP, συμπεριλαμβανομένου του PEAP και EAP-TTLS. Συμπεριλαμβάνονται περισσότερα από 100 λεξικά προμηθευτών, εξασφαλίζοντας συμβατότητα με ένα ευρύ φάσμα συσκευών NAS.
Η έκδοση 2.0.0 πρόσθεσε υποστήριξη για εικονική φιλοξενία (virtual hosting), IPv6, VMPS, και μια γλώσσα πολιτικής (policy) που απλοποιεί πολλές σύνθετες διαμορφώσεις.

Επισκόπηση
Ο FreeRADIUS είναι μια modular, υψηλής επίδοσης, δωρεάν RADIUS σουίτα που αναπτύσσεται και διανέμεται υπό την *GNU General Public License* έκδοση 2, και είναι ελεύθερη για download και χρήση. Η σουίτα FreeRADIUS περιλαμβάνει έναν RADIUS server, μια *BSD-licensed* RADIUS βιβλιοθήκη πελάτη, μια βιβλιοθήκη PAM, ένα Apache module, και πολυάριθμες πρόσθετες, σχετικές με το RADIUS, χρησιμότητες και βιβλιοθήκες ανάπτυξης.
Στις περισσότερες περιπτώσεις, η λέξη «FreeRADIUS» αναφέρεται στον ελεύθερο open source RADIUS server από αυτήν την σουίτα ο οποίος είναι και ο δημοφιλέστερος παγκοσμίως.
Υποστηρίζει όλα τα κοινά πρωτόκολλα πιστοποίησης, και ο server συνοδεύεται από ένα PHP-based εργαλείο διαχείρισης χρήστη web, αποκαλούμενο *dialupadmin*. Μια νέα υλοποίηση εφαρμογής Ιστού που κατασκευάστηκε στον Ισημερινό για το FreeRADIUS ονομάζεται SAAAS!. Είναι η βάση για πολλά εμπορικά προϊόντα RADIUS και υπηρεσίες, όπως ενσωματωμένα συστήματα, συσκευές RADIUS οι οποίες υποστηρίζουν έλεγχο προσπέλασης και δίκτυα WiMAX. Υποστηρίζει τις AAA ανάγκες πολλών επιχειρήσεων, telcos και Tier 1 ISPs. Επίσης χρησιμοποιείται ευρέως στην ακαδημαϊκή κοινότητα, με το *eduroam* (education roaming). Ο server είναι γρήγορος, πλούσιος σε γνωρίσματα, εξελικτικός και αποτελείται από πολλές υπομονάδες (*modular*).
Δεδομένου ότι η κύρια open source RADIUS σουίτα συμπεριλαμβάνεται ως τυποποιημένο πακέτο σε πολυάριθμα λειτουργικά συστήματα, έχει binary packages για πολλές άλλες και έχει διαθέσιμη πηγή (*source*) που είναι γνωστή ότι μπορεί να «χτιστεί» (*build*) σχεδόν σε οτιδήποτε. Οι εφαρμογές παραγωγής περιλαμβάνουν μεγάλης κλίμακας εγκαταστάσεις αποτελούμενες από πολλαπλούς AAA servers με πάνω από δέκα εκατομμύρια χρήστες και αιτήσεις ανά ημέρα. Υποστηρίζει proxy αιτήσεις, με *fail-over* και εξισορρόπηση φορτίου, καθώς επίσης και τη δυνατότητα να υπάρχει πρόσβαση σε πολλούς τύπους *back-end* βάσεων δεδομένων. Διαφορετικές κλάσεις αιτημάτων πιστοποίησης μπορούν να προκαλέσουν την πρόσβαση σε διαφορετικές βάσεις δεδομένων πιστοποίησης (authentication) και εξουσιοδότησης (authorization) (με διαδοχική υποχώρηση), και οι εγγραφές λογαριασμών (accounting) μπορούν να καταγραφούν ταυτόχρονα σε πολλαπλές διαφορετικές βάσεις δεδομένων αποθήκευσης και σε καταλόγους.
Για την περίπτωση του FreeRADIUS οι λεπτομέρειες της υλοποίησης είναι οι εξής:

- Για τη λειτουργία *authentication* μπορούν να χρησιμοποιηθούν πολλαπλές μέθοδοι ταυτόχρονα. Μία από αυτές είναι η χρήση LDAP server στον οποίο απευθύνεται ο RADIUS server για την αναζήτηση των στοιχείων του κάθε χρήστη.
- Η λειτουργία του *authorization* υλοποιείται μέσω RADIUS Attributes από τις οποίες κάποιες είναι κοινές για όλους τους χρήστες και αποθηκευμένες σε configuration files, ενώ κάποιες άλλες υπάρχουν per-user-based αποθηκευμένες στον LDAP.
- Στα πλαίσια του *accounting*, τα sessions καταγράφονται σε βάση δεδομένων η οποία στην περίπτωση του dialupadmin θεωρείται ότι είναι η MySQL.

Χαρακτηριστικά FreeRADIUS

- Ολοκληρωμένη υποστήριξη για RFC 2865 και RFC 2866 attributes.
- EAP με EAP-MD5, EAP-SIM, EAP-TLS, EAP-TTLS, EAP-PEAP, και Cisco LEAP
- Vendor-Specific Attributes για σχεδόν εκατό προμηθευτές, όπως BinTec, Foundry, Cisco, Juniper, Lucent/Ascend, HP ProCurve, Microsoft, USR/3Com, Acc/Newbridge κ.α.
- Υποστηρίζονται όλοι οι RADIUS Clients: RADIUS Clients, EAP Clients

Ευέλικτη Διαμόρφωση

Ο FreeRADIUS παρέχει ένα ευρύ φάσμα μεθόδων για να επιλεχθούν οι διαμορφώσεις χρήστη. Ο server μπορεί να επιλέξει μια διαμόρφωση βασισμένη σε οποιοδήποτε από τα παρακάτω κριτήρια:

- Attributes που έχουν μια δεδομένη τιμή
- Attributes που δεν έχουν μια δεδομένη τιμή
- Attributes που βρίσκονται στην αίτηση (ανεξαρτήτως της τιμής τους)
- Attributes που δεν βρίσκονται στην αίτηση
- String attributes που ταιριάζουν σε μια συνηθισμένη έκφραση
- Integer attributes που ταιριάζουν σε μια σειρά (π.χ. , =)
- Διεύθυνση IP πηγής της αίτησης. (Μπορεί να διαφέρει από την NAS-IP-Address)
- Όνομα που ορίζεται για ένα NAS box. (Μπορεί να διαφέρει από το NAS-Identifier)
- Ομάδα των NAS boxes. (Μπορεί να ομαδοποιείται με βάση την Source IP address, NAS-IP-Address, ή οποιαδήποτε άλλη διαμόρφωση)
- User-Name
- DEFAULT πρότυπο διαμόρφωσης
- Πολλά διαδοχικά DEFAULT πρότυπα διαμορφώσεων

Επιπλέον, ο FreeRADIUS υποστηρίζει εικονικούς εξυπηρετητές (virtual servers) που επιτρέπουν αρκετά ξεχωριστά σύνολα από δεδομένα διαμόρφωσης να συνυπάρχουν μέσα στον ίδιο server.

5 Πρακτικό Μέρος

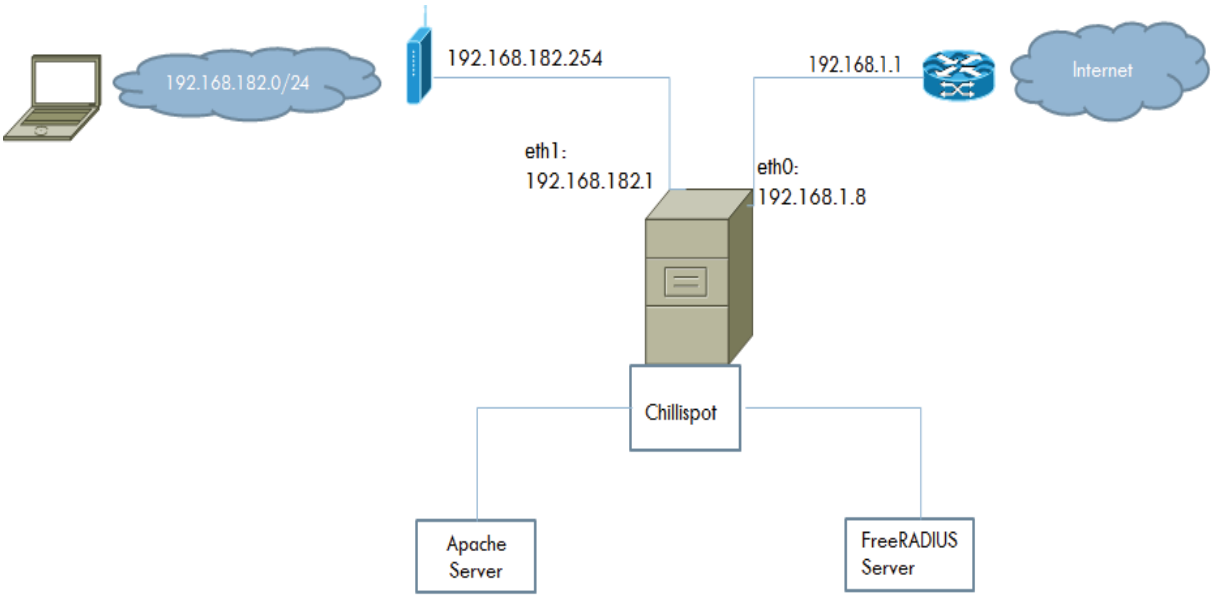
5.1 Σκοπός

Στόχος μας είναι η δημιουργία μιας ασύρματης δικτυακής υποδομής hotspot, στην οποία θα συνδέονται οι ασύρματοι πελάτες ώστε να τους παρέχεται πρόσβαση στο Internet και στον Παγκόσμιο Ιστό. Προτού όμως καταφέρουν να έχουν πρόσβαση στις υπηρεσίες αυτές, θα πρέπει να πιστοποιούνται μέσω μιας σελίδας Login η οποία θα εμφανίζεται στον browser τη στιγμή που θα θελήσουν να πλοηγηθούν στον ιστό. Αν τα στοιχεία που θα πληκτρολογήσουν δεν είναι σωστά, δεν θα τους επιτρέπεται η πρόσβαση. Σε αντίθετη περίπτωση, αν τα στοιχεία είναι όντως σωστά, θα ενημερώνονται για την επιτυχής σύνδεσή τους και θα ξεκινούν το "σερφάρισμα".

5.2 Απαιτήσεις υλικού-λογισμικού

Για την υλοποίηση και ανάπτυξη του Hotspot στην περίπτωσή μας χρειάζονται τα εξής:

1. Ένα PC Desktop (με λειτουργικό σύστημα Ubuntu 12.04) το οποίο φιλοξενεί τους servers και έχει δύο κάρτες δικτύου
2. PC Laptop για τον ρόλο του wireless client (για να ελέγξουμε το πείραμά μας)
3. wireless LAN access point στο οποίο θα συνδέονται οι clients
4. Internet connection
5. ChilliSpot software για το PC Desktop
6. Radius server (*Freeradius*)
7. Web server (*Apache*)



Εικόνα 32 Τοπολογία του hotspot.

Authentication Web Server

Ένας authentication web server για να πιστοποιεί τους χρήστες χρησιμοποιεί μια *universal access method*. Η διεπαφή επικοινωνίας υλοποιείται χρησιμοποιώντας μόνο το πρωτόκολλο *HTTP*. Δεν απαιτείται καμία επανάκκλιση από τον web server στο chilli προκειμένου να πιστοποιήσει τον πελάτη. Το HotSpot μπορεί να τοποθετηθεί πίσω από ένα NAT gateway, proxy ή firewall, ενώ ο web server τοποθετείται στο δημόσιο Internet. Ο web server παρέχει ένα cgi script το οποίο ρωτάει τον χρήστη για το δικό του username και password. Αφού οι πληροφορίες αυτές εισαχθούν από τον χρήστη, το κρυπτογραφημένο password στέλνεται πίσω στο chilli το οποίο προωθεί την αίτηση στον

freeradius server. Καλό είναι να χρησιμοποιείται *SSL/TLS* στον web server για να προστατεύονται τα username και passwords. Το SSL/TLS είναι κρυπτογραφικά πρωτόκολλα για ασφαλή επικοινωνία στο Internet.

Chillispot

Το *ChilliSpot* είναι ένα *open source captive portal* ή ασύρματο *LAN access point controller*. Χρησιμοποιείται για να πιστοποιεί τους χρήστες ενός wireless LAN. Υποστηρίζει *web based login* το οποίο είναι σήμερα δεδομένο στα δημόσια *Hotspots*. Οι λειτουργίες *authentication*, *authorization* και *accounting* (AAA) διαχειρίζονται από τον *radius server*.
Η τεχνική ***captive portal*** αναγκάζει έναν *HTTP client* του δικτύου να δει μια ειδική *web σελίδα* (συνήθως για σκοπούς πιστοποίησης) προτού χρησιμοποιήσει κανονικά το Internet. Ένα captive portal μετατρέπει έναν Web browser σε μία συσκευή πιστοποίησης. Αυτό γίνεται αναχαιτίζοντας όλα τα πακέτα, ασχέτως της address ή της port, μέχρι ο χρήστης να ανοίξει έναν browser και να προσπαθήσει να έχει πρόσβαση στο Internet. Εκείνη την στιγμή ο browser ανακατευθύνεται σε μια web page η οποία μπορεί να απαιτεί πιστοποίηση ή και πληρωμή, ή απλώς δείχνοντας μια αποδοχή χρήσης πολιτικής και απαιτώντας από τον χρήστη να συμφωνήσει. Τα Captive portals χρησιμοποιούνται σε πολλά Wi-Fi hotspots, καθώς και για τον έλεγχο της ασύρματης πρόσβασης.
Το Chilli, στην δική μας περίπτωση, υποστηρίζει τη μέθοδο πιστοποίησης UAM (*Universal Access Method*). Με την UAM ο ασύρματος πελάτης ζητά μία IP address, και του παρέχεται μία IP address από το Chilli. Όταν ο χρήστης ξεκινήσει έναν *web browser* το *chilli* θα συλλάβει την σύνδεση *tcp* και θα ανακατευθύνει το *browser* σε έναν *authentication web server*. Ο *web server* ρωτάει τον χρήστη για το δικό του *username* and *password*. Το password κρυπτογραφείται και στέλνεται πίσω στο chilli. Το chilli προωθεί την αίτηση πιστοποίησης στον *freeradius server*. Ο freeradius server στέλνει ένα *access-accept* μήνυμα πίσω στο chilli εάν η πιστοποίηση ήταν επιτυχής. Αλλιώς επιστρέφει ένα *access-reject*. Για την UAM χρησιμοποιείται το CHAP-Challenge και CHAP-Password όπως ορίζεται από το RFC 2865.
Το Chilli είναι μόνο διαθέσιμο για Linux.
Το chilli έχει τρία βασικά interfaces:

1. Ένα downlink interface για να δέχεται συνδέσεις από τους πελάτες
2. Ένα radius interface για να πιστοποιεί τους πελάτες
3. Ένα uplink network interface για να προωθεί την κίνηση σε άλλα δίκτυα

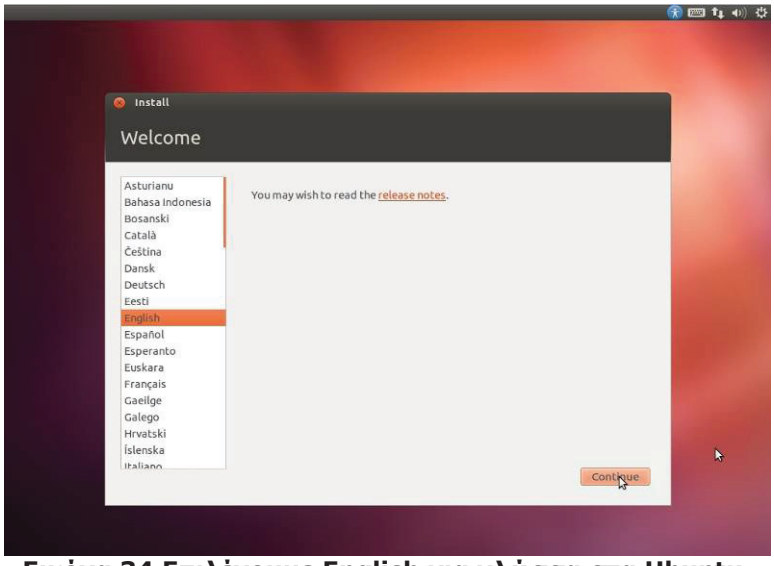
Το downlink interface δέχεται αιτήσεις DHCP και ARP από τους clients. Ο client μπορεί να είναι σε δύο καταστάσεις: Unauthenticated και authenticated. Σε unauthenticated κατάσταση οι αιτήσεις web από τον πελάτη ανακατευθύνονται στον authentication web server. Εάν η πιστοποίηση είναι επιτυχής η κατάσταση του πελάτη αλλάζει ως πιστοποιημένου (authenticated).
Το uplink interface υλοποιείται με την χρήση ***TUN/TAP driver***. Όταν το **chilli** ξεκινά, εγκαθίσταται ένα tun interface, και προαιρετικά καλείται ένα εξωτερικό configuration script.
Το **TUN** και **TAP** είναι virtual network διατάξεις του kernel που υποστηρίζονται παντού στο software.
Το **TAP** εξομοιώνει μια διάταξη *link layer* και λειτουργεί με πακέτα *layer 2* όπως τα *Ethernet frames*. Το **TUN** εξομοιώνει μία *network layer* διάταξη και λειτουργεί με πακέτα *layer 3* όπως τα πακέτα IP. Το TAP χρησιμοποιείται για να δημιουργήσει μια *network bridge*, ενώ το TUN χρησιμοποιείται με την δρομολόγηση.
Στα συγκεκριμένα Ubuntu 12.04 το tun module περιέχεται κατά την εγκατάσταση.
Σε άλλα linux όμως πρέπει να εγκατασταθεί.

