Τμήμα Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών
Παράρτημα Σπάρτης
Α.Τ.Ε.Ι Καλαμάτας

ΤΙΤΛΟΣ ΕΡΓΑΣΙΑΣ

"ΜΕΛΕΤΗ ΑΣΦΑΛΟΥΣ ΑΣΥΡΜΑΤΗΣ ΠΡΟΣΒΑΣΗΣ ΜΕ ΧΡΗΣΗ ΕΙΚΟΝΙΚΩΝ ΔΙΚΤΥΩΝ"

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ ΤΟΥ

ΠΑΠΑΔΟΠΟΥΛΟΥ ΠΑΥΛΟΥ

Α.Μ. 2006016

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ

ΓΕΩΡΓΙΟΣ ΜΑΚΡΟΔΗΜΗΤΡΗΣ

ΣΠΑΡΤΗ

ΔΕΚΕΜΒΡΙΟΣ 2013

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ	ΥΠΟΓΡΑΦΕΣ
1.	
2.	
3.	

Υπεύθυνη Δήλωση

Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς, είτε παραφρασμένες. Επίσης, βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών του Α.Τ.Ε.Ι. Καλαμάτας.

Ο συγγραφέας,

Παπαδόπουλος Παύλος

Ευχαριστίες

Έχοντας φτάσει στο τέλος της πτυχιακής μου εργασίας, αισθάνομαι υποχρεωμένος να μιλήσω για κάποιους ανθρώπους, που ο καθένας με τον δικό του τρόπο σηματοδότησε την πορεία των χρόνων μου στις προπτυχιακές σπουδές μου και να τους ευχαριστήσω.

Πρώτα απ' όλα, θα ήθελα να ευχαριστήσω τον επιβλέποντα μου, κύριο Μακροδημήτρη Γιώργο, Επιστημονικό Συνεργάτη του Τμήματος Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών του Α.Τ.Ε.Ι. Καλαμάτας, διότι η συνεργασία μαζί του ήταν ένας καταλύτης για την ολοκλήρωση των προπτυχιακών σπουδών μου. Τα αποτελέσματα της εργασίας αυτής είναι από τη συνεργασία με τον κ. Μακροδημήτρη. Η συνεργασία μας ξεκίνησε μαζί με αυτή την πτυχιακή εργασία που αφορά στην μελέτη και την εγκατάσταση ενός ασύρματου δικτύου για τον δήμο Αμαρουσίου. Χαίρομαι που έστω και στους τελευταίους μήνες των σπουδών μου στο τμήμα ΤΕ.ΠΛΗ.Τ. του ΑΤΕΙ Καλαμάτας, τον γνώρισα και συνεργάστηκα μαζί του. Επίσης θα ήθελα να ευχαριστήσω θερμά τους κυρίους καθηγητές μου, Ν. Πανάγο, Γ. Ν. Μπάρδη και Ι. Λιαπέρδο καθώς ήταν οι άνθρωποι που με παρακίνησαν να ασχοληθώ περισσότερο με το αντικείμενο μου και να το αγαπήσω ακόμη πιο πολύ.

Τέλος, θα ήθελα να ευχαριστήσω τον πατέρα μου Θεόδωρο για την αμέριστη υποστήριξή του όλον αυτό τον καιρό, των προπτυχιακών σπουδών μου. Αφιερώνω αυτή την εργασία στον πατέρα μου, ως ελάχιστη ευγνωμοσύνη για την κατανόηση και την υπομονή του όλα αυτά τα χρόνια.

.....

Σπάρτη, 2013

Περίληψη

Στην εργασία αυτή θέλησα να καλύψω τις ανάγκες εγκατάστασης και μελέτης ενός ασύρματου δικτύου για την κάλυψη των αναγκών του δήμου Αμαρουσίου. Το δίκτυο του δήμου ήταν ενσύρματο και χρειάστηκε η μελέτη για την σωστή μεταφορά του σε ασύρματο. Στις παρακάτω σελίδες θα βρείτε μια μικρή αναφορά στα ασύρματα δίκτυα (πρώτη ασύρματη μετάδοση, ιστορία και εξέλιξη), ανάλυση των πρωτοκόλλων των ασύρματων δικτύων, ανάλυση των θεμάτων ασφαλείας που έχουν να κάνουν με την ασύρματη δικτύωση και μια μικρή αναφορά σε επιθέσεις που έγιναν για την καλύτερη κατανόηση των θεμάτων αυτών. Στη συνέχεια υπήρξε μελέτη του χώρου για την σωστή εγκατάσταση των συσκευών που θα καλύψουν το δίκτυο (Access Points), μελέτη για το subnetting ώστε να χωριστούν σωστά τα υποδίκτυα του δήμου, βάσει πάντα των εκάστοτε αναγκών σε διευθύνσεις και στήσιμο όλου του εξοπλισμού και σετάρισμά του.

Στην μελέτη αυτή θα βρείτε αρκετές εικόνες που θα σας βοηθήσουν να καταλάβετε καλύτερα τα προβλήματα που υπήρξαν και πώς λύθηκαν. Επίσης στο τέλος της εργασίας, υπάρχουν δύο (2) ειδικά παραρτήματα που αφορούν το configuration των συσκευών και αναλύονται με σχόλια. Να σημειωθεί εδώ ότι όλες οι συσκευές που έχουν σεταριστεί με τις εκάστοτε ρυθμίσεις, είναι συσκευές της Cisco και τα βασικά χαρακτηριστικά τους αναλύονται στο ειδικό παράρτημα.

Το γενικό πλάνο του κτηρίου του δήμου αποτελείται από τέσσερις (4) ορόφους, υπόγειο, ισόγειο, πρώτος και δεύτερος όροφος, και το μοντέλο που ακολουθείται για το στήσιμο των switches στους ορόφους αυτούς είναι το επίσημο μοντέλο που προτείνει η Cisco και αποτελείται από τρία (3) επίπεδα σε μορφή πυραμίδας. Τα επίπεδα αυτά αναφορικά, είναι τα Access, Distribution και Core.

Στην ανάλυση του κτηρίου που βρίσκεται το πέμπτο (5°) κεφάλαιο, θα δείτε πώς γίνεται η κατανομή των Access Points για την πλήρη και σωστή κάλυψη του κτηρίου και επεξηγείται αναλυτικά η τοποθέτηση των εκάστοτε συσκευών (δικτυακών και μη) στον κάθε όροφο.

Επίσης να σημειωθεί πως γίνεται και μελέτη και εγκατάσταση ενός VPN δικτύου, το οποίο καλύπτει τη διοίκηση του κτηρίου (επικοινωνία δημάρχου με τον αντιδήμαρχο) για μεγαλύτερη ασφάλεια στη μεταξύ τους επικοινωνία.

Τέλος πρέπει να αναφέρουμε πως έγινε προσπάθεια για ελάχιστο κόστος μεταφοράς του ήδη υπάρχοντος δικτύου από ενσύρματο σε ασύρματο. Επίσης χρησιμοποιήθηκαν προγράμματα ανοιχτού λογισμικού για διάφορες ενέργειες που έπρεπε να γίνουν για την επίτευξη μερικών επιθέσεων σε ασύρματα δίκτυα κ.α.

1. Ασύρματα Δίκτυα

1.1 Γέννηση των Ασύρματων Δικτύων

Η πρώτη ουσιαστική ασύρματη αποστολή δεδομένων έγινε το 1880 από τους Alexander Graham Bell και Charles Sumner Tainte, οι οποίοι κατασκεύασαν και καταχώρησαν με δίπλωμα ευρεσιτεχνίας το "φωτοτηλέφωνο" (photophone). Ουσιαστικά, πρόκειται για ένα τηλέφωνο μέσω του οποίου μπορούσαν να διεξαχθούν συνομιλίες οι οποίες μεταφέρονταν ασύρματα, μέσω διαμορφωμένων ακτίνων φωτός (πολύ κοντά στα ηλεκτρομαγνητικά κύματα). Να σημειωθεί ότι ήταν απαραίτητη η οπτική επαφή μεταξύ πομπού και δέκτη (κάτι που και στις μέρες μας, τις περισσότερες φορές είναι επίσης απαραίτητο).

1.2 Εξέλιξη των Ασύρματων Δικτύων

Από το 1880 και αργότερα είχαμε αρκετές νέες ασύρματες μεταδόσεις. Το 1888 ο Thomas Edison κατάφερε να πάρει ένα δίπλωμα ευρεσιτεχνίας για ένα σύστημα σηματοδότησης που εφηύρε και χρησιμοποίησε στο Lehigh Valley Railroad. Την ίδια χρονιά έχουμε και την "παρατήρηση" του Heinrich Rudolf Hertz πως τα ηλεκτρομαγνητικά κύματα ταξιδεύουν στον χώρο σε ευθείες γραμμές ενώ δίνει διάφορους τρόπους για το πώς μπορούν να αποσταλούν και να παραληφθούν. Στη συνέχεια το 1901, ο Ιταλός φυσικός Guglielmo Marconi πραγματοποίησε την επίδειξη ενός ασύρματου τηλέγραφου για επικοινωνία πλοίου με την ακτή, χρησιμοποιώντας τον κώδικα Morse. Αυτή η εφεύρεση σε συνδυασμό με την τεχνογνωσία και την συνεισφορά στο ραδιόφωνο και την ασύρματη τηλεγραφία του Karl Ferdinand Braun, έφερε και στους δύο το βραβείο Νόμπελ Φυσικής του έτους 1909.

Μετά από αρκετές μελέτες και εξελίξεις στο χώρο των ασύρματων επικοινωνιών, φτάνουμε στην δεκαετία του 1970, όπου στο Πανεπιστήμιο της Χαβάης, από την ομάδα του Norman Abramson, χρησιμοποιείται για πρώτη φορά μία ασύρματη επικοινωνία για τη διασύνδεση διάφορων υπολογιστών (διασκορπισμένοι σε νησιά) με τον κεντρικό server που βρισκόταν στο νησί Oahu.

1.3 Πλεονεκτήματα και Μειονεκτήματα των Ασύρματων Δικτύων

Τα ασύρματα δίκτυα στην εποχή μας έχουν γίνει όλο και πιο διαδεδομένα. Χαρακτηριστικό του ότι έχει αλλάξει κατά πολύ ο καθημερινός τρόπος ζωής μας, είναι ότι από το 2005 και μετά στην παγκόσμια αγορά πληροφορικής, οι φορητοί υπολογιστές (Laptops) έχουν μεγαλύτερο κομμάτι αγοράς από τους προσωπικούς (σταθερούς) υπολογιστές. Αυτό καθ' αυτό μας δείχνει, το ότι εκτός της λειτουργικότητας ενός υπολογιστή, ο χρήστης νοιάζεται πολύ και για την φορητότητά του. Ποια είναι όμως τα συν και τα πλην των ασύρματων επικοινωνιών; Αναφορικά είναι τα ακόλουθα:

Πλεονεκτήματα:

- Φορητότητα
- Κόστος
- Λιγότερη καλωδίωση
- Ευκολία εγκατάστασης (μικρές επιχειρήσεις/σπίτι)

Μειονεκτήματα:

- Ταχύτητα
- Ασφάλεια
- Σωστή κάλυψη περιοχής (μεγάλα και παλιά κτήρια)
- Σε μεγάλες περιοχές (εκτός κτηρίων) επιρροή από καιρικά φαινόμενα

Το βασικό πλεονέκτημα των ασύρματων δικτύων είναι φυσικά η φορητότητα. Πλέον οι περισσότεροι μπορούν να δουλέψουν και από το σπίτι και υπάρχουν πολλές εταιρείες που βασίζονται σ' αυτό το πρότυπο. Εκτός αυτού, ακόμη και στο σπίτι μας, με μία νέα σύνδεση, παίρνουμε αυτόματα και ένα modem/router με δυνατότητα ασύρματου δικτύου. Στις περισσότερες περιπτώσεις, οι υπάλληλοι κινούνται συνεχώς με ένα laptop, ένα netbook, ένα tablet ή ακόμη και με το κινητό τους τηλέφωνο, μέσα και έξω από τον χώρο της εταιρείας. Ένα ακόμη σημαντικό πλεονέκτημα είναι το κόστος, το οποίο είναι αρκετά μειωμένο σε σχέση με ένα ενσύρματο δίκτυο, μόνο και μόνο λόγω της καλωδίωσης. Χονδρικά, η καλωδιώση ενός ολόκληρου κτηρίου με switches και routers , για κάθε όροφο και για την μεταξύ τους επικοινωνία, μπορεί να φτάσει τις μερικές χιλιάδες Ευρώ (αν μιλήσουμε και για σωστή backbone καλωδίωση με οπτική ίνα), ενώ αν καταφύγουμε στην ασύρματη επικοινωνία για το κτήριο, σε κάθε όροφο, μπορεί να χρειαστούμε από ένα μέχρι μερικά Access Points (ανάλογα πάντα τα τ.μ. και την αρχιτεκτονική του κάθε ορόφου), των οποίων το κόστος είναι αρκετά μικρότερο. Επίσης, με την χρήση ασύρματου δικτύου στο κτήριο της επιχείρησης, δεν χρησιμοποιούνται πιθανόν και αρκετά switches, που σε ένα ενσύρματο δίκτυο θα είχαμε για λόγους συνδεσιμότητας. Η λιγότερη καλωδίωση, εκτός από οικονομικούς λόγους, είναι καλή και για χωροταξικούς. Δεν χρειάζεται μελέτη για κάποιο ψευδοπάτωμα/ψευδοροφή κτλ για την σωστή κατανομή και στήσιμο των καλωδιών στο χώρο, ούτε ο κίνδυνος έκθεσης κάποιου καλωδίου σε χώρο που μπορεί να προκαλέσει κάποια βλάβη ή ακόμη καν να κοπεί και να έχουμε απώλειες, είτε να μαζέψει υγρασία. Το τελευταίο σημαντικό πλεονέκτημα των ασύρματων δικτύων είναι η σχετική ευκολία στο στήσιμο του δικτύου. Λόγω της μειωμένης καλωδίωσης, με μία απλή μελέτη του χώρου για σωστή κάλυψη, το μόνο που χρειάζεται είναι η σωστή τοποθέτηση των APs (Access Points) στον χώρο για την σωστή κάλυψη.

Στα μειονεκτήματα τώρα έχουμε για αρχή την ταχύτητα. Οι ταχύτητες που μπορεί να επιτύχει η μετάδοση κάπου σήματος στον αέρα είναι πολύ μικρότερες από αυτές που μπορεί να πετύχει στον

χαλκό ή ακόμη και στο φως (οπτική ίνα). Αν και έχουν γίνει αρκετές βελτιώσεις στις ταχύτητες, με τα σημερινά δεδομένα, δεν πρόκειται ποτέ να ξεπεραστεί η ταχύτητα μετάδοσης μέσω καλωδίου. Ένα δεύτερο και εξίσου σημαντικό μειονέκτημα είναι η ασφάλεια των επικοινωνιών μας. Οι περισσότερες επιθέσεις βέβαια που μπορούν να γίνουν ενάντια σε ένα ενσύρματο δίκτυο, μπορούν επίσης να γίνουν και σε ένα ασύρματο, αλλά η πρόσβαση στο δεύτερο γίνεται πολύ πιο εύκολα. Με μια απλή κεραία, μπορούμε να αποκτήσουμε "πρόσβαση" στην περιοχή που εκπέμπει κάποιο ασύρματο δίκτυο και να αρχίσουμε να "συλλέγουμε" πακέτα που εκπέμπονται (data sniffing). Κάτι τέτοιο μπορεί να αποτραπεί μέσω διάφορων μεθόδων (που θα δούμε αργότερα), αλλά και πάλι η πρόσβαση στο μέσο -που στην προκειμένη περίπτωση είναι ο αέρας- είναι πολύ πιο εύκολη. Επίσης αν και θεωρείται πλεονέκτημα σε μία μικρή περιοχή (π.χ. ο χώρος ενός σπιτιού), σε μία μεγάλη εταιρεία, μπορεί να θεωρηθεί και μειονέκτημα η σωστή κάλυψη ενός χώρου. Τα σήματα δεν έχουν την τάση να περνάνε μέσα από τοίχους, αλλά να αντανακλώνται σε αυτούς και ειδικά σε περιπτώσεις που έχουν να κάνουν με παλαιότερα κτήρια, που οι τοίχοι έχουν σχεδόν διπλάσιο μέγεθος, μπορούμε εύκολα να βρεθούμε προ εκπλήξεων κατά τον σχεδιασμό του ασύρματου δικτύου, γιατί σε αντίστοιχες περιπτώσεις, όταν ένα μόνο Access Point μπορούσε να καλύψει ας υποθέσουμε 2 δωμάτια των 25 τ.μ., εδώ να μην είναι αρκετό και στο ένα από τα δύο δωμάτια να έχουμε ελάχιστο ή και καθόλου σήμα. Το τελευταίο σημαντικό μειονέκτημα των ασύρματων δικτύων είναι η επιρροή που μπορεί να ασκηθεί από τον καιρό. Μπορεί βέβαια να μας προσφέρουν μεγάλη ευκολία και να μπορούμε να έχουμε επικοινωνία με περιοχές που δεν υπάρχει υποδομή για ενσύρματη καλωδίωση, αλλά αν τα καιρικά φαινόμενα είναι άσχημα σε αυτή την περιοχή, τότε "απειλείται" και η επικοινωνία μας. Ένα χαρακτηριστικό παράδειγμα, είναι η ζεύξη Ρόδου – Καστελόριζου για παροχή Internet στην περιοχή του Καστελόριζου, η οποία είναι μία λύση που δίνει πρόσβαση στους πολίτες του νησιού στο Διαδίκτυο, αλλά τις μέρες που υπάρχει κακοκαιρία υπάρχουν και αρκετά προβλήματα επικοινωνίας.

Όλα τα παραπάνω (μειονεκτήματα & πλεονεκτήματα) θα τα συναντήσουμε σιγά σιγά στο σχεδιασμό και στο στήσιμο του δικτύου μας για τον δήμο και θα δούμε πως μπορούμε να τα προσπεράσουμε ή να ελαχιστοποιήσουμε τους κινδύνους που μπορεί να κρύβονται.

Στον ακόλουθο πίνακα βλέπουμε μια γενική εικόνα των διαφορών των ενσύρματων και των ασύρματων δικτύων.

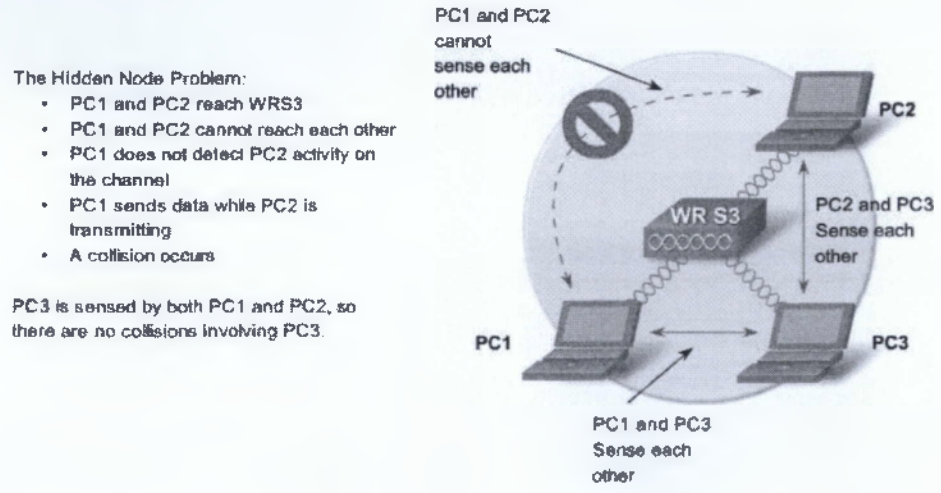
Characteristic	802.11 Wireless LAN	802.3 Ethernet LANs
Physical Layer	Radio Frequency (RF)	Cable
Media Access	Collision Avoidance	Collision Detection
Availability	Anyone with a radio NIC in range of an access point	Cable connection required
Signal Interference	Yes	Inconsequential
Regulation	Additional regulation by local authorities	IEEE standard dictates

Εικ. 1.1 Χαρακτηριστικά ενσύρματων & ασύρματων δικτύων

1.4 CSMA/CD και CSMA/CA

Υπάρχουν δύο βασικά πρότυπα που ακολουθούνται στις τοπολογίες δικτύων. Το ένα που είναι το CSMA/CD (Carrier Sense Multiple Access / Collision Detect) και ακολουθείται στα ενσύρματα δίκτυα και το CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance) που ακολουθείται στα ασύρματα δίκτυα. Στο πρώτο (CSMA/CD), ο κάθε κόμβος πριν αποστείλει τα δεδομένα του, ελέγχει το μέσο για κάποιο μικρό χρονικό διάστημα και αν είναι διαθέσιμο (κάποιος άλλος κόμβος δεν το χρησιμοποιεί), τότε ξεκινάει την αποστολή των πακέτων του. Σε περίπτωση που δύο ή περισσότεροι κόμβοι ξεκινήσουν ταυτόχρονα την αποστολή των πακέτων τους, τότε δημιουργείται σύγκρουση στο κανάλι (collision). Σε περίπτωση σύγκρουσης, το κανάλι γεμίζει με πακέτα για να ενημερωθούν όλοι οι κόμβοι για την σύγκρουση αυτή και ο κάθε αποστολέας περιμένει κάποιο τυχαίο χρονικό διάστημα (μικρό) μέχρι να ξαναελέγξει το κανάλι.

Στην περίπτωση του CSMA/CA, ακολουθείται διαφορετική τακτική. Στη μέθοδο αυτή, το κανάλι ουσιαστικά μοιράζεται και ο κάθε κόμβος όταν αποστέλει κάθε πακέτο, λαμβάνει και μία επιβεβαίωση από το Access Point ότι παραδόθηκε. Όταν γίνεται αυτό, το μέσο είναι κλειστό για αποστολή δεδομένων από άλλους κόμβους. Υπάρχει και εδώ έλεγχος του μέσου πριν την αποστολή δεδομένων, με την διαφορά όμως πως υπάρχει το πρόβλημα, γνωστό και ως, "κρυφός κόμβος" (hidden node). Αυτό έχει να κάνει με την περίπτωση που δύο κόμβοι δεν "βλέπουν" ο ένας τον άλλον (λόγω διαφορετικών δωματιών ή θέσεων στο χώρο) και υπάρχει μεγαλύτερη περίπτωση ταυτόχρονης αποστολής δεδομένων και από τους δύο ταυτόχρονα και αυτόματα μεγαλύτερη πιθανότητα συγκρούσεων στο κανάλι. Λόγω αυτού του προβλήματος, ακολουθείται η μέθοδος CSMA/CA στα ασύρματα δίκτυα και όχι αυτή του CSMA/CD, που χρησιμοποιείται κατά κόρον στα ενσύρματα.



Εικ. 1.2 Το πρόβλημα του κρυφού κόμβου (hidden node problem)

2. Πρωτόκολλα Ασύρματων Δικτύων

2.1 802.11

Τα ασύρματα δίκτυα υπολογιστών βασίστηκαν στο πρωτόκολλο του 802.11. Δημιουργήθηκε από την επιτροπή IEEE LAN/MAN Standards (IEEE 802) και η πρώτη βασική έκδοση ανακοινώθηκε το 1997 με μερικές μεταγενέστερες τροποποιήσεις. Να σημειωθεί ότι η ταχύτητα μετάδοσης που υποστήριζε το αρχικό 802.11 ήταν μόλις 1-2Mbps. Το βασικό αυτό standard ξεκίνησε στα μέσα της δεκαετίας του 1990 και αυτή την στιγμή αποτελείται από οχτώ (8) υποκατηγορίες (εκτός της 802.11 legacy). Όλες αυτές αναπτύχθηκαν σταδιακά και συνεχίζονται να αναπτύσσονται μερικές από αυτές και να συγχωνεύονται πολλές νέες στο standard 802.11. Ένας συγκεντρωτικός πίνακας των "βασικών" υποκατηγοριών που χρησιμοποιούνται ως επί το πλείστον στις μέρες μας είναι ο ακόλουθος.

Standard	Year Ratified	RF Band	Modulation	Data Rate	Range
802.11b	1999	2.4-GHz	DSSS	Up to 11Mbps	150ft, or 35m
802.11a	1999	5-GHz	OFDM	Up to 54Mbps	150ft, or 35m
802.11g	2003	2.4-GHz	OFDM and DSSS	Up to 54Mbps	150ft, or 35m
802.11n	2008	2.4-GHz 5-GHz	MIMO OFDM	248Mbps	230ft, or 70m

Εικ. 2.1 Πρότυπα 802.11a/b/g/n

2.2 802.11a

Το 802.11a ανακοινώθηκε σαν πρότυπο το 1999. Λειτουργεί στην μπάντα των 5GHz, με διαμόρφωση σήματος του προτύπου OFDM (κωδικοποιεί τα δεδομένα σε πολλαπλές συχνότητες) και μπορούμε να επιτύχουμε ταχύτητες του ύψους των 54Mbps και σε αποστάσεις που φτάνουν μέχρι τα 35 μέτρα. Αν και θεωρητικά οι αποστάσεις που μπορεί να φτάσει το συγκεκριμένο πρότυπο είναι ίδιες με αυτές του 802.11b/g, εδώ υπάρχει μία διαφορά. Η απόφαση του συγκεκριμένου προτύπου να λειτουργεί στα 5GHz έδωσε ένα πλεονέκτημα μεν, γιατί δεν χρησιμοποιείται αυτή η μπάντα από τα περισσότερα άλλα πρότυπα, από την άλλη δε, έδωσε και ένα μειονέκτημα. Χρησιμοποιώντας την συγκεκριμένη συχνότητα, λόγω του μικρότερου μήκους κύματος, έχει την τάση να "χάνει" δεδομένα που απορροφώνται από τοίχους και άλλα στερεά αντικείμενα και κατ' επέκταση να μην μπορεί να φτάσει σε μεγαλύτερες αποστάσεις.

Ένα ακόμη μειονέκτημα του 802.11a είναι οι παρεμβολές που δέχεται από άλλες συσκευές που μπορεί να λειτουργούν στην ίδια συχνότητα, αν και αυτές είναι πολύ λιγότερες από τις συσκευές που παρεμβάλουν τις επικοινωνίες που βασίζονται στην συχνότητα των 2.4GHz.