5.3 Εγκατάσταση του λειτουργικού συστήματος Ubuntu 12.04 LTS 32-bit

1. Με τη χρήση usb installer (universal usb installer) επιλέγουμε *install Ubuntu on a Hard Disk*
   σύμφωνα με την παρακάτω εικόνα που βλέπουμε στην οθόνη.

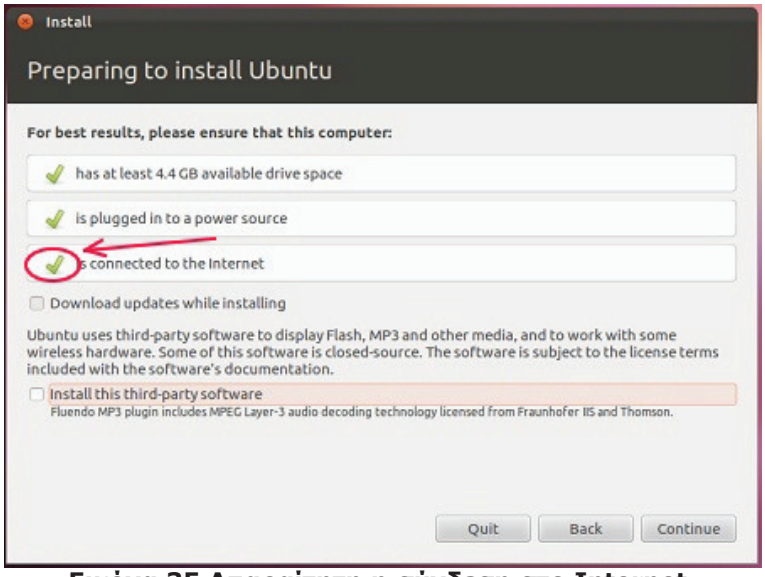
Εικόνα 33 Install Ubuntu on a Hard Disk.

2. Πατώντας TAB διαμορφώνουμε την εντολή
   >/casper/vmlinuz noprompt cdrom-detect/try-usb=true file=/cdrom/preseed/ubuntu.seed boot-casper persistent initrd=/casper/initrd.lz splash –
   σε
   >/casper/vmlinuz noprompt cdrom-detect/try-usb=true file=/cdrom/preseed/ubuntu.seed boot-casper persistent initrd=/casper/initrd.lz splash nomodeset—
3. Πατώντας ENTER ακολουθεί η εικόνα
4. Επιλέγουμε English → continue



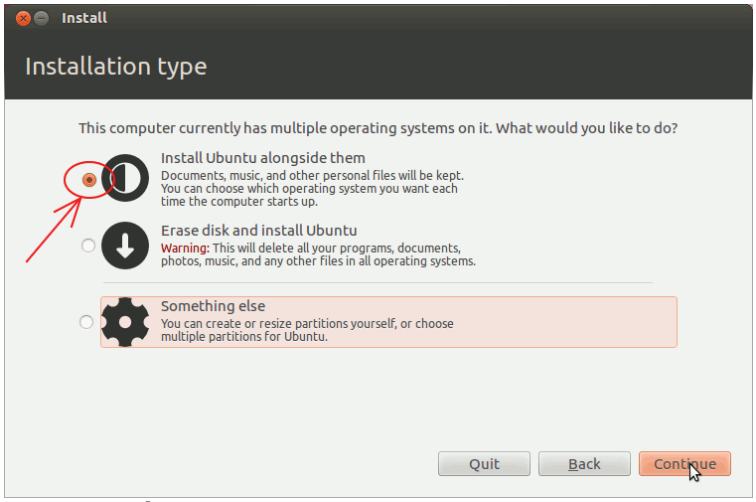
Εικόνα 34 Επιλέγουμε English για γλώσσα στα Ubuntu.

5. Σιγουρευόμαστε ότι είμαστε συνδεδεμένοι στο internet → continue



Εικόνα 35 Απαραίτητη η σύνδεση στο Internet.

6. Επιλέγουμε Install Ubuntu alongside them → continue



Εικόνα 36 Install Ubuntu alongside them.

Στις επόμενες οθόνες θα πρέπει να συμπληρωθούν οι δικές μας πληροφορίες (username, password, e.t.c.) και τελικά η εγκατάσταση θα ξεκινήσει.

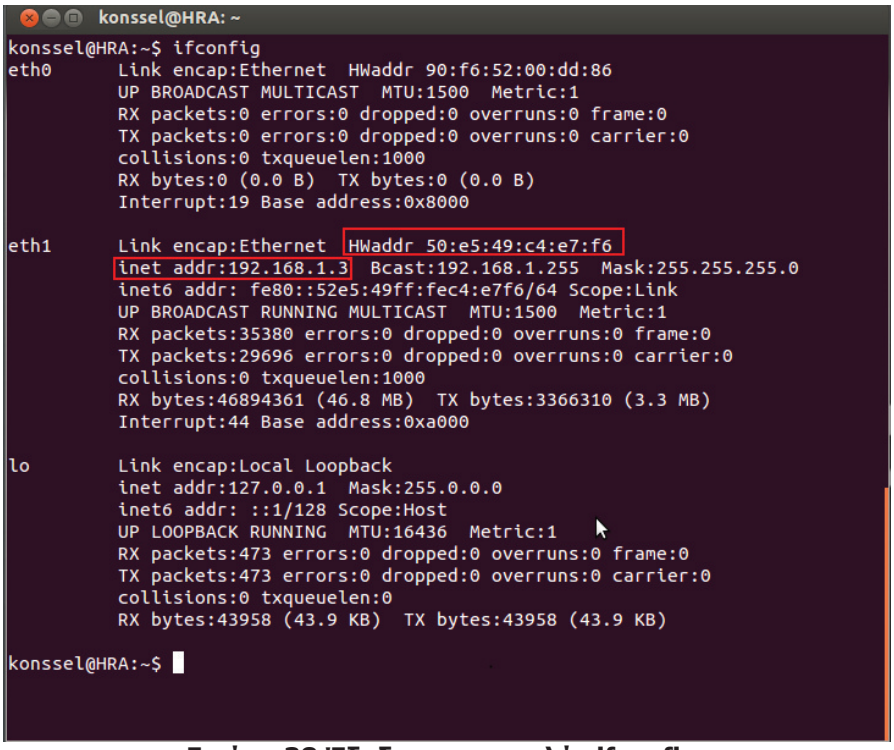
Εικόνα 37 Έναρξη Εγκατάστασης.

7. Όταν τελειώσει εκτελούμε Restart όπως απαιτείται.

5.4 Διαμόρφωση των interfaces

Απαιτείται η χρήση δύο καρτών δικτύου, δηλαδή η ύπαρξη δύο network interfaces. Η eth0 χρησιμοποιείται για πρόσβαση στο Internet ενώ η eth1 για σύνδεση με Wireless Access Point (Cisco Aironet 1100) (ή PC laptop για testing στο πειραμά μας). Αρχικά πρέπει να δούμε ποια interfaces υπάρχουν και σε τι διευθύνσεις αντιστοιχούν.

1. Έτσι ανοίγουμε ένα τερματικό (ALT+CTRL+T) και πληκτρολογούμε την εντολή *& ifconfig*
   Και η έξοδος πρέπει να είναι κάπως έτσι:



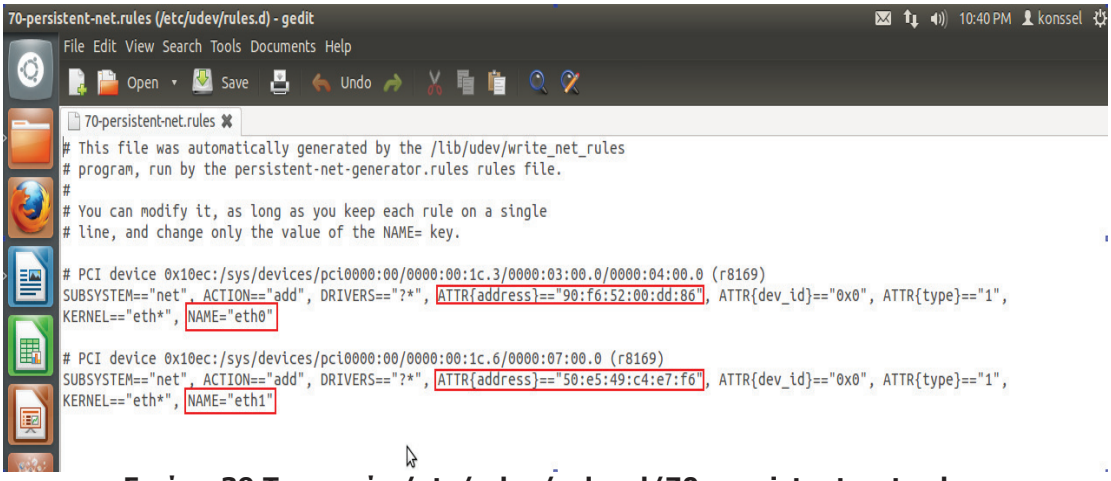
Εικόνα 38 Έξοδος της εντολής ifconfig.

Στην περίπτωσή μας παρατηρούμε ότι το αποτέλεσμα δεν είναι το επιθυμητό. Θα θέλαμε η *eth0* να αντιστοιχεί στην παροχή σύνδεσης στο Internet (να συνδέεται δηλαδή με το *router*), και η *eth1* να χρησιμοποιείται εκεί που θα ακούει το *Captive Portal* και θα συνδέεται το *Access Point*.

2. Προκειμένου να αποδώσουμε στην αντίστοιχη MAC address το επιθυμητό interface (*eth0 / eth1*) ανοίγουμε το αρχείο ***/etc/udev/rules.d/70-persistent-net.rules***
   Από το τερματικό αυτό γίνεται πληκτρολογώντας

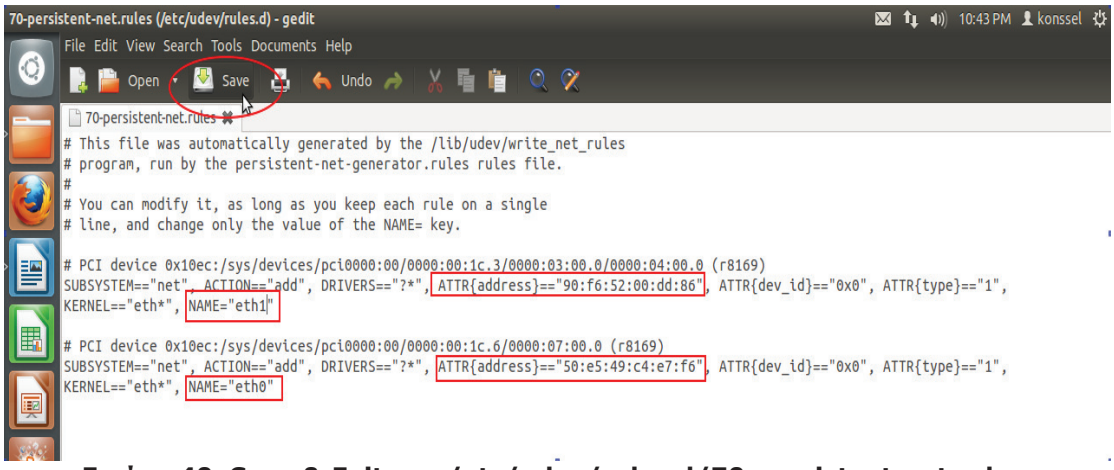
   $sudo gedit /etc/udev/rules.d/70-persistent-net.rules

   (sudo είναι απαραίτητο για να διαμορφώσει κανείς το οτιδήποτε σχεδόν μέσα στο /etc/ παρέχοντας περισσότερα προνόμια στον χρήστη). Το gedit ανοίγει το αρχείο και βλέπουμε τις διευθύνσεις των καρτών μας καθώς και τα ονόματά τους. Εμείς απλώς αντιστρέφουμε τα στοιχεία στο NAME όπως φαίνεται παρακάτω.



Εικόνα 39 Το αρχείο /etc/udev/rules.d/70-persistent-net.rules.

3. save και exit



Εικόνα 40 Save & Exit του /etc/udev/rules.d/70-persistent-net.rules.

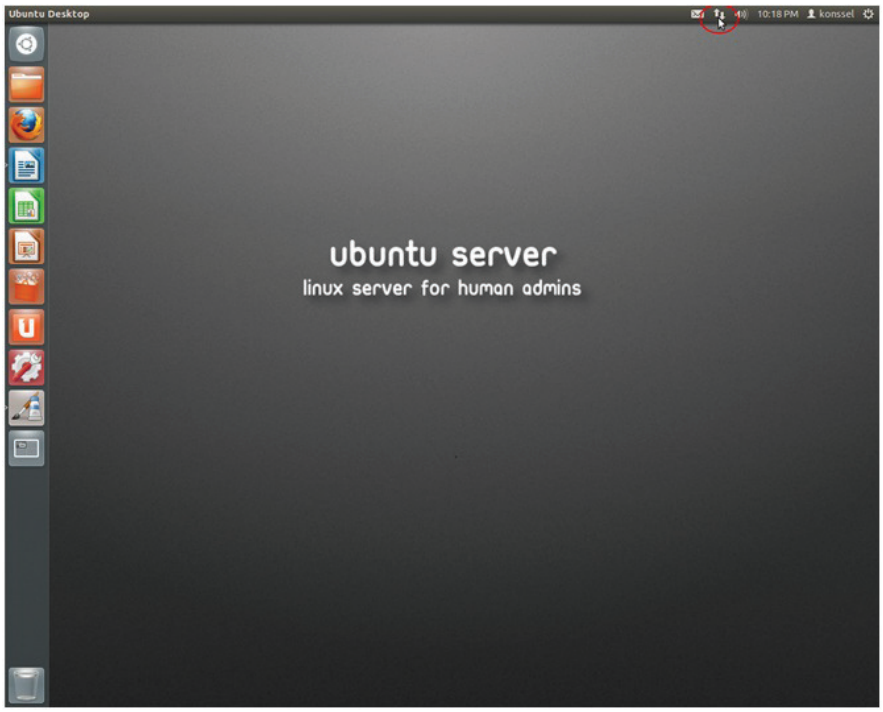
4. Για να έχουν αποτέλεσμα οι αλλαγές πρέπει να γίνει reboot.

<u>Μετά το reboot</u>

Για να ελέγξουμε αν οι ρυθμίσεις έγιναν σωστά χρησιμοποιούμε την εντολή:
& route -n ή εναλλακτικά netstat -nr

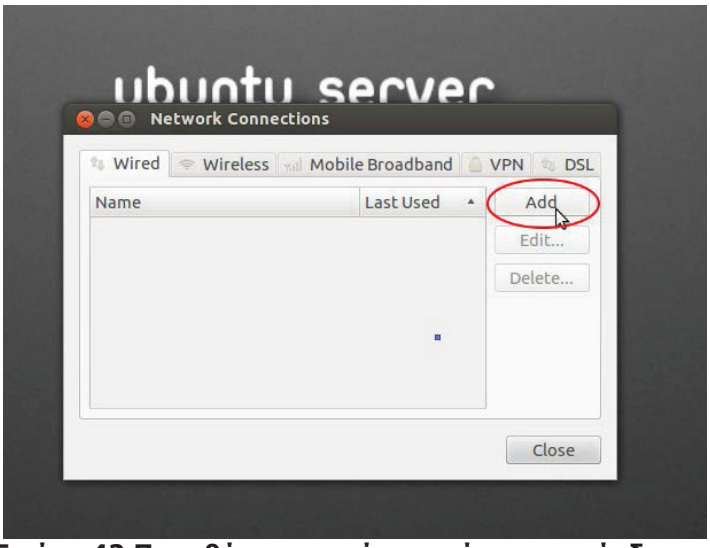
Πρέπει να διαμορφώσουμε δύο connections.
Η πρώτη είναι για internet connection (eth0)

1. Έτσι ανοίγουμε το *network manager → edit connections*



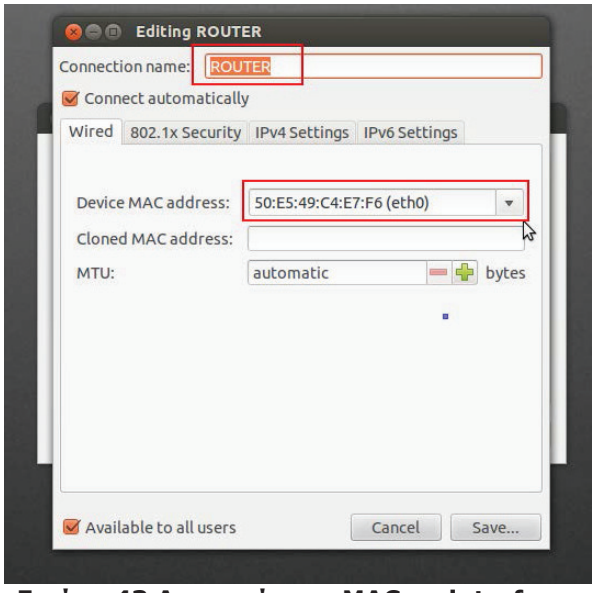
Εικόνα 41 Network Manager για διαμόρφωση των interfaces.