2.3 802.11b/g

Το 802.11b ανακοινώθηκε κι αυτό την ίδια χρονιά με το 802.11a, το 1999. Το συγκεκριμένο πρότυπο λειτουργεί στην μπάντα των 2.4GHz, με διαμόρφωση σήματος DSSS (τεχνική που στέλνει τα σήματα σε όλο το εύρος ζώνης της συχνότητας εκπομπής της συσκευής), μπορούμε να επικοινωνήσουμε σε αποστάσεις μέχρι τα 35 μέτρα και να επιτύχουμε ταχύτητες που φτάνουν τα 11Mbps. Το συγκεκριμένο πρότυπο (όπως και το 802.11g) λόγω της συχνότητας στην οποία λειτουργεί, δέχεται πολλές παρεμβολές από μία μεγάλη γκάμα συσκευών, οι οποίες τις περισσότερες φορές μπορεί να λειτουργούν στους ίδιους (ή σε κοντινούς) χώρους με τα Access Points. Οι συσκευές αυτές είναι:

- Φούρνοι μικροκυμάτων
- Συσκευές Bluetooth
- Συσκευές παρακολούθησης μωρών / Ασύρματα συστήματα ασφαλείας
- Ασύρματα τηλέφωνα
- Ερασιτεχνικός ραδιοεξοπλισμός

Το 802.11g ξεκίνησε το 2003, λειτουργεί στην ίδια συχνότητα με το 802.11b (2.4GHz). Για διαμόρφωση σήματος χρησιμοποιεί το DSSS και το OFDM και μπορούμε να φτάσουμε στις ίδιες αποστάσεις επικοινωνίας, αλλά με μεγαλύτερες ταχύτητες από το 802.11b, αφού μπορούμε να αγγίξουμε τα 54Mbps.

2.4 802.11n

Το συγκεκριμένο πρωτόκολλο ανακοινώθηκε το έτος 2008 και θεωρείται από τα καλύτερα των ημερών μας. Λειτουργεί σε δύο συχνότητες, στα 2.4GHz αλλά και στα 5GHz, χρησιμοποιεί OFDM και MIMO (χρησιμοποιεί πολλές κεραίες σαν αποστολείς, αλλά και σαν παραλείπτες) για την διαμόρφωση του σήματος, μπορεί να φτάσει σε αποστάσεις των 70 μέτρων και οι ταχύτητες που μπορεί να προσφέρει αγγίζουν τα 248Mbps.

Το 802.11n έχει γίνει αρκετά καλύτερο, όσον αφορά στις ταχύτητες και τον Οκτώβριο του 2009, η IEEE σε συνεργασία με την Wi-Fi Alliance, ανακοίνωσαν την νέα έκδοση η οποία υποστηρίζει ταχύτητες του εύρους 54Mbps – 600Mbps.

2.5 802.11ac/ad

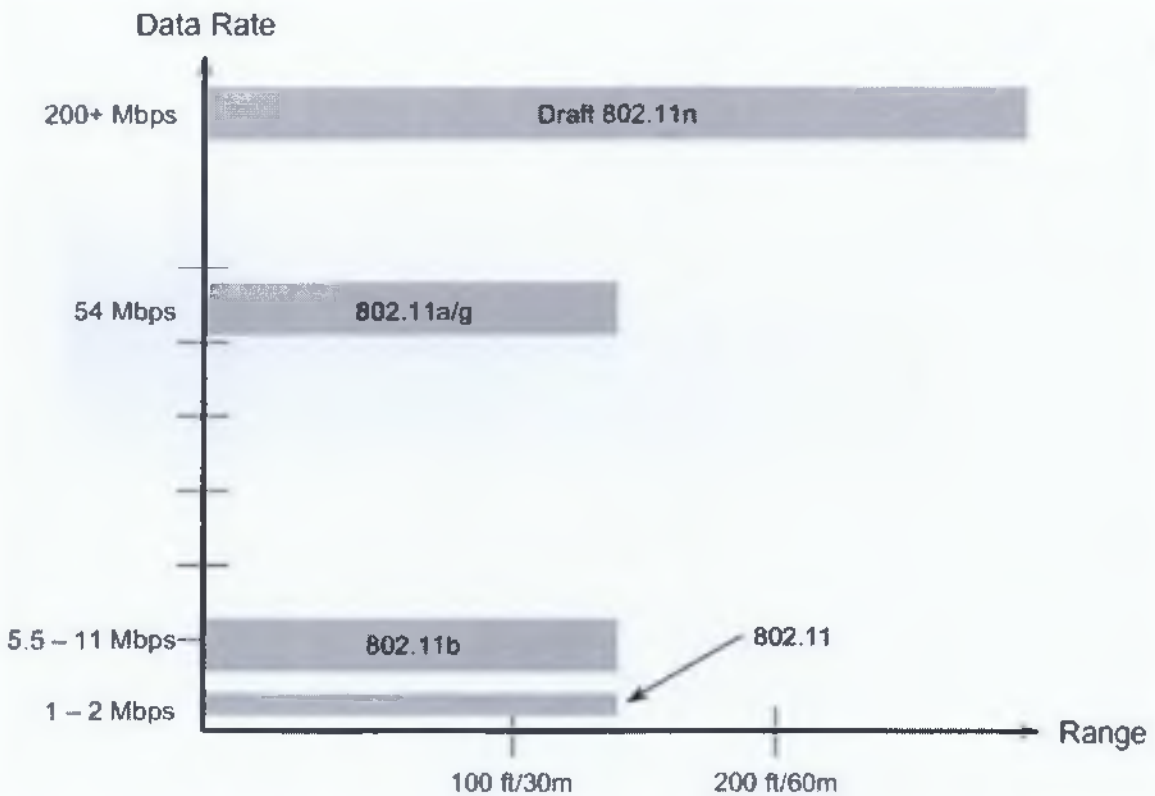
Υπό κατασκευή βρίσκεται και ένα πρότυπο ακόμη, το 802.11ac, το οποίο θα λειτουργεί στην μπάντα των 5GHz και θα έχει την δυνατότητα -μέσω MIMO- αποστολής δεδομένων σε ταχύτητες του 1Gbps και με μία κεραία -μέσω OFDM- των 500Mbps.

Τον Ιούλιο του 2012 ανακοινώθηκε το πρότυπο IEEE 802.11ad "WiGig" το οποίο αναμένεται στην αγορά στις αρχές του 2014. Θεωρητικά οι ταχύτητες που θα φτάνει, θα αγγίζουν τα 7Gbps(!) στην συχνότητα των 60GHz.

Υπό κατασκευή βρίσκονται αρκετά πρότυπα ακόμη, τα οποία αναμένονται την τριετία 2014 – 2016. Αυτά είναι τα ακόλουθα:

- 802.11af
- 802.11aj
- 802.11ai
- 802.11ah
- 802.11aq
- 802.11mc
- 802.11ak

*Περισσότερες πληροφορίες για τα υπό κατασκευή εδώ [https://en.wikipedia.org/wiki/IEEE_802.11] και επίσης εδώ [http://standards.ieee.org/about/get/802/802.11.html]



Εικ. 2.2 Γενική εικόνα ταχύτητας/απόστασης των προτύπων 802.11a/b/g/n

2.6 Τοπολογίες Ασύρματων Δικτύων

Οι τοπολογίες στα ασύρματα δίκτυα υπολογιστών είναι αρκετά διαφορετικές από αυτές των ενσύρματων δικτύων. Αναφορικά είναι οι ακόλουθες:

- Ad-hoc
- BSS
- ESS

Ad-hoc

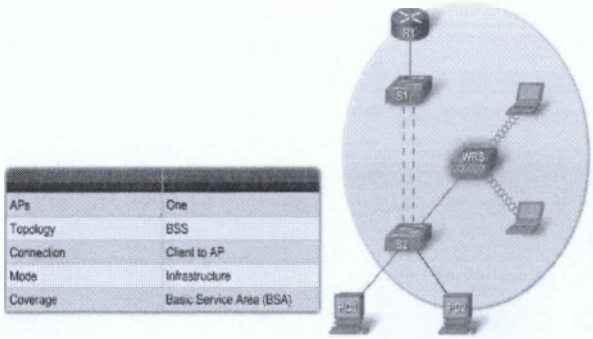
Η τοπολογία Ad-hoc ουσιαστικά είναι και η πιο απλή. Αφορά στην σύνδεση δύο μόνο συσκευών μεταξύ τους, χωρίς να παρεμβαίνει κάποια άλλη ενδιάμεσα. Ένα παράδειγμα μιας τέτοιας τοπολογίας είναι η σύνδεση δύο συσκευών μέσω Bluetooth. Στο πρότυπο IEEE 802.11 οι τοπολογίες Ad-hoc αναφέρονται και ως "ανεξάρτητα BSS" (IBSS: Independent Basic Service Sets).

BSS (Basic Service Sets)

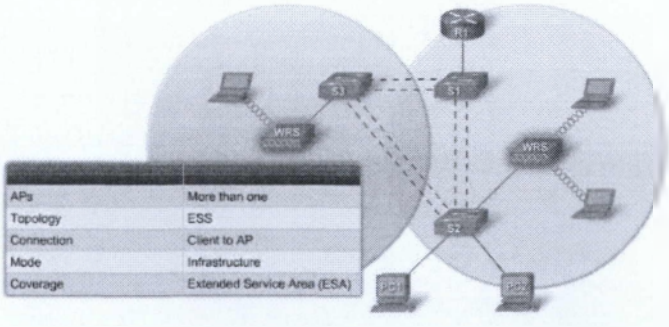
Η BSS τοπολογία είναι μια μικρή επέκταση του ήδη υπάρχοντος ενσύρματου δικτύου μας, προσφέροντας και ασύρματη κάλυψη σε κάποιο μέρος πέραν αυτού. Μια τέτοια τοπολογία μπορεί να θεωρηθεί η σύνδεση ενός Access Point σε κάποιο switch του δικτύου μας, παρέχοντας έτσι κάποια μεγαλύτερη κάλυψη (ασύρματη). Η περιοχή κάλυψης που αφορά μία Ad-hoc τοπολογία (IBSS) και μία BSS τοπολογία, ονομάζεται και BSA (Basic Service Area).

ESS (Extended Service Sets)

Η συγκεκριμένη τοπολογία είναι ουσιαστικά η επέκταση μίας τοπολογίας BSS, με άλλα λόγια η προσθήκη παραπάνω του ενός Access Point σε διάφορα (ή και στο ίδιο) switch/es για κάλυψη μιας ακόμη μεγαλύτερης περιοχής. Η περιοχή που καλύπτεται σε αυτή την περίπτωση ονομάζεται και ESA (Extended Service Area).



Εικ. 2.3 Τοπολογία BSS (Basic Service Sets)



Εικ. 2.4 Τοπολογία ESS (Extended Service Sets)

2.7 Βασική Σύνδεση και Λειτουργία Ενός Ασύρματου Δικτύου

Από την στιγμή που έχουμε έναν πομπό που εκπέμπει (Access Point) και ένα δέκτη ο οποίος θέλει να συνδεθεί (κόμβος με δυνατότητα ασύρματης σύνδεσης) υπάρχει μία συγκεκριμένη διαδικασία που ακολουθείται. Για να επιτευχθεί λοιπόν μία σύνδεση σε ένα ασύρματο δίκτυο, υπάρχουν τρία (3) βήματα που πρέπει να γίνουν και τα οποία είναι τα εξής:

- 802.11 probing
- 802.11 authentication
- 802.11 association

Στο πρώτο βήμα (probing), οι clients (κόμβοι) στέλνουν κάποια μηνύματα σε διάφορα κανάλια τα οποία ονομάζονται probe requests, και τα οποία καθορίζουν το όνομα του ασύρματου δικτύου στο οποίο θέλουν να συνδεθούν (SSID). Σε περίπτωση που ο κόμβος δεν ξέρει σε ποιο ασύρματο δίκτυο θέλει να συνδεθεί ή θέλει να κάνει μία σάρωση των δικτύων της περιοχής, τότε απλά στέλνει τα ίδια πακέτα, τα οποία όμως δεν περιέχουν το πεδίο του SSID. Εάν το Access Point έχει απενεργοποιημένο το broadcast του SSID, τότε με μία τέτοια απλή σάρωση το δίκτυο αυτό δεν θα εμφανιστεί στην λίστα των ασύρματων δικτύων που καλύπτουν την περιοχή στην οποία βρίσκεται ο κόμβος.

Στο δεύτερο βήμα (authentication), το αρχικό 802.11 υλοποιήθηκε με δύο βασικές μεθόδους. Η πρώτη αφορούσε στην ανοιχτή πιστοποίηση. Ο κάθε κόμβος ζητούσε από το Access Point μία πιστοποίηση ότι μπορεί να συμμετάσχει στο δικτύο και την λάμβανε αυτόματα. Να σημειωθεί ότι αυτή η μέθοδος χρησιμοποιούταν σχεδός σε όλες τις υλοποιήσεις του 802.11. Η δεύτερη μέθοδος ονομάζεται "πιστοποίηση κοινού κλειδιού" (shared key authentication) η οποία βασίζεται στο WEP (Wired Equivalency Protection) και θα αναλυθεί εκτενέστερα σε επόμενο κεφάλαιο. Η γενική ιδέα είναι ότι το κλειδί WEP διαμοιράζεται μεταξύ των κόμβων και του Access Point και όταν ο κόμβος ζητήσει άδεια για να συνδεθεί τότε λαμβάνει ένα "challenge text" (σε plain text) το οποίο το κρυπτογραφεί χρησιμοποιώντας το κλειδί που έχει και στη συνέχεια το Access Point το αποκρυπτογραφεί βάσει του κλειδιού του δικτύου. Αν τα δύο μηνύματα είναι ίδια, τότε ο κόμβος μπορεί να πιστοποιηθεί για είσοδο στο δίκτυο. Αυτό βέβαια κρύβει άλλους κινδύνους.

Στο τρίτο και τελευταίο βήμα, έχουμε τη συσχέτιση του νέου κόμβου με το υπόλοιπο δίκτυο (association). Στην ουσία δημιουργείται ένα ακόμη λογικό κανάλι για τον νέο κόμβο που εισέρχεται στο δίκτυο από την πλευρά του Access Point το οποίο ονομάζεται AID (Association Identifier) και το οποίο αντιστοιχεί σε κάποια θύρα του εκάστοτε switch στο οποίο συνδέεται το συγκεκριμένο AP. Με το που ολοκληρωθεί και το τελευταίο βήμα, τότε έχουμε ένα νέο κόμβο ο οποίος μπορεί να αποστείλει και να λάβει δεδομένα μέσα στο δίκτυο.

3. Ασφάλεια Δικτύων

3.1 Γενικές Απειλές Δικτύων

Η ασφάλεια της πληροφορίας και των επικοινωνιών είναι ένα πολύ σοβαρό κομμάτι της Πληροφορικής, που δυστυχώς, τις περισσότερες φορές δεν λαμβάνεται σοβαρά υπόψην. Οι μελέτες που αφορούν την ασφάλεια, μας δίνουν πολύ άσχημα αποτελέσματα όσον αφορά σχεδόν το κάθε κομμάτι της επικοινωνίας μέσω ηλεκτρονικών υπολογιστών. Από τους κωδικούς για την σύνδεση στο σύστημα, μέχρι τα προγράμματα που κατεβάζει ο μέσος χρήστης από το Διαδίκτυο, βλέπουμε ότι υπάρχει αρκετή άγνοια. Το κομμάτι της ασφάλειας που μας ενδιαφέρει για αυτήν την εργασία αφορά τα δίκτυα των υπολογιστών, ενσύρματα και ασύρματα. Οι διαφορές μεταξύ αυτών των δύο τύπων δικτύου, στα θέματα ασφαλείας είναι ελάχιστες. Αναφορικά, αν μπορούμε να χωρίσουμε τις απειλές που μπορεί να δεχτεί το δίκτυο μας, είναι οι ακόλουθες τρεις (3) κατηγορίες:

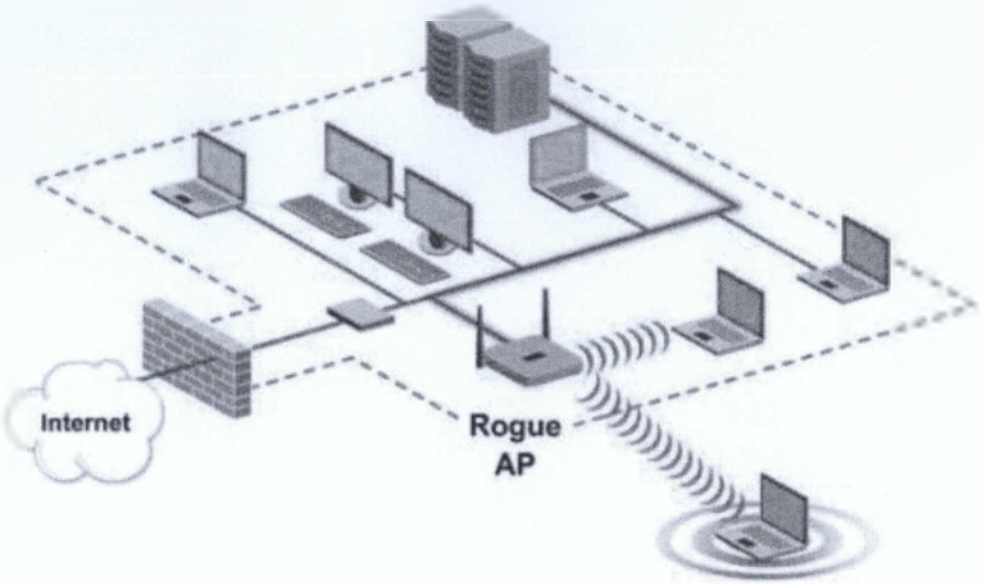
- War drivers
- Hackers (Crackers)
- Υπάλληλοι

Πιο αναλυτικά, οι "War drivers" χρησιμοποιούν ένα αυτοκίνητο και με ένα laptop κάνουν ουσιαστικά βόλτες σε γειτονιές ψάχνοντας για ανοιχτά δίκτυα τα οποία είναι ευάλωτα σε επιθέσεις. Ο συγκεκριμένος τρόπος επίθεσης, με την ονομασία "war driving" είχε μεγάλη δημοτικότητα στη δεκαετία του 2000 με 2010, όταν τα περισσότερα ασύρματα δίκτυα ήταν ανοιχτά από τους κατασκευαστές τους και οι περισσότεροι πελάτες δεν γνώριζαν για το τι κινδύνους έκρυβε κάτι τέτοιο. Αν πάρουμε σαν παράδειγμα τα ασύρματα modem/routers που έδιναν οι μεγάλοι πάροχοι Διαδικτύου στην χώρα μας (ISPs: Internet Service Provider), όπως ο Ο.Τ.Ε. και η Forthnet το 90% περίπου των συσκευών που έδιναν στους πελάτες τους ήταν ξεκλείδωτες (χωρίς κάποιο κλειδί ασφαλείας) ή χρησιμοποιούσαν την πιο απλή μέθοδο, WEP, με αποτέλεσμα να έχουμε πολλά κρούσματα με τους πελάτες να βλέπουν ξαφνικά ότι χάνουν ταχύτητες ή δεδομένα και να μην ξέρουν τον λόγο. Να αναφερθεί εδώ το ότι για να "σπάσει" ένα ασύρματο δίκτυο το οποίο προστατεύεται με WEP, με τις προδιαγραφές και τις δυνατότητες που έχουν –κατά μέσο όρο- οι υπολογιστές στα σπίτια μας, χρειάζεται λιγότερο από ένα (1) λεπτό(!).

Όσον αφορά στους hackers: Ο όρος hacker αναφέρεται σε άτομα τα οποία μπορούν να βρίσκουν αδυναμίες σε ένα σύστημα, σε ένα δίκτυο κτλ για εκπαιδευτικούς σκοπούς ή με απώτερο σκοπό να ενημερώσουν τον διαχειριστή του εκάστοτε συστήματος για κάποια "τρύπα" ασφαλείας και έτσι να βελτιωθεί και το security του συστήματος και να μην υπάρχουν απώλειες από αυτό. Γι' αυτό το λόγο καλύτερο είναι να χρησιμοποιήσουμε τον όρο cracker, ο οποίος κάνει το ίδιο πράγμα με τον hacker, με οικονομικό ή προσωπικό όμως όφελος. Το hacking/cracking σε περιπτώσεις που αφορούν ένα ασύρματο δίκτυο δεν είναι και ιδιαίτερα δύσκολο. Τα περισσότερα εργαλεία που χρησιμοποιούνται από τους αναλυτές ασφαλείας χρησιμοποιούνται και από αυτή την πλευρά, την "κακή", ενώ είναι πολύ εύκολο να βρεθούν και το μεγαλύτερο μέρος αυτών είναι ελεύθερο. Μία εύκολη μέθοδος είναι το

"sniffing" ενός ασύρματου δικτύου και όσα περισσότερα πακέτα μαζεύει ο επιτιθέμενος, τόσο αυξάνονται και οι πιθανότητές του για να μπει στο δίκτυο ακόμη πιο γρήγορα. Το μεγάλο πλεονέκτημα άλλωστε που ταυτόχρονα θεωρείται και μεγάλο μειοντέκτημα στα ασύρματα δίκτυα, είναι ότι είναι ασύρματα. Έτσι όπως μπορεί ο υπάλληλος μιας εταιρείας να έχει εύκολα πρόσβαση σ' αυτό (χωρίς την ανάγκη για κάποιο καλώδιο κτλ), έτσι και ένας κακόβουλος χρήστης μπορεί να κάθεται στο δίπλα δωμάτιο και να προσπαθεί να υποκλέψει δεδομένα μέσω sniffing. Εκτός των εργαλείων, μπορείς πολύ εύκολα να σπάσεις ένα ασύρματο δίκτυο απλά με την χρήση μιας μηχανής αναζήτησης (π.χ. Google). Ένα από τα μειονεκτήματα των default ρυθμίσεων σε συσκευές, είναι ότι αυτές μπορεί να τις βρει ο καθένας στο εκάστοτε manual. Έτσι αν ο επιτιθέμενος γνωρίζει ότι ο Ο.Τ.Ε. αυτή την περίοδο δίνει στους πελάτες του συσκευές Huawei και ZTE, σκανάρει την περιοχή γύρω από το σπίτι του και αν βρει αρκετά δίκτυα με τις default ονομασίες τους (π.χ. OTE_4321, OTE_NETWORK_4533 κτλ), τότε έχει και μεγάλες πιθανότητες να μαντέψει το σωστό κλειδί για να μπει στα δίκτυα αυτά, μόνο και μόνο ψάχνοντας τις default ρυθμίσεις στο manual(!). Αυτό το θέμα με τις standard default ρυθμίσεις για το εκάστοτε μοντέλο που παρέχουν οι ISPs σιγά-σιγά λύθηκε, και πλέον οι περισσότερες έρχονται με "σεταρισμένο" το WPA2 και με διαφορετικό κλειδί για το κάθε μηχάνημα που βρίσκεται συνήθως κολλημένο στο κάτω μέρος της συσκευής. Έτσι δεν μπορεί ο καθένας απλά με μερικές αναζητήσεις στο Internet να μπορεί να αποκτά πρόσβαση (τόσο εύκολα τουλάχιστον) στο ασύρματο δίκτυο του καθενός. Όχι ότι το WPA2 δεν μπορεί να παραβιαστεί, αλλά σίγουρα είναι πολύ πιο ασφαλές από το WEP και το WPA.

Η τρίτη κατηγορία αφορά τους υπαλλήλους. Στη συντριπτική πλειοψηφία των περιπτώσεων κενών ασφαλείας έχουμε αναφορές για άτομα της ίδιας της εταιρείας(!). Τις περισσότερες φορές δεν πρόκειται για εσκεμμένες ενέργειες με σκοπό την βλάβη της εταιρείας, αλλά γίνονται λόγω ελλιπούς ενημέρωσης ή αδιαφορίας. Γενικά το θέμα της ασφαλείας στην Πληροφορική, όπως αναφέρθηκε και πιο πριν, δυστυχώς δεν συγκινεί όσο θα έπρεπε. Άλλες υπόλοιπες φορές έχει να κάνει και με ηθελημένες προσπάθειες διάφορων υπαλλήλων οι οποίοι σ' αυτή την περίπτωση ονομάζονται crackers. Δύο χαρακτηριστικά παραδείγματα για την κάθε περίπτωση. Στην πρώτη (μη εσκεμμένη) ενέργεια, μπορεί κάποιος υπάλληλος να συνδέσει σε μία θύρα του switch του ορόφου στον οποίον εργάζεται, ένα Access Point (Rogue Access Point), για να μπορεί να έχει πρόσβαση στο Internet και μέσω του smart phone του, και ενώ γι' αυτόν να είναι κάτι απλό και ανευ σημασίας να δημιουργεί εκείνη την στιγμή μια πολύ μεγάλη τρύπα στην ασφάλεια του δικτύου. Θα δούμε πως μπορούμε να προστατευτούμε από αυτό στο επόμενο κεφάλαιο. Στη δεύτερη (ηθελημένη) ενέργεια, ο "κακός" υπάλληλος της εταιρείας, μπορεί να τοποθετήσει ένα φορητό υπολογιστή, ένα netbook κτλ σε μία θύρα ενός switch και μέσω μίας τεχνικής, που θα αναλύσουμε αργότερα (man-in-the-middle-attack), να μπορεί να καταγράφει όλη την κίνηση του δικτύου η οποία λόγω της μεθόδου αυτής θα περνάει πρώτα από τον υπολογιστή αυτό και μετά θα πηγαίνει προς τον router ή οποιαδήποτε άλλη συσκευή εντός ή εκτός δικτύου.



Εικ. 3.1 Rogue Access Point

Και οι τρεις (3) γενικές κατηγορίες απειλών ενός δικτύου καλό θα ήταν να μη περνάνε στα ψιλά γράμματα. Στις μικρομεσαίες επιχειρήσεις όμως συνήθως κάτι τέτοιο γίνεται. Μια καλή τεχνική, εκτός από την ασφάλεια του δικτύου από τους διαχειριστές του, είναι και η σωστή ενημέρωση του προσωπικού. Πολλές φορές, άθελα του, δημιουργεί μεγάλα κενά ασφαλείας, τα οποία μπορεί να περάσει αρκετός καιρός μέχρι να φανερωθούν ή μπορεί και ποτέ. Ένα "security policy" είναι πλέον απαραίτητο να υπάρχει, το οποίο θα αναφέρει όλους τους πιθανούς κινδύνους και το τι απαγορεύεται να κάνουν οι υπάλληλοι με το δίκτυο της εταιρείας. Εκτός από ένα Rogue AP, το οποίο μπορεί να τοποθετηθεί ηθελημένα ή μη, υπάρχουν πολλοί κίνδυνοι ακόμα που μπορούν να θέσουν την ασφάλεια του δικτύου ή και ολόκληρου του Πληροφοριακού Συστήματος (ΠΣ) της εκάστοτε εταιρείας στον αέρα. Αναφορικά:

- Hackers*/Crackers
- Rogue Access Points
- Spammer
- Phishing emails
- Phreaker

* Οι hackers χωρίζονται σε δύο βασικές ομάδες (white και black) με αρκετές υποκατηγορίες.

3.2 Μέθοδοι Πιστοποίησης και Κίνδυνοι

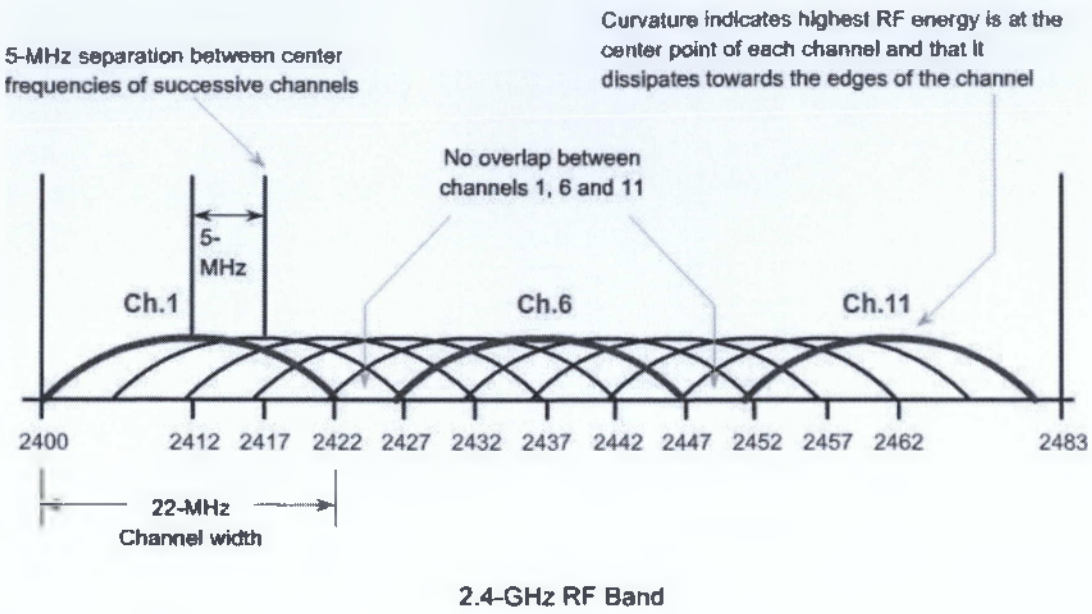
Όπως αναφέρθηκε και παραπάνω, οι γενικές απειλές που μπορεί να δεχθεί ένα δίκτυο χωρίζονται σε τρεις (3) κατηγορίες. Πως υλοποιούνται όμως; Πως μπορεί κάποιος να αποκτήσει πρόσβαση στο δίκτυο μας (και στην συγκεκριμένη περίπτωση στο ασύρματο δίκτυο μας); Για να γίνουν κατανοητές οι απειλές

και οι τρόποι επίθεσης και άμυνας, που θα αναλυθούν στο επόμενο κεφάλαιο, θα πρέπει να κατανοήσουμε πρώτα τα πρωτόκολλα (πιστοποιήσεις) ασφαλείας που υπάρχουν μέχρι σήμερα στα ασύρματα δίκτυα υπολογιστών και ο τρόπος με τον οποίον υλοποιούνται. Αναφορικά χωρίζονται σε τέσσερις (4) κατηγορίες, βάσει του χρόνου που υλοποιήθηκαν και χρησιμοποιήθηκαν. Οι κατηγορίες αυτές (ανά χρόνο) είναι οι εξής:

- Ανοιχτή πρόσβαση (Open Access) – SSID
- Πρώτη γενιά κρυπτογράφησης (First Generation Encryption) – WEP
- Ενδιάμεση περίοδος (Interim) – WPA
- Το παρόν (Present) – WPA2/802.11i

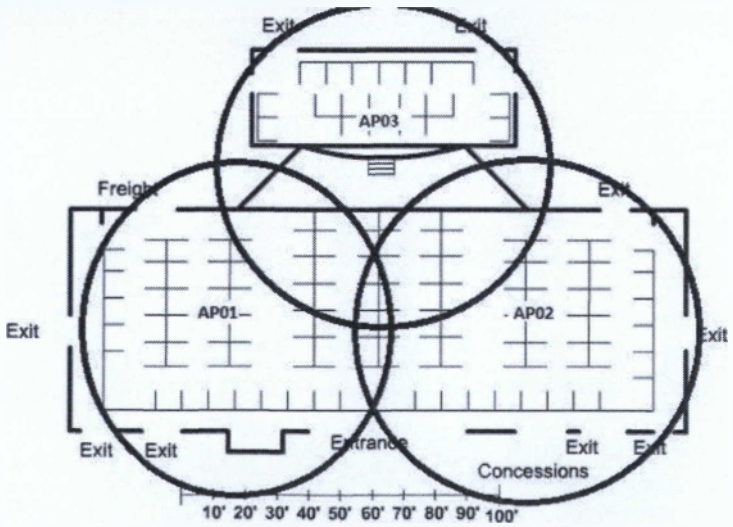
3.2.1 SSID (Service Set Identification)

Το SSID που αναφέρεται και ως όνομα δικτύου (ασύρματου), είναι ένα αλφαριθμητικό μεγέθους έως 32 bytes, το οποίο ουσιαστικά ανακοινώνει στην ευρύτερη περιοχή το όνομα του δικτύου. Αν για παράδειγμα ρυθμίσουμε στο Access Point το SSID να έχει την τιμή "My Personal Network", τότε στην περιοχή που καλύπτεται από αυτό το Access Point, οποιαδήποτε συσκευή με δυνατότητα σύνδεσης σε ασύρματα δίκτυα, κάνει ένα scan, θα βρει μέσα στα ασύρματα δίκτυα και το συγκεκριμένο με την ονομασία που του δώσαμε (My Personal Network). Να αναφερθεί εδώ πως όταν μιλάμε για περιοχές μεγαλύτερες του ενός σπιτιού για παράδειγμα (περίπου 70 – 80 τ.μ.), όταν δηλαδή ένα μόνο Access Point δεν μπορεί να καλύψει την περιοχή, τότε χρησιμοποιούμε πολλά APs, με την ίδια συνήθως ονομασία δικτύου (SSID), αλλά πρέπει να "παίζουν" σε διαφορετικά κανάλια. Αυτό γίνεται γιατί αν το A Access Point, του οποίου η μπάντα συχνότητας βρίσκεται στο ίδιο ή σε κοντινό κανάλι με το B Access Point, τότε έχουμε παρεμβολές στο σήμα. Αυτό μπορεί να συμβεί ακόμη και στις οικίες γειτόνων, που μπορεί να παρεμβαίνει ένας μόνο τοίχος μεταξύ των δύο (2) modem/router με δυνατότητα ασύρματης σύνδεσης, τα οποία χρησιμοποιούν ας υποθέσουμε το ίδιο πρότυπο (π.χ. το 802.11b) και χρησιμοποιούν το ίδιο κανάλι ή δύο (2) διαφορετικά κανάλια τα οποία δεν έχουν απόκλιση τουλάχιστον πέντε (5) (δηλαδή το ένα να χρησιμοποιεί το κανάλι 1 και το άλλο τουλάχιστον το κανάλι 6). Τότε και οι δύο (2) θα έχουν πιθανότατα προβλήματα με τις παρεμβολές στο εκάστοτε δίκτυο του σπιτιού τους. Γενικά η οικογένεια πρωτοκόλλων 802.11b/g/n, αποτελείται από δεκατέσσερα (14) κανάλια. Τα πρώτα δεκατρία (13) χρησιμοποιούνται στην Ευρώπη, ενώ το δέκατο τέταρτο (14ο) χρησιμοποιείται μόνο στην Ιαπωνία. Το κάθε κανάλι αλληλοπαρεμβάλλεται με τέσσερα (4) κανάλια στα αριστερά του και τέσσερα (4) στα δεξιά του. Γι' αυτό ακολουθείται και η τακτική της απόστασης τουλάχιστον πέντε (5) καναλιών μεταξύ τους, για να αποφύγουμε τυχόν παρεμβολές.



Εικ. 3.2 Μη-επικαλυπτόμενα κανάλια στην συχνότητα των 2.4GHz

Έτσι και βάσει του παραπάνω σχήματος (που πρέπει να λαμβάνεται πάντα υπόψι), όταν πρόκειται να καλύψουμε περιοχές με παραπάνω από ένα Access Points, τότε πρέπει πάντα τα γειτονικά APs, να "παίζουν" σε κανάλια που μεταξύ τους θα απέχουν τουλάχιστον πέντε (5). Αν έχουμε να καλύψουμε μία περιοχή όπως η παρακάτω:



Εικ. 3.3 Χώρος κάλυψης με τρία (3) Access Points

τότε το AP01 θα πρέπει να λειτουργεί στο πρώτο (1ο) κανάλι, το AP02 στο έκτο (6ο) και το τρίτο AP (AP03) στο κανάλι έντεκα (11). Έτσι, αν και τα τρία (3) APs γειτονεύουν μεταξύ τους, δεν θα υπάρχουν παρεμβολές. Σε περίπτωση που βρεθούμε σε χώρο που εκπέμπουν περισσότερα του ενός APs, και θέλουμε να γλυτώσουμε χρόνο ή δεν έχουμε πρόσβαση στο configuration των APs, τότε με ένα laptop, μπορούμε να τρέξουμε την παρακάτω εντολή (σε Linux OS):

$iwlist scan (με δικαιώματα **root [υπερχρήστη]**)

και θα πάρουμε μια αναλυτική λίστα για τα κανάλια που χρησιμοποιούνται από τα APs που εκπέμπουν στο χώρο αυτό.

Ένα τελευταίο χαρακτηριστικό του SSID είναι η δυνατότητα της απόκρυψής του. Μπορούμε, δηλαδή, να ρυθμίσουμε το εκάστοτε Access Point ώστε να μην κάνει broadcast την ονομασία του ασύρματου δικτύου. Αυτό είναι το μόνο κομμάτι ασφαλείας που μπορεί να μας παρέχει. Βέβαια αυτό δεν σημαίνει πως δεν μπορεί να γίνει αναγνώριση του οποιουδήποτε SSID, έστω κι αν αυτό δεν εκπέμπεται. Ένα απλό scan, δεν θα μας δώσει αποτελέσματα, αλλά με μερικά εργαλεία, τα οποία θα τα χρησιμοποιήσουμε αργότερα, θα δούμε ότι η ανακάλυψη του SSID είναι μία αρκετά απλή διαδικασία.

3.2.2 WEP (Wired Equivalent Privacy)

Το WEP ήταν ο πρώτος αλγόριθμος (πιστοποίηση) ασφαλείας για τα IEEE 802.11 ασύρματα δίκτυα. Πρωτοπαρουσιάστηκε το Σεπτέμβριο του 1999 σαν κομμάτι του αρχικού προτύπου 802.11. Το WEP μέχρι και πριν λίγα χρόνια ήταν η default επιλογή από τους κατασκευαστές των Access Points. Αυτό βέβαια ήταν κάτι αρκετά αρνητικό γιατί όπως θα δούμε και αργότερα, ο αλγόριθμος αυτός είναι αρκετά εύκολο να σπάσει και μάλιστα σε ιδιαίτερα μικρό χρόνο.

Υπάρχουν δύο (2) γενικά standards του WEP. Το πρώτο είναι το Standard 64-bit WEP (γνωστό και ως WEP-40), το οποίο χρησιμοποιεί 40 bits για το κλειδί και 24 bits για την δημιουργία του initialization vector (μια σειρά από ψευδοτυχαίους αριθμούς για την κρυπτογράφηση). Με το που συντάχθηκε το συγκεκριμένο πρότυπο και άρχισε να χρησιμοποιείται, λόγω περιορισμών της κυβέρνησης των Η.Π.Α., οι κατασκευαστές δημιούργησαν άλλο ένα πρότυπο βασιζόμενο στο WEP. Το συγκεκριμένο ονομάζεται WEP-104 και χρησιμοποιεί 104 bits για τον βέκτορα των ψευδοτυχαίων αριθμών και συνολικά το μέγεθός του αγγίζει τα 128 bits (λόγω και των bits που χρησιμοποιούνται σαν κλειδί).

Το στήσιμο ενός Access Point με τον αλγόριθμο WEP είναι αρκετά απλό (όπως και οι υπόλοιποι αλγόριθμοι). Οι χαρακτήρες που δέχεται ο συγκεκριμένος αλγόριθμος είναι από το 0 (μηδέν) έως το 9 (εννιά) και οι χαρακτήρες a ή A έως και το f ή F. Ο περιορισμός σε αυτούς τους χαρακτήρες οφείλεται στο ότι ο αλγόριθμος δέχεται σαν κλειδιά μόνο(!) δεκαεξαδικούς χαρακτήρες (hexadecimal).

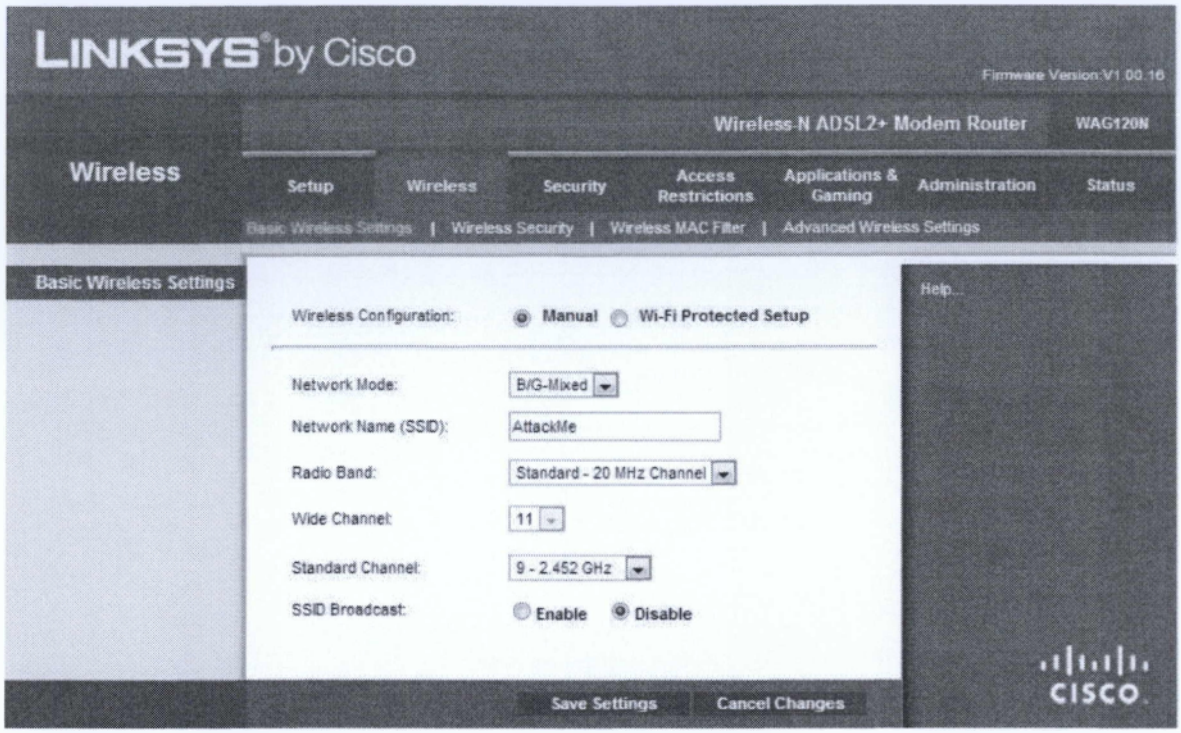
Η εικόνα που ακολουθεί μας δείχνει το σετάρισμα ενός modem/router το οποίο θα το χρησιμοποιήσουμε για τους σκοπούς της εργασίας μόνο ως Access Point και όλες οι επιθέσεις που θα γίνουν, για να δούμε τις δυνατότητες των αλγορίθμων κρυπτογράφησης θα γίνουν σ' αυτό. Αναφορικά, όλες οι επιθέσεις θα γίνουν μέσω του Backtrack 5r3 (distribution του Linux, πληθώρα εφαρμογών που αφορούν την ασφάλεια) και το AP που θα δεχθεί τις επιθέσεις αυτές είναι το WAG 120N της Linksys.

Εικ. 3.4 Σετάρισμα του AP με κρυπτογράφηση WEP

Επίσης βλέπουμε πως με την επιλογή "Generate" του AP, δημιουργήσαμε ψευδοτυχαία το κλειδί που θα πρέπει να έχει ο κόμβος για να συνδεθεί στο ασύρματο δίκτυο. Πρέπει να αναφερθεί και το γεγονός πως χρησιμοποιούμε την "καλύτερη" από τις δύο (2) μεθόδους του WEP, δηλαδή αυτή που υποστηρίζει 104 bits για τον βέκτορα παραγωγής ψευδοτυχαίων αριθμών και 26 bits για το κλειδί. Στο επόμενο κεφάλαιο θα δούμε και με ποιον τρόπο και πόσο γρήγορα θα μπορέσουμε να σπάσουμε τον συγκεκριμένο αλγόριθμο.

Για τους σχολαστικούς ακολουθούν και τα χαρακτηριστικά του υπολογιστή του επιτιθέμενου. Αυτό για να δείξουμε πως με ένα σχετικά παλιό μηχάνημα, μπορούμε να πετύχουμε αρκετά γρήγορες ταχύτητες στο σπάσιμο ενός ασύρματου δικτύου. Έτσι μπορούμε να φανταστούμε περίπου την διαφορά που θα μπορούσαμε να έχουμε, αν ο υπολογιστής αυτός ήταν πιο κοντά στα σημερινά μοντέλα, με πολλή περισσότερη μνήμη και αρκετά καλύτερη επεξεργαστική δυνατότητα. Τα χαρακτηριστικά λοιπόν, είναι τα εξής:

- Επεξεργαστής: Intel Pentium Dual Core (2.2 GHz)
- Μνήμη RAM: 2GB (DDR2-667MHz)
- Σκληρός δίσκος: WD 160GB (5400RPM)



Εικ. 3.5 Σετάρισμα πρωτοκόλλου/συχνότητας, καναλιού και SSID

Στην παραπάνω εικόνα βλέπουμε το βασικό σετάρισμα του AP. Αυτό είναι και ένα από τα πρώτα πράγματα που αλλάζουμε με το που αρχίσουμε να ρυθμίζουμε το AP. Πιο αναλυτικά, έχουμε βάλει σαν SSID ή αλλιώς σαν ονομασία του ασύρματου δικτύου το "AttackMe", έτσι θα φαίνεται το δίκτυο μας αν κάνουμε ένα σκανάρισμα της περιοχής που εκπέμπει. Ή μήπως όχι; Με ένα απλό σκανάρισμα δεν θα φανεί το SSID γιατί έχουμε επιλέξει το "Disable" στο "SSID Broadcast", αλλά με ένα διαφορερικό σκανάρισμα που θα δούμε στο επόμενο κεφάλαιο, θα ανακαλύψουμε ότι αυτή η επιλογή δεν είναι και τόσο δραστική. Στα υπόλοιπα χαρακτηριστικά, βλέπουμε πώς χρησιμοποιούμε το πρότυπο του 802.11b/g mixed, δηλαδή θα επιλέξει αυτόματα το καλύτερο (το AP), βάσει της περιοχής και των υπόλοιπων δικτύων που μπορεί πιθανόν να εκπέμπουν στον ίδιο χώρο. Τέλος το κανάλι που έχουμε επιλέξει είναι το εννέα (9), κι αυτό για το λόγο του ότι στην περιοχή αυτή έγινε ένα scan νωρίτερα και παρατηρήθηκε πως τα περισσότερα APs εκπέμπουν στα κανάλια 1 έως 4 και έτσι πήγαμε τουλάχιστον πέντε (5) κανάλια παρακάτω για να μην έχουμε παρεμβολές.

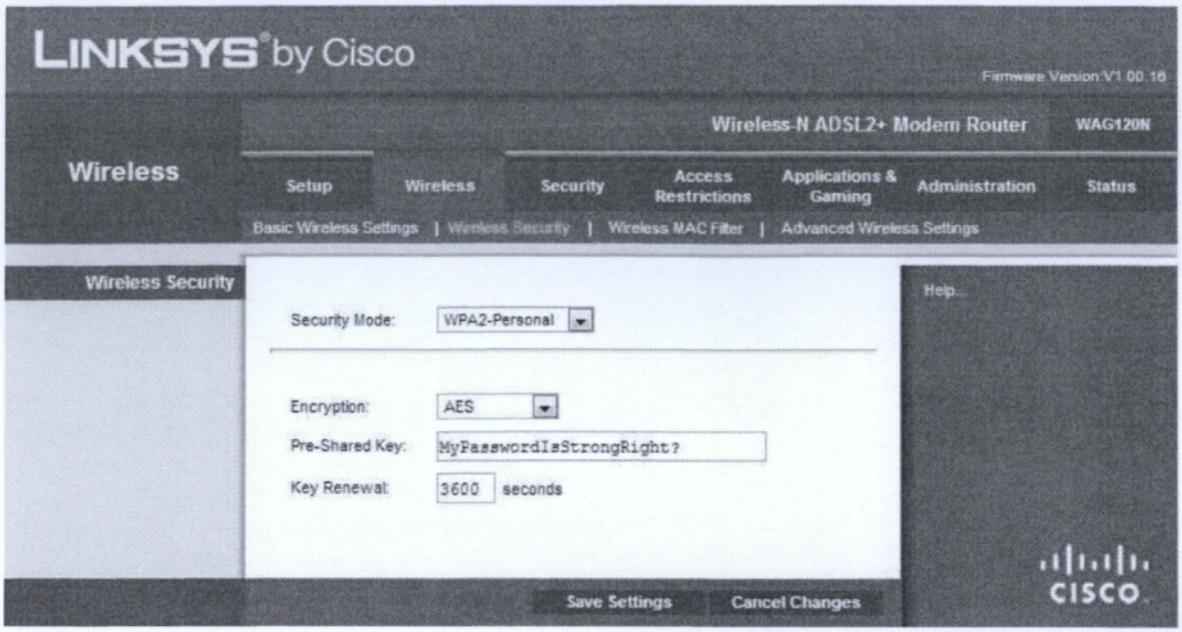
Υπενθυμίζουμε ότι για να δούμε σε μία λίστα το ποια δίκτυα εκπέμπουν και σε ποια κανάλια και με ποια πρότυπα, χρησιμοποιούμε σε Linux την εντολή **$iwlist scan**, η οποία αναγνωρίζει αυτόματα όλα τα network interfaces του υπολογιστή μας και με όσα είναι δυνατόν (μόνο δηλαδή αυτά των ασύρματων καρτών δικτύου), πραγματοποιεί το scan και μας δίνει τα αποτελέσματα που επιθυμούμε.

3.2.3 WPA & WPA2 (Wi-Fi Protected Access & Wi-Fi Protected Access II)

Τα δύο (2) αυτά πρωτόκολλα ασφαλείας για ασύρματα δίκτυα δημιουργήθηκαν από την Wi-Fi Alliance το 2003 (WPA) και το 2004 (WPA2). Το πρώτο είναι και το προσχέδιο του προτύπου IEEE 802.11i, ενώ το δεύτερο είναι ουσιαστικά και η "στενογραφία" του 802.11i-2004 (όπως είναι και η πλήρης ονομασία του). Και τα δύο φτιάχτηκαν για να καλύψουν τα κενά ασφαλείας που άφηνε το WEP. Όταν πρωτοπαρουσιάστηκε το WPA, μέσω firmware upgrades, οι κάτοχοι ασύρματων καρτών που μέχρι πρότινος υποστήριζαν μόνο το WEP, πλέον μπορούσαν να υποστηρίξουν και το WPA. Για πρώτη φορά βλέπουμε να χρησιμοποιείται και η τεχνολογία TKIP (Temporal Key Integrity Protocol), βάσει της οποίας δημιουργείται ένα κλειδί ανά πακέτο, μεγέθους 128 bit. Επίσης το WPA, όπως και το WEP, χρησιμοποιεί και το CRC (Circle Redundancy Check) ως έναν έλεγχο για την ακεραιότητα των πακέτων που λαμβάνονται και αποστέλλονται. Το CRC χρησιμοποιείται σε διάφορα κομμάτια των δικτύων (σε switches κ.α.) και είναι ένας γενικός κανόνας που συνήθως ακολουθείται για τον έλεγχο του κάθε πακέτου. Περισσότερες πληροφορίες για το CRC, μπορούμε να βρούμε εδώ [https://en.wikipedia.org/wiki/Cyclic_redundancy_check]. Με λίγα λόγια αυτό που κάνει το CRC, είναι ότι με βάση κάποια ψηφία (σε δυαδικό σύστημα), κάνει κάποιες προσθέσεις στο κάθε πακέτο που δέχεται και αν το αποτέλεσμα της εκάστοτε πράξης είναι ίδιο με το αποτέλεσμα που πήρε όταν απέστειλε το πακέτο, τότε το πακέτο αυτό θεωρείται πως δεν έχει αλλοιωθεί και συνεχίζει την πορεία του στο δίκτυο.

Το WPA2 είναι και ο ακόλουθος του WPA. Ένα χρόνο αργότερα μετά από το πρώτο, ξεκίνησε και η διαδικασία πιστοποίησής του (Σεπτέμβριος του 2004) και μετά από δύο (2) σχεδόν χρόνια (Μάρτιος του 2006), το WPA2 επίσημα υποστηρίζεται από κάθε φορητή συσκευή η οποία φέρει το λογότυπο της Wi-Fi Alliance. Με τον ερχομό του το WPA2, έφερε και μία νέα (σχετικά) τεχνολογία διαφορετική από το TKIP, η οποία ονομάζεται AES (Advanced Encryption Standard) η οποία υλοποιήθηκε από το NIST (National Institute of Standards and Technology) των Ηνωμένων Πολιτειών το 2001. Είναι ένας συμμετρικός αλγόριθμος κρυπτογράφησης (symmetric-key algorithm), δηλαδή χρησιμοποιεί το ίδιο κλειδί για την κρυπτογράφηση αλλά και την αποκρυπτογράφηση των δεδομένων. Περισσότερες πληροφορίες για τον AES μπορούμε να βρούμε και εδώ [https://en.wikipedia.org/wiki/Advanced_Encryption_Standard].