2. *ADD connection*



Εικόνα 42 Προσθήκη μιας νέας ενσύρματης σύνδεσης.

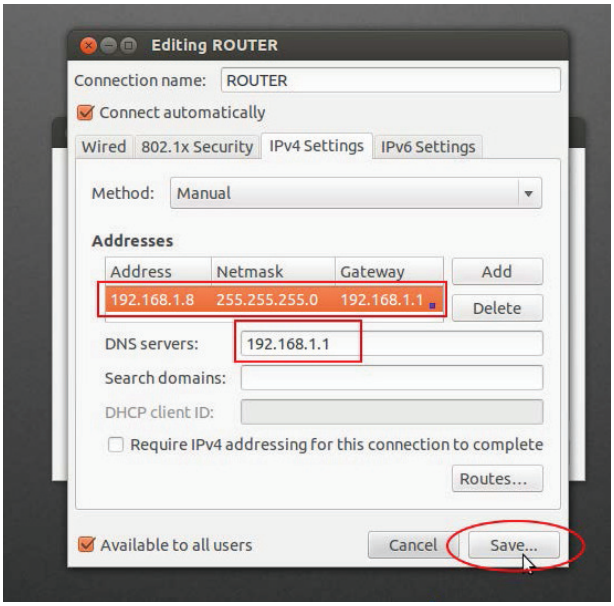
3. Κάτω από το tab 'wired'
   Connection name: ROUTER
   Device mac address: eth0



Εικόνα 43 Αντιστοίχηση MAC με interface.

4. Κάτω από το tab ipv4 settings
   Method>Manual προκειμένου να ορίσουμε static ip address
   Address: 192.168.1.9 (static ip για την eth0)
   Subnet Mask: 255.255.255.0
   Gateway: 192.168.1.1 (ip router)
   DNS Sever: 192.168.1.1

5. Save και exit.

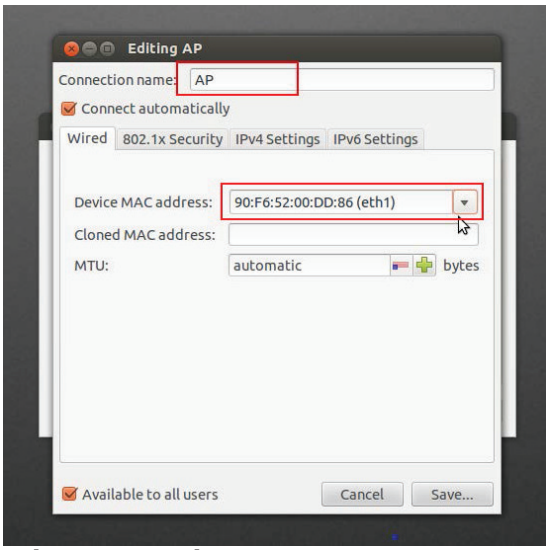


Εικόνα 44 Static Ip για το eth0.

Πρέπει να κάνουμε το ίδιο και για την eth1 στην οποία θα ακούει το Chillispot και θα συνδέεται το Access Point.

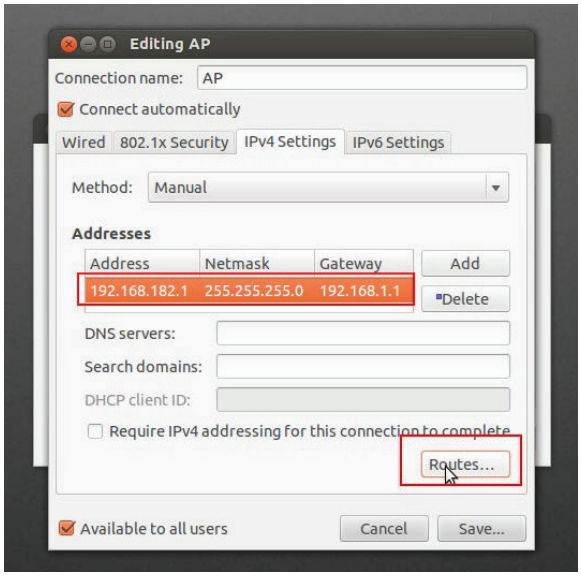
1. edit connections → ADD
- Κάτω από το tab 'wired'

Connection name: AP
Device mac address: eth1



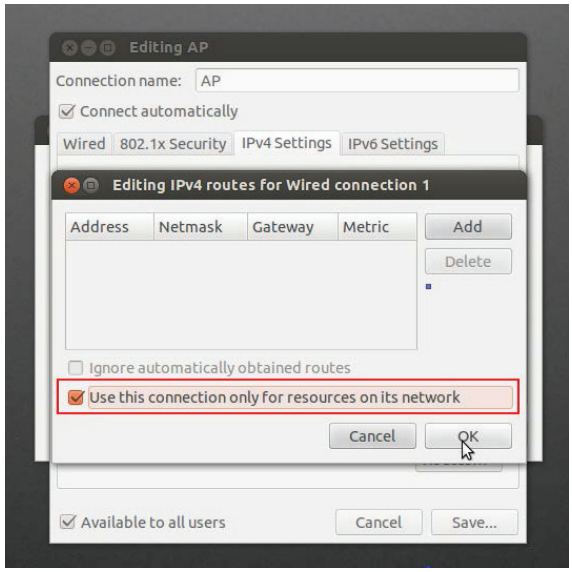
Εικόνα 45 Διαμόρφωση του eth1 interface.

- Κάτω από το tab ipv4 settings
  Address: 192.168.182.1 (το Chillispot ακούει by default MONO στο υποδίκτυο 192.168.182.0/24)
  Subnet Mask: 255.255.255.0
  Gateway: 192.168.1.1 (Router's ip)



Εικόνα 46 Satic IP για το eth1 interface.

2. Επίσης πρέπει να πάμε στο κουμπί 'Routes' και να ενεργοποιήσουμε την επιλογή *Use this connection only for resources on its network*
3. Εάν δεν το κάνουμε θα έχουμε είτε την eth0 είτε την eth1, ποτέ μαζί και δεν θα καταφέρουμε να συνδεόμαστε στο Internet.



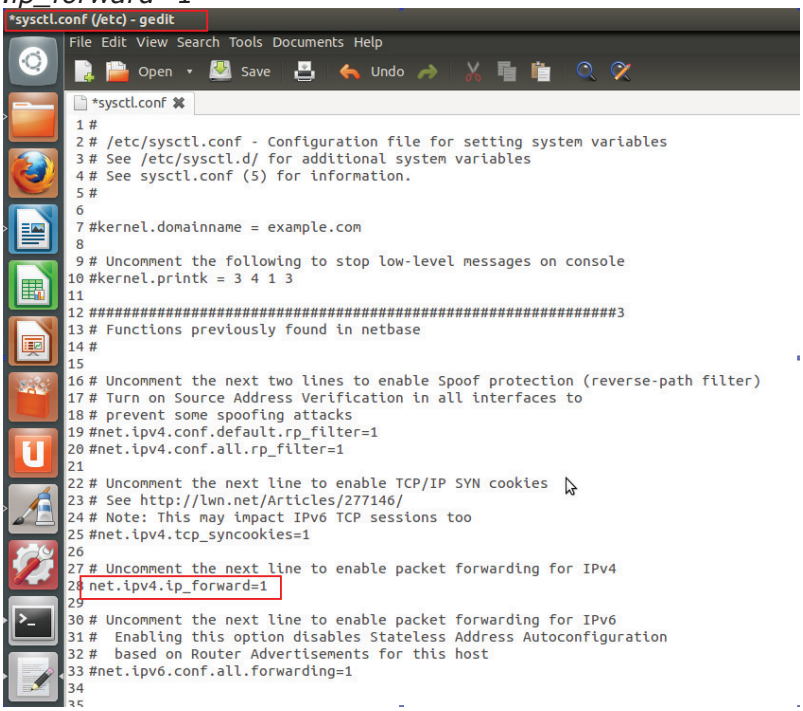
Εικόνα 47 Use this connection only for resources on its network.

- ✓ Σημαντικό είναι να βεβαιωθούμε ότι είναι ενεργοποιημένο το ipv4 packet forwarding στο αρχείο ***/etc/sysctl.conf***, πατώντας την εντολή

  & cat /proc/sys/net/ipv4/ip_forward (θα πρέπει να βγάζει έξοδο 1 αν είναι ενεργοποιημένο)

  ή με την εντολή

  & sudo gedit /etc/sysctl.conf και κάνοντας *uncomment την γραμμή 28 > net.ipv4.ip_forward=1*



Εικόνα 48. Το αρχείο /etc/sysctl.conf.

- ♦ Οι συσκευές μας προωθούν τα πακέτα ipv4 η μία στην άλλη. Γι' αυτό δίνουμε την εντολή:

& echo 1 > /proc/sys/net/ipv4/ip_forward

- Για να σιγουρευτούμε ότι δεν θα υπάρχει κάποιο πρόβλημα σχετικά με το firewall κάνουμε όλες τις IP που θα βγαίνουν από την eth0 (δηλαδή που θα έχουν πρόσβαση στο Internet) να φαίνονται σαν μία ΜΟΝΑΔΙΚΗ IP πληκτρολογώντας στο τερματικό:

  & iptables -t nat -A POSTROUTING -j MASQUERADE -o eth0

- Για να ισχύουν οι εντολές σε κάθε reboot του υπολογιστή χωρίς να χρειάζεται να τις δίνουμε εμείς manually κάθε φορά διαμορφώνουμε το αρχείο ***/etc/rc.local***

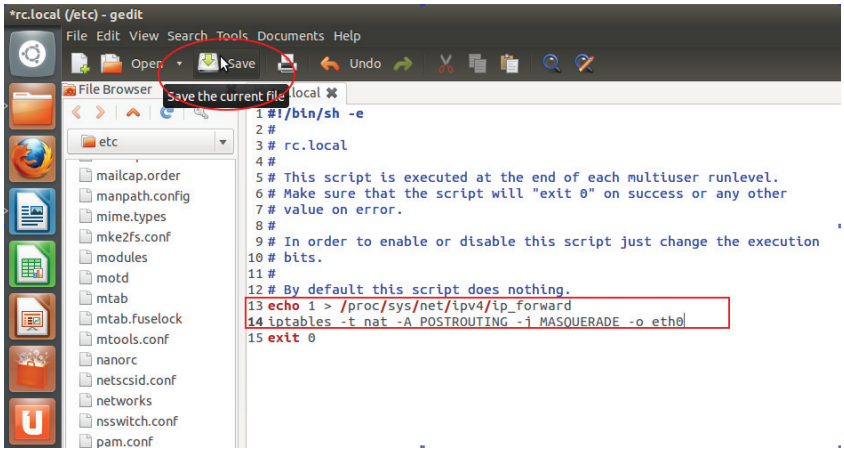
  & sudo gedit /etc/rc.local

  προσθέτοντας (πριν το exit 0)

  echo 1 > /proc/sys/net/ipv4/ip_forward

  iptables -t nat -A POSTROUTING -j MASQUERADE -o eth0

  save και exit



Εικόνα 49 Διαμόρφωση του αρχείου /etc/rc.local.

- Έπειτα με την εντολή

  $ chmod 755 rc.local

  ορίζουμε ότι μπορούν να το διαβάζουν και να το εκτελούν όλοι και επιπλέον ο κάτοχος του αρχείου μπορεί να γράψει σε αυτό.

5.5 Εγκατάσταση του Apache 2

1. Η λήψη των πακέτων γίνεται με την εξής εντολή:

   $ sudo apt-get install apache2 apache2-mpm-worker apache2-utils apache2.2-bin apache2.2-common libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap

2. Για να ξεκινήσει ο apache2:
   & sudo /etc/init.d/apache2 start

Εάν κατά την εκκίνηση του apache φανεί το παρακάτω:

konssell@HRA:~$ sudo /etc/init.d/apache2 start
[sudo] password for konssell:
 * Starting web server apache2 apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName
httpd (pid XXXXX) already running
[OK]

πρέπει να πάμε στο αρχείο ***/etc/apache2/httpd.conf*** και να εισάγουμε την παρακάτω γραμμή:

ServerName localhost

Και στο αρχείο **/etc/hosts**

127.0.0.1 localhost
127.0.1.1 HRA HRA.local

(προσθέτουμε ένα επιπλέον host το οποίο αντιστοιχεί στο όνομα του υπολογιστή που εισάγαμε κατά το installation των Ubuntu).
Για να λειτουργήσουν οι αλλαγές εκτελούμε reboot.
Έτσι ο apache server ακούει μόνο στην port 80 (*http*) και πρέπει να επιτρέψουμε να ακούει και στην port 443 (*SSL,https*).

ΣΗΜΕΙΩΣΗ

Στο αρχείο ***/etc/hosts*** κάθε γραμμή ξεκινά με μια *IP address* που συνοδεύεται από το σχετικό *hostname* με την παρακάτω μορφή.

127.0.0.1 localhost
127.0.1.1 <hostname> <hostname>.<domain.name>

Το Debian ή το Ubuntu installer δημιουργούν την γραμμή 127.0.1.1, για ένα σύστημα με μια μη μόνιμη IP address, η οποία μπορεί να μην συναντιέται σε άλλα linux. Κάποια λογισμικά (όπως το Gnome) αναμένουν το hostname του συστήματος να αναλύεται σε μια IP address με ένα κανονικό πλήρης domain name. Αυτό κανονικά είναι ανάρμοστο γιατί hostnames και domain names είναι δύο διαφορετικά πράγματα. Για την υποστήριξη, λοιπόν, αυτού του λογισμικού είναι απαραίτητο να εξασφαλισθεί ότι το hostname του συστήματος μπορεί να αναλυθεί. Αν το σύστημα έχει μια μόνιμη IP address, αντικαθιστούμε την IP 127.0.1.1 με την μόνιμη.

5.6 Εγκατάσταση mysql server

Για να δημιουργήσουμε cerificates για https πρέπει να εγκαταστήσουμε mysql server.

$ sudo apt-get install libdbd-mysql-perl libdbi-perl libhtml-template-perl libmysqlclient18 libnet-daemon-perl libplrpc-perl mysql-client-5.5 mysql-client-core-5.5 mysql-common mysql-server mysql-server-5.5 mysql-server-core-5.5

Όταν ξεκινά η εγκατάσταση, ένα GUI μας ζητά να εισάγουμε το δικό μας mysql server Admin password. Για να συμβεί αυτή η διαμόρφωση απαιτείται reboot.

5.7 Κατασκευή των certificates

Θα δημιουργήσουμε *snakeoil certificate*. *Self-signed certificate* είναι ένα πιστοποιητικό ταυτότητας το οποίο υπογράφεται από την ίδια οντότητα της οποίας πιστοποιεί την ταυτότητα. Αυτός ο όρος δεν έχει καμία σχέση με την ταυτότητα του προσώπου ή της οργάνωσης που εκτέλεσαν πραγματικά τη διαδικασία υπογραφής. Με τεχνικούς όρους, ένα self-signed certificate είναι αυτό που υπογράφεται με το δικό του *private key*.

Δημιουργία ενός self-signed certificate:

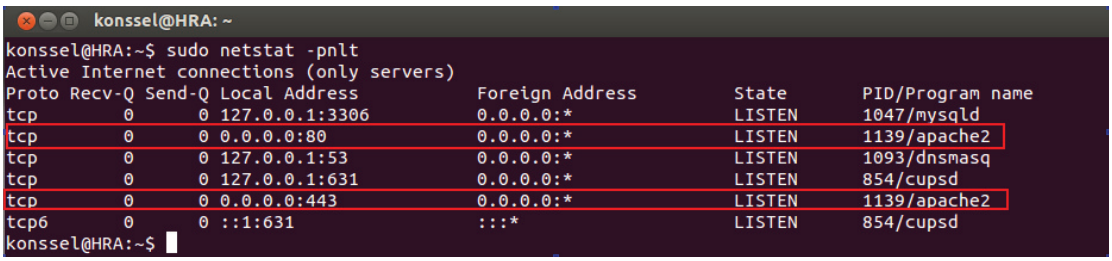
$ make-ssl-cert generate-default-snakeoil –force-overwrite

Δημιουργεί τα επόμενα αρχεία:
/etc/ssl/private/ssl-cert-snakeoil.key
/etc/ssl/certs/ssl-cert-snakeoil.pem

- Ενεργοποίηση του Apache SSL module:
  $ a2enmod ssl
- Ενεργοποίηση του Apache default ssl virtual host:
  $ a2ensite default-ssl
- Restart Apache:
  $ service apache2 restart
  Ή εναλλακτικά
  & sudo /etc/init.d/apache2 restart

Για να δούμε εάν η διαμόρφωση του apache2 έγινε σωστά, εκτελούμε:
& sudo netstat -pnlt

Η έξοδος αυτής της εντολής φαίνεται παρακάτω:



Εικόνα 50 Έλεγχος σε ποιές ports ακούει ο apache με την εντολή sudo netstat –pnlt.

Όπως βλέπουμε ο Apache ακούει και στα δύο ports :80 και :443.

5.8 Εγκατάσταση του Freeradius

Με την εντολή:

$ sudo apt-get install freeradius freeradius-common freeradius-mysql freeradius-utils libfreeradius2

Διαμόρφωση του Freeradius

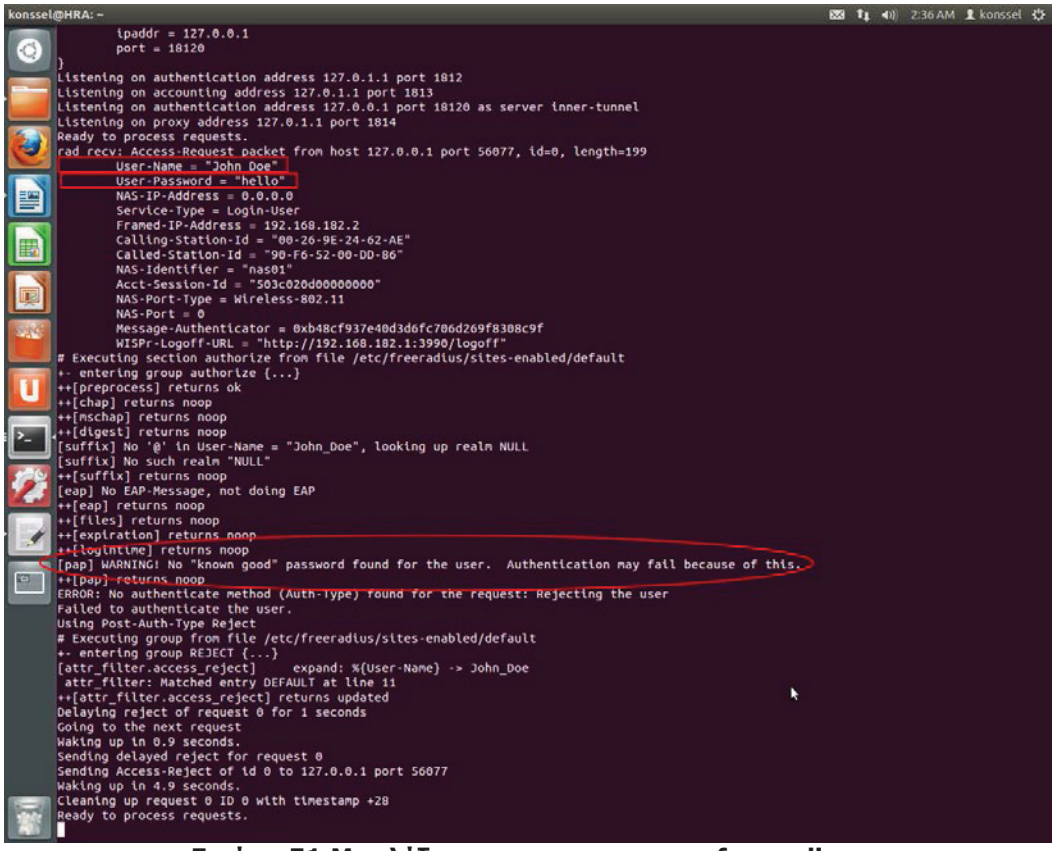
1. Στο αρχείο ***/etc/freeradius/users*** προσθέτουμε έναν χρήστη:
   #echo '"chilliuser"Cleartext-Password := "chillipassword"' >>/etc/freeradius/users

ή ανοίγουμε το αρχείο ***/etc/freeradius/users*** με το gedit και προσθέτουμε τις γραμμές:

"chilli user" Cleartext-Password := "chillipassword"
Reply-Message = "Hello, %{User-Name}, welcome to our hotspot!"

2. Διαμορφώνουμε το αρχείο ***/etc/freeradius/radiusd.conf***
   Για authentication
   line 273>ipaddr = 127.0.1.1
   line 283> port = 1812
   Για accounting
   line 316> ipaddr = 127.0.1.1
   line 318> port = 1813
3. Στο αρχείο ***/etc/freeradius/clients.conf***
   client localhost {
   ipaddr = 127.0.0.1
   ...
   secret = myfreesecret (είναι το μυστικό μεταξύ freeradius και localhost)
   }
   Και προσθέτουμε έναν ακόμα client
   client 127.0.1.1 {
   secret = myfreesecret (είναι το μυστικό μεταξύ freeradius και client)
   }

ΣΗΜΕΙΩΣΗ
Προτείνεται η χρήση μίας λέξης για user-name και μίας λέξης για password επειδή μερικές φορές παρατηρείται το εξής (π.χ εάν κάνουμε uncomment τη γραμμή 90 στο **/etc/freeradius/users** #"John Doe" Cleartext-Password := "hello"):



Εικόνα 51 Μια λέξη για username στον freeradius.

Γι' αυτόν τον λόγο πρέπει να διαμορφώσουμε το αρχείο ***eap.conf*** το οποίο βρίσκεται στο **/etc/freeradius/** και να πράξουμε ανάλογα. Ωστόσο, με την *pap authentication* δεν πρέπει να χρησιμοποιούμε κενά στο *username* και *password*.

5.9 Chillispot

Εγκατάσταση Chillispot
Για την εγκατάσταση του *chillispot* (version 1.0-10.1) χρησιμοποιούμε την εντολή:

$ sudo apt-get install chillispot

Κατά τη διάρκεια της εγκατάστασης, μας ζητείται να συμπληρώσουμε τις παρακάτω δικές μας πληροφορίες μέσω ενός *GUI:*
Radius shared secret : myfreesecret
Ethernet interface for DHCP to listen : eth1
Url of UAM server :https://192.168.1.8/cgi-bin/hotspotlogin.cgi
Url of UAM homepage : https://192.168.1.8
Shared password between chillispot and webserver: mychillisecret

Διαμόρφωση του Chillispot
Στο αρχείο ***/etc/chilli.conf***, uncomment και edit τα παρακάτω:

59 dns1 192.168.1.1
66 dns2 192.168.1.1
72 domain key.chillispot.org
99 radiusserver1 127.0.1.1
106 radiusserver2 127.0.1.1
113 radiusauthport 1812
120 radiusacctport 1813
125 radiussecret myfreesecret
176 dhcpif eth1
196 uamserver https://192.168.1.8/cgi-bin/hotspotlogin.cgi
203 #uamhomepage https://192.168.1.8 *must be commented*
207 uamsecret mychillisecret

Οπωσδήποτε η γραμμή 203 (uamhomepage) πρέπει να είναι σε σχόλιο (commented) γιατί θέλουμε όλοι οι χρήστες να περνάνε από την σελίδα hotspotlogin.cgi για authentication. Εάν δεν μπει, όλοι οι clients θα γίνονται redirect στην σελίδα του apache και δεν θα υπάρχει τρόπος να πιστοποιηθούν.
Εκτελούμε τις εντολές:

$sudo cp /usr/share/doc/chillispot/hotspotlogin.cgi /usr/lib/cgi-bin/
$sudo chmod 755 /usr/lib/cgi-bin/hotspotlogin.cgi

Και στο αρχείο ***/usr/lib/cgi-bin/hotspotlogin.cgi***

line 27> $uamsecret = "ht2eb8ej6s4et3rg1ulp"; (uncomment)
αντικαθιστούμε με
$uamsecret = "mychillisecret";
line 31>$userpassword=1; (uncomment)

5.10 Iptables

Εκτελούμε τις εντολές:

$ sudo cp /usr/share/doc/chillispot/firewall.iptables /etc/init.d/chilli.iptables
$ sudo chmod u+x /etc/init.d/chilli.iptables

$ ln -s /etc/init.d/chilli.iptables /etc/rcS.d/S40chilli.iptables

Καθώς και

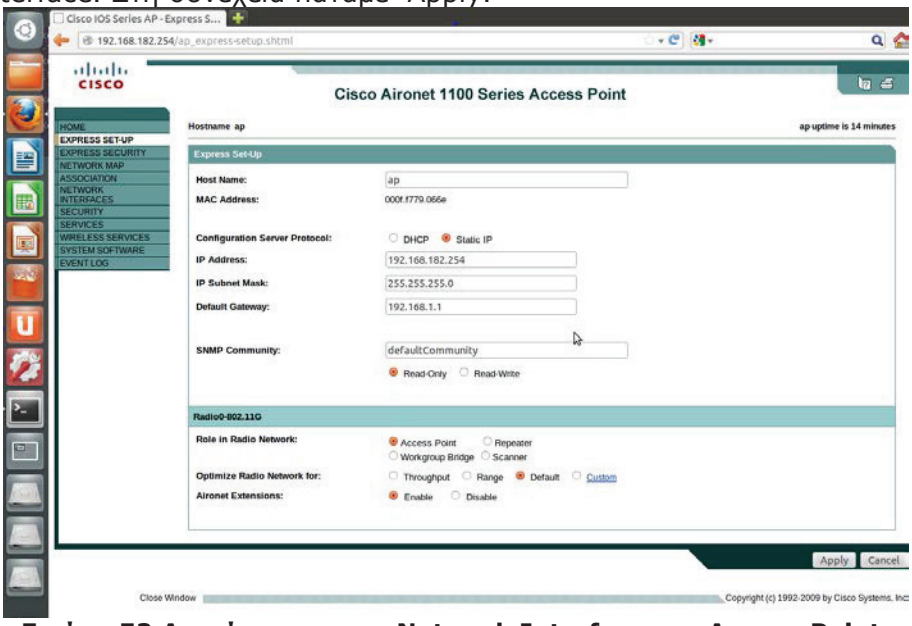
$sudo su
#iptables -I FORWARD -i eth0 -o eth1 -j ACCEPT
#iptables -I FORWARD -i eth1 -o eth0 -j ACCEPT

γιατί θέλουμε η κίνηση να προωθείται από την eth0 στην eth1 και αντίστροφα.

5.11 Διαμόρφωση του Access Point

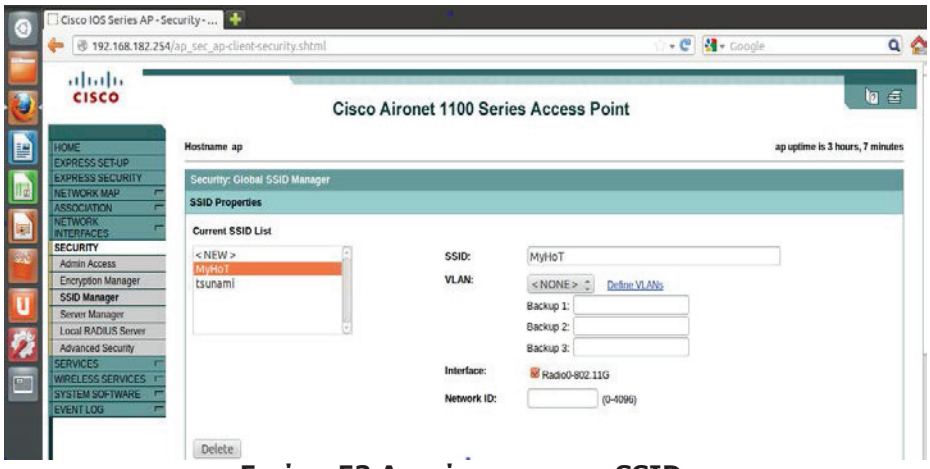
Cisco Aironet 1100
Static ip address: 192.168.182.254
Subnet Mask 255.255.255.0
Default Gateway: 192.168.182.1

Δεν πρέπει να είναι καμία πολιτική ασφαλείας επιλεγμένη, ούτε DHCP server. Όλη την δουλειά την κάνει το Chillispot αντί για το Access Point. Το Access Point απλώς προσφέρει μια ασύρματη διεπαφή που μπορεί να δέχεται τους ασύρματους Clients.
Από το μενού επιλέγουμε EXPRESS SETUP και πληκτρολογούμε τις πληροφορίες για το Network Interface. Στη συνέχεια πατάμε Apply.



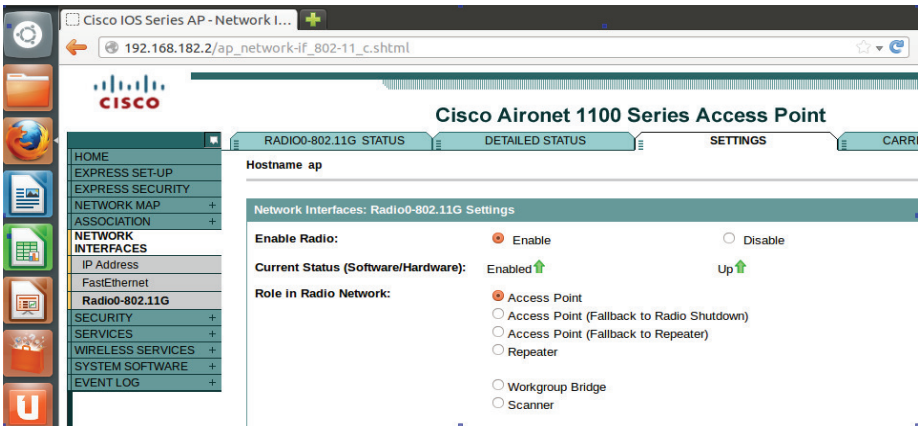
Εικόνα 52 Διαμόρφωση του Network Interface του Access-Point.

Στο Tab *SECURITY->SSID MANAGER* δημιουργούμε ένα *SSID:MyHoT* και κλικάρουμε το *RADIO-802.11g.* Τέλος, Apply.



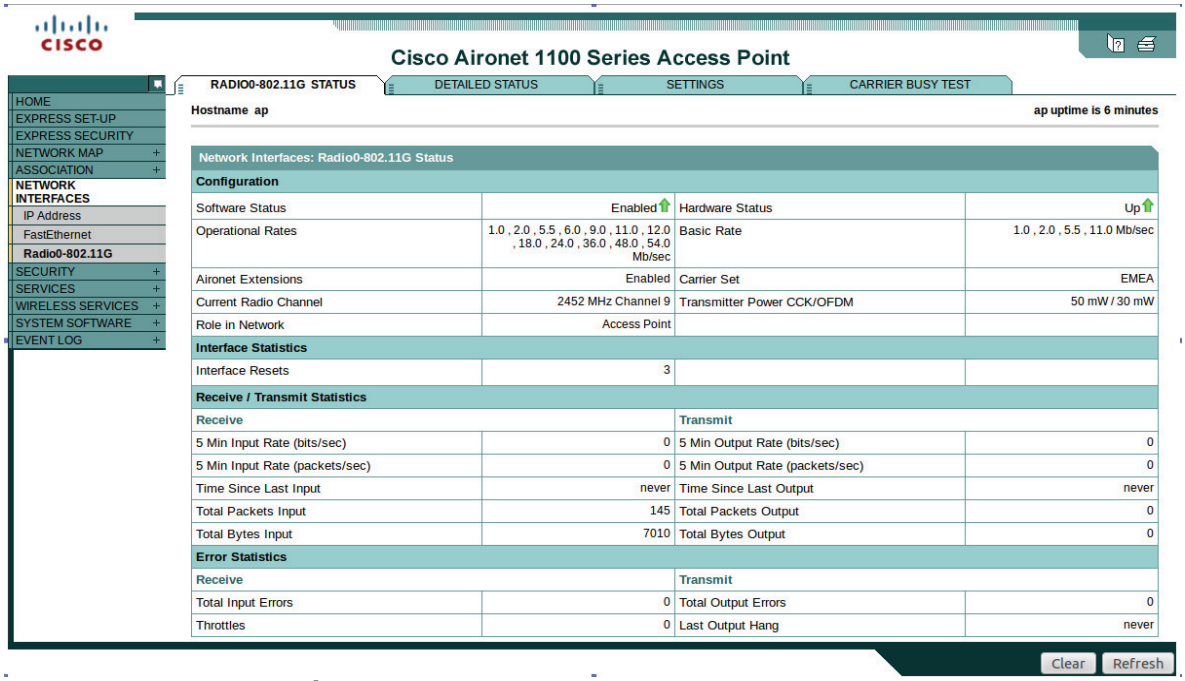
Εικόνα 53 Διαμόρφωση του SSID.