Το WPA2 είναι η εφαρμογή του 802.11i-2004 που το 2007 πήρε και την σημερινή του μορφή, με την ονομασία IEEE 802.11-2007. Αυτό που ουσιαστικά γίνεται στο συγκεκριμένο standard είναι ότι οριοθετείται μια χειραψία τεσσάρων (4) βημάτων (four-way handshake) για την έγκριση του οποιουδήποτε κόμβου που θέλει να αποκτήσει πρόσβαση στο ασύρματο δίκτυο. Αυτή η διαδικασία βεβαίως γίνεται μεταξύ του κόμβου/σταθμού (STA) και του Access Point μέσω του οποίου θέλει να αποκτήσει πρόσβαση. Περισσότερες πληροφορίες και πλήρη ανάλυση του συγκεκριμένου προτύπου καθώς και τον τρόπο με τον οποίο υλοποιείται και τις αδυναμίες του, μπορούμε να βρούμε εδώ [https://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=1318903&contentType=Standards&sortType%3Dasc_p_Sequence%26filter%3DAND%28p_Publication_Number%3A9214%29].



Εικ. 3.6 Σετάρισμα του AP με WPA2

Στην παραπάνω εικόνα βλέπουμε το σετάρισμα του AP με WPA2. Επίσης η μέθοδος κρυπτογράφησης είναι η AES, ενώ να σημειωθεί εδώ ότι μπορούσαμε να επιλέξουμε και την TKIP. Το κλειδί που αρχικά θα δοκιμάσουμε για τις επιθέσεις στο συγκεκριμένο AP είναι το "MyPasswordIsStrongRight?" και θα δούμε ότι με τα κατάλληλα εργαλεία, αν και φαίνεται σχετικά δυνατό κλειδί (λόγω μεγέθους, συνδυασμού κεφαλαίων και μικρών χαρακτήρων και ειδικού χαρακτήρα στο τέλος [?]), μπορεί να σπάσει σχετικά εύκολα. Αναφορικά, καλό θα ήταν για κλειδιά να χρησιμοποιούνται μεγάλες προτάσεις, οι οποίες δεν θα περιέχουν εύκολες λέξεις (λέξεις που βρίσκονται σε λεξικά ή που έχουν σχέση με εμάς), να συνδυάζονται κεφαλαία και μικρά γράμματα, να χρησιμοποιούνται ειδικοί χαρακτήρες (%, #, @, *, κτλ) και να περιέχουν και νούμερα. Μία γραφή που θα δούμε ότι μπορεί να έχει αποτέλεσμα (αν χρησιμοποιηθεί σωστά), είναι η ελίτ (Elite ή Leet ή 1337). Στη συγκεκριμένη γραφή, αλλάζουμε γράμματα της αλφαβήτου με αντίστοιχα νούμερα και έτσι δημιουργούμε ένα ακόμη πιο ισχυρό password. Να σημειωθεί εδώ πως η elite γραφή έχει πολλές μεθόδους που μπορεί να χρησιμοποιηθεί και μερικές είναι αρκετά προβλέψιμες. Επίσης θα δούμε πως με ένα απλό εργαλείο και μέσα σε πολύ λίγο χρόνο μπορούμε να παράγουμε λεξικά (txt αρχεία που περιέχουν διάφορες λέξεις), βασιζόμενοι σε κάποιο δικό μας αρχικό λεξικό (συνήθως περιέχει λέξεις κλειδιά που υποθέτουμε ότι μπορεί να χρησιμοποιούνται από το εκάστοτε σύστημα), τα οποία θα έχουν ένα αρκετά μεγάλο μέγεθος και θα συνδιάζουν λέξεις, φράσεις, νούμερα, ειδικούς χαρακτήρες και την ελίτ γραφή.

3.3 Γενική Επισκόπηση Ασφαλείας και Security Policy

Τα βασικά "μοντέλα" ασφαλείας ενός ασύρματου δικτύου είναι αυτά που είδαμε παραπάνω. Γενικά για να στηθεί ένα ασύρματο δίκτυο και να θεωρείται αρκετά ασφαλές, πρέπει να υπάρξει σωστή μελέτη και σωστός σχεδιασμός τόσο σε τεχνικό, όσο και σε ανθρώπινο υπόβαθρο. Αυτό με άλλα λόγια σημαίνει πως εκτός από τους κινδύνους που κρύβονται πίσω από ένα μικρό αλφαριθμητικό που μπορεί να χρησιμοποιείται σαν κλειδί ασφαλείας για την είσοδο ενός τερματικού στο ασύρματο δίκτυο, πρέπει πάντα να υπολογίζεται και ο ανθρώπινος παράγοντας.

Σε γενικές γραμμές ένα καλό στήσιμο, μπορεί να περιλαμβάνει τη μη-εκπομπή του SSID, τη χρήση του ισχυρότερου αλγορίθμου ασφαλείας για το κλείδωμα του ασύρματου δικτύου (WPA2) και πάνω απ' όλα τη σωστή ενημέρωση του προσωπικού για τα θέματα ασφαλείας. Αυτό μπορεί να γίνει και με την συγγραφή ενός "security policy" το οποίο θα αναφέρει ρητά το τι επιτρέπεται και τι απαγορεύεται να κάνει κανείς σε ό,τι αφορά το συνολικό δίκτυο του δήμου. Αν αναλογιστεί κανείς το πόσες φορές μπορεί να έχει βρει σε κάποια υπηρεσία, δήμο, τράπεζα κτλ τους υπαλλήλους να έχουν κολλημένα χαρτάκια με διάφορες πληροφορίες που μπορούν να δώσουν στον οποιοδήποτε τον πλήρη έλεγχο ενός υπολογιστή ή κάποιου μηχανήματος του δικτύου, τότε μπορούμε να καταλάβουμε το μέγεθος του προβλήματος. Δυστυχώς δεν υπάρχει σωστή ενημέρωση γύρω από το θέμα της ασφαλείας και πολλές φορές περνάει στα ψιλά γράμματα. Αυτό βέβαια τις περισσότερες φορές είναι η νούμερο ένα απειλή για το οποιοδήποτε δίκτυο, όσο καλά ασφαλισμένο κι αν είναι σε επίπεδο συσκευών και κωδικών. Όσο καλά και αν κλειδώσεις το σπίτι σου, αν δίνεις όλες τις πληροφορίες στον κλέφτη για το που κρύβεις το κλειδί σου, κάνεις πολύ πιο εύκολη την εισβολή του.

Ένα παράδειγμα για το τι περίπου μπορεί να περιέχει ένα "security policy" το οποίο πρέπει να έχουν διαβάσει **όλοι** όσοι απασχολούνται στο κτήριο του δήμου είναι το ακόλουθο.

Security policy:

- Δεν δίνουμε πουθενά τα στοιχεία του υπολογιστή μας (κωδικοί, διευθύνσεις δικτύου κτλ).
- Δεν κολλάμε αυτοκόλλητα με τα στοιχεία σύνδεσης μας στον υπολογιστή ή σε άλλα σημεία που μπορεί να είναι ορατά προς τρίτους.
- Δεν χρησιμοποιούμε οικείες συσκευές για να συνδεθούμε στο δίκτυο (όπως κινητά τηλ).
- Δεν χρησιμοποιούμε δικά μας switch/router που έχουμε φέρει από το σπίτι κτλ.
- Όταν πληκτρολογούμε τους κωδικούς του συστήματος μας, αποφεύγουμε να το κάνουμε μπροστά σε τρίτους .
- Δεν τρέχουμε λογισμικό από ιστοσελίδες (εκτός της ιστοσελίδας του δήμου μας).
- Σε περίπτωση οποιουδήποτε μηνύματος στον Η/Υ μας, άγνωστο προς εμάς, ενημερώνουμε αμέσως τους διαχειριστές του δικτύου.

• Σε περίπτωση προβλήματος σύνδεσης του υπολογιστή μας στο δίκτυο του δήμου ενημερώνουμε τους διαχειριστές και δεν προσπαθούμε να το λύσουμε μόνοι μας.

• Δεν ανοίγουμε email με "περίεργο" περιεχόμενο ή emails που περιέχουν κάποιο αρχείο εκτός του δήμου ή emails που μας ζητάνε να συμπληρώσουμε πληροφορίες που έχουν να κάνουν με το δήμο, το δίκτυο, τους κωδικούς μας κτλ. Δεν υπάρχει περίπτωση κάποιος από τους διαχειριστές να σας ζητήσει τους κωδικούς σας μέσω email ή οτιδήποτε αντίστοιχο.

• Σε περίπτωση ασυνήθιστης λειτουρίας του υπολογιστή μας, ενημερώνουμε αμέσως του διαχειριστές.

• Αν βρούμε σε οποιοδήποτε σημείο του κτηρίου κάποια συσκευή η οποία δεν ανήκει σε κανέναν ή δεν υπήρχε εκεί, ενημερώνουμε αμέσως του διαχειριστές.

• Δεν χρησιμοποιούμε εκτός των ειδικών χώρων συσκευές που εκπέμπνουν μαγνητική ακτινοβολία όπως ασύρματα τηλέφωνα, φούρνους μικροκυμάτων, συσκευές ενδοεπικοινωνίας κτλ. Οποιαδήποτε τέτοια ή αντίστοιχη συσκευή μπορεί να προκαλέσει σοβαρό πρόβλημα στο δίκτυο του δήμου μας.

• Δεν επιτρέπουμε σε κανένα τρίτο να έχει πρόσβαση σε σημεία του δήμου στα οποία μπορεί να υπάρχουν σημαντικά έγγραφα ή πληροφορίες που αφορούν το δήμο ή το δίκτυο του. Σε περίπτωση που βρούμε κάποιον τρίτο να περιφέρεται σε χώρους του κτηρίου του δήμου, ενημερώνουμε την ασφάλεια του κτηρίου και τους διαχειριστές για να ελεγχτούν οι χώροι. Ο οποιοσδήποτε, μπορεί να αφήσει το οτιδήποτε.

• Δεν επιτρέπουμε σε τρίτους να έχουν την οποιαδήποτε επαφή με του υπολογιστές μας. Υπάρχουν ειδικοί χώροι για πρόσβαση στο Διαδίκτυο σε κάθε όροφο αναμονής των δημοτών μας.

• Σε περίπτωση ξαφνικής απώλειας πρόσβασης στον υπολογιστή μας (μέσω του κωδικού μας) ενημερώνουμε αμέσως τους διαχειριστές.

• Δεν χρησιμοποιούμε συσκευές αποθηκευτικών μέσων όπως εξωτερικούς σκληρούς δίσκους, usb sticks κτλ τα οποία φέραμε από το σπίτι μας ή μας τα έδωσα τρίτοι.

• Αν παρατηρήσουμε κάποια ασυνήθιστη καθυστέρηση στο δίκτυο του δήμου ή στον Η/Υ μας, ενημερώνουμε τους διαχειριστές για να γίνει άμεσως έλεγχος.

Το παραπάνω είναι ένα ενδεικτικό παράδειγμα για το τι μπορεί να περιέχει ένα security policy. Ένα τέτοιο έγγραφο παρεμπιπτόντως, πρέπει να βρίσκεται σε κάθε υπηρεσία, δήμο, εταιρεία κτλ και να διαβάζεται **πάντα** απ' όλους τους υπαλλήλους που εργάζονται σ' αυτή. Βέβαια το εκάστοτε security policy μπορεί να διαφέρει αρκετά. Πρέπει πάντα όμως να δημιουργείται και να στοχεύει σε όλα τα θέματα που μπορούν να δημιουργήσουν τρύπες και κενά ασφαλείας στο δίκτυο.

4. Επιθέσεις και Συγκρίσεις Μοντέλων Ασφαλείας

Υπενθυμίζουμε πως όλες οι επιθέσεις που έγιναν για την ανάγκη αυτή της εργασίας, έγιναν σε τοπικά μηχανήματα. Χρησιμοποιήθηκαν οι ακόλουθες συσκευές και τα εξής προγράμματα:

- 2 φορητοί υπολογιστές, με λειτουργικά συστήματα Linux (Backtrack 5 R3 & Fedora 18) και Windows 7. Οι περισσότερες επιθέσεις έγιναν με χρήση του Backtrack 5.

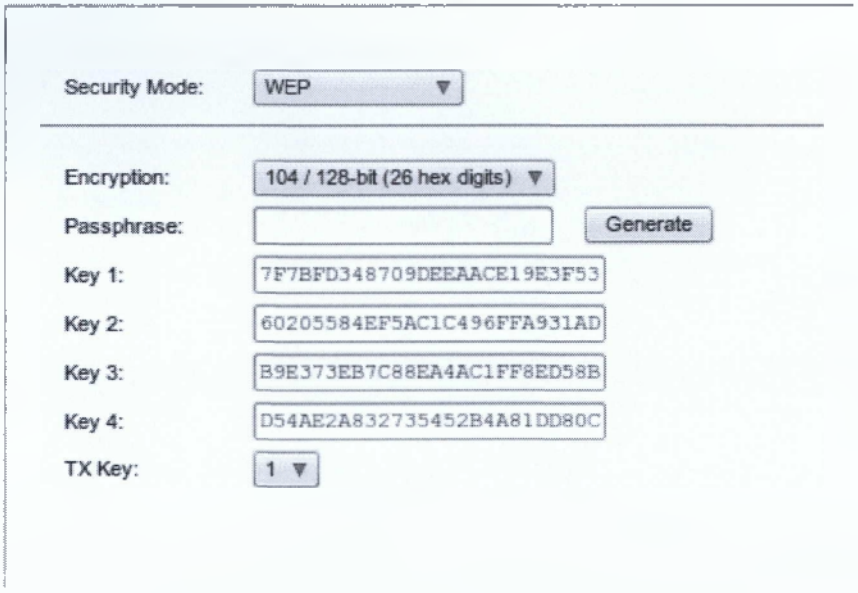
- Ένα modem/router με δυνατότητα ασύρματης επικοινωνίας της Linksys (μοντέλο WAG120N), το οποίο χρησιμοποιήθηκε σαν Access Point για να δοκιμαστούν τα πρωτόκολλα ασφαλείας.

- Τα προγράμματα Cisco Packet Tracer και GNS3 για υλοποίηση μεγαλύτερων τοπολογιών και "σετάρισμα" των μηχανημάτων (routers, switches κτλ).

- Όσα προγράμματα και εργαλεία χρησιμοποιήθηκαν για τις επιθέσεις και την παραγωγή κωδικών αναφέρονται ονομαστικά και είναι όλα ανοιχτού κώδικα (open source).

4.1 Επίθεση σε WEP

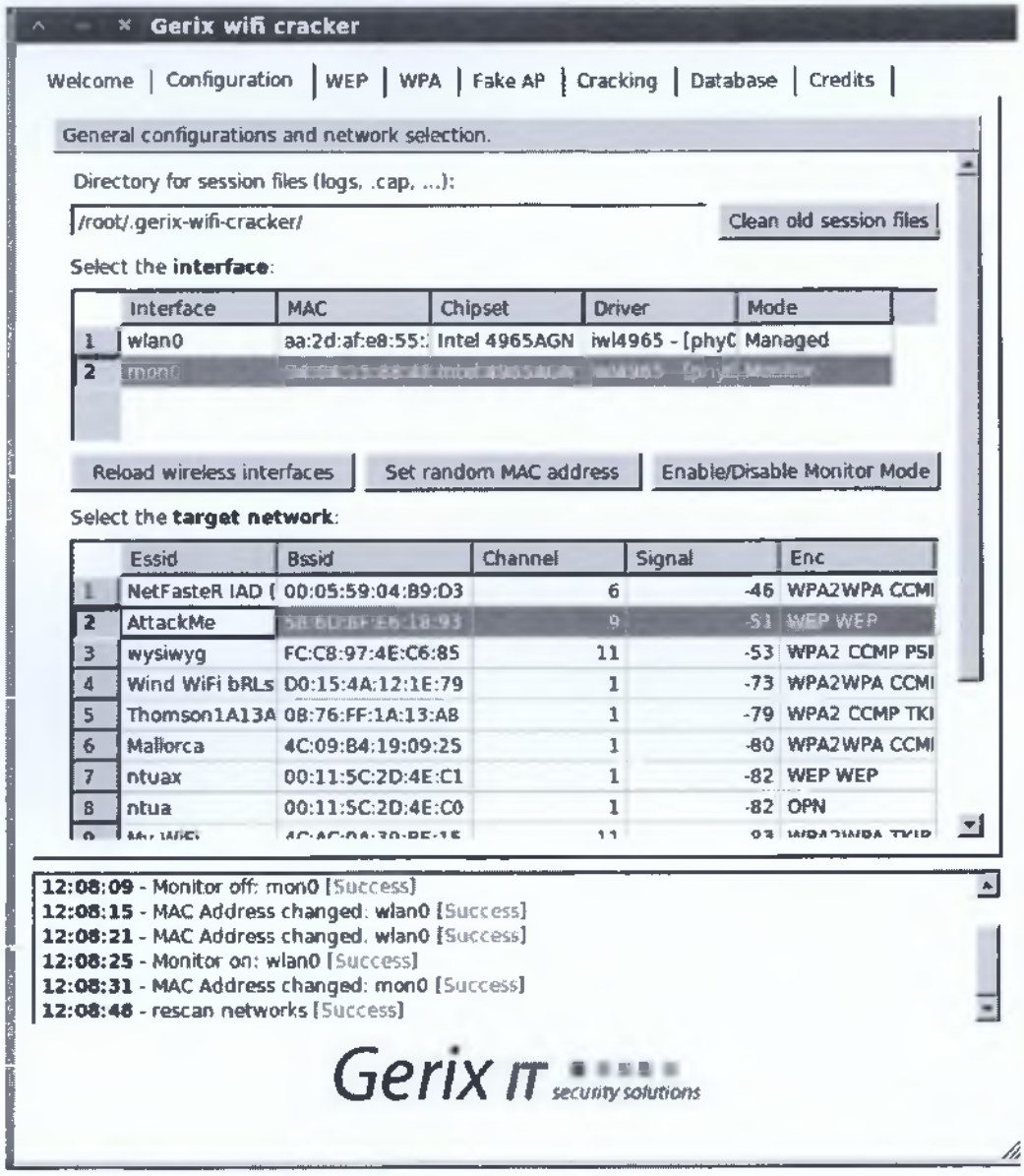
Η πρώτη επίθεση έγινε στο Access Point το οποίο ήταν σεταρισμένο με κρυπτογράφηση WEP. Το σετάρισμα έγινε με τον ίδιο τρόπο που δείξαμε στην εικόνα 3.5 στη σελίδα 24. Τα μηχανήματα της Linksys έχουν τη δυνατότητα να παράγουν τρία (3) "ισχυρά" κλειδιά. Ακολουθεί η διαδικασία μέσω screenshots.



Εικ. 4.1 Σετάρισμα του WEP στο Access Point

Το στήσιμο της ασφαλείας στην προκειμένη περίπτωση έχει να κάνει με το WEP. Χρησιμοποιήθηκε ξανά η αυτόματη παραγωγή τυχαίων αλφαριθμητικών (δεκαεξαδικού τύπου, 0 – 9 & A – F), έτσι ώστε ο επιτιθέμενος να μην μπορεί να μαντέψει το κλειδί. Αν ο επιτιθέμενος ξέρει μερικά πράγματα για εμάς,

όπως, στοιχεία της εταιρείας, ονόματα σημαντικά, ημερομηνίες που αφορούν την εταιρεία ή μέλη της κτλ, τότε με την χρήση ενός απλού μόνου εργαλείου μπορεί να παράγει μέσα σε ελάχιστο χρόνο ένα αρκετά μεγάλο λεξικό, το οποίο αργότερα μπορεί να χρησιμοποιήσει για τις επιθέσεις του. Κάτι τέτοιο θα το δούμε αναλυτικότερα στην επίθεση που θα αναλύσουμε σε ένα WPA2 ασύρματο δίκτυο.



Εικ. 4.2 Σετάρισμα και σκανάρισμα με το Gerix

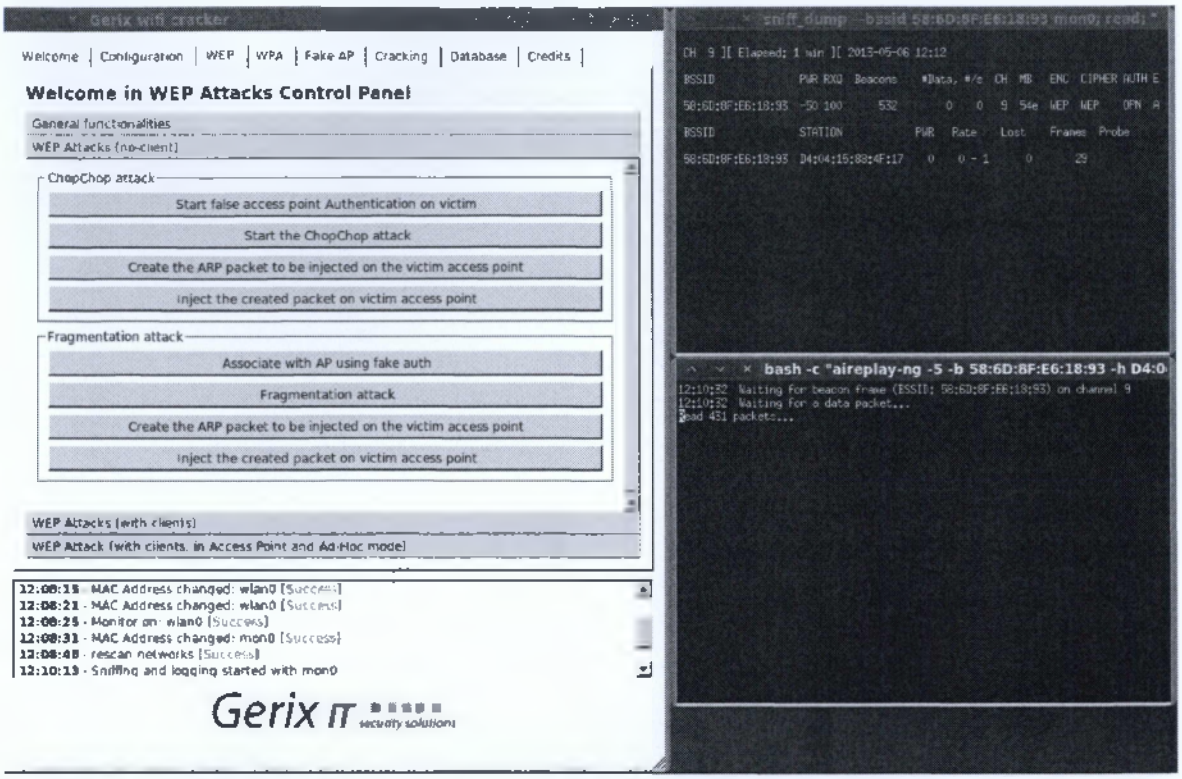
Στην παραπάνω εικόνα (4.2), βλέπουμε το εργαλείο που χρησιμοποιούμε για το scan των δικτύων που εκπέμπουν στο χώρο που έχουμε τοποθετήσει το laptop. Χρησιμοποιήσαμε το συγκεκρίμενο εργαλείο για λόγους ευκολίας. Όλα αυτά μπορούν να επιτευχθούν και μέσω προγραμμάτων κονσόλας, αλλά αυτή η διαδικασία είναι αρκετά πιο αργή για τους περισσότερους χρήστες οι οποίοι δεν είναι

εξοικειωμένοι με αυτό τον τρόπο χρήσης προγραμμάτων. Το Gerix μας προσφέρει όλα όσα μπορούμε να κάνουμε με την χρήση της γνωστής σουίτας εφαρμογών για ξεκλείδωμα δικτύων aircrack-ng. Η βασική τους διαφορά έγκειται στο ότι το ένα χρησιμοποιείται μέσω κονσόλας (aircrack-ng), ενώ το άλλο υποστηρίζεται μέσω γραφικού περιβάλλοντος (Gerix). Ας αναλύσουμε λίγο την παραπάνω εικόνα.