Επίσης ελέγχουμε αν το RADIO-802.11G είναι enabled και up στο Network Interfaces->Radio-802.11G->SETTINGS->Enable Radio=enabled.



Εικόνα 54 Διαμόρφωση του RADIO-802.11G να είναι enabled και up.

Σιγουρευόμαστε για την σωστή διαμόρφωση του RADIO-802.11G στο RADIO-802.11G Status->Software Status.



Εικόνα 55 RADIO-802.11G status, enabled & up.

5.12 Χρήσιμες Εντολές

```
netstat -ilpn   --> Kernel Interface table
netstat -ilpne          (ifconfig)
sudo netstat -nr        (route -n)
            -n, --numeric       don't resolve names
            -r, --route         display routing table
sudo netstat -penaltu
            -p, --programs          display PID/Program name for sockets
            -e, --extend            display other/more information
            -n, --numeric           don't resolve names
            -a, --all, --listening  display all sockets (default: connected)
            -l, --listening         display listening server sockets
            -t, --tcp
            -u, --udp
```

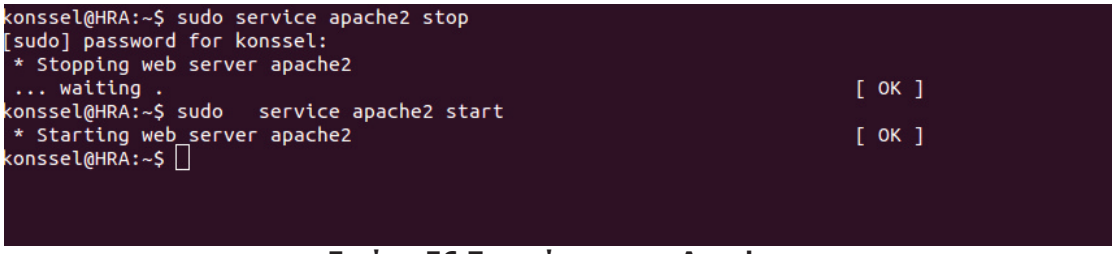
5.13 Debugging

Freeradius: & sudo freeradius -X
Chillispot: & sudo chilli --debug --fg

5.14 Λειτουργία

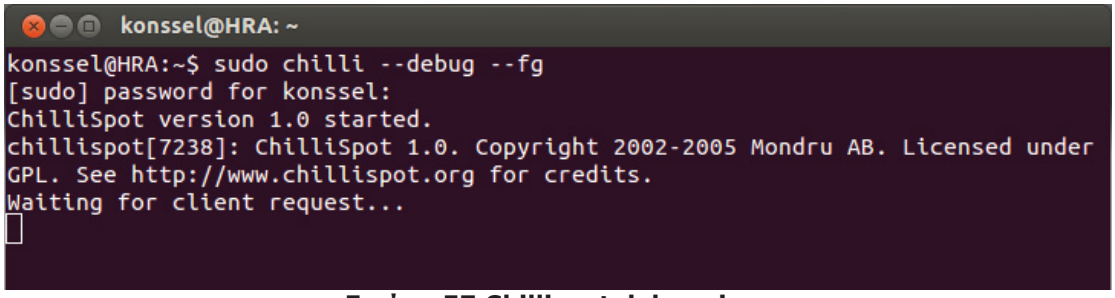
Start τον Apache:

& sudo service apache start

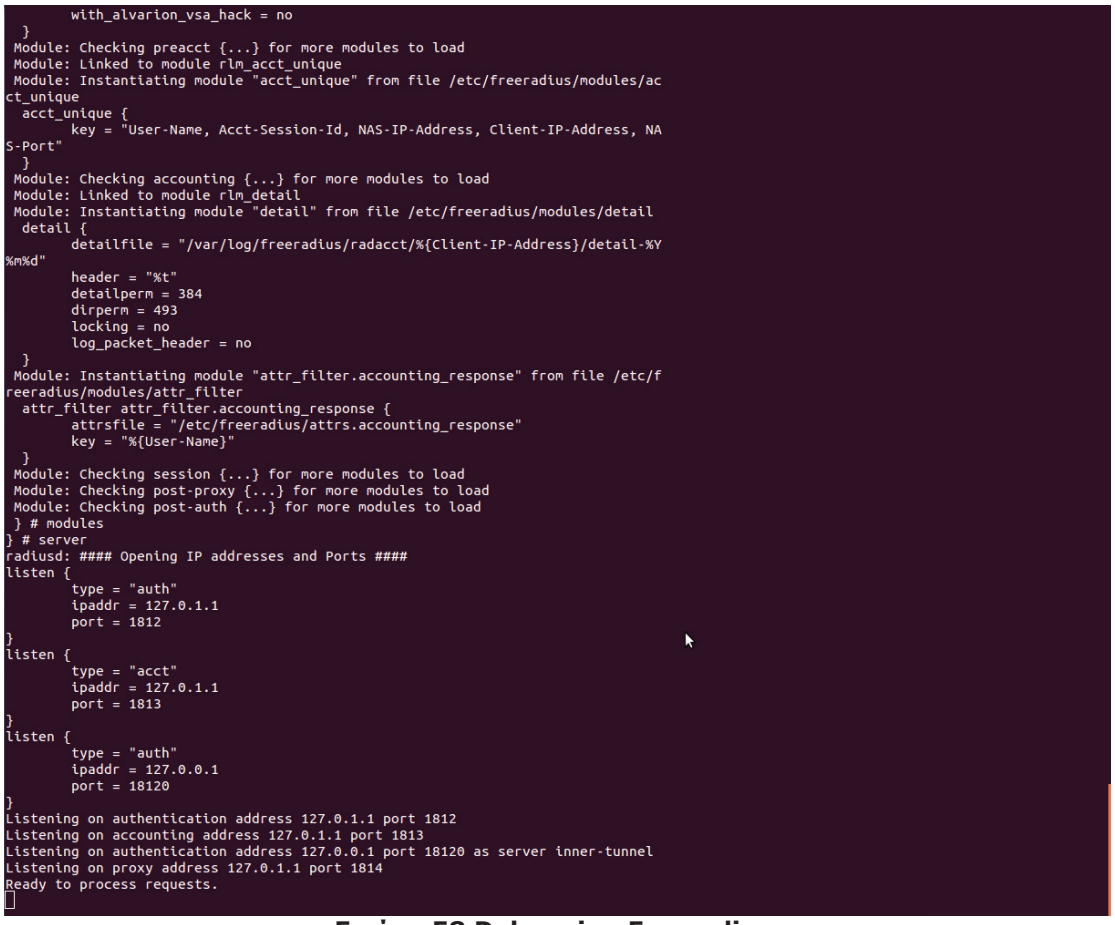


Εικόνα 56 Ξεκινώντας τον Apache.

Debug τον Freeradius και το Chillispot.

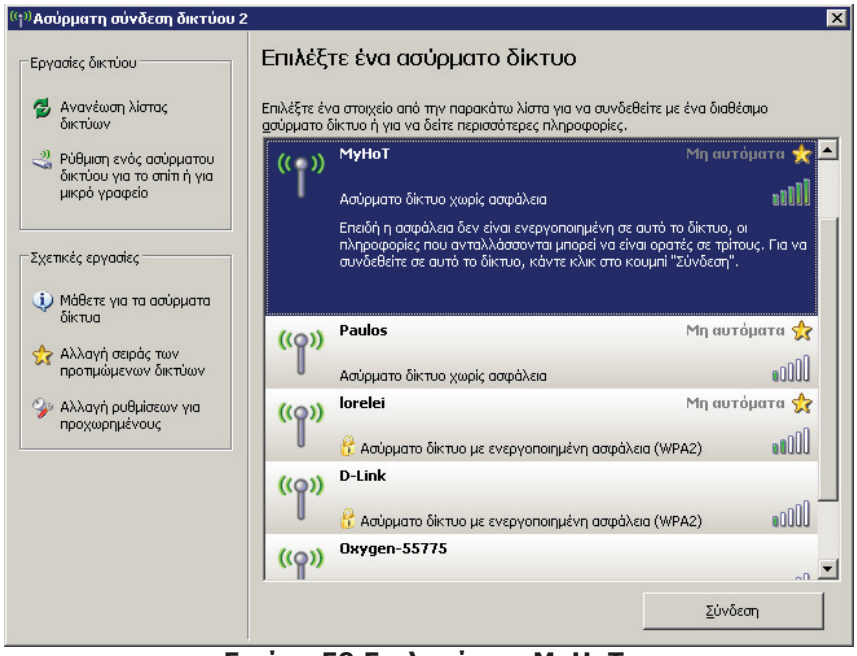


Εικόνα 57 Chillispot debugging.

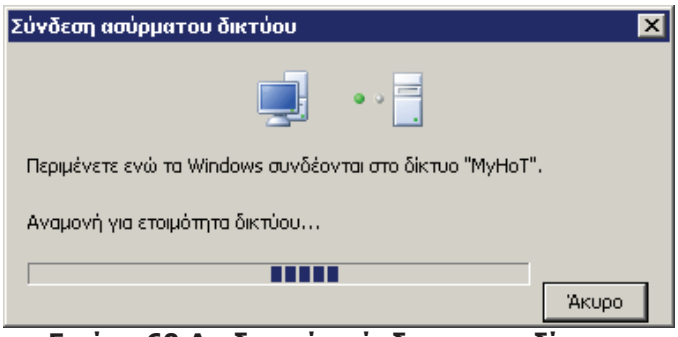


Εικόνα 58 Debugging Freeradius.

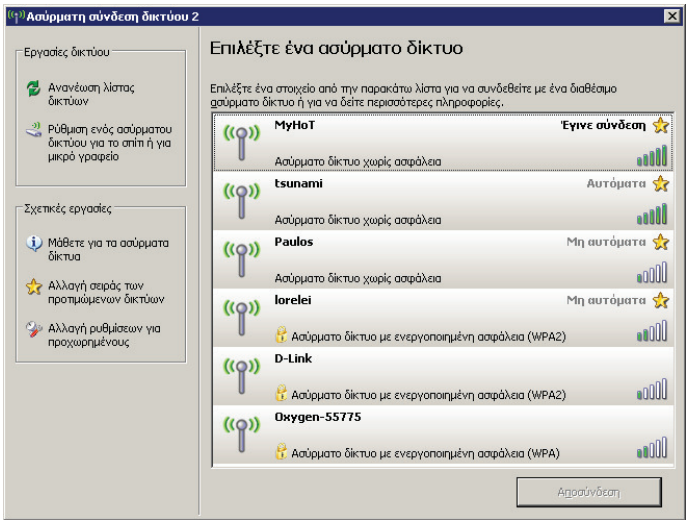
Αφού βεβαιωθούμε ότι όλα λειτουργούν, δοκιμάζουμε το test μέσω ενός laptop (ACER Aspire one με λειτουργικό σύστημα Windows XP) που παίζει τον ρόλο ενός client. Πηγαίνουμε στα ασύρματα δίκτυα και επιλέγουμε το MyHoT που αντιστοιχεί στο δικό μας.



Εικόνα 59 Επιλογή του MyHoT.

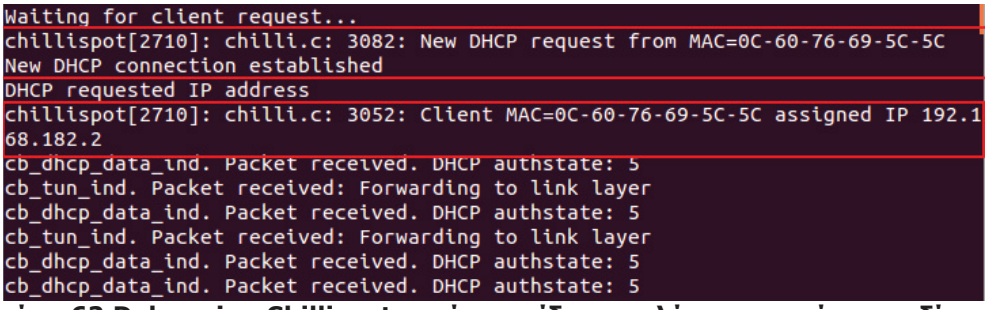


Εικόνα 60 Διαδικασία σύνδεσης στο δίκτυο.



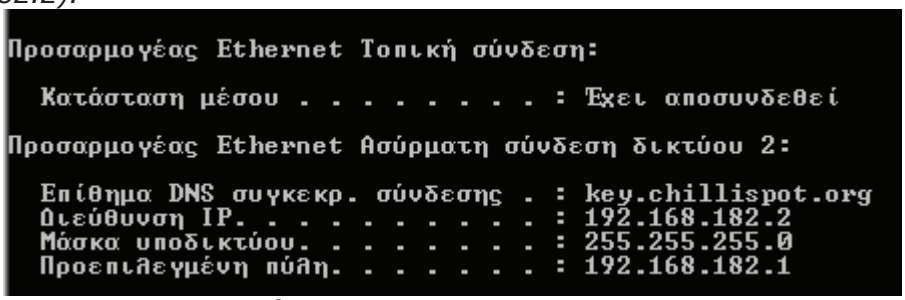
Εικόνα 61 Επιτυχής σύνδεση στο MyHoT.

Κατά τη διάρκεια της σύνδεσης στο Myhotspot, αυτό που βλέπουμε στο chillispot είναι η παρακάτω οθόνη.



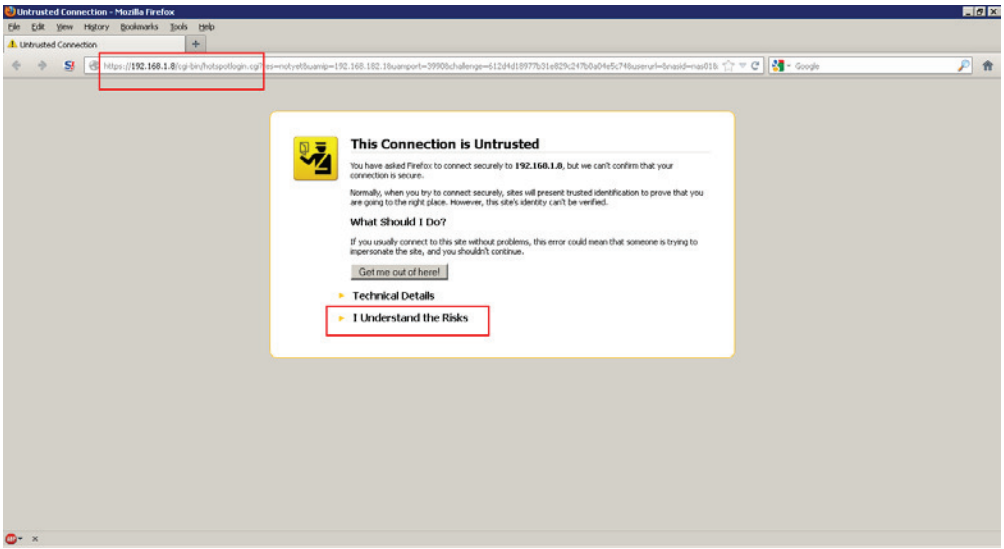
Εικόνα 62 Debugging Chillispot κατά την είδοσο πελάτη στο ασύρματο δίκτυο.

Επιπλέον, στο netbook, πηγαίνωντας στο command line των Windows, πληκτρολογούμε την εντολή *ipconfig* και βλέπουμε την ίδια IP με αυτή που μας έδωσε το *Chilli (192.168.182.2).*



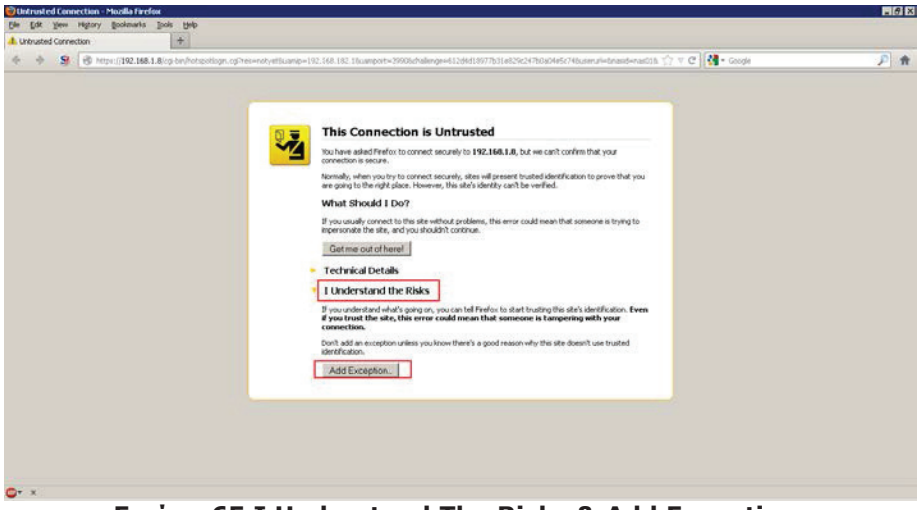
Εικόνα 63 Ipconfig στο netbook.

Στη συνέχεια ανοίγουμε τον browser. Πληκτρολογούμε μία διεύθυνση (www.tesyd.teimes.gr).



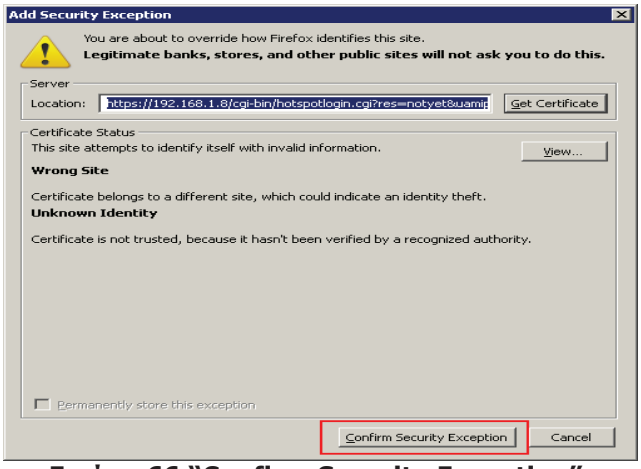
Εικόνα 64 Ανακατεύθυνση της διεύθυνσης.

Βλέπουμε ότι μας ανακατευθύνει στον Apache και συγκριμένα στο *hotspotlogin.cgi* το οποίο είναι η σελίδα login του chillispot για authentication. Επειδή η σελίδα είναι *https://* πρέπει να επιλέξουμε *"I Understand The Risks"*. Στη συνέχεια ξεδιπλώνεται ένα κείμενο και μια επιλογή *"Add Exception"* την οποία πρέπει να κλικάρουμε.



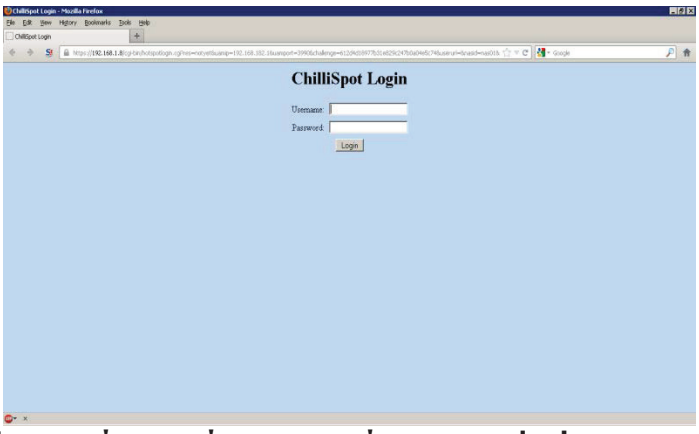
Εικόνα 65 I Understand The Risks & Add Exception.

Ανοίγει ένα παράθυρο στο οποίο πρέπει να πατήσουμε *"Confirm Security Exception"*.



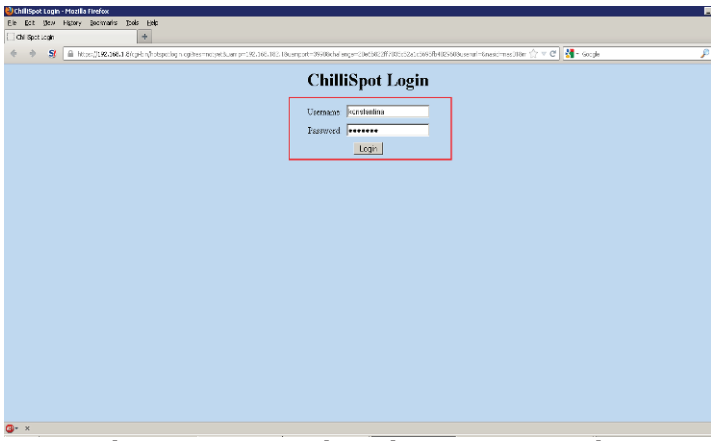
Εικόνα 66 "Confirm Security Exception".

Τελικά θα εισέλθουμε στην σελίδα login του chillispot για να εισάγουμε τα στοιχεία μας προς πιστοποίηση.



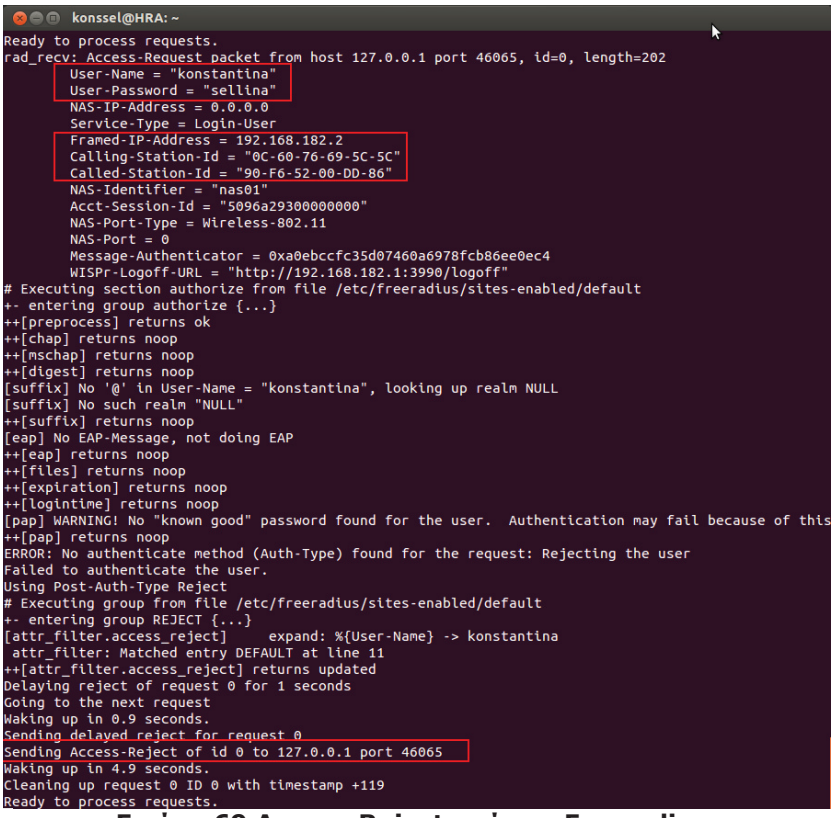
Εικόνα 67 Εισαγωγή στοιχείων πιστοποίησης στην login page του chillispot.

Εισάγουμε Username=konstantina Password=sellina, τα οποία δεν είναι έγκυρα.



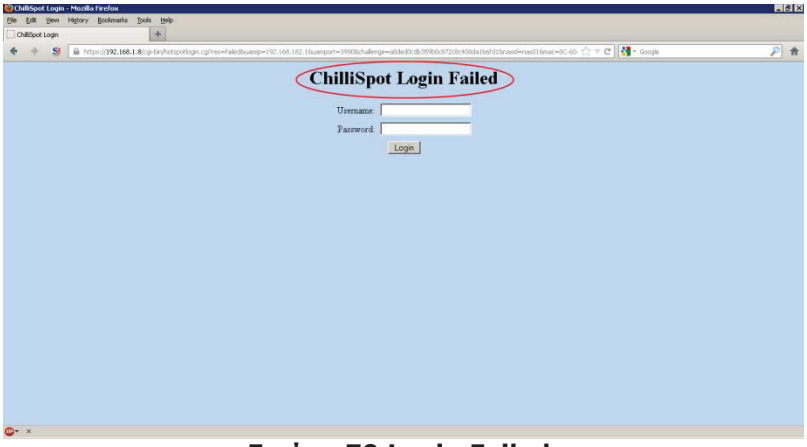
Εικόνα 68 Εισαγωγή μη έγκυρων στοιχείων.

Έτσι, παρατηρούμε στον freeradius ένα Access-Reject γι' αυτόν τον χρήστη με αυτά τα στοιχεία.



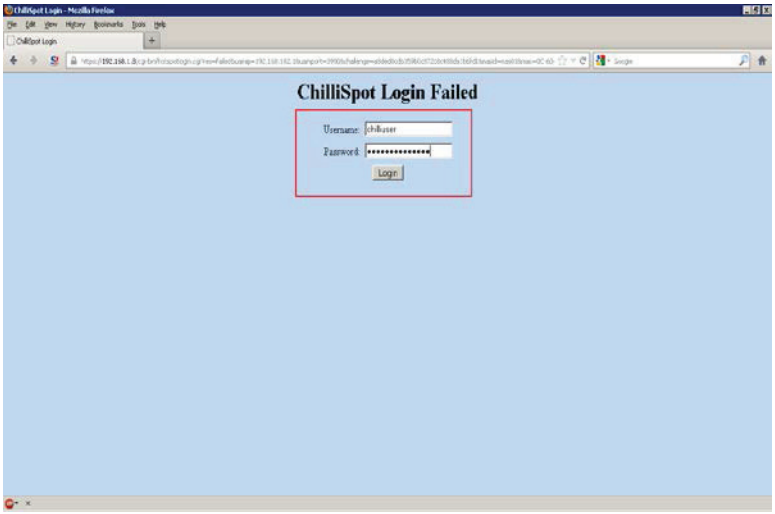
Εικόνα 69 Access-Reject από τον Freeradius.

Καθώς επίσης και στην login σελίδα παρατηρούμε το Login Failed.



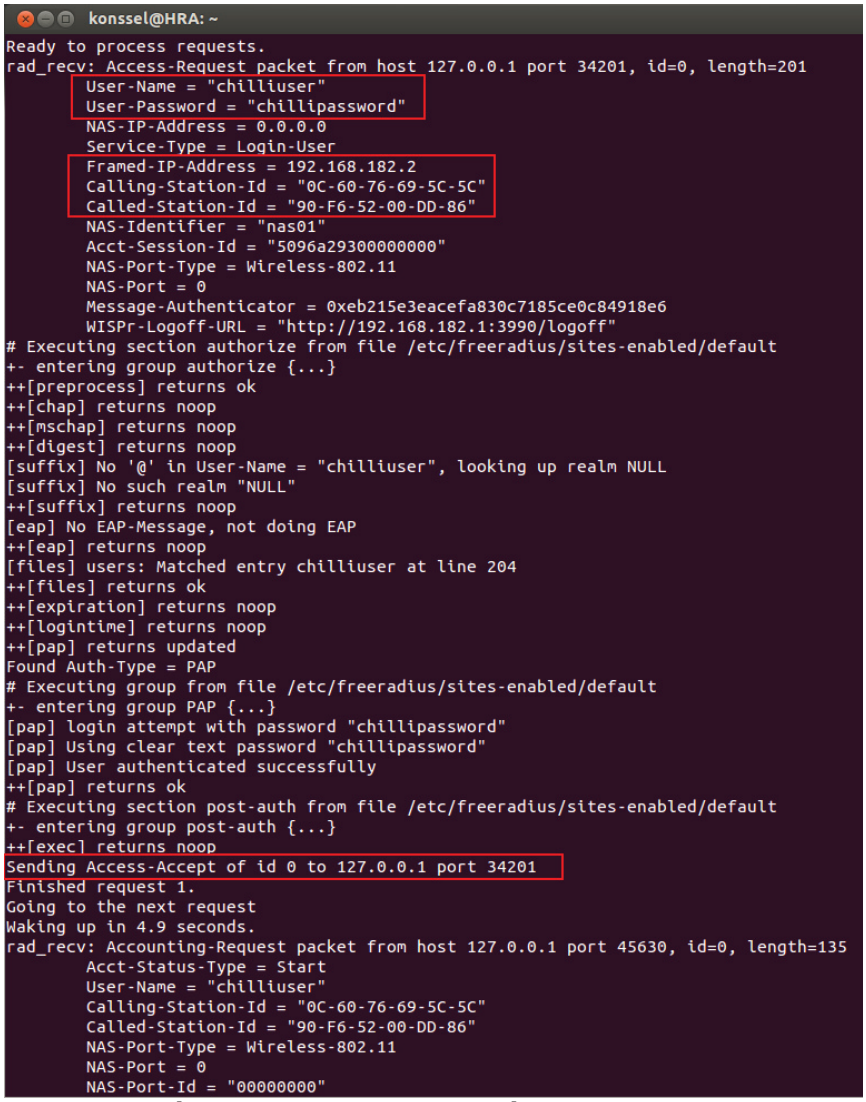
Εικόνα 70 Login Failed.

Στη συνέχεια εισάγουμε τα στοιχεία Username=chilliuser Password=chillipassword τα οποία είναι έγκυρα και υπάρχουν στο αρχείο users του Freeradius.



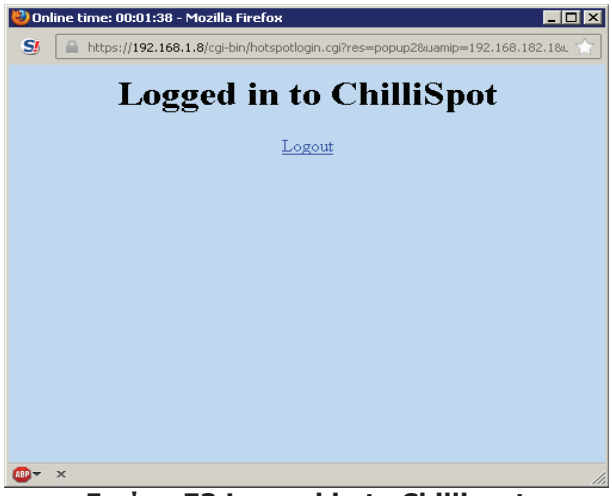
Εικόνα 71 Εισαγωγή έγκυρων στοιχείων.

Στον Freeradius βλέπουμε μια απάντηση Access-Accept.



Εικόνα 72 Access-Accept από τον Freeradius.

Και η είσοδός μας στο Chillispot είναι επιτυχής.



Εικόνα 73 Logged in to Chillispot

Η έξοδος στην οθόνη του chillispot κατά το επιτυχές login στο chillispot είναι η παρακάτω. Βλέπουμε το DHCP authstate από 5 να αλλάζει σε 2 καθώς και το μήνυμα *"Successful UAM login from username=chilliuser IP=192.168.182.2".*

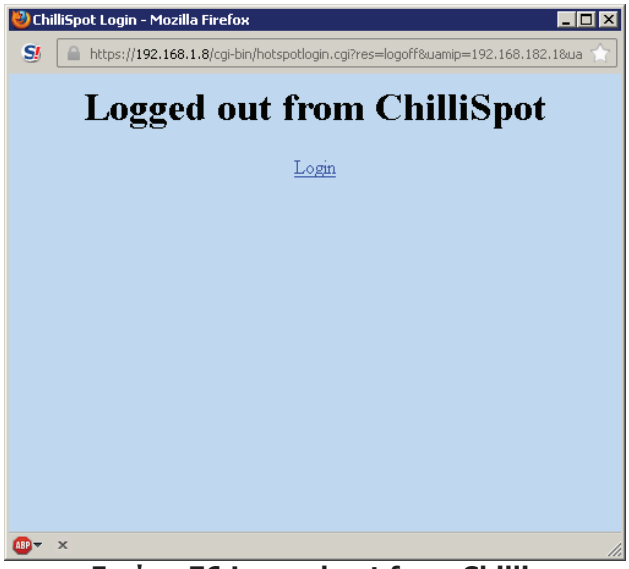
```
cb_tun_ind. Packet received: Forwarding to link layer
cb_dhcp_data_ind. Packet received. DHCP authstate: 5
cb_tun_ind. Packet received: Forwarding to link layer
cb_dhcp_data_ind. Packet received. DHCP authstate: 5
cb_dhcp_data_ind. Packet received. DHCP authstate: 5
cb_tun_ind. Packet received: Forwarding to link layer
chillispot[2710]: chilli.c: 3326: Successful UAM login from usernam
e=chilliuser IP=192.168.182.2
Received login from UAM
cb_tun_ind. Packet received: Forwarding to link layer
cb_tun_ind. Packet received: Forwarding to link layer
cb_dhcp_data_ind. Packet received. DHCP authstate: 2
cb_dhcp_data_ind. Packet received. DHCP authstate: 2
cb_tun_ind. Packet received: Forwarding to link layer
cb_dhcp_data_ind. Packet received. DHCP authstate: 2
```

Εικόνα 74 Debugging chillispot κατά το επιτυχές login.

Τώρα μπορούμε να μπούμε στην επιθυμητή σελίδα.

Εικόνα 75 Έναρξη ελεύθερης πλοήγησης στον Ιστό.

Όταν επιλέξουμε να αποσυνδεθούμε από το Chillispot (Logoff), τότε δεν μπορούμε να έχουμε πρόσβαση σε καμία ιστοσελίδα.



Εικόνα 76 Logged out from Chilli.