Στην καρτέλα του configuration έχουμε ουσιαστικά τρεις (3) βασικές επιλογές. Πρώτον, τον φάκελο στον οποίο θα αποθηκεύονται τα δεδομένα που θα παραχθούν από τις διάφορες εργασίες μας. Δεύτερον, έχουμε την δυνατότητα επιλογής του interface που θα χρησιμοποιηθεί για το σκανάρισμα των ασύρματων δικτύων και τη δυνατότητα αλλαγής της mac-address της κάρτας δικτύου μας. Αυτό μπορεί να φαίνεται περιττό ή χάσιμο χρόνου, αλλά αν ο επιτιθέμενος θέλει να μειώσει δραστικά τις πιθανότητες του να τον βρουν, τότε αυτό το βήμα είναι αναγκαίο. Άλλωστε, το 99% των συσκευών ενός δικτύου (routers, switches, access points κτλ), κρατάνε κάποιο log αρχείο για όλες τις ενέργειες που επιτελούν στο δίκτυο ή για το ποιος μπήκε, τι IP πήρε και ποια mac-address είχε. Έτσι μέσα από μια μικρή έρευνα μετά το συμβάν της οποιαδήποτε επίθεσης, μπορεί να ανιχνευτούν τέτοια στοιχεία και να βοηθήσουν στην εύρεση του "δράστη". Στην προκειμένη περίπτωση, το laptop που χρησιμοποιήσαμε έχει μόνο μία ασύρματη κάρτα δικτύου (wlan0) και επιλέγοντάς την και στη συνέχεια κλικάροντας στην επιλογή "Set random MAC address", πήραμε ένα νέο interface με την ονομασία mon0, το οποίο ουσιαστικά είναι το ίδιο με αυτό της wlan0, μόνο που έχει φορτωθεί στη μνήμη του υπολογιστή μας με διαφορετική mac-address. Έτσι για οποιαδήποτε δικτυακή κίνηση και για οποιοδήποτε πακέτο μπορεί να παράγει αυτό το interface, σαν source mac-address του αποστολέα (laptop επιτιθέμενου), θα φαίνεται η random mac-address που δημιούργησε το Gerix για εμάς, απλά και μόνο με ένα κλικ(!). Επίσης σε περίπτωση που έχουμε και άλλες κάρτες δικτύου (NICs), τότε με την επιλογή "Reload wireless interfaces" θα μπορέσουμε να τις δούμε στην λίστα. Τρίτη και τελευταία κατάσταση ακρόασης: Ουσιαστικά αυτό που γίνεται είναι να ελέγχει τον αέρα και να συλλέγει μηνύματα από τους πομπούς του εκάστοτε δικτύου. Αφού γίνει αυτή η διαδικασία, τότε βρίσκουμε τα αποτελέσματα των δικτύων που βρέθηκαν στην λίστα όπως φαίνεται και στην εικόνα. Να σημειωθεί εδώ πως όταν χρησιμοποιούμε εφαρμογές όπως το Gerix, το aircrack-ng κτλ, τότε στα αποτελέσματα των ασύρματων δικτύων "στόχων", εμφανίζονται και αυτά τα οποία έχουν απενεργοποιημένο το broadcast SSID. Τόσο απλά, βλέπουμε πως κάτι τέτοιο, δεν δυσκολεύει ιδιαίτερα τη ζωή του επιτιθέμενου. Στην λίστα καναλιών τώρα εμφανίζονται οι εξής πληροφορίες που αφορούν το Access Point:

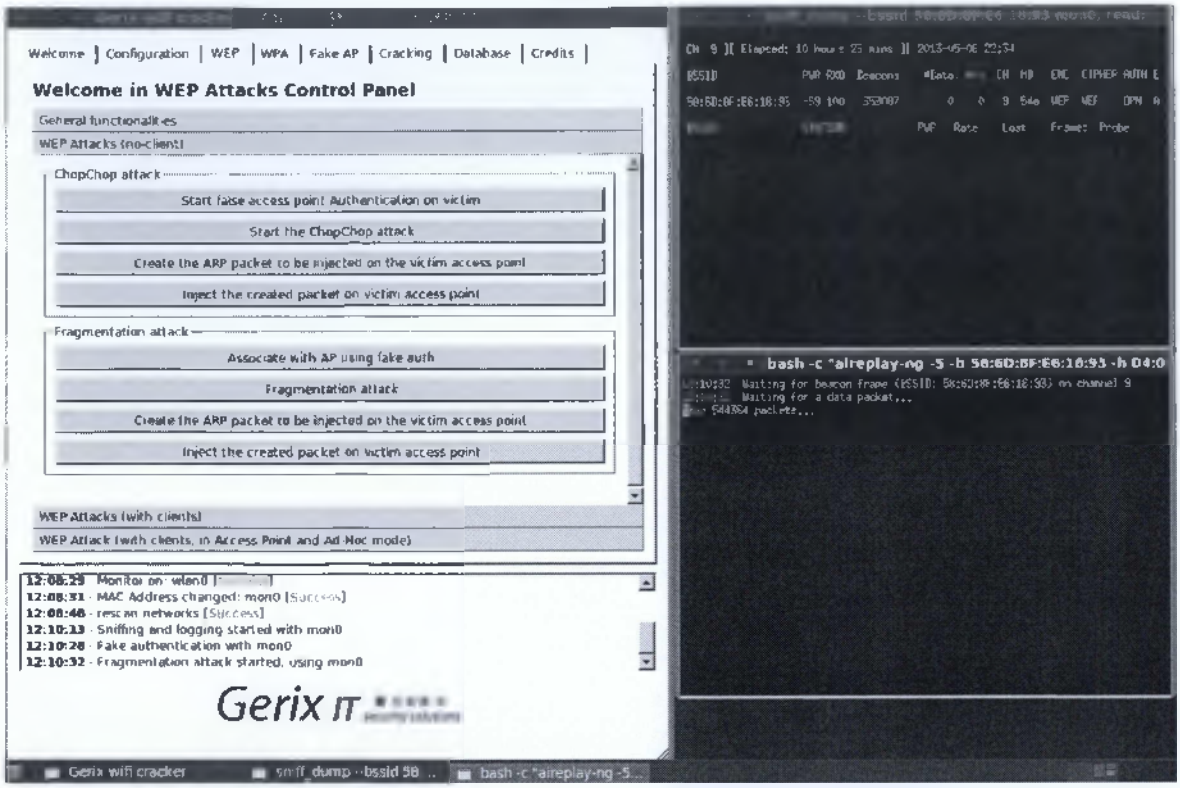
- SSID
- Κανάλι
- Ισχύς σήματος
- MAC address του AP
- Μέθοδος κρυπτογράφησης

Στην εικόνα έχουμε επιλέξει το "προτότυπο" όνομα δικτύου (SSID) "AttackMe" και βλέπουμε πως η mac-address του AP είναι η 58:6d:8f:e6:18:93, το κανάλι που εκπέμπει είναι το ένατο (9), η ισχύς σήματος είναι γύρω στα -51dB και η μέθοδος κρυπτογράφησης της επικοινωνίας γίνεται με την χρήση του WEP. Αφού έχουμε κλικάρει στο δίκτυο που θέλουμε να επιτεθούμε (AttackMe), τότε πηγαίνουμε στο επόμενο tab επιλογών του προγράμματος, ανάλογα με τη μέθοδο κρυπτογράφησης. Στην προκειμένη περίπτωση δηλαδή στο tab που αφορά το WEP.



Εικ. 4.3 Επιλογές του WEP στο Gerix

Σε αυτό το σημείο με λίγα μόνο κλικ, ουσιαστικά δίνουμε εντολή στον υπολογιστή μας να προχωρήσει στην επίθεση για την εύρεση του κλειδιού που μπορούμε να χρησιμοποιήσουμε για να μπούμε στο ασύρματο δίκτυο. Τα δύο είδη επιθέσεων που αναφέρονται και βάσει αυτών προχωράμε στην επίθεσή μας, αυτή την στιγμή δεν μας ενδιαφέρουν άμεσα για ανάλυση. Εδώ όμως ενώ περιμέναμε να γίνει αρκετά γρήγορα και εύκολα (λόγω WEP), το Linksys μας ξεγέλασε. Ας περιγράψουμε όμως λίγο την διαδικασία. Για να μπορέσει να χτυπηθεί ένα ασύρματο δίκτυο, πρέπει πρώτα να γίνει μία συλλογή πακέτων από αυτό. Αυτό γίνεται πολύ απλά. Αφού επιλέξαμε το δίκτυο, επιλέξαμε το "Fragmentation Attack" το οποίο ουσιαστικά συλλέγει οποιοδήποτε πακέτο το οποίο μπορεί να κατευθυνθεί από και προς το AP. Έτσι δημιουργεί μία μεγάλη γκάμα επιλογών για δειγματοληψία και δοκιμές διάφορων κλειδιών, μέχρι την εύρεση του σωστού (κλειδιού). Να σημειωθεί εδώ πως με τον ίδιο υπολογιστή, έγινε η ίδια επίθεση σε ασύρματο δίκτυο το οποίο ήταν σεταρισμένο με τα ίδια κλειδιά ασφαλείας, αλλά σαν AP είχαμε ένα Thomson (speedtouch 716). Σε εκείνη την περίπτωση τα πακέτα που χρειάστηκαν να συλλεχθούν μέχρι να δημιουργηθεί το κατάλληλο πακέτο για το σπάσιμο του κλειδιού ήταν γύρω στα 400 – 550, κάτι που αναλογεί σε χρόνο λιγότερου του ενός (1) λεπτού(!). Στην περίπτωση του Linksys όμως οι χρόνοι αυτοί αλλάζουν δραματικά. Αναλυτικότερα μπορούμε να μελετήσουμε την παρακάτων εικόνα.



Εικ. 4.4 Συλλογή πακέτων μέσω Gerix

Αν παρατηρήσουμε την εικόνα θα δούμε πως έχει φτάσει στα 544384(!) πακέτα και ακόμη δεν μπόρεσε να βρει το σωστό κλειδί για την παραγωγή του κατάλληλου πακέτου που θα αποσταλεί στο AP. Να σημειωθεί εδώ πως τη συγκεκριμένη επίθεση την αφήσαμε για περίπου εφτά (7) ώρες και τελικά το κλειδί δεν μπόρεσε να βρεθεί. Βέβαια αν το δίκτυο που θέλουμε να χτυπήσουμε είναι ενεργό την ώρα του σκαναρίσματος, δηλαδή υπάρχει τουλάχιστον ένας χρήστης στο δίκτυο και το χρησιμοποιεί, τότε μπορούμε να συλλέξουμε ένα μεγάλο αριθμό πακέτων σε πολύ λιγότερο χρόνο από αυτό των εφτά (7) ωρών.

Αυτό που θέλαμε να δείξουμε με την παραπάνω επίθεση και την σύγκρισή της μεταξύ των διαφορετικών συσκευών (Linksys & Thomson), είναι πως ναι μεν τα πρότυπα μπορεί να είναι ίδια και να ακολοθούνται κάποια standards, αλλά αυτό δε, αλλά αυτό δεν μπορεί να σημαίνει πως η κάθε εταιρεία υλοποιεί αυτά τα standards με τον ίδιο τρόπο. Βέβαια ξέρουμε με σιγουριά πως ένα ασύρματο δίκτυο το οποίο βασίζεται στο WEP για την προστασία των δεδομένων του, είναι σίγουρο πως θα σπάσει. Αυτό όμως διαφέρει από εταιρεία σε εταιρεία. Έτσι βλέπουμε ξεκάθαρα πως η Linksys στο συγκεκριμένο τουλάχιστον θέμα έχει κάνει αρκετά καλή δουλειά, αφού στο αντίστοιχο σετάρισμα του Thomson, μπορέσαμε να αποκτήσουμε πρόσβαση σε λιγότερο από δύο (2) λεπτά(!) με τη συλλογή περίπου 500 πακέτων από το δίκτυο, ενώ στην περίπτωση του Linksys, αφήσαμε την κάρτα δικτύου να σκανάρει για περίπου εφτά (7) ολόκληρες ώρες(!) και να συλλέξει παραπάνω από 500000 πακέτα και δεν κατάφερε να παράγει το σωστό πακέτο για το σπάσιμο του ασύρματου δικτύου.

4.2 Επίθεση σε WPA2 και Δημιουργία Λεξικών

Το WPA και το WPA2 όπως έχουμε αναφέρει, υποστηρίζουν πλήρως όλα τα σύμβολα που μπορεί να χρησιμοποιήσει ένας χρήστης. Υπενθυμίζουμε το ότι το WEP υποστηρίζει μόνο χαρακτήρες του δεκαεξαδικού συστήματος μέτρησης, δηλαδή από το 0 μέχρι το 9 και τους χαρακτήρες a έως f (κεφαλαίους και πεζούς).

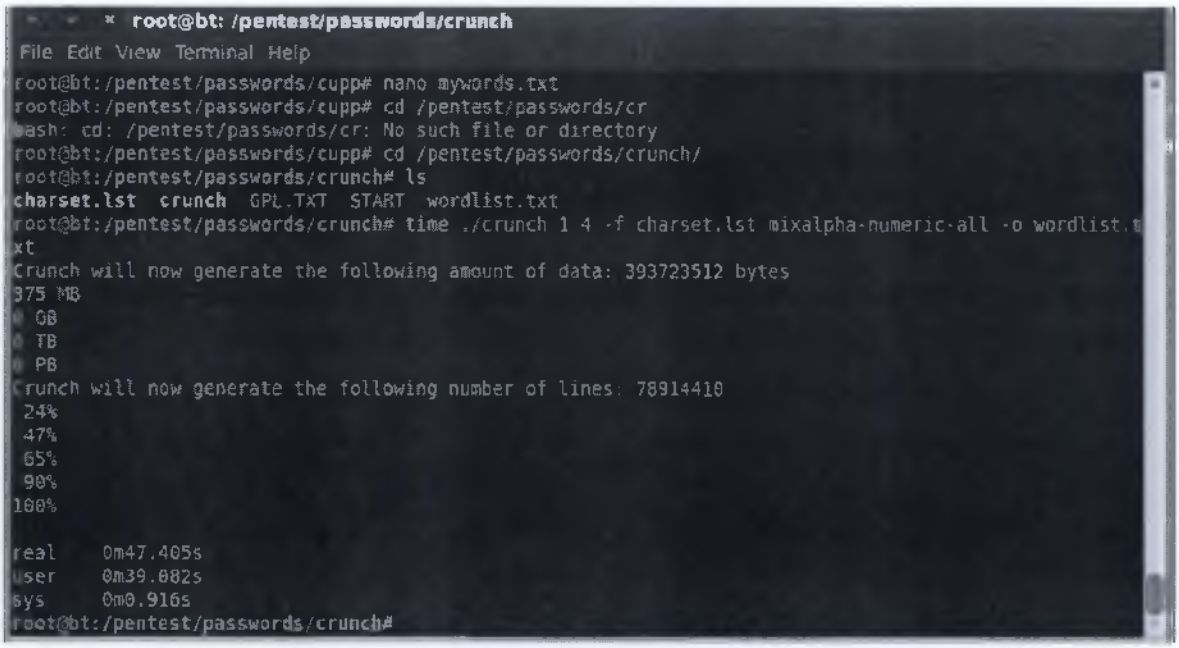
Στο WPA και στο WPA2 λοιπόν ο επιτιθέμενος έχει αρκετά πιο δύσκολο έργο στην εύρεση του σωστού κλειδιού το οποίο θα του δώσει τη δυνατότητα εισχώρησης στο δίκτυο. Πως όμως μπορεί να γίνει κάτι τέτοιο; Θα δούμε παρακάτω δύο εργαλεία open source κώδικα τα οποία βρίσκονται προεγκατεστημένα στην έκδοση Backtrack του λειτουργικού συστήματος Linux. Ας τα εξετάσουμε λίγο πιο αναλυτικά πρώτα.

Το πρώτο εργαλείο είναι το crunch. Το συγκεκριμένο εργαλείο βασίζεται σε ένα αρκετά μικρό αρχείο κειμένου το οποίο διαχωρίζει σε διάφορες κατηγορίες τα αλφαριθμητικά που μπορεί να χρειαστούμε για την παραγωγή κάποιου λεξικού κωδικών. Το αρχείο αυτό είναι το charset.lst και είναι αυτό που φαίνεται παρακάτω.

Εικ. 4.5 Αρχείο charset.lst του εργαλείου crunch

Αν παρατηρήσουμε λίγο το αρχείο βλέπουμε τον διαχωρισμό αυτό. Για παράδειγμα, η λίστα numeric, περιέχει μόνο τα ψηφία του δεκαδικού συστήματος (0 – 9), ενώ η λίστα lalpha, περιέχει όλους τους χαρακτήρες του λατινικού αλφαβήτου, μόνο όμως τους πεζούς (a – z). Για την δημιουργία ενός σύνθετου όμως κωδικού, ο επιτιθέμενος θα χρησιμοποιήσει μία λίστα όπως η mixalpha-numeric-all ή η mix-alpha-numeric-all-space. Η πρώτη περιέχει όλους του χαρακτήρες του λατινικού αλφαβήτου (πεζά και κεφαλαία), όλα τα νούμερα του δεκαδικού (0 – 9) και όλα τα σύμβολα που μπορούν να χρησιμοποιηθούν (!, @, #, $ κ.α.). Η δεύτερη λίστα, περιέχει όλα τα παραπάνω συν του κενού διαστήματος.

Ας δούμε τώρα πως λειτουργεί το crunch και πως μπορούμε βάσει αυτού του αρχείου να δημιουργήσουμε ένα ολόκληρο λεξικό. Η διαδικασία είναι αρκετά απλή και αρκετά γρήγορη για τον άνθρωπο, αλλά μπορεί να είναι αρκετά αργή για τον υπολογιστή (ανάλογα με τη λίστα που θα χρησιμοποιηθεί και το μέγεθος του κωδικού που θέλουμε να δημιουργήσουμε).



Εικ. 4.6 Δημιουργία κωδικών μεγέθους 1 έως 4 χαρακτήρων με το crunch

Στην παραπάνω εικόνα βλέπουμε τη δημιουργία ενώς λεξικού κωδικών με το εργαλείο crunch. Στο συσγκεκριμένο παράδειγμα χρησιμοποιούμε το αρχείο charset.lst με τη λίστα mixalpha-numeric-all και τα αποτελέσματα που θα παραχθούν αποθηκεύονται στο αρχείο wordlist.txt. Επίσης είναι σημαντικό να δούμε πως μπορούμε να ορίσουμε και το μέγεθος των κωδικών που θέλουμε να παράξουμε. Στην προκειμένη περίπτωση έχουμε δώσει την παράμετρο "1 - 4", δηλαδή να παραχθούν λέξεις/φράσεις με μέγεθος από έναν (1) έως τέσσερις (4) χαρακτήρες. Αν για παράδειγμα ο επιτιθέμενος θέλει να παράξει χαρακτήρες μεγέθους ενός αποκλειστικού αριθμού χαρακτήρων, γιατί μπορεί να γνωρίζει ότι η εκάστοτε εταιρεία χρησιμοποιεί τέτοιους κωδικούς ως πολιτική ασφαλείας, τότε σαν παράμετρος θα μπει ο αριθμός αυτός δύο φορές. Για παράδειγμα, αν θέλουμε να παράξουμε κωδικούς αποκλειστικού

μεγέθους δέκα (10) χαρακτήρων, τότε η παράμετρος "1 - 4" που χρησιμοποιήθηκε παραπάνω θα γίνει "10 - 10". Με την παρακάτω εικόνα βλέπουμε πως για την παραγωγή κωδικών οι οποίοι φτάνουν μέχρι τους τέσσερις (4) χαρακτήρες, ο υπολογιστής χρειάστηκε μόλις 47 δεπτερόλεπτα(!) για την παραγωγή τους και το μέγεθος του αρχείου αγγίζει τα 375 MB.

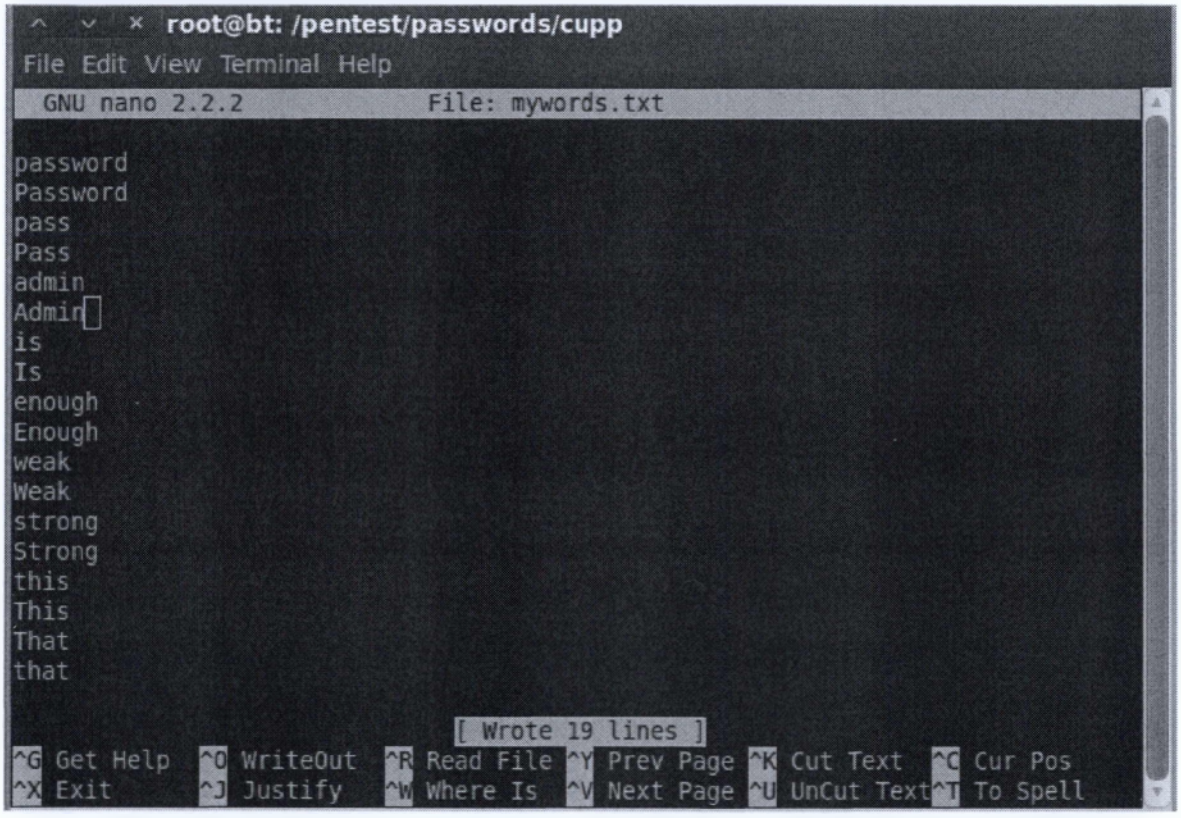
Ένα εργαλείο σαν το crunch είναι αρκετά χρήσιμο και αρκετά εύκολο για τον επιτιθέμενο, αλλά προτιμάται σε περιπτώσεις που ο επιτιθέμενος δεν έχει αρκετά στοιχεία για τον στόχο του. Ας υποθέσουμε ότι για την επιχείρηση που θέλει να επιτεθεί, γνωρίζει μόνο ότι χρησιμοποιεί κωδικούς μεγέθους είκοσι (20) χαρακτήρων σαν πολιτική ασφαλείας. Αν δοκιμάσουμε να φτιάξουμε ένα τέτοιο αρχείο κωδικών (λεξικό), εκτός από τον χρόνο που θα χρειαστεί, το μεγαλύτερο πρόβλημα είναι ο χώρος.

Εικ. 4.7 Δημιουργία λεξικού που περιέχει κωδικούς των 20 χαρακτήρων με το crunch

Όπως βλέπουμε παραπάνω για την δημιουργία αυτού του λεξικού θα χρειαστεί ο επιτιθέμενος να διαθέτει τουλάχιστον 8315 PB(!) ελεύθερου χώρου στον δίσκο του. Κάτι τέτοιο βέβαια είναι αδιανόητο. Επίσης μπορούμε να δούμε και το πλήθος των γραμμών (ένας κωδικός ανά γραμμή), ο οποίος είναι τεράστιος(!).

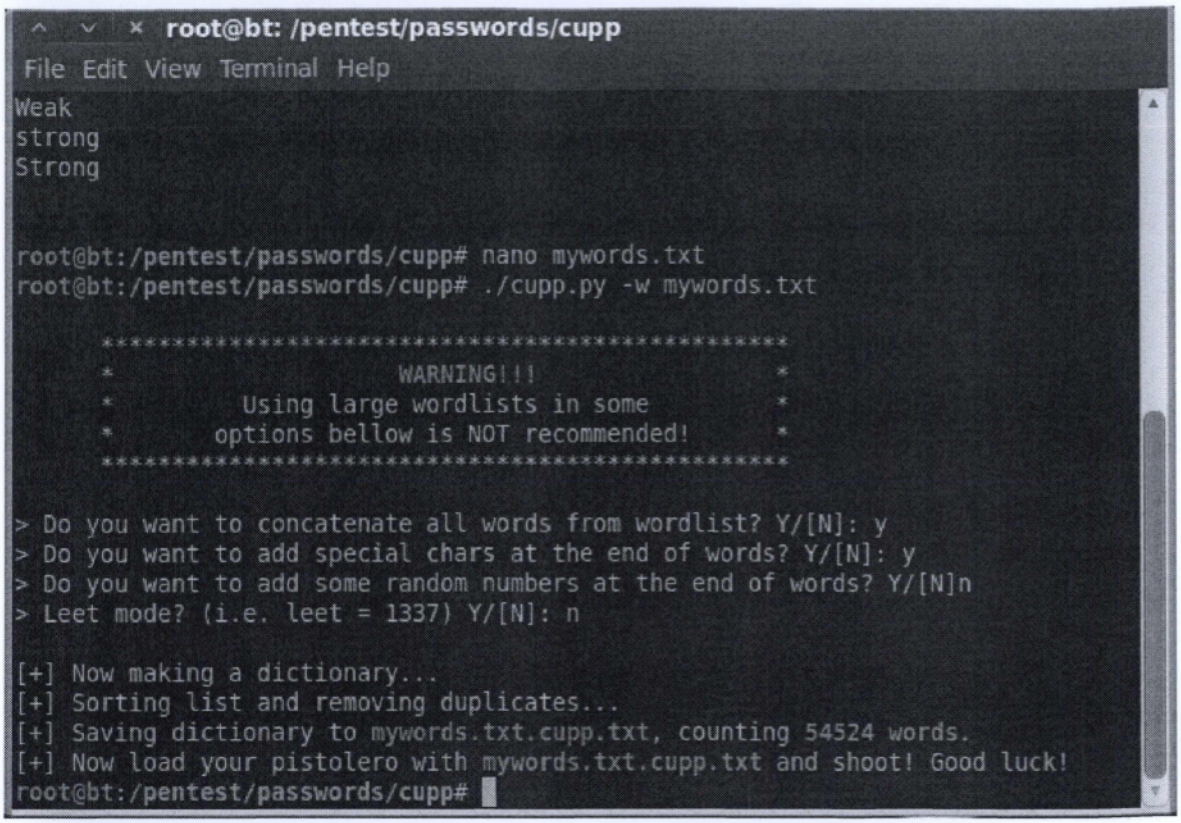
Κυρίως για τους παραπάνω λόγους (χρόνο και χώρο), οι επιθέσεις που αφορούν πρόσβαση σε δίκτυα εταιρειών, ιδιωτών κτλ, ο επιτιθέμενος προσπαθεί να κάνει μία έρευνα για το θύμα. Αυτή η έρευνα γίνεται με μεθόδους social engineering, οι οποίες όμως δεν χρειάζονται να αναλυθούν για τις ανάγκες αυτής της εργασίας. Από την έρευνα αυτή ο επιτιθέμενος προσπαθεί να βρει οποιαδήποτε πληροφορία η οποία μπορεί να φανεί χρήσιμη για την επίτευξη της επίθεσής του. Αυτό που κάνει δηλαδή, είναι να συλλέγει λέξεις κλειδιά, τις οποίες θα χρησιμοποιήσει ως αρχικό λεξικό για την παραγωγή του νέου του λεξικού που θα χρησιμοποιήσει για την επίθεσή του. Αυτό θα γίνει με το εργαλείο cupp.

Από τη στιγμή που ο επιτιθέμενος συλλέξει όσα στοιχεία μπορεί να χρησιμοποιήσει σαν λέξεις κλειδιά για την παραγωγή του λεξικού των κωδικών που θα δοκιμάσει για την επίθεσή του, μπορεί να το κάνει αρκετά απλά, με την χρήση ενός εργαλείου, όπως το cupp. Το cupp προσφέρει τη δυνατότητα στο χρήστη του να φορτώσει ένα αρχείο με λέξεις κλειδιά και αυτό στη συνέχεια (το cupp), να αρχίσει να παράγει κλειδιά με διάφορους συνδυασμούς, βασιζόμενο πάντα στο αρχικό αρχείο που έχει δώσει ο χρήστης.



Εικ. 4.8 Αρχικό αρχείο λεξικού που δημιούργησε ο χρήστης

Στην παραπάνω εικόνα βλέπουμε ένα αρχείο λεξικού που δημιούργησε ο χρήστης βασιζόμενος σε διάφορα στοιχεία που μπόρεσε να συλλέξει από την ερευνά του. Είναι σημαντικό να παρατηρήσουμε πως όλες οι εγγραφές είναι διπλές, αλλάζει μόνο το πρώτο γράμμα (κεφαλαίο ή πεζό), αφού οι κωδικοί πάντα είναι case sensitive, δηλαδή ο κωδικός "Password" είναι διαφορετικός από τον κωδικό "password". Κάπως έτσι ο χρήστης δημιουργεί το αρχικό του λεξικό και το αποθηκεύει σε ένα φάκελο. Στη συνέχεια αναλαμβάνει δράση το cupp. Αυτό το αρχείο που βλέπουμε παραπάνω, είναι το αρχείο που θα φορτωθεί στο cupp και στη συνέχεια θα παραχθούν οι νέοι κωδικοί και θα αποθηκευτούν σε ένα νέο αρχείο.



Εικ. 4.9 Δημιουργία νέου αρχείου κωδικών με χρήση του cupp

Η σύνταξη για την δημιουργία του νέου λεξικού απ' ό,τι βλέπουμε στην παραπάνω εικόνα είναι πολύ απλή. Απλά ο χρήστης καλεί το πρόγραμμα και σαν μοναδική παράμετρο, δίνει το όνομα του αρχείου που έχει δημιουργήσει (το αρχείο δηλαδή της εικόνας 4.7). Στην συγκεκριμένη περίπτωση το αρχείο αυτό το ονομάσαμε mywords.txt. Με το που πληκτρολογήσει αυτή την εντολή στην κονσόλα, το cupp προσφέρει στο χρήστη τέσσερις (4) επιλογές στις οποίες μπορεί να απαντήσει με ένα ναι ή ένα όχι. Οι επιλογές αυτές έχουν να κάνουν με το αν θέλει ο χρήστης να ενωθούν όλες οι λέξεις σε συνδιασμούς για την παραγωγή κωδικών, αν θέλει να προστεθούν ειδικοί χαρακτήρες στο τέλος του κάθε κωδικού, αν θέλει να προστεθούν διάφορα νούμερα (τυχαία) στο τέλος των κωδικών και τέλος αν θέλει να χρησιμοποιηθεί και η ελίτ γραφή. Όλα αυτά θα βασίζονται στις αρχικές λέξεις κλειδιά.

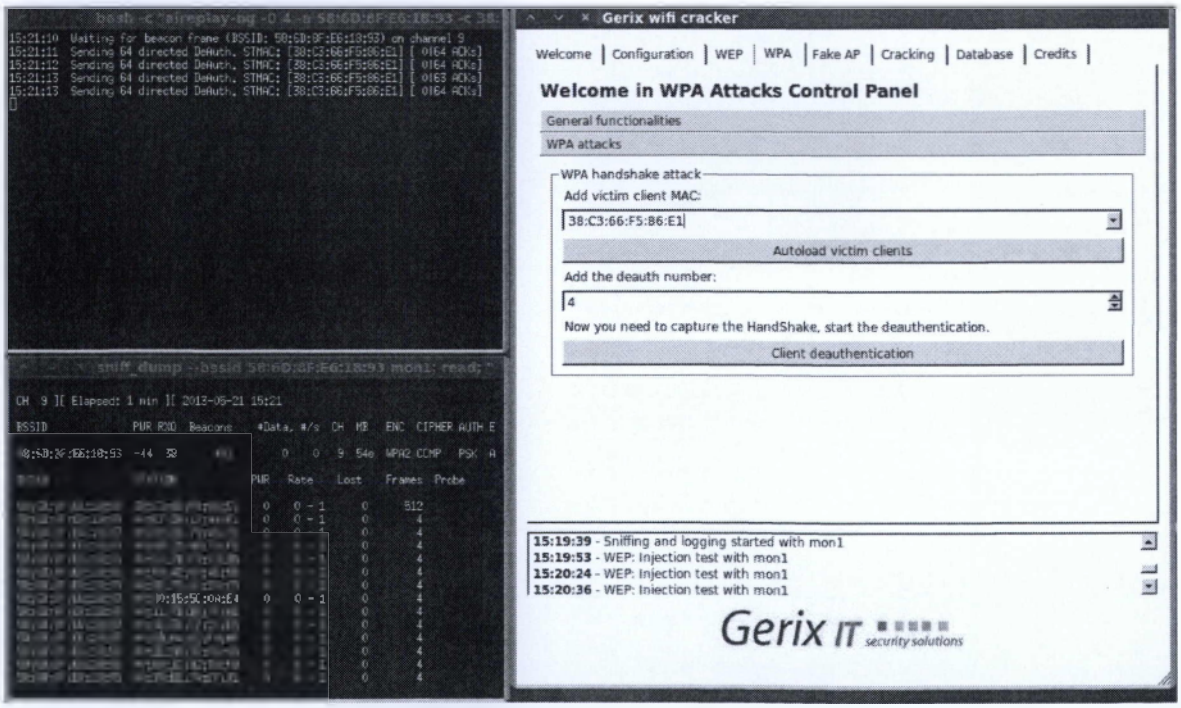
Στο παραπάνω παράδειγμα, απαντήσαμε καταφατικά σε όλες τις ερωτήσεις, εκτός από την πρόσθεση τυχαίων αριθμών στο τέλος των κωδικών. Βλέπουμε πως μόνο με τόσες λίγες λέξεις κλειδιά από το αρχικό μας λεξικό (λιγότερες από είκοσι), το cupp, δημιούργησε 54524(!) νέες λέξεις και τις αποθήκευσε σε ένα txt αρχείο με ονομασία mywords.txt.cupp.txt.

Με πολύ λίγο κόπο και χρόνο βλέπουμε πως η παραγωγή λεξικών αρκετά μεγάλων σε μέγεθος, μπορεί να γίνει σε ελάχιστο χρόνο και με πολύ λίγη πληκτρολόγηση. Το πιο σημαντικό σε αυτό για τον επιτιθέμενο, είναι πως βασίζεται σε γεγονότα και λέξεις που περιγράφουν τον χρήστη/θύμα, και είναι πολύ πιθανό να τις χρησιμοποιεί για κάποιο password.

Οι επιθέσεις μετά από την παραγωγή ενός λεξικού γίνονται αρκετά εύκολα με την χρήση του Gerix (όπως είδαμε και για το WEP) και άλλων εργαλείων όπως το aircrack-ng κτλ. Επίσης μπορούν να χρησιμοποιηθούν και άλλα προγράμματα παραγωγής λεξικών όπως το John the ripper κ.α.

Όλα τα παραπάνω αναφέρονται για να δώσουμε μια αναλυτικότερη εικόνα για την ευκολία παραγωγής κωδικών και τον μέσο χρόνο που χρειάζεται κάτι τέτοιο. Αναφέρουμε για ακόμη μια φορά ότι δυστυχώς η ασφάλεια περνάει στα ψιλά γράμματα στις περισσότερες περιπτώσεις και αυτό δίνει πολλές δυνατότητες εύκολων χτυπημάτων σε διάφορα δίκτυα, υπολογιστές κτλ. Η διαδικασία του χτυπήματος τώρα ενός WPA2 ή ενός WPA δικτύου, σε γενικές γραμμές είναι η ίδια με αυτή που περιγράψαμε και παραπάνω για το WEP. Απλά τώρα η brute force επίθεση βασίζεται στα λεξικά που δημιουργήσαμε και όπως είδαμε δεν είναι κάτι το ιδιαίτερο δύσκολο, ούτε προϋποθέτει κάποιες εξειδικευμένες γνώσεις από τον χρήστη. Το μόνο που χρειάζεται είναι μία διανομή Linux και μερικά downloads προγραμμάτων όπως το cupp και το crunch (αν δεν είναι ήδη προεγκατεστημένα όπως στο Backtrack) και μετά πολύ λίγο χρόνο για την δημιουργία κάποιων λεξικών, αν έχει ήδη συλλέξει τα στοιχεία που θέλει.

Να αναφέρουμε εδώ πως όταν πρόκειται να χτυπηθεί το δίκτυο που θέλουμε, αφού έχει γίνει η εύρεση του κλειδιού που χρειαζόμαστε, το μόνο που κάνει το εκάστοτε πρόγραμμα σπασίματος του δικτύου, είναι ένα deauthenticate των σταθμών που είναι ήδη συνδεδεμένα σ' αυτό, και έτσι γίνεται η επαλήθευση του κλειδιού (στην προσπάθεια επανασύνδεσης των σταθμών).



Εικ. 4.10 Deauthenticate σταθμών με τη χρήση του Gerix

4.3 Αναφορά Ασφαλείας και Δημιουργίας Ισχυρών Κλειδιών

Όπως είδαμε στο κεφάλαιο τέσσερα (4) αναλύσαμε τις βασικές αρχές επίθεσης σε ένα ασύρματο δίκτυο. Για τα δύο (2) χτυπήματα που εξαπολύσαμε χρησιμοποιήσαμε (όπως αναφέραμε και παραπάνω) προγράμματα ανοιχτού κώδικα που μπορούμε να κατεβάσουμε για όλες τις διανομές του Linux και μερικά από αυτά μπορούμε να τα βρούμε και στο λειτουργικό σύστημα των Windows.

Στη μία επίθεση είχαμε σαν στόχο ένα Access Point το οποίο ήταν κλειδωμένο με προστασία WEP. Η διαδικασία σπασίματος του δικτύου ήταν πολύ απλή και αρκετά γρήγορη. Σε σύγκριση που έγινε επίσης, είδαμε πως το AP της εταιρείας Linksys, άντεξε πολύ περισσότερο χρόνο σε σχέση με αυτό της εταιρείας Thomson.

Στη δεύτερη επίθεση, είχαμε σαν στόχο το ίδιο Access Point, μόνο που στην προκειμένη περίπτωση ήταν σεταρισμένο με προστασία WPA2. Εδώ είδαμε και τους δύο τρόπους παραγωγής λεξικών για επιθέσεις brute force. Σε περίπτωση που ο επιτιθέμενος έχει κάνει μία έρευνα γύρω από το θύμα και γνωρίζει μερικά στοιχεία γι' αυτό (το θύμα), τότε χρησιμοποιεί εργαλεία στα οποία φορτώνει το αρχικό λεξικό το οποίο περιέχει μερικές λέξεις κλειδιά και τότε παράγεται το τελικό λεξικό από τα εργαλεία αυτά τα οποία προσφέρουν μια πληθώρα επιλογών για την δημιουργία του τελικού αυτού αρχείου. Σε περίπτωση που ο επιτιθέμενος δεν γνωρίζει κάποιο στοιχείο το οποίο να μπορεί να χρησιμοποιήσει για την παραγωγή λέξεων κλειδιών, τότε υπάρχουν αρκετά εργαλεία που τον βοηθούν να παράγει ένα μεγάλο ή μικρό λεξικό (ανάλογα με τις ανάγκες του) για την επίτευξη της επίθεσης.

Οι δύο παραπάνω μέθοδοι χρησιμοποιούνται κατά κόρον για την γρήγορη δημιουργία λεξικών. Όμως στην δεύτερη περίπτωση (δημιουργία λεξικού χωρίς λέξεις κλειδιά), υπάρχουν δύο βασικά μειονεκτήματα. Χρόνος και χώρος. Αν πάλι μπορέσει ο επιτιθέμενος να αποκτήσει μερικά Gigabyte στον δίσκο του, και πάλι δεν θα μπορέσει να καλύψει ένα αρκετά μεγάλο αριθμό λέξεων για την παραγωγή του κλειδιού. Έτσι, αν το θύμα γνωρίζει ότι οποιαδήποτε στιγμή μπορεί να δεχτεί επίθεση στο δίκτυο του, τότε προσπαθεί να δημιουργήσει ένα αρκετά ισχυρό κωδικό. Πώς γίνεται όμως αυτό;

Για την δημιουργία ενός αρκετά ισχυρού κωδικού ο οποίος θα μας δίνει περισσότερες πιθανότητες στο να μην υπάρξει πρόσβαση στο δίκτυο μας, πρέπει να λάβουμε σοβαρά υπόψι τα παρακάτω:

- Ο κωδικός πρέπει να έχει μεγάλο μέγεθος. Όσο μεγαλύτερος σε μέγεθος, τόσο το καλύτερο. Ιδανικοί κωδικοί θεωρούνται αυτοί που αποτελούνται από τουλάχιστον είκοσι (20) χαρακτήρες.

- Καλό είναι οι λέξεις που απαρτίζουν τον κωδικό να μην ξεκινάνε με κεφαλαίους χαρακτήρες, αλλά αν περιέχουν τέτοιους, να τους βάλουμε σε διάφορα σημεία των λέξεων.

- Ο κωδικός μας δεν πρέπει σε καμία περίπτωση να αποτελείται από λέξεις που μπορούν να υπάρχουν σε λεξικά, έτσι ώστε να γίνει ακόμη πιο δύσκολος ο εντοπισμός του.

- Ο κωδικός δεν πρέπει να περιέχει στοιχεία στις λέξεις του που να αφορούν εμάς, την εταιρεία μας ή υπαλλήλους αυτής.

• Σημαντικό είναι ο κωδικός μας να αποτελείται από χαρακτήρες πεζούς και κεφαλαίους, σύμβολα και αριθμούς. Επίσης, προτείνεται και η ελίτ γραφή.

Ένα παράδειγμα ενός ισχυρού κωδικού για τον δήμο μας, θα μπορούσε να είναι το εξής:

"th1$p4SsW0rD!5f0rp3R50N4LU53=!%"

Στο παραπάνω κλειδί, μπορεί οι λέξεις που χρησιμοποιήσαμε να είναι συνηθισμένες, αλλά έχουν γραφτεί και με ελίτ γραφή και χρησιμοποιούν πεζά και κεφαλαία και επίσης περιέχουν διάφορους ειδικούς χαρακτήρες. Επίσης, το συγκεκριμένο κλειδί, αποτελείται από τριάντα έναν (31) χαρακτήρες, κάτι που από μόνο του, το κάνει αρκετά ισχυρό. Η πρόταση που έχει γραφτεί παραπάνω και αποτελεί το κλειδί για την πρόσβασή μας στο ασύρματο δίκτυο είναι η «**This password is for personal use**». Κάτι τέτοιο βέβαια είναι αρκετά απλό σε απλή γραφή, αλλά με λίγους συνδυασμούς και λίγη φαντασία, μπορεί να γίνει αρκετά περίπλοκο.

Με αυτό το κεφάλαιο καλύψαμε τα βασικά της ασφάλειας σε ένα ασύρματο δίκτυο και δείξαμε με λίγες λεπτομέρειες τις επιθέσεις και τα αντίμετρα που μπορούμε να πάρουμε. Για περαιτέρω πληροφορίες σχετικά με την ασφάλεια στα ασύρματα δίκτυα, τις επιθέσεις που μπορούν να δεχτούν και τους τρόπους άμυνας ενάντια σ' αυτές, μπορείτε να ανατρέξετε και στην πτυχιακή εργασία των συναδέλφων Κουρμπέλη Αθανάσιου και του Ψωρομύτη Γεώργιου η οποία εκπονήθηκε κατά το έτος 2012 και καλύπτει διάφορα θέματα ασφαλείας των ασύρματων δικτύων.

5. Μελέτη Χώρου και Διαχωρισμός Υποδικτύων

5.1 Μελέτη Χώρου και Διαμοιρασμός Δικτυακών Συσκευών

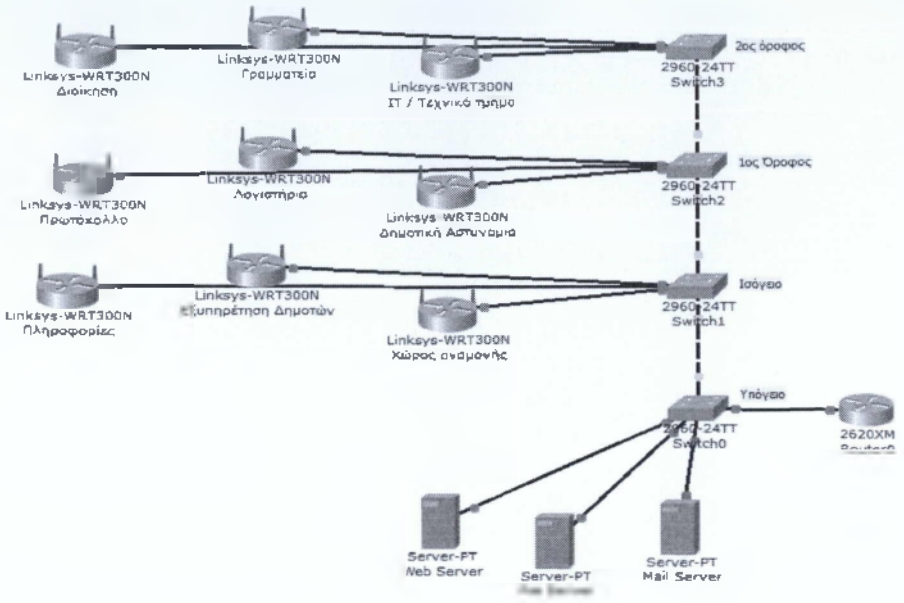
Το κτήριο του δήμου αποτελείται από τέσσερις (4) ορόφους. Πιο αναλυτικά, από το υπόγειο, το ισόγειο, τον πρώτο και το δεύτερο όροφο. Στο υπόγειο βρίσκεται ένα Switch το οποίο αποτελείται από πέντε (5) συνδέσεις. Στις τρεις (3) πρώτες θύρες του, συνδέονται οι τρεις (3) εξυπηρετητές του δικτύου του δήμου, δηλαδή ο File Server, ο Mail Server και ο Web Server, στην τελευταία θύρα του συνδέεται ο μοναδικός δρομολογητής (router) του δικτύου (στην θύρα fa0/24 συγκεκριμένα) και στην Gigabit θύρα του συνδέεται με το switch που βρίσκεται στο ισόγειο του κτηρίου.

Στο ισόγειο του κτηρίου βρίσκουμε το switch του ορόφου που αυτό με τη σειρά του συνδέεται με πέντα (5) συσκευές. Οι δύο Gigabit θύρες του ενώνονται με τους δύο ορόφους που γειτονεύει (με το υπόγειο και τον πρώτο όροφο) και οι πρώτες τρεις (3) θύρες του συνδέονται με τα τρία (3) Access Points που βρίσκονται στο ισόγειο. Το ένα AP εξυπηρετεί τις ανάγκες του τμήματος Πληροφοριών του δήμου (συνδέεται στη θύρα fa0/1 του switch), το δεύτερο εξυπηρετεί τις ανάγκες της Εξυπηρέτησης Δημοτών του δήμου (συνδέεται στη θύρα fa0/2 του switch) και το τρίτο βρίσκεται στο χώρο Αναμονής των Δημοτών (συνδέεται στη θύρα fa0/3 του switch) και δίνει τη δυνατότητα ελεύθερης πλοήγησης στο Internet για τους δημότες που βρίσκονται σε αναμονή μέχρι να εξυπηρετηθούν από τον αρμόδιο υπάλληλο του δήμου.

Στο πρώτο όροφο του δήμου συναντάμε πάλι ένα κεντρικό switch που και αυτό με την σειρά του συνδέεται με πέντε (5) άλλες συσκευές. Οι δύο είναι τα switches των γειτονικών ορόφων (ισογείου και δεύτερου ορόφου) και συνδέονται στις δύο (2) Gigabit θύρες του switch. Οι πρώτες τρεις (3) θύρες του switch του πρώτου ορόφου συνδέονται με τρία (3) Access Points που βρίσκονται στον ίδιο όροφο. Το πρώτο AP (συνδέεται στη θύρα fa0/1 του switch), εξυπηρετεί το τμήμα Πρωτοκόλλου του δήμου, το δεύτερο AP (συνδέεται στη θύρα fa0/2 του switch), εξυπηρετεί τις ανάγκες του τμήματος του Λογιστηρίου και το τρίτο και τελευταίο AP (συνδέεται στη θύρα fa0/3 του switch) και εξυπηρετεί τις ανάγκες της Δημοτικής Αστυνομίας που έχει το κεντρικό της γραφείο σ' αυτό τον όροφο του κτηρίου του δήμου.

Στο δεύτερο όροφο του κτηρίου στήνουμε άλλο ένα switch το οποίο συνδέεται με τέσσερις (4) διαδικτυακές συσκευές. Έχει μία σύνδεση σε θύρα Gigabit η οποία συνδέεται με το switch του πρώτου ορόφου. Οι πρώτες τρεις (3) θύρες συνδέονται με τα τρία Access Points που υπάρχουν και σ' αυτό τον όροφο. Το πρώτο AP συνδέεται στη θύρα fa0/1 του switch και εξυπηρετεί τις ανάγκες της Διοίκησης του δήμου. Το δεύτερο AP συνδέεται στη θύρα fa0/2 του switch και εξυπηρετεί τις ανάγκες της γραμματείας του δήμου. Το τρίτο και τελευταίο AP συνδέεται στη θύρα fa0/3 του switch και εξυπηρετεί τις ανάγκες του IT του κτηρίου του δήμου.

Η βασική τοπολογία των συσκευών δικτύου που θα στηθούν στο δήμο είναι αυτή που περιγράφτηκε παραπάνω. Σ' αυτό το σημείο πλέον, μας ενδιαφέρει και η υποδικτύωση του δικτύου, το λεγόμενο subnetting. Για να προχωρήσουμε στην διαδικασία αυτή πρέπει πρώτα να δούμε και τις ανάγκες για διευθύνσεις IP του εκάστοτε τμήματος, για να γίνει το σωστό subnetting και να διαχωριστούν τα VLAN του δικτύου βάσει αυτού.



Εικ. 5.1 Διάταξη διαδικτυακών συσκευών στο κτήριο του δήμου ανά όροφο

5.2 Subnetting και VLSM

Για τη σωστή υποδικτύωση, πρέπει να λάβουμε υπόψι τις ανάγκες διευθυνσιοδότησης του εκάστοτε τμήματος του δήμου, όπως αναφέραμε και πιο πάνω.

Οι ανάγκες ανά τμήμα φαίνονται στον ακόλουθο πίνακα.

Τμήμα Δήμου	**Ανάγκες για διευθύνσεις IP**
Διοίκηση	10
Γραμματεία	15
IT / Τεχνικό τμήμα	20
Πρωτόκολλο	5
Λογιστήριο	10
Δημοτική Αστυνομία	25
Πληροφορίες	3
Εξυπηρέτηση Δημοτών	20
Servers	3
Zero Subnet	62

Τον παραπάνω πίνακα τον πήραμε αφού υπολογίσαμε τις ανάγκες διευθυνσιοδότησης για τις συσκευές δικτύου που θα βρίσκονται στο δίκτυο του δήμου. Οι συσκευές αυτές είναι οι υπολογιστές, τα laptops, οι εκτυπωτές (δικτυακοί) κτλ. Όλες οι συσκευές δηλαδή που βρίσκονται σε ένα δίκτυο και για την επικοινωνία τους χρειάζονται μία IP διεύθυνση.

Λόγω των διαφορετικών αναγκών ανά τμήμα σε διευθύνσεις, δεν θα χωρίσουμε τα υποδίκτυα βάσει του κλασικού subnetting, αλλά θα χρησιμοποιήσουμε την τεχνική του VLSM (Variable Length Subnet Mask). Ακολουθούμε αυτή την τεχνική γιατί το κλασικό subnetting χωρίζει σε ισομερή κομμάτια το δίκτυο, ανάλογα με το πόσα υποδίκτυα θέλουμε. Στο VLSM όμως, μπορούμε να χωρίσουμε το κάθε υποδίκτυο βάσει των αναγκών που έχουμε και έτσι στην περίπτωση του συγκεκριμένου δήμου, που οι ανάγκες για το κάθε υποδίκτυο είναι διαφορετικές (όσον αφορά στις διευθύνσεις), η ανάγκη χρήσης του VLSM, για τον σωστότερο διαχωρισμό του δικτύου, είναι επιτακτική. Για τον διαχωρισμό του δικτύου βάσει του VLSM, θα χρησιμοποιήσουμε την αρχική διεύθυνση δικτύου **10.10.10.0** με Subnet Mask **/24**. Στη διαδικασία χωρισμού των υποδικτύων με την τεχνική του VLSM, χωρίζουμε τα υποδίκτυα βάσει του πλήθους των IP που χρειάζονται και ξεκινάμε να "σπάμε" το δίκτυο αρχίζοντας από το υποδίκτυο με το μεγαλύτερο αριθμό IP. Στη συνέχεια συνεχίζουμε το σπάσιμο του δικτύου με το αμέσως μικρότερο και ούτω καθ' εξής. Δηλαδή σε καθαρά νούμερα, αν χρειαζόμαστε πέντε (5) υποδίκτυα με ανάγκες για IP, 20, 40, 20, 45, τότε ο υπολογισμός των υποδικτύων θα γίνει με την ακόλουθη σειρά: 45, 40, 20, 20.

Το subnetting και το VLSM κατ' επέκταση, βασίζονται σ' ένα απλό πίνακα που περιέχει τις δυνάμεις του 2 υψωμένες από το 0 μέχρι και το 7. Αυτό οφείλεται στο ότι θέλουμε για μεγαλύτερη ευκολία να μετατρέψουμε τα νούμερα του δυαδικού (εξού και το 2) σε δεκαδικό σύστημα για γρηγορότερη επίλυση του προβλήματός μας. Ο πίνακας αυτός, είναι ο ακόλουθος:

128 (2^7)	64 (2^6)	32 (2^5)	16 (2^4)	8 (2^3)	4 (2^2)	2 (2^1)	1 (2^0)

Η μεγαλύτερη ανάλυση για την επίτευξη του subnetting ή του VLSM δεν είναι αναγκαίο να καλυφθεί σ' αυτή την εργασία και μπορούμε να βρούμε αρκετές πληροφορίες γι' αυτά σε διάφορους διαδικτυακούς τόπους όπως στην ακόλουθη διεύθυνση που δίνεται μία αρκετά καλή περιγραφή γι' αυτό [http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a00800a67f5.shtml].