Αυτό που θα δούμε στο Chilli debugging αντικατοπτρίζεται στην παρακάτω εικόνα.

```
cb_dhcp_data_ind. Packet received. DHCP authstate: 2
cb_dhcp_data_ind. Packet received. DHCP authstate: 2
cb_tun_ind. Packet received: Forwarding to link layer
chillispot[2745]: chilli.c: 3388: Received UAM logoff from username=c
hilliuser IP=192.168.182.2
Received logoff from UAM
cb_tun_ind. Packet received: Forwarding to link layer
cb_tun_ind. Packet received: Forwarding to link layer
cb_dhcp_data_ind. Packet received. DHCP authstate: 5
cb_dhcp_data_ind. Packet received. DHCP authstate: 5
```

Εικόνα 77 Chilli debugging κατά το Logoff.

Τέλος, στον Freeradius φαίνονται τα παρακάτω.

```
konssel@HRA: ~
Ready to process requests.
rad_recv: Accounting-Request packet from host 127.0.0.1 port 45630, id=1, length=183
        Acct-Status-Type = Stop
        User-Name = "chilliuser"
        Calling-Station-Id = "0C-60-76-69-5C-5C"
        Called-Station-Id = "90-F6-52-00-DD-B6"
        NAS-Port-Type = Wireless-802.11
        NAS-Port = 0
        NAS-Port-Id = "00000000"
        NAS-IP-Address = 0.0.0.0
        NAS-Identifier = "nas01"
        Framed-IP-Address = 192.168.182.2
        Acct-Session-Id = "5096a2930000000"
        Acct-Input-Octets = 15725
        Acct-Output-Octets = 158568
        Acct-Input-Gigawords = 0
        Acct-Output-Gigawords = 0
        Acct-Input-Packets = 118
        Acct-Output-Packets = 151
        Acct-Session-Time = 216
        Acct-Terminate-Cause = User-Request
# Executing section preacct from file /etc/freeradius/sites-enabled/default
+- entering group preacct {...}
++[preprocess] returns ok
[acct_unique] Hashing 'NAS-Port = 0,Client-IP-Address = 127.0.0.1,NAS-IP-Address = 0.0.0.0,Acct-Session-Id = "509
6a2930000000",User-Name = "chilliuser"'
[acct_unique] Acct-Unique-Session-ID = "cacd7962dd3ac099".
++[acct_unique] returns ok
[suffix] No '@' in User-Name = "chilliuser", looking up realm NULL
[suffix] No such realm "NULL"
++[suffix] returns noop
++[files] returns noop
# Executing section accounting from file /etc/freeradius/sites-enabled/default
+- entering group accounting {...}
[detail]        expand: /var/log/freeradius/radacct/%{Client-IP-Address}/detail-%Y%m%d -> /var/log/freeradius/rad
acct/127.0.0.1/detail-20121104
[detail] /var/log/freeradius/radacct/%{Client-IP-Address}/detail-%Y%m%d expands to /var/log/freeradius/radacct/12
7.0.0.1/detail-20121104
[detail]        expand: %t -> Sun Nov  4 19:21:08 2012
++[detail] returns ok
++[unix] returns ok
[radutmp]       expand: /var/log/freeradius/radutmp -> /var/log/freeradius/radutmp
[radutmp]       expand: %{User-Name} -> chilliuser
++[radutmp] returns ok
++[exec] returns noop
[attr_filter.accounting_response]       expand: %{User-Name} -> chilliuser
 attr_filter: Matched entry DEFAULT at line 12
++[attr_filter.accounting_response] returns updated
Sending Accounting-Response of id 1 to 127.0.0.1 port 45630
Finished request 3.
Cleaning up request 3 ID 1 with timestamp +433
Going to the next request
Ready to process requests.
```

Εικόνα 78 Freeradius Debugging κατά το Logoff.

Βιβλιογραφία

1. *Computer Networks (2003), Fourth Edition, Tanenbaum Andrew S.*
2. *Computer Networking: A Top-Down Approach (2008), Fourth Edition, James F. Kurose-Keith W.Ross*
3. *Ασύρματα Δίκτυα (2006), P. Nicopolitidis – M. S. Obaidat – G. I. Papadimitriou – A. S. Pomportsis*
4. *Δίκτυα Ευρείας Ζώνης (2007), δεύτερη έκδοση, Ιάκωβος Στ. Βενιέρης*
5. *«Μελέτη Ασύρματων Ευρυζωνικών Δικτύων Πρόσβασης WLAN και WiMAX»(2007), Χρυσάνθη Θ. Γκέκα, διπλωματική εργασία, ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ*
6. *«Υλοποίηση κρυπτογραφικού συστήματος σε υλικό για ασύρματες επικοινωνίες» (2008), ΠΡΑΣΣΑ ΔΙΟΝΥΣΙΑ, διπλωματική εργασία, ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ*
7. *«Ανάλυση και Αξιολόγηση Μηχανισμών Επικοινωνίας VoIP πάνω σε Υποδομές Ασυρμάτων Δικτύων Τεχνολογίας Wi-Fi» (2007), Abu-Farha Sami - Ishag Abdelrahman - Κωνσταντίνου Δημήτριος, διπλωματική Εργασία, ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ*
8. *Υπηρεσίες Ηλεκτρονικών Επικοινωνιών-Ο Οδηγός του Ενημερωμένου Καταναλωτή(2009), 2η Έκδοση, Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων ΕΕΤΤ*
9. *«Μελέτη Συνύπαρξης Ασύρματων Δικτύων Αισθητήρων και Δικτύων Wi-Fi σε Πραγματικό Περιβάλλον» (2011), Χρηστίνα Α. Μακρή, διπλωματική εργασία, ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ*
10. *« Σχεδίαση και κατασκευή κατευθυντικών κεραιών για χρήση σε ασύρματα δίκτυα Wi-Fi» (2011), Κρομμύδας Μάνθος- Ραυτόπουλος Παναγιώτης, πτυχιακή εργασία, ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΚΡΗΤΗΣ*
11. *«Ανάλυση της επίδοσης βιντεοπόρων WINDOWS MEDIA και QUICK TIME μέσα από ασύρματα τοπικά δίκτυα 802.11b» (2007), Νίκος Ιωάννου, διπλωματική εργασία, ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ*
12. *«Ανάπτυξη εκπαιδευτικού λογισμικού αυτό-διδασκαλίας Πρωτοκόλλων Ασυρμάτων Δικτύων» (2005), ΡΟΥΠΑΣ ΧΡΥΣΟΣΤΟΜΟΣ – ΘΕΙΑΚΟΥΛΗ ΑΓΓΕΛΙΚΗ, ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ*
13. *Το Αλφαβητάρι της Ασύρματης Δικτύωσης, Γιαννακός Νικήτας-Κοσσιφίδης Νικόλαος-Πανουσίου Σωκράτης-Πεϊκίδης Ιωάννης*
14. *Τεχνολογίες σύγχρονων ασύρματων δικτύων δεδομένων (2007), ΚωνσταντίνοςΓεωργακόπουλος, Σχολή Τεχνολογικών Εφαρμογών, Τμήμα Βιομηχανικής Πληροφορικής, ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΚΑΒΑΛΑΣ*
15. *802.11 Wireless Networks Security and Analysis (2010), Alan Holt - Chi-Yu Huang, Springer-Verlag London*
16. *Ad Hoc Mobile Wireless Networks Principles, Protocols, and Applications (2008), Subir Kumar Sarkar-T G Basavaraju-C Puttamadappa, Auerbach Publications*
17. *Fourth-Generation Wireless Networks: Applications and Innovations (2010), Sasan Adibi-Amin Mobasher-Tom Tofigh, Information Science Reference*
18. *«Ασφάλεια σε Ασύρματα Δίκτυα 802.11»(2010), Μαρκομανωλάκη Αικατερίνη, πτυχιακή εργασία, ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΚΡΗΤΗΣ*
19. *Wireless Communications (2005), Andrea Goldsmith, Cambridge University Press*
20. *Wireless LAN MAC protocols (2000), Sushant Jain-Ratul Mahajan*
21. *Ad Hoc Mobile Wireless Networks: Protocols and Systems, C.-K. Toh, Prentice Hall*
22. *WIRELESS AD HOC NETWORKING: Personal-Area, Local-Area, and the Sensory-Area Networks (2007), Shih-Lin Wu -Yu-Chee Tseng, Auerbach Publications*
23. *WLAN Quick Guide 2008, Javvin Technologies, Javvin Press*

24. *«Μελέτη του πρωτοκόλλου SCTP και ανάπτυξη σχετικών opensource προγραμμάτων»(2008), Γεωργακάκης Χρήστος, πτυχιακή εργασία, ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΘΕΣΣΑΛΟΝΙΚΗΣ*
25. *The NATO Research and Technology Organisation (RTO) : RTO-TR-IST-035 - Awareness of Emerging Wireless Technologies: Ad-hoc and Personal Area Networks Standards and Emerging Technologies, ISBN 978-92-837-0052-4*
26. *«Μελέτη Τεχνολογίας και Εφαρμογών WiMAX» (2009), Κουρούς Ιωάννης, μεταπτυχιακή εργασία, ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ*
27. *«Τεχνολογίες ασύρματων τοπικών δικτύων και η χρήση τους σε περιβάλλοντα γραφείου»(2007), ΓΕΩΡΓΙΟΥ ΓΙΩΡΓΟΣ-ΚΑΡΑΒΙΔΑΣ ΜΙΧΑΛΗΣ, πτυχιακή εργασία, ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΑΤΡΩΝ*
28. *«WIMAX: Ανασκόπηση Τεχνολογίας και μοντέλα αγοράς»(2009),ΦΙΛΙΠΠΟΣ Δ. ΚΑΚΛΑΜΑΝΟΣ - ΡΑΠΤΟΔΗΜΟΣ Π. ΔΗΜΗΤΡΙΟΣ, πτυχιακή εργασία, ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΛΑΡΙΣΑΣ*
29. *802 Wireless Access Techniques Overview, Markku Renfors, Institute of Communications Engineering,Tampere University of Technology*
30. *Protocol and methods for LR-WPANs:(Low-Rate Wireless Personal Networks) a survey on existing standards and interconnection issues, Jacopo Mondi, Corso di Sistemi e Reti Wireless, Laurea magistrale in informatica, June 7, 2011*
31. *Wi-Fi Handbook: Buildint 802.11b Wireless Networks (2003), Frank Ohrtman & Konrad Roeder, McGraw-Hill*
32. *Hotspot Networks: Wi-Fi for public access locations (2003), Daniel Minoli, McGraw-Hill*
33. *Real 802.11 security: Wi-Fi Protected Access and 802.11i (2003), Jon Edney & William A. Arbaugh, Pearson Education, Inc.*
34. *Emerging Technologies in Wireless LANs: Theory, Design, and Deployment (2007), Benny Bing, Georgia Institute of Technology, Cambridge University Press*
35. *Securing Hotspots with RADIUS (2004), Interlink Networks, Inc, White Paper*
36. *«Κατασκευή Ασφαλούς Ασύρματου Σημείου Πρόσβασης και εγκατάσταση στο τμήμα Πληροφορικής» (2006), Αλέξανδρος Στεργιάκης & Γεώργιος Παπαδόπουλος, πτυχιακή εργασία, ΑΛΕΞΑΝΔΡΕΙΟ ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ*
37. *Building A Cisco Wireless Lan (2002), Eric Ouellet Robert Padjen Arthur Pfund Ron Fuller Tim Blankenship, Syngress Publishing, Inc*
38. *Cisco Wireless Lan Security (2004), Krishna Sankar Sri Sundaralingam Andrew Balinsky Darrin Miller, Cisco Press*
39. *Aironet Wireless LAN Fundamentals (2003), Cisco Systems, Inc., Student Guide*
40. *Deploying License-Free Wireless Wide-Area Networks (2003), Jack Unger, Cisco Press*
41. *Designing and Deploying 802.11n Wireless Networks (2010), Jim Geier, Cisco Press*
42. *Controller-Based Wireless LAN Fundamentals (2010), Jeff Smith Jake Woodhams Robert Marg, Cisco Press*
43. *Deploying and Troubleshooting Cisco Wireless LAN Controllers (2009), Mark L. Gress CCIE 25539 & Lee Johnson, Cisco Press*
44. *«Ασύρματες Ευρυζωνικές Τεχνολογίες Πρόσβασης» (2004), Κωνσταντίνος Γ. Κοσμάς, διπλωματική εργασία, Τμήμα Μηχανικών Ηλεκτρονικών Υπολογιστών και Πληροφορικής, Πανεπιστήμιο Πατρών*

45. *«Ασύρματα Τοπικά Δίκτυα» (2008), Περγκαντή Ευστρατία, εργασία στα πλαίσια του μαθήματος «Δίκτυα Δημόσιας Χρήσης και Διασύνδεση Δικτύων», Τμήμα Μηχανικών Ηλεκτρονικών Υπολογιστών και Πληροφορικής, Πανεπιστήμιο Πατρών*
46. *The State of Wi-Fi Security Wi-Fi CERTIFIED WPA2TM Delivers Advanced Security to Homes, Enterprises and Mobile Devices, Wi-Fi Alliance, January 2012*
47. *Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks, Wi-Fi Alliance, April 29 2003*
48. *Deploying Wi-Fi Protected Access (WPA™) and WPA2™ in the Enterprise, Wi-Fi Alliance, March 2005*
49. *802.16/WiMAX EECS 228a, Spring 2006, Shyam Parekh, University of California at Berkeley, http://robotics.eecs.berkeley.edu*

Παράρτημα Α: Διευθύνεις Internet

1. *http://www.tekradius.com*
2. *http://www.freeradius.org*
3. *http://www.noc.ntua.gr/index.php?module=ContentExpress&func=display&ceid=118*
4. *http://www.chillispot.info/*
5. *http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Linux.Wireless.std.html*
6. *http://www.ieee802.org/11/Reports/802.11_Timelines.htm*
7. *http://www.wikipedia.org*
8. *http://www.ieee802.org/16/published.html*
9. *http://www.ieee.org*
10. *http://www.worldcat.org*
11. *http://www.moonblinkwifi.com/2point4freq.cfm*
12. *http://www.informit.com/articles/article.aspx?p=413459*

Παράρτημα Β: Επεξηγήσεις τεχνικών όρων

Vendor Dictionaries:
Αυτά τα λεξικά καλύπτουν πάνω από 4000 ιδιότητες (attributes), και πάνω από 5000 ονομαστικές τιμές. Οι νέοι ορισμοί για τους προμηθευτές, τις ιδιότητες, ή τις ονομαστικές τιμές μπορούν να προστεθούν σε μια απλή μορφοποίηση κειμένου. Αυτό το χαρακτηριστικό γνώρισμα επιτρέπει την υποστήριξη νέου εξοπλισμού χωρίς οποιεσδήποτε αλλαγές στον source code του server.

Modules:
Η πολυτμηματικότητα (*modularity*) είναι ο βαθμός στον οποίο τα τμήματα ενός συστήματος μπορούν να χωριστούν και να επανασυνδυαστούν στον σχεδιασμό λογισμικού και αναφέρεται σε έναν λογικό χωρισμό του «σχεδίου λογισμικού» που επιτρέπει την ευχρηστία ενός σύνθετου λογισμικού με σκοπό την εφαρμογή και τη συντήρηση. Η λογική του χωρισμού μπορεί να βασιστεί σε σχετικές λειτουργίες, εκτιμήσεις εφαρμογής, συνδέσμους δεδομένων, ή άλλα κριτήρια.

MySQL:
Η MySQL είναι ένα σύστημα διαχείρισης σχεσιακών βάσεων δεδομένων που μετρά περισσότερες από 11 εκατομμύρια εγκαταστάσεις. Το πρόγραμμα τρέχει έναν server παρέχοντας πρόσβαση πολλών χρηστών σε ένα σύνολο βάσεων δεδομένων. Ο κωδικός του εγχειρήματος είναι διαθέσιμος μέσω της *GNU General Public License*, καθώς και μέσω ορισμένων ιδιόκτητων συμφωνιών. Ανήκει και χρηματοδοτείται από μία και μοναδική κερδοσκοπική εταιρεία, τη σουηδική MySQL AB, η οποία σήμερα ανήκει στην Oracle.

PostgreSQL:
Η PostgreSQL είναι μια σχεσιακή βάση δεδομένων ανοικτού κώδικα με πολλές δυνατότητες. Η ανάπτυξη της διαρκεί ήδη πάνω από δύο δεκαετίες και βασίζεται σε μια αποδεδειγμένα καλή αρχιτεκτονική η οποία έχει δημιουργήσει μια ισχυρή αντίληψη των χρηστών της γύρω από την αξιοπιστία, την ακεραιότητα δεδομένων και την ορθή λειτουργία PostgreSQL. Τρέχει σε όλα τα βασικά λειτουργικά συστήματα, στα οποία περιλαμβάνονται Linux, UNIX (AIX, BSD, HP-UX, SGI, IRIX, MAC OS X, Solaris, Tru64) και τα Windows. Είναι συμβατή με ACID (atomicity, consistency, isolation, durability), και συμπεριλαμβάνει τους περισσότερους SQL92 και SQL99 τύπους δεδομένων (INTEGER, NUMERIC, BOOLEAN, CHAR, VARCHAR, DATE, INTERVAL και TIMESTAMP). Επίσης υποστηρίζει αποθήκευση μεγάλων δυαδικών αντικειμένων (binary), όπως εικόνες, ήχος ή βίντεο. Διαθέτει περιβάλλοντα προγραμματισμού για τις γλώσσες προγραμματισμού C, C++, Java, Perl, Python, Ruby, Tcl, και υποστήριξη για την πλατφόρμα .NET και το πρότυπο ODBC, καθώς και εξαιρετικό εγχειρίδιο χρήσης.