VLSM

10.10.10.0 /24

ΤΜΗΜΑ (ΑΝΑΓΚΗ IPs)	ΥΠΟΔΙΚΤΥΟ / ΜΑΣΚΑ	ΕΥΡΟΣ IPs ΥΠΟΔΙΚΤΥΟΥ	BROADCAST IP
Zero Subnet (1 - 62)	10.10.10.0 /26	10.10.10.1 - 10.10.10.62	10.10.10.63
Δημοτική Αστ. (25)	10.10.10.64 /27	10.10.10.65 - 10.10.10.94	10.10.10.95
Εξυπηρέτηση Δημ. (20)	10.10.10.96 /27	10.10.10.97 - 10.10.10.126	10.10.10.127
IT (20)	10.10.10.128 /27	10.10.10.129 - 10.10.10.158	10.10.10.159
Γραμματεία (15)	10.10.10.160 /27	10.10.10.161 - 10.10.10.190	10.10.10.191
Διοίκηση (10)	10.10.10.192 /28	10.10.10.193 - 10.10.10.206	10.10.10.207
Λογιστήριο (10)	10.10.10.208 /28	10.10.10.209 - 10.10.10.222	10.10.10.223
Πρωτόκολλο (5)	10.10.10.224 /29	10.10.10.225 - 10.10.10.230	10.10.10.231
Πληροφορίες (3)	10.10.10.232 /29	10.10.10.233 - 10.10.10.238	10.10.10.239
Servers (3)	10.10.10.240 /29	10.10.10.241 - 10.10.10.246	10.10.10.247

Βάσει του παραπάνω πίνακα βλέπουμε ότι μέσω της τεχνικής του VLSM, καλύψαμε τις ανάγκες μας για την κάλυψη των διευθύνσεων IP που θα χρειαστούμε για το δίκτυο μας και για το κάθε υποδίκτυο που αυτό αποτελείται. Να σημειωθεί εδώ, πως από την διεύθυνση 10.10.10.248 μέχρι και την 10.10.10.255, όλες αυτές είναι διαθέσιμες για οποιοδήποτε σκοπό τις χρειαστούμε για μελλοντική χρήση. Επίσης εκτός από αυτές τις IP που βρίσκονται στο τέλος, δημιουργήσαμε και ένα ακόμη υποδίκτυο, το επονομαζόμενο Zero Subnet, το οποίο μπορεί να καλύψει ανάγκες διευθυνσιοδότησης που φτάνουν μέχρι και τις 62 IP. Αυτό έγινε ώστε σε περίπτωση κάποιας αλλαγής ή προσθήκης στα υποδίκτυα, να μην χρειάζεται νέα μελέτη βάσει VLSM.

Βέβαια οι ανάγκες, και βάσει αυτής της τεχνικής, δεν καλύπτουν ακριβώς τα νούμερα που θέλουμε, π.χ. στο υποδίκτυο της Γραμματείας, που χρειαζόμαστε 25 IP διευθύνσεις, παίρνουμε το βήμα 32 (2^5 = 32) και αφαιρούμε από αυτό δύο (2) γιατί αυτές οι 2 IPs χρησιμοποιούνται για το Subnet ID και για την Broadcast IP. Έτσι για οποιοδήποτε νούμερο IP θέλουμε να υπολογίσουμε, βασιζόμαστε στον τύπο **"n^2 – 2"** και βρίσκουμε ποιο νούμερο πέφτει πιο κοντά στις ανάγκες μας. Μια καλή τεχνική είναι και σε περιπτώσεις που το νούμερο που θέλουμε από IPs, να συμπίπτει ακριβώς με το νούμερο που θα βρούμε από τον παραπάνω τύπο, να παίρνουμε το αμέσως επόμενο. Έτσι μπορεί ναι μεν να έχουμε μερικές μικρές απώλειες από μη χρησιμοποιούμενες IPs, αλλά σε περίπτωση επέκτασης του εκάστοτε υποδικτύου, δεν θα χρειαστεί να κάνουμε μελέτη VLSM από την αρχή.

Σε αυτή την περίπτωση είχαμε την ανάγκη για 111 IP διευθύνσεις, σε ένα block 254 διευθύνσεων και μετά το VLSM, έχουμε ακόμη 143 ελεύθερες διευθύνσεις. Αυτό σημαίνει πως χρησιμοποιούμε περίπου το 54% από τις διαθέσιμες IP που έχουμε (254 στο σύνολο, 111 χρησιμοποιούνται). Σε περίπτωση υλοποίησης του κλασικού subnetting, τότε θα θεωρούσαμε ότι ο μέγιστος αριθμός από IP που χρειαζόμαστε είναι το νούμερο 25 και έτσι θα έπρεπε το κάθε υποδίκτυο να έχει βήμα 32, δηλαδή να ήταν με μάσκα υποδικτύου /27. Αυτό σημαίνει μεγάλη σπατάλη από IP και επίσης ότι ένα μόνο block από τα τέσσερα (4) μίας IP διεύθυνσης, θα μας έφτανε και πάλι για να καλύψουμε τις ανάγκες μας, αλλά θα είχαμε μεγάλη σπατάλη από διευθύνσεις που δεν χρησιμοποιούνται. Αυτό βέβαια γιατί στην περίπτωση μας τα περισσότερα υποδίκτυα έχουν άλλες ανάγκες σε διαθέσιμες IP από τα άλλα. Αν οι ανάγκες του κάθε υποδικτύου είναι κοντά στις ανάγκες των άλλων, τότε θα μπορούσαμε να υλοποιήσουμε την υποδικτύωση με την χρήση της μεθόδου του κλασικού subnetting.

5.3 Διαχωρισμός VLAN

Τα VLAN (Virtual Local Area Network ή Virtual LAN) μας βοηθούν και στην υποδικτύωση. Είναι ένα εργαλείο που υποστηρίζεται από τα περισσότερα switch μίας μεγάλης γκάμας εταιρειών παρασκευής διαδικτυακών συσκευών και ο τρόπος υλοποιήσής τους είναι αρκετά όμοιος. Τι είναι όμως το VLAN;

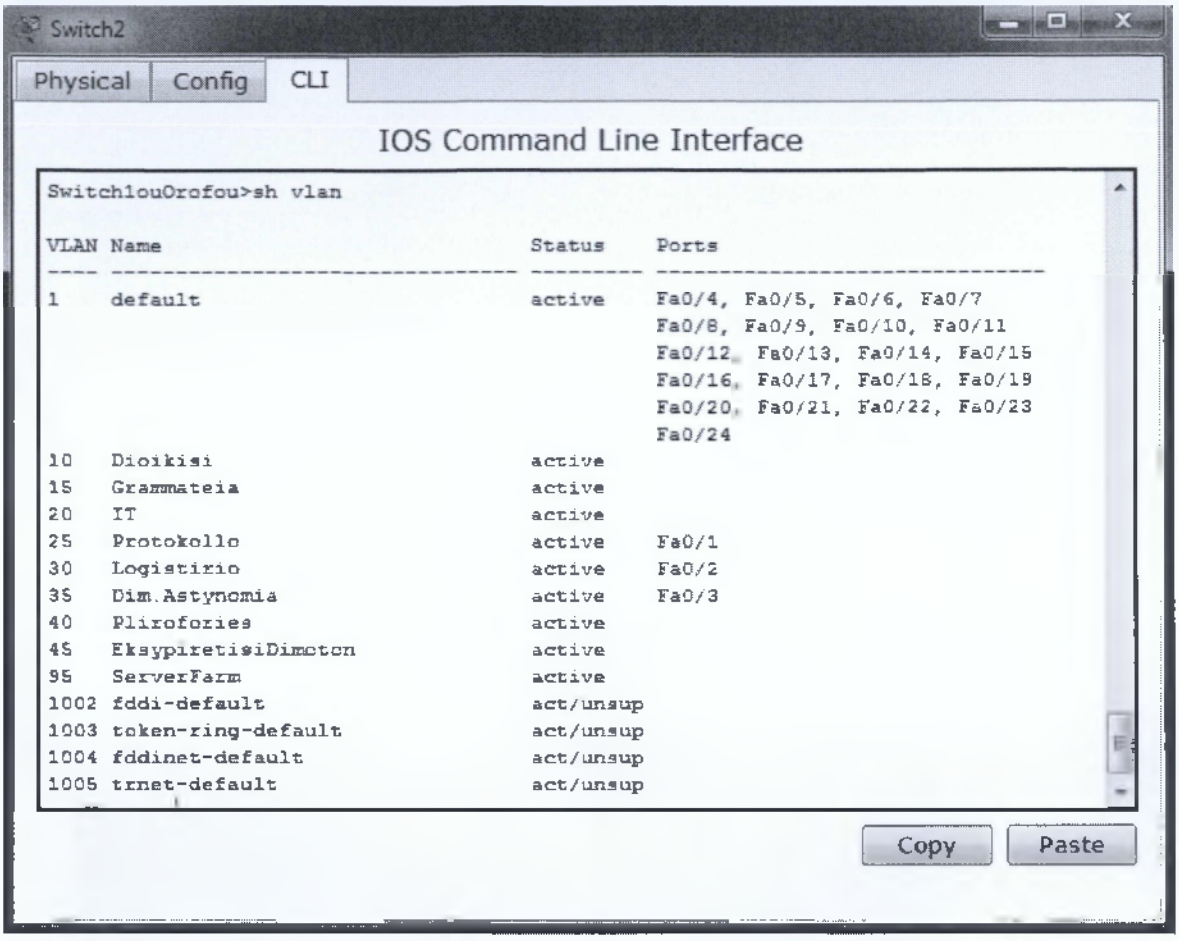
Ένα VLAN χωρίζει και αυτό με την σειρά του ένα δίκτυο σε μικρότερα κομμάτια. Η λεγόμενη υποδικτύωση. Αφού λοιπόν κάνουμε την μελέτη σ' ένα δίκτυο όσον αφορά στην υποδικτύωση με βάση το layer 3 του OSI (επίπεδο δικτύου, routers), τότε μία καλή τεχνική είναι και ο διαμοιρασμός του και σε layer 2 του OSI (επίπεδο σύνδεσης, switches). Έτσι μετά το subnetting ή το VLSM που θα υλοποιήσουμε, στη συνέχεια, βάσει αυτού, χωρίζουμε το κάθε υποδίκτυο σε διαφορετικά VLAN. Ακολουθεί ένας πίνακας ο οποίος περιέχει την αντιστοιχία του τμήματος με το VLAN στο οποίο ανήκει.

Να σημειωθεί εδώ πως ο παρακάτω πίνακας ακολουθείται και στο σετάρισμα των Cisco συσκευών (switches).

ΤΜΗΜΑ ΔΗΜΟΥ	ΑΝΤΙΣΤΟΙΧΙΑ VLAN
ΔΙΟΙΚΗΣΗ	10
ΓΡΑΜΜΑΤΕΙΑ	15
IT	20
ΠΡΩΤΟΚΟΛΛΟ	25
ΛΟΓΙΣΤΗΡΙΟ	30
ΔΗΜΟΤΙΚΗ ΑΣΤΥΝΟΜΙΑ	35
ΠΛΗΡΟΦΟΡΙΕΣ	40
SERVERS	95

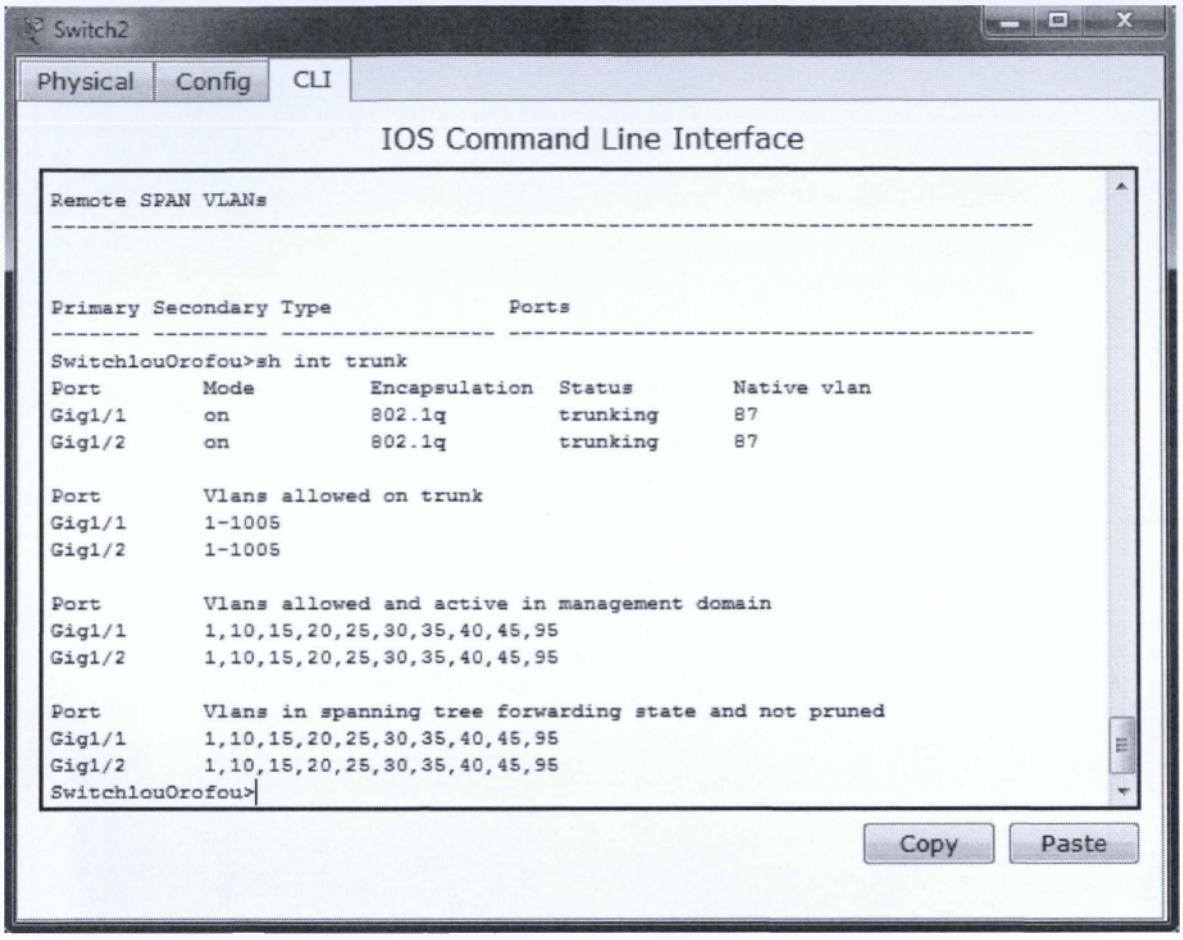
Με το κάθε VLAN, ξεχωρίζουμε και το κάθε υποδίκτυο και απαγορεύεται η μεταξύ τους επικοινωνία. Έτσι με το πρώτο σετάρισμα των συσκευών, ο εκάστοτε υπολογιστής του VLAN του IT για παράδειγμα, δεν θα μπορεί να δει τον οποιοδήποτε υπολογιστή ή εκτυπωτή που ανήκει σε οποιοδήποτε άλλο VLAN. Για να επιτευχθεί κάτι τέτοιο, μπορούμε να εφαρμόσουμε δύο τεχνικές, οι οποίες θα αναλυθούν στο επόμενο κεφάλαιο που αφορά τις ρυθμίσεις και το σετάρισμα των συσκευών σε κονσόλα. Εδώ θα αναφέρουμε ακόμα ότι προς το παρόν οι μόνες συνδέσεις που δεν ανήκουν σε κάποιο VLAN, είναι αυτές που συνδέουν τα switches μεταξύ τους και μεταξύ του switch του υπογείου με το router. Αυτές οι συνδέσεις ονομάζονται trunk και ουσιαστικά επιτρέπουν την κίνηση οποιασδήποτε πληροφορίας, από όποιο VLAN κι αν προέρχεται. Αυτό γίνεται για δύο λόγους. Πρώτον, γιατί οι δικτυακές συσκευές μπορεί να χρειάζεται να έχουν πρόσβαση σε κομμάτια εκτός του συνολικού δικτύου, όπως π.χ. το Διαδίκτυο και δεύτερον, γιατί μπορεί να χρειαστεί μερικές συσκευές να επικοινωνούν με άλλες, εκτός του υποδικτύου τους. Όλα τα υποδίκτυα π.χ. μπορεί να χρειάζεται να έχουν πρόσβαση στο υποδίκτυο που ανήκουν οι Servers του δήμου, δηλαδή στο VLAN 95.

Μία ιδέα για τον διαχωρισμό των VLAN μπορούμε να πάρουμε από την παρακάτω εικόνα, που μας δείχνει πως φαίνονται τα VLAN μέσα στο switch.



Εικ. 5.2 Εμφάνιση των VLAN με την εντολή #show vlan

Με την εντολή **#sh vlan** (sh = show), σε ένα switch της Cisco, βλέπουμε όλα τα διαθέσιμα VLAN που υπάρχουν στη συσκευή (switch). Στην προκειμένη περίπτωση, χρειαστήκαμε εννέα (9) διαφορετικά VLAN, όπως είδαμε και παραπάνω, τα οποία φτιάχτηκαν βάσει των τμημάτων του δήμου. Να σημειώσουμε εδώ πως εκτός από τα εννέα (9) VLAN που φτιάξαμε για τις ανάγκες του δήμου, στην συσκευή βλέπουμε και άλλα πέντε (5). Το VLAN 1 είναι το default και όλες οι θύρες ενός switch ανήκουν σ' αυτό αν δεν γίνει κάποια αλλαγή. Τα VLAN 1002 μέχρι και το VLAN 1005, χαρακτηρίζονται ως legacy, δηλαδή υπάρχουν για λόγους συμβατότητας με προηγούμενες τεχνολογίες, αν και πλέον δεν χρησιμοποιούνται καθόλου. Επίσης, αν παρατηρήσουμε την εικόνα, βλέπουμε πως με την συγκεκριμένη εντολή μπορούμε να εντοπίσουμε σε ποιο VLAN ανήκει η κάθε θύρα (port) του switch. Οι θύρες fa0/4 έως και την fa0/24 στο συγκεκριμένο switch (1^{ου} ορόφου), ανήκουν στο default VLAN, δηλαδή στο VLAN 1. Οι πρώτες όμως τρεις (3) θύρες ανήκουν η κάθε μία σε ξεχωριστό VLAN. Το fa0/1, ανήκει στο VLAN 25, που αντιστοιχεί στο τμήμα του **Πρωτοκόλλου**. Το fa0/2, ανήκει στο VLAN 30, που αντιστοιχεί στο τμήμα του Λογιστηρίου. Τέλος, το fa0/3, ανήκει στο VLAN 35, που αντιστοιχεί στο τμήμα της Δημοτικής Αστυνομίας. Να σημειωθεί εδώ πως η κάθε θύρα του switch και στην συγκεκριμένη περίπτωση οι πρώτες τρεις (3), συνδέονται με ένα Access Point.



Εικ. 5.3 Εμφάνιση Trunk θυρών με την εντολή #show interface trunk

Με την παραπάνω εντολή, όπως φαίνεται και στην εικόνα, μπορούμε να δούμε με λεπτομέρειες ποιες είναι οι θύρες που λειτουργούν σαν trunk στο switch και επίσης εκτός αυτού, ποιο encapsulation mode ακολουθούν, στην προκειμένη το 802.1q και επίσης ποια VLAN επιτρέπει η εκάστοτε trunk θύρα να περάσουν μέσα από αυτή. Τέλος, βλέπουμε και την ονομασία Native VLAN. Στην εικόνα είναι το νούμερο 87. Βάσει cisco, το native vlan είναι από default πάλι το VLAN 1. Για λόγους ασφαλείας το αλλάζουμε και βάζουμε ένα νούμερο τυχαίο. Να σημειωθεί πως για σωστή επικοινωνία μεταξύ των switches του δικτύου, όλες οι trunk θύρες σε όλα τα switches, πρέπει να έχουν την ίδια τιμή. Αναφορικά, για να αλλάξουμε το native VLAN μίας trunk θύρας, δίνουμε την ακόλουθη εντολή σε επίπεδο θύρας:

Switch(config-if)#switchport trunk native vlan 87

Αυτή η εντολή και όλες όσες χρησιμοποιηθούν αναλύονται στο τέλος της εργασίας σε ειδικό παράρτημα. Κάτι σημαντικό που επίσης πρέπει να αναφερθεί εδώ, είναι το πρωτόκολλο VTP (VLAN Trunking Protocol) της Cisco. Μέσω αυτού του πρωτοκόλλου γλιτώνουμε αρκετό χρόνο στο στήσιμο του δικτύου. Πιο συγκεκριμένα, με το VTP, μπορούμε να ορίσουμε ένα domain, το οποίο μπορεί να

προστατεύεται κι από κάποιο password και για το κάθε switch μπορούμε να επιλέξουμε ένα ρόλο (Server ή Client). Η διαφορά μεταξύ Server και Client έγκειται στο γεγονός πως ο πρώτος μπορεί να παραμετροποιήσει τα VLAN κάποιου άλλου switch του δικτύου, σε περίπτωση που ο δεύτερος δεν έχει ενημερωμένο τον πινάκα με τα VLAN του. Αυτό ελέγχεται μέσω του "Configuration Revision" και το switch που έχει το μεγαλύτερο νούμερο, θεωρείται πως είναι και αυτό με τις περισσότερες αλλαγές και κατ' επέκταση και το πιο ενημερωμένο. Μέσα από το VTP λοιπόν, γλιτώνουμε αρκετό χρόνο, αφού ουσιαστικά σετάρουμε τα VLAN όλου του δικτύου μόνο σε ένα switch και μετά αυτά αποθηκεύονται και στα υπόλοιπα switches. Για το δήμο Αμαρουσίου, ορίσαμε σαν VTP Servers δύο (2) switches (Switch2rouOrofou & SwitchYpogeiou), ορίσαμε domain με την ονομασία "DimosAmarousiou" και δώσαμε και έξτρα ασφάλεια στις πληροφορίες αυτές μέσω ενός κωδικού που είναι ο "s4F3z0ne!". Για να ορίσουμε αυτές τις παραμέτρους, χρησιμοποιήσαμε τις παρακάτω εντολές:

Switch(config)#vtp mode server

Switch(config)#vtp domain DimosAmarousiou

Switch(config)#vtp password s4F3z0ne!

Οι εντολές αυτές βέβαια πρέπει να περαστούν σε όλα τα switch που θέλουμε να πάρουν αυτόματα τα VLAN που δημιουργήθηκαν στο πρώτο switch ή σε οποιοδήποτε switch παίζει τον ρόλο του server, ο οποίος, από default, είναι ενεργοποιημένος στο κάθε switch. Όλα τα switches δηλαδή, με το που συνδεθούν στο δίκτυο, λειτουργούν σαν VTP Servers και αυτό βέβαια είναι αρκετά κακό, γιατί σε περίπτωση που ενσωματώσουμε κάποιο παλιότερο switch σε ένα υπάρχον δίκτυο και οι συσκευές του τωρινού δικτύου λειτουργούν με τις default ρυθμίσεις και το παλιό switch επίσης, τότε αν το παλιότερο μηχάνημα έχει υψηλότερο "Configuration Revision" number από τα υπόλοιπα, θα χάσουμε τα υπάρχοντα VLAN του δικτύου μας, τα οποία θα αντικατασταθούν από τις εγγραφές του παλιού μηχανήματος μας. Μην ξεχνάμε πως η ασφάλεια είναι από τα πιο σημαντικά κομμάτια ενός δικτύου και πρέπει πάντα(!) να αποφεύγουμε όλες τις default επιλογές μιας συσκευής.

Για μεγαλύτερη ασφάλεια στο δίκτυο μας, μπορούμε να παραμετροποιήσουμε μερικές ακόμη συνθήκες. Πρώτον, μπορούμε να προσθέσουμε κάποια/ες ACL στο router που βρίσκεται στο υπόγειο του κτηρίου και επίσης να αλλάξουμε το στήσιμο του δικτύου και να δώσουμε τη δυνατότητα για free WiFi στους δημότες, μέσω ενός ξεχωριστού modem/router με δυνατότητες ασύρματης σύνδεσης, παρόμοιο με αυτό που χρησιμοποιούμε οι περισσότεροι στα σπίτια μας και το οποίο δεν θα συνδέεται καθόλου στο δίκτυο του δήμου. Δεύτερον, μπορούμε να προσθέσουμε δύο ακόμη τεχνικές για έξτρα ασφάλεια στο δίκτυο μας. Οι τεχνικές αυτές ονομάζονται IDS και IPS.

5.4 IDS, IPS & ACLs

Intrusion Detection System

Το IDS (Intrusion Detection System) υλοποιείται μέσω hardware σ' ένα δίκτυο και ουσιαστικά λειτουργεί σαν μία σειρήνα ειδοποίησης, η οποία ενεργοποιείται κάθε φορά που το δίκτυο μπορεί να δεχθεί κάποια επίθεση. Η λειτουργία του όμως τελειώνει εκεί. Δεν γίνεται κάποιο μπλοκάρισμα των δεδομένων στο δίκτυο ή κάτι αντίστοιχο. Το IDS επίσης πρέπει να ενημερώσουμε πως για να

υλοποιηθεί σωστά, η συσκευή που θα το υποστηρίζει, πρέπει να βρίσκεται σε σημείο του δικτύου που από εκεί θα φιλτράρει όλη την κίνηση του. Έτσι το κάθε πακέτο που θα κυκλοφορεί στο δίκτυο, θα περνάει μέσα από το IDS και στη συνέχεια θα προωθείται στον παραλήπτη ή στο επόμενο βήμα (hop) μέχρι να φτάσει στον τελικό προορισμό του.

Intrusion Prevention System

Το IPS (Intrusion Prevention System) μπορεί να υλοποιηθεί μέσω hardware ή και software. Χρησιμοποιείται in-line στο δίκτυο και έτσι αντί για μία μόνο ειδοποίηση επίθεσης ή κακόβουλου πακέτου, το IPS σε αντίθεση με το IDS, προχωράει ένα βήμα παρακάτω. Μπορεί να μπλοκάρει την IP που αποστέλει κακόβουλα δεδομένα, να ρίξει τη θύρα (reset) του εκάστοτε switch μέσω της οποίας περνάνε τα δεδομένα αυτά και να κάνει drop τα κακόβουλα πακέτα. Επίσης το IPS μπορεί να διορθώσει λάθη στο CRC (Circle Redundancy Check), να "ξεμπουκώσει" το κανάλι σε κάποια θύρα η οποία μπορεί να δέχεται ένα μεγάλο μέγεθος από πακέτα που δεν προλαβαίνει να προωθήσει σε σωστό χώρο κ.α.

Βέβαια το IPS σε σχέση με IDS, λόγω όλων των παραπάνω επιλογών που προσφέρει, είναι αρκετά πιο αργό. Και εδώ τίθεται το ερώτημα χρόνου και ταχύτητας, ενάντια σε αποτελεσματικότητα.

Αν το IT του δήμου ασχολείται με τα log files που παράγει το IDS, τότε η ανάγκη για την εγκατάσταση ενός IPS είναι μικρή έως και περιττή, αφού θα μειώσει κατά πολύ τις ταχύτητες που έχουμε στο δίκτυο μας. Σε περίπτωση όμως που το τμήμα του IT, δεν ασχολείται με τα log files και δεν επιτηρεί σε συχνά χρονικά διαστήματα την κίνηση στο δίκτυο για να κάνει συγκρίσεις και να βλέπει σε πραγματικό χρόνο την κίνηση του δικτύου, τότε η ανάγκη για εγκατάσταση ενός IPS συστήματος, είναι επιτακτική.