Oracle:
Το *Oracle Database* είναι λογισμικό διαχείρισης σχεσιακών βάσεων δεδομένων. Είναι δημιουργία και ιδιοκτησία της εταιρείας Oracle Corporation. Το Oracle αποτελείται από ένα σύστημα κατανεμημένων διεργασιών. Υποστηρίζεται από διαφόρων τύπων servers, όπως π.χ. ο Apache. Το σύστημα διαχείρισης της βάσης μπορεί να φορτωθεί σε υπολογιστές που χρησιμοποιούν λειτουργικά συστήματα Linux, Windows, Solaris, κ.ά.

Virtual Hosting:
Virtual Hosting είναι μια μέθοδος για τη φιλοξενία πολλαπλών domain names (με το χωριστό χειρισμό κάθε ονόματος) σε έναν μοναδικό server (ή ομάδα servers). Αυτό επιτρέπει σε έναν server να μοιράζεται τους πόρους του, όπως μνήμη και επεξεργαστές, χωρίς την απαίτηση να χρησιμοποιείται το ίδιο host name σε όλες τις υπηρεσίες που παρέχονται. Ο όρος virtual hosting χρησιμοποιείται συνήθως αναφορικά με web servers. Είναι επίσης πολύ κοινό για μια ενιαία οντότητα να θέλει να χρησιμοποιήσει πολλαπλά ονόματα στην ίδια μηχανή έτσι ώστε τα ονόματα να μπορούν να απεικονίσουν τις υπηρεσίες που προσφέρονται παρά το πού εκείνες οι υπηρεσίες φιλοξενούνται. Υπάρχουν δύο κύριοι τύποι εικονικής φιλοξενίας:

Name based η οποία χρησιμοποιεί το host name που παρουσιάζεται από τον πελάτη. Αυτό σώζει τις διευθύνσεις IP και σχετικό administrative overhead αλλά το πρωτόκολλο που εξυπηρετείται πρέπει να παρέχει το host name σε ένα κατάλληλο σημείο. Ειδικότερα, υπάρχουν σημαντικές δυσκολίες στην χρήση name based εικονικής φιλοξενίας με SSL/TLS.
IP based η οποία χρησιμοποιεί μια χωριστή διεύθυνση IP για κάθε host name και μπορεί να εκτελεσθεί με οποιοδήποτε πρωτόκολλο αλλά απαιτεί να αφιερώνεται μια διεύθυνση IP για κάθε domain name που εξυπηρετείται.
Σε γενικές γραμμές είναι επίσης δυνατή η Port based εικονική φιλοξενία αλλά χρησιμοποιείται σπάνια στην πράξη επειδή είναι μη φιλική στους χρήστες. Οι Name based και IP based μπορούν να συνδυαστούν, ένας server μπορεί να έχει πολλαπλές διευθύνσεις IP και να εξυπηρετεί πολλαπλά ονόματα σε μερικές ή όλες αυτές τις διευθύνσεις IP. Αυτή η τεχνική μπορεί να είναι χρήσιμη όταν χρησιμοποιείται SSL/TLS με wildcard certificates. Παραδείγματος χάριν εάν ένας server είχε δύο πιστοποιητικά ένα για *.example.com και ένα για *.example.net θα μπορούσε να εξυπηρετήσει το foo.example.com και το bar.example.com υπό την ίδια διεύθυνση IP αλλά θα χρειαζόταν μια χωριστή διεύθυνση IP για το baz.example.net.

VMPS:
VLAN Management Policy Server ή "VMPS" είναι ένα switch δικτύου που περιέχει μια χαρτογράφηση με πληροφορίες των συσκευών στο VLAN. Ο κύριος στόχος του VMPS είναι ο προσδιορισμός VLAN για γενικούς σκοπούς διαχείρισης του δικτύου, αλλά επίσης μπορεί να χρησιμοποιηθεί για την παροχή ασφάλειας διαμέσω του διαχωρισμού των πελατών με μια άγνωστη MAC address, ή διαμέσω περεταίρω επεκτάσεων του πρωτόκολλου για να παρέχει login για Cisco ACIS. Αυτή η τελευταία λειτουργία αποδοκιμάζεται από την Cisco, εξαιτίας του 802.1x, και καθώς η τεχνολογία VMPS είναι μόνο της Cisco, ο προσδιορισμός VLAN μπορεί να έρθει εις πέρας στη δομή 802.1x.

Open Source:
Στην παραγωγή και την ανάπτυξη, open source είναι μια φιλοσοφία που προωθεί την ελεύθερη ανακατανομή και την πρόσβαση στις λεπτομέρειες του σχεδίου και της εκτέλεσης ενός τελικού προϊόντος. Η φράση open source κατοχυρώθηκε με την άνοδο του Διαδικτύου, και τη ακόλουθη ανάγκη για την μαζική επισκευή του υπολογιστικού κώδικα πηγής. Το άνοιγμα του κώδικα πηγής επέτρεψε μια αυτοεμπλουτιζόμενη ποικιλομορφία των προτύπων παραγωγής, των διαδρομών επικοινωνίας, και των διαδραστικών κοινοτήτων. Το κίνημα του open source λογισμικού γεννήθηκε για να περιγράψει το περιβάλλον που δημιούργησαν τα νέα πνευματικά δικαιώματα, η χορήγηση αδειών, η περιοχή και τα καταναλωτικά ζητήματα. Το πρότυπο open source περιλαμβάνει την έννοια των ταυτόχρονων, όμως διαφορετικών, ημερήσιων διατάξεων και των διαφορετικών προσεγγίσεων στην παραγωγή, σε αντίθεση με τα συγκεντρωτικά πρότυπα της ανάπτυξης όπως εκείνα που χρησιμοποιούνται χαρακτηριστικά στις εμπορικές εταιρείες λογισμικού. Η βασική αρχή και πρακτική της ανάπτυξης λογισμικού ανοιχτού κώδικα είναι η ομότιμη παραγωγή, μέσω ανταλλαγής και συνεργασίας, του τελικού προϊόντος, source-material και διαθέσιμων εγγράφων με καθόλου κόστος στο κοινό.

BSD-licensed library:
Berkeley Software Distribution (BSD, μερικές φορές ονομάζεται Berkeley Unix) είναι ένα Unix παράγωγο λειτουργικό σύστημα που αναπτύσσεται και που διανέμεται από τη Computer Systems Research Group (CSRG) του Πανεπιστημίου της Καλιφόρνιας, Μπέρκλεϋ, από το 1977 ως το 1995. Σήμερα ο όρος «BSD» χρησιμοποιείται συχνά μη-συγκεκριμένα για να αναφερθεί σε οποιοιδήποτε από τους απογόνους BSD που διαμορφώνουν μαζί έναν κλάδο της οικογένειας των Unix-like λειτουργικών συστημάτων. Τα λειτουργικά συστήματα που προέρχονται από τον αρχικό κώδικα BSD παραμένουν ενεργά αναπτυγμένα και ευρέως χρησιμοποιημένα. Οι πιό πρόσφατες εκδόσεις BSD

παρείχαν μια βάση για διάφορες open source μελέτες ανάπτυξης, π.χ. FreeBSD, NetBSD, OpenBSD, οι οποίες βρίσκονται σε εξέλιξη. Αυτές, στη συνέχεια, έχουν ενσωματωθεί γενικά ή εν μέρει στα σύγχρονα ιδιόκτητα λειτουργικά συστήματα, π.χ. TCP/IP (IPv4 μόνο) κώδικας δικτύωσης στα Microsoft Windows ή το ίδρυμα της Mac OS X της Apple.

PAM library:
Pluggable Authentication Modules (PAM), επιτρέπει την εφαρμογή των μηχανισμών πιστοποίησης ξεχωριστά από την επίκληση εκείνων των μηχανισμών στα προγράμματα. Με τη PAM, οι μηχανισμοί πιστοποίησης εφαρμόζονται από τις δυναμικά συνδεμένες κοινές βιβλιοθήκες αποκαλούμενες PAM modules. Πολλές PAM modules είναι δημόσια διαθέσιμες, καλύπτοντας μια σειρά των σχεδίων πιστοποίησης συμπεριλαμβανομένου την τυποποιημένη UNIX System username/password πιστοποίηση, Kerberos. Το UnixWare PAM είναι βασισμένο σε μια open-source έκδοση της PAM γνωστή ως Linux-PAM.
Διαχείριση Authentication: πιστοποιεί τους χρήστες και παρέχει επίσης τις πληροφορίες για τους χρήστες στην εφαρμογή.
Διαχείριση Account: καθιερώνει εάν ένας επικυρωμένος χρήστης επιτρέπεται να αποκτήσει πρόσβαση, π.χ., με τον έλεγχο ότι το όνομα χρήστη ή/και ο κωδικός πρόσβασης δεν έχουν λήξει.
Διαχείριση Session: εκτελεί οποιουσδήποτε στόχους που απαιτούνται στην έναρξη και τη λήξη μιας συνόδου.
Διαχείριση Password: αναθέτει ή αλλάζει τα στοιχεία πιστοποίησης του χρήστη.

Dialupadmin:
Ο FreeRADIUS server συμπεριλαμβάνει ένα ισχυρό web interface γραμμένο σε PHP για να διαχειρίζεται τους radius χρήστες, το οποίο ονομάζεται dialupadmin. Το Dialup Admin υποστηρίζει χρήστες είτε σε SQL (MySQL ή PostgreSQL) ή σε LDAP. Εκτός από τις ιστοσελίδες, περιλαμβάνει επίσης έναν αριθμό scripts για να διευκολύνει τον διαχειριστή**.**

Telcos:
Μια εταιρεία τηλεφωνίας (γνωστή ως a telco, telecommunications operator, communications service provider, ή CSP) είναι ένας πάροχος υπηρεσιών τηλεπικοινωνίας όπως τηλεφωνία και πρόσβαση σε επικοινωνίες δεδομένων.

Tier 1 ISP:
Ένα δίκτυο tier 1 είναι ένα IP δίκτυο που συμμετέχει στο Διαδίκτυο απλώς μέσω ελεύθερου διακανονισμού διασύνδεσης, γνωστού ώς settlement-free peering. Αν και δεν υπάρχει καμία αρχή που καθορίζει τις σειρές των δικτύων που συμμετέχουν στο Διαδίκτυο, ο πιό κοινός καθορισμός ενός tier 1 δικτύου είναι ένας που μπορεί να φθάσει σε κάθε άλλο δίκτυο στο Internet χωρίς την αγορά της διέλευσης IP ή πληρωμή των διακανονισμών. Κατά συνέπεια, ο όρος «tier 1 δίκτυο» χρησιμοποιείται στη βιομηχανία για να δηλώσει ένα δίκτυο χωρίς τους προφανείς διακανονισμούς, δηλαδή μια νομισματική δαπάνη για το ποσό, την κατεύθυνση, ή τον τύπο κυκλοφορίας που στέλνεται μεταξύ των δικτύων.

Eduroam:
Education roaming είναι η ασφαλής, παγκόσμια roaming υπηρεσία πρόσβασης που αναπτύσσεται για τη διεθνή έρευνα και ακαδημαϊκή κοινότητα. Το eduroam επιτρέπει στους σπουδαστές, στους ερευνητές και στο προσωπικό να λάβουν σύνδεση στο Διαδικτύο στον χώρο της πανεπιστημιούπολης και κατά την επίσκεψη άλλων συμμετεχόντων οργάνων, απλώς ανοίγοντας το laptop τους.

Binary Packages:
Ένας φάκελος αρχείων που περιέχει όλα τα αρχεία και τους καταλόγους που πρέπει να εγκατασταθούν προκειμένου να γίνει μια λειτουργική εγκατάσταση του προγράμματος που περιλαμβάνεται στο πακέτο, καθώς και τα scripts συντήρησης τα οποία είναι απαραίτητα για την εγκατάσταση. Ένα binary package είναι συνήθως συγκεκριμένο για μια ορισμένη πλατφόρμα, σε αντίθεση με ένα source package.

Build Source:
Αφού συναρμολογηθεί ένα πακέτο, πρέπει να καθοριστεί το package build προτού να μπορέσει να «χτιστεί» και να επεκατθεί στους τερματικούς σταθμούς και τους servers. Η διαδικασία build διαβάζει την κεντρική πηγή αντικειμένων δεδομένων για τον path code που καθορίζεται στο πακέτο. Αυτές οι πληροφορίες μετατρέπονται έπειτα από μια μορφοποίηση σχεσιακής βάσης δεδομένων στα αντεγραμμένα αντικείμενα, τα οποία τοποθετούνται μόνα τους στο πακέτο.

Proxy Request:
Στα δίκτυα υπολογιστών, ένας proxy server είναι ένας server (σύστημα υπολογιστή ή εφαρμογή) που λειτουργεί ενδιάμεσα για αιτήσεις από τους πελάτες ψάχνοντας πόρους από άλλους servers. Ένας πελάτης συνδέεται σε έναν proxy server, αναζητώντας κάποια υπηρεσία, όπως έναν φάκελο, σύνδεση, ιστοσελίδα, ή άλλους διαθέσιμους πόρους από έναν διαφορετικό server. Ο proxy server αποτιμεί τις αιτήσεις με έναν τρόπο που απλοποιεί και ελέγχει την πολυπλοκότητά τους. Σήμερα οι περισσότεροι proxies είναι web proxies, οι οποίοι διευκολύνουν την πρόσβαση στο περιεχόμενο του Παγκόσμιου Ιστού.

Fail Over:
Είναι η αυτόματη μεταγωγή σε ένα εφεδρικό ή σε ετοιμότητα computer server, σύστημα, στοιχείο hardware ή δίκτυο κατά την αποτυχία ή τον ανώμαλο τερματισμό της προηγούμενης ενεργής εφαρμογής, server, συστήματος, στοιχείου hardware, ή δικτύου. Failover και switchover είναι βασικά η ίδια λειτουργία, εκτός ότι το failover είναι αυτόματο και συνήθως λειτουργεί χωρίς προειδοποίηση ενώ το switchover απαιτεί ανθρώπινη μεσολάβηση.

Back-end data base:
Μια back-end database είναι μια βάση δεδομένων που προσπελάζεται από χρήστες, έμμεσα, μέσω μιας εξωτερικής εφαρμογής παρά με τον προγραμματισμό εφαρμογής που αποθηκεύεται μέσα στη βάση δεδομένων μόνη της ή από το χαμηλού επιπέδου χειρισμό των δεδομένων (π.χ. μέσω των εντολών SQL). Μια βάση δεδομένων back-end αποθηκεύει τα δεδομένα αλλά δεν περιλαμβάνει τα στοιχεία εφαρμογής τελικών χρηστών όπως οι αποθηκευμένες queries, οι φόρμες, οι μακροεντολές ή οι αναφορές.

RFC 2865:
Remote Authentication Dial In User Service (RADIUS)

RFC 2866:
RADIUS Accounting
Αυτό το έγγραφο περιγράφει ένα πρωτόκολλο που μεταφέρει πληροφορίες accounting μεταξύ ενός Network Access Server και ενός κοινού Accounting Server.

RADIUSClients:
ChilliSpot/CoovaChilli, JRadius,mod_auth_radius, pam_radius_auth, Pyrad,Radiusclient, Radiusclient-ng,PHP Radius Extension, Radlogin, WPA Supplicant, Dialupadmin.

EAP Clients:
eapclient, Windows XP supplicant, SecureW2, NetworkManager, wpa_supplicant, Xsupplicant, rad_eap_test.

Virtual Server:
Ο FreeRADIUS 2.0 υποστηρίζει virtual servers. Αυτή είναι πιθανόν η μοναδική μεγαλύτερη αλλαγή η οποία δεν είναι προς τα πίσω συμβατή με το 1.x. Ένας virtual server είναι ένας σχεδόν ολοκληρωμένος RADIUS server, όπως ακριβώς ένα configuration για τον FreeRADIUS 1.x. Ωστόσο, ο FreeRADIUS μπορεί τώρα να τρέξει πολλούς virtual servers την ίδια χρονική στιγμή. Οι virtual servers μπορούν ακόμα να κάνουν proxy αιτήσεις μεταξύ τους. Η ισχύς των virtual servers στηρίζεται στην ικανότητά τους να ξεχωρίζουν πολιτικές. Μια πολιτική μπορεί να τοποθετηθεί μέσα σε έναν virtual server, όπου εγγυάται

να επιρεάζει μόνο αιτήσεις που περνούν διαμέσω εκείνου του virtual server. Στο 1.x, οι πολιτικές ήταν σφαιρικές, και μερικές φορές ήθελε μεγάλη προσπάθεια για να γράψεις μια πολιτική έτσι ώστε να εφαρμοζόταν μόνο σε ιδιαίτερες περιορισμένες κατασάσεις.