Στην μελέτη της εγκατάστασης του δικτύου μας για το δήμο Αμαρουσίου, αφήνουμε χωρίς κάποιο IPS το δίκτυο στην αρχή, αλλά θα δούμε πως μπορεί να εγκατασταθεί και πως λειτουργεί σε περίπτωση προσθήκης ενός τέτοιου συστήματος στο μέλλον. Να προστεθεί εδώ, πως η οικονομική επιβάρυνση για την εγκατάσταση ενός IPS είναι αρκετά μεγαλύτερη σε σχέση μ' αυτή ενός IDS.

Access Control List

Οι ACLs (Access Control Lists) στην ουσία είναι μερικές εντολές που προσθέτουμε στο κεντρικό router του δικτύου μας για να ελέγχει το κάθε πακέτο και να το αφήνει ή να το μπλοκάρει βάσει αυτών (των εντολών). Μία ACL στην ουσία είναι ένα αρχείο το οποίο πάντα τελειώνει με την εντολή **deny all**. Αυτό πρακτικά σημαίνει πως από την στιγμή που θα δώσουμε στο router την πρώτη εντολή για την δημιουργία της ACL, ό,τι κι αν προσθέσουμε σ' αυτή, στο τέλος πάντα θα υπάρχει ένα deny all. Πιο αναλυτικά:

Οι ACLs χωρίζονται σε δύο βασικές κατηγορίες. Στις Standard ACL με αριθμό από 1 έως και 99 και στις Extended ACL με αριθμό από 100 έως και 199. Οι αριθμοί ουσιαστικά είναι σαν ονόματα για να ξεχωρίζουμε την μία ACL από την άλλη. Ο κανόνας είναι πως μπορούμε να δημιουργήσουμε μία ACL ανά πρωτόκολλο, ανά κατεύθυνση και ανά θύρα. Δηλαδή στην θύρα fa0/0 ενός router για παράδειγμα, μπορούμε να έχουμε μέχρι και πέντε (5) ACLs που θα ελέγχουν την κίνηση. Μία που θα είναι πάνω στην θύρα, μία που θα ελέγχει την κίνηση προς τα μέσα, μία που θα ελέγχει την κίνηση προς τα έξω,

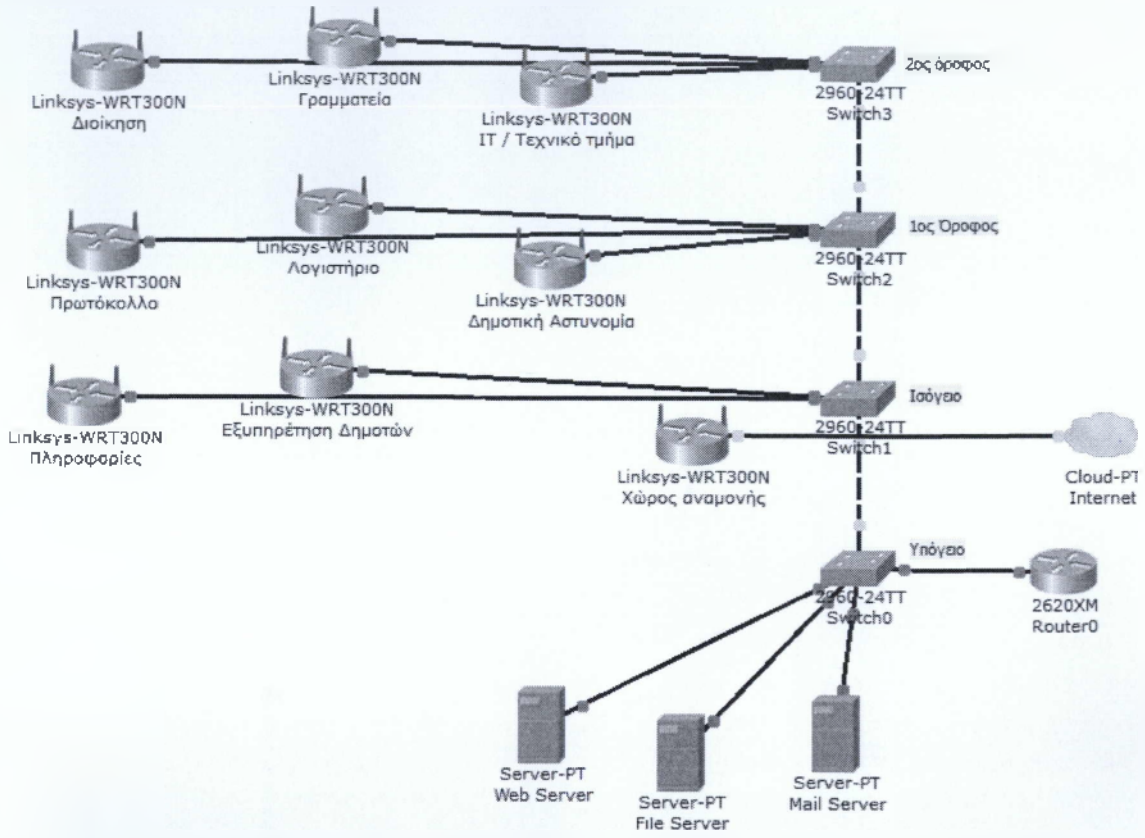
μία που θα ελέγχει τα πακέτα που βασίζονται στο IP πρωτόκολλο και μία τελευταία που θα ελέγχει τα πακέτα που βασίζονται στο IPX πρωτόκολλο. Από αυτό καταλαβαίνουμε πως όσο περισσότερες ACLs έχουμε και όσο πιο μεγάλες είναι, τόσο περισσότερο χρόνο χρειάζεται η συσκευή και υπολογιστική δύναμη επίσης, στο να διαβάσει την κάθε γραμμή (της ACL) για το κάθε πακέτο που διέρχεται από το router.

Έτσι σε περίπτωση που το δίκτυο μας χρειάζεται κάποιο firewall, δηλαδή μία ACL σε κάποιο ή κάποια από τα routers του, τότε θα πρέπει να είμαστε πολύ προσεκτικοί στο να μην υπερβάλλουμε και έτσι δημιουργήσουμε μεγάλες και σε μερικές περιπτώσει περιττές, καθυστερήσεις στο δίκτυό μας. Στην περίπτωση του δήμου Αμαρουσίου θα ήταν καλό να δημιουργηθεί μία ACL η οποία θα μπλόκαρε HTTP και TELNET συνδέσεις από οποιαδήποτε διεύθυνση εκτός του δικτύου προς τα μέσα. Βέβαια το μπλοκάρισμα του TELNET ή του SSH δεν θα ήταν και τόσο καλή πρακτική για μία άλλη επιχείρηση, αλλά στην περίπτωση του δήμου, που πάντα θα βρίσκονται άτομα μέσα στο κτήριο και στο δίκτυο, δεν θα έχουμε πρόβλημα σε περίπτωση ελέγχου κάποιας δικτυακής συσκευής. Από εκεί και πέρα, βασιζόμενοι στο ότι το IT ασχολείται με την "υγεία" του δικτύου και όλοι οι εργαζόμενοι του δήμου έχουν διαβάσει και ακολουθούν πιστά το security policy, παραπάνω έλεγχοι θα ήταν περιττοί, αφού εμπιστευόμαστε τους υπαλλήλους μας. Η ανάγκη για μεγαλύτερους ελέγχους, θα υπήρχε σε περίπτωση που είχαμε τους δημότες που βρίσκονται με διάφορες ασύρματες συσκευές στο χώρο αναμονής, σε κάποιο υποδίκτυο από αυτά που δημιουργήσαμε παραπάνω. Κάτι τέτοιο βέβαια δεν θα γίνει και η εικόνα 5.1 που δείχνει αυτό το στήσιμο, είναι για λόγους κατανόησης της βασικής τοποθέτησης των συσκευών του δικτύου στον κάθε όροφο. Όπως αναφέραμε και προηγουμένως, οι ανάγκες του free WiFi, θα καλυφθούν από μία απλή συσκευή η οποία καλύπτει επαρκώς το χώρο αναμονής και θα παρέχει ελεύθερη πλοήγηση στους δημότες, χωρίς όμως να χρειάζονται έξτρα μέτρα προστασίας του δικτύου του δήμου.

Το configuration της ACL που θα χρειαστούμε για τους βασικούς ελέγχους, θα το δούμε στο κεφάλαιο που δείχουμε τα στησίματα όλων των δικτυακών συσκευών (ενσύρματων και ασύρματων).

5.5 Χώρος Αναμονής Δημοτών

Στην εικόνα που ακολουθεί φαίνεται η τοπολογία στο επόμενο στάδιο αφού κατανοήθηκε πλήρως η ανάγκη για ξεχωριστή σύνδεση του Χώρου αναμονής για τους δημότες οι οποίοι θα μπορούν να πλοηγηθούν στο Διαδίκτυο.



Εικ. 5.4 Ξεχωριστό δίκτυο για τον Χώρο αναμονής του δήμου (free WiFi)

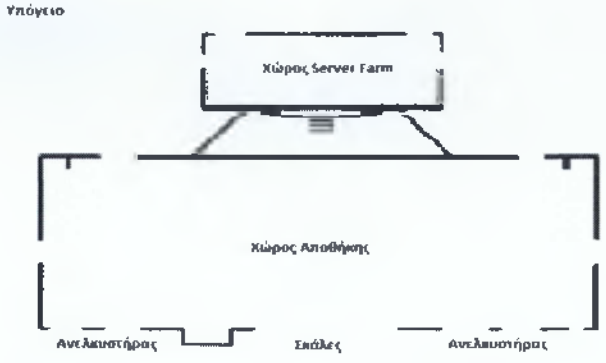
Το σετάρισμα που ακολουθείται για αυτή τη συσκευή είναι το απλούστερο που μπορεί να γίνει. Ουσιαστικά δεν ακολουθείται καμία πολιτική ασφαλείας και οι δημότες που χρησιμοποιούν αυτό το ασύρματο δίκτυο είναι υπεύθυνοι για τα δεδομένα που στέλνουν. Πιο συγκεκριμένα, το SSID του δικτύου αυτού είναι το "Free WiFi – Dimos Amarousiou", εκπέμπει στο κανάλι 11 και χρησιμοποιεί το πρωτόκολλο 802.11b/g (σε mix-mode). Δεν υπάρχει κανένα πρωτόκολλο ασφαλείας όπως WEP, WPA ή WPA2 που να υλοποιείται σε αυτό το Access Point. Δηλαδή το δίκτυο εκπέμπει κανονικά το όνομά του και είναι πλήρως ελεύθερο προς χρήση από τον καθένα που μπορεί να βρίσκεται στην περιοχή που εκπέμπει. Στη συνέχεια το Access Point, συνδέεται ουσιαστικά με τον πάροχο που ο δήμος έχει συνεργασία μαζί του (O.T.E., Forthnet, HoL κτλ). Στην ουσία δεν πρόκειται για κάποιο απλό AP, αλλά για ένα modem/router με δυνατότητες ασύρματης σύνδεσης. Η μόνη ασφάλεια που υπάρχει στο συγκεκριμένο μηχάνημα, είναι πως έχει αλλαχθεί το default username και password για την είσοδο στο web interface της συσκευής και παραμετροποίηση της. Επίσης έχει αλλαχθεί η IP της συσκευής και από την 192.168.1.1, μετατράπηκε σε 192.168.1.254 και μέσω DHCP δίνει αυτόματα IP διευθύνση σε οποιαδήποτε συσκευή προσπαθεί να συνδεθεί από το εύρος της 192.168.1.1 έως και την 192.168.1.253. Όλες οι παραπάνω πληροφορίες σεταρίσματος της συσκευής αυτής εμφανίζονται στον παρακάτω πίνακα.

SSID	Free WiFi – Dimos Amarousiou
Κανάλι	11
Πρωτόκολλο	802.11b/g (mixed)
Κρυπτογράφηση	Καμία
Προεπιλεγμένη Πύλη	192.168.1.254
Εύρος IP προς χρήση	192.168.1.1 – 192.168.1.253

Για ευνόητους λόγους στην αίθουσα αναμονής των δημοτών, μπορεί να υπάρχει μία ανακοίνωση σε εμφανές σημείο, που θα ενημερώνει τους πολίτες πως δεν υπάρχει κάποιο επίπεδο ασφαλείας της ασύρματης επικοινωνίας τους κι έτσι θα πρέπει να είναι πολύ προσεκτικοί στα δεδομένα που αποστέλουν γιατί ο καθένας μπορεί να τα "διαβάσει" χωρίς να χρειαστεί να καταβάλει ιδιαίτερο κόπο. Από εκείνο το σημείο και έπειτα, ο δήμος Αμαρουσίου δεν φέρει καμία ευθύνη σε περίπτωση οποιασδόποτε απώλειας δεδομένων από τις συσκευές των πολιτών που χρησιμοποιούν το συγκεκριμένο ασύρματο δίκτυο για την πλοήγησή τους στο Διαδίκτυο.

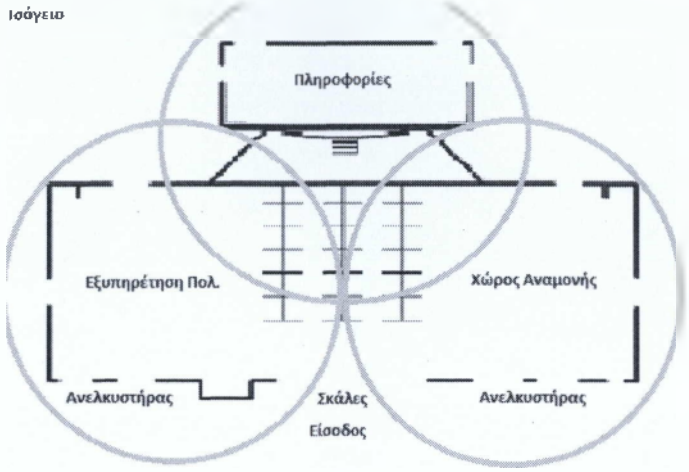
5.6 Σχέδια Κτηρίου Δήμου ανά Όροφο και Ασύρματη Κάλυψη

Αφού μελετήσαμε τα τμήματα του δήμου και των τρόπο που χωρίζουμε τα υποδίκτυα ας δούμε τα σχέδια του κτηρίου του δήμου. Το κτήριο αυτό είναι ένα νεοκλασικό το οποίο έχει την ίδια διαρύθμιση σε όλους τους ορόφους του. Η μόνη διαφορά είναι στο υπόγειο, που έχει γκρεμιστεί η μεσοτοιχία και υπάρχει ένα μεγάλο δωμάτιο που το χρησιμοποιούν οι υπάλληλοι ως αποθήκη. Ας προχωρήσουμε στα σχέδια.



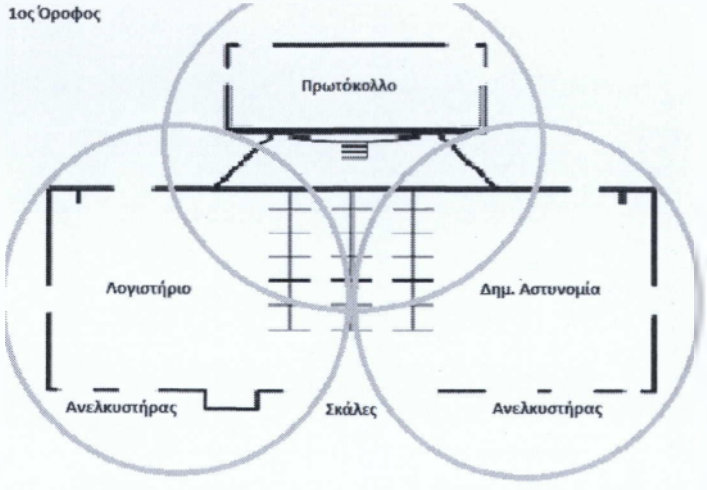
Εικ. 5.5 Χώρος υπογείου

Στο χώρο του υπογείου υπάρχει ο μεγάλος χώρος που προαναφέραμε και λειτουργεί ως αποθήκη, καθώς και ένα δωμάτιο στο οποίο υπάρχουν οι τρεις (3) Servers του δημαρχείου.



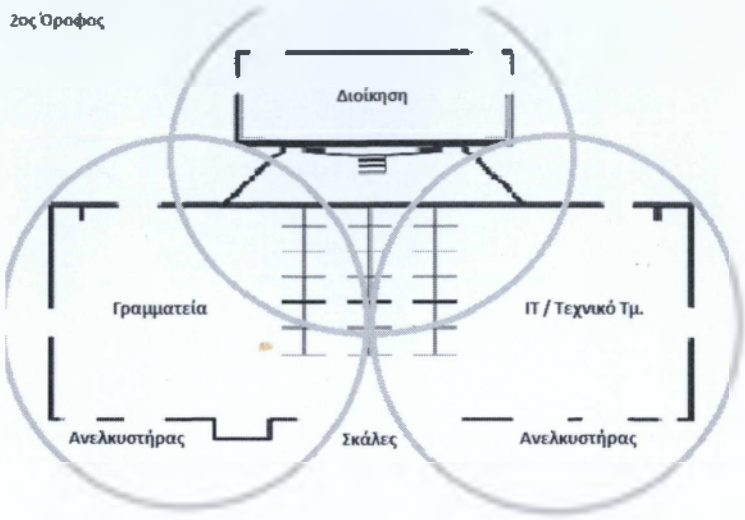
Εικ. 5.6 Χώρος Ισογείου

Στο χώρο του ισογείου, βρίσκουμε τη μεσοτοιχία η οποία μετά την είσοδο διαχωρίζει το τμήμα της Εξυπηρέτησης Πολιτών με το Χώρο Αναμονής. Επίσης, υπάρχει και μία ξεχωριστή αίθουσα στο βόρειο κομμάτι του κτηρίου, στην οποία στεγάζεται το τμήμα των Πληροφοριών. Οι μπλε κύκλοι συμβολίζουν την ασύρματη κάλυψη στους χώρους αυτούς. Στο κέντρο του κάθε κύκλου είναι τοποθετημένο (στο ταβάνι) το εκάστοτε Access Point.



Εικ. 5.7 Χώρος 1ου ορόφου

Στον πρώτο όροφο έχουμε τον ίδιο διαχωρισμό των χώρων του κτηρίου. Με το που ανέβουμε τις σκάλες, στο δεξί μας χέρι βρίσκουμε τον χώρο που στεγάζεται το τμήμα της Δημοτικής Αστυνομίας και στο αριστερό μας χέρι, βρίσκουμε το τμήμα του Λογιστηρίου του δήμου. Στο βάθος του κτηρίου (από τις σκάλες), βρίσκουμε το τμήμα του Πρωτοκόλλου. Για ακόμη μια φορά βλέπουμε με τους μπλε κύκλους τους χώρους που καλύπτουν τα τρία (3) AP του ορόφου.



Εικ. 5.8 Χώρος 2ου ορόφου

Στον δεύτερο και τελευταίο όροφο του κτηρίου, ακολουθείται η ίδια αρχιτεκτονική κτηρίου. Κι εδώ έχουμε τρία (3) διαφορετικά τμήματα, δηλαδή τρία (3) διαφορετικά AP, σε τρεις (3) διαφορετικούς χώρους. Από τον δεξί ανελκυστήρα, με το που βγούμε στον χώρο, συναντάμε το τμήμα του IT/Τεχνικών, ενώ από τον αριστερό ανελκυστήρα, συναντάμε το τμήμα της Γραμματείας. Στο βάθος του κτηρίου βρίσκεται και ο χώρος της διοίκησης, στον οποίο έχουμε τα γραφεία του Δημάρχου, του Αντιδημάρχου και την αίθουσα συσκέψεων του διοικητικού συμβουλίου. Για ακόμη μια φορά, οι μπλε κύκλοι εκπροσωπούν τους χώρους κάλυψης της ασύρματης σύνδεσης των Access Points.

Βάσει των παραπάνω εικόνων, έχουμε πλέον μία ξεκάθαρη εικόνα για την αρχιτεκτονική του κτηρίου και τους χώρους που έχει. Η αναλύση των ρυθμίσεων των συσκευών και ειδικότερα των AP, ώστε να μην έχουμε προβλήματα απωλειών ή θορύβων στο κανάλι, λόγω του ότι τα σήματα που εκπέμπει το κάθε AP "πέφτουν" πάνω στα σήματα των άλλων, γίνεται στο επόμενο κεφάλαιο και θα δούμε πως δεν υπάρχει κανένα πρόβλημα παρεμβολής, λόγω της σωστής τροποποίησης των καναλιών των Access Points στου χώρους του κτηρίου.

Επίσης καλό είναι να σημειώσουμε εδώ πως το σήμα εκπέμπει και σε μια μικρή περιοχή εκτός κτηρίου. Αυτό βέβαια δίνει στον οποιοδήποτε επιτηθέμενο τη δυνατότητα να πραγματοποιήσει διάφορες επιθέσεις, χωρίς να βρίσκεται καν μέσα στο κτήριο του δημαρχείου. Η παραμετροποίηση όμως των συσκευών που θα δούμε στο επόμενο κεφάλαιο είναι αρκετά ισχυρή και μία εισβολή στο δίκτυο του δήμου είναι αρκετά δύσκολη. Το δίκτυο δεν είναι άτρωτο, όπως και όλα τα δίκτυα άλλωστε, αλλά σίγουρα είναι αρκετά καλά ασφαλισμένο, βάσει πάντα των δυνατοτήτων που έχουν οι ασύρματες συσκευές στις μέρες μας.

6. Εγκατάσταση Δικτύου και Έλεγχος Λειτουργίας

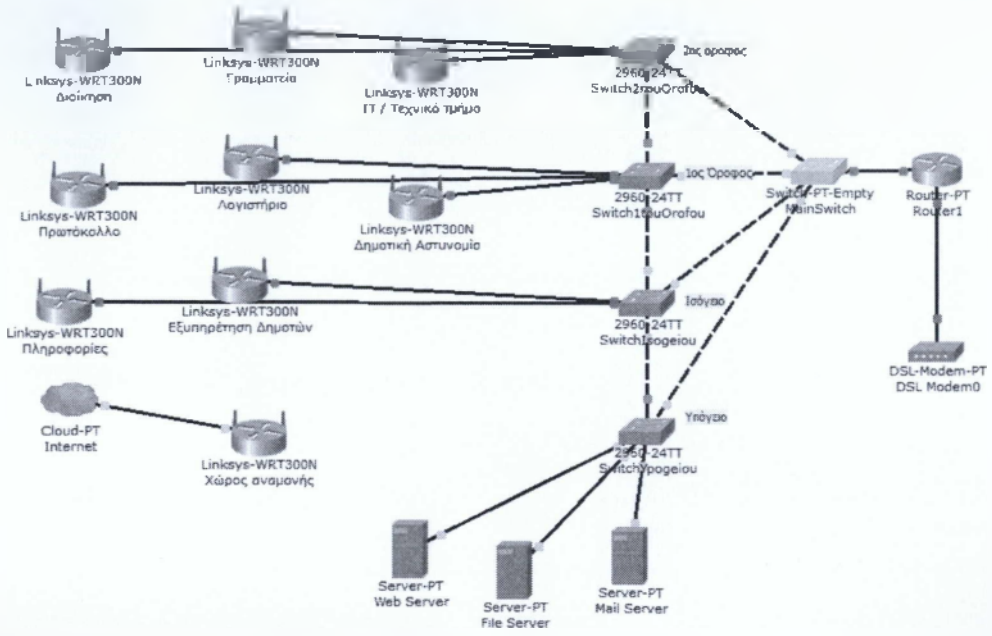
6.1 Τοπολογία Συσκευών και Προσθήκη Ενός Main Switch

Όπως αναλύσαμε στο προηγούμενο κεφάλαιο για λόγους ασφαλείας, καλό θα ήταν αν όχι και αναγκαίο να τοποθετηθεί ένα σύστημα IDS ή IPS. Για να γίνει όμως κάτι τέτοιο, η τοπολογία του δικτύου μας πρέπει να αλλάξει λίγο. Πλέον με την προσθήκη ενός ακόμη switch, μέσω του οποίου θα περνάει όλη η κίνηση του δικτύου και των υποδικτύων, θα μπορούμε να υλοποιήσουμε ένα τέτοιο σύστημα. Ας δούμε όμως πρώτα πως θα επιτευθεί κάτι τέτοιο, από την στιγμή που όλα τα switch του κάθε ορόφου συνδέονται άμεσα με τους γείτονες τους και επίσης συνδέονται και με το Main Switch που μόλις τοποθετήσαμε.

Σε όλες τις Catalyst (switches) συσκευές της Cisco, με το που τις ενεργοποιήσουμε, τρέχει αυτόματα το πρωτόκολλο STP (Spanning Tree Protocol). Αυτό το πρωτόκολλο, στην ουσία αυτός ο αλγόριθμος, ελέγχει όλα τα μονοπάτια που μπορεί να ακολουθήσει μέσα από τις θύρες του και μέσω κάποιων συναρτήσεων μπορεί να μας "υποσχεθεί" μηδέν(!) συγκρούσεις στο κανάλι (μέχρι εφτά συσκευές στη σειρά ή αλλιώς, εφτά hops). Ας το δούμε καλύτερα μέσω ενός παραδείγματος. Το switch που βρίσκεται στο ισόγειο του κτηρίου, επικοινωνεί με τα γειτονικά του switch (1^{ου} ορόφου και υπογείου) μέσω δύο οδών. Συνδέεται άμεσα με ένα Cross-over καλώδιο και επίσης μέσω ενός άλλου συνδέεται στο νέο switch που προσθέσαμε (Main Switch), το οποίο και αυτό με τη σειρά του επικοινωνεί άμεσα με όλα τα switch του κάθε ορόφου του κτηρίου (τέσσερα για την ακρίβεια). Αυτό μας δημιουργεί δύο προβλήματα. Πρώτον, μπορούν να δημιουργηθούν συγκρούσεις, αφού η πληροφορία που θέλει να περάσει από τον 1° όροφο στο ισόγειο μπορεί να περάσει μέσα από δύο οδούς και δεύτερον, δεν μπορούμε να ελέγξουμε την πληροφορία από κάποια συσκευή (για την εγκατάσαση του IDS ή του IPS), αφού περνάει από διαφορετικά μονοπάτια. Το STP ελέγχει διάφορες παραμέτρους της εκάστοτε σύνδεσης, όπως, την ταχύτητα της θύρας, τα βήματα που χρειάζονται κ.α. και βάσει του αλγορίθμου του, ορίζει μία βασική διαδρομή και από το σημείο εκείνο και μετά, λειτουργεί μόνο αυτή και όλες οι υπόλοιπες πιθανές διαδρομές μπαίνουν σε ένα stand-by mode, και είναι έτοιμες να ανοίξουν με το που υπάρξει κάποιο πρόβλημα επικοινωνίας στο βασικό δίαυλο. Το STP μπορούμε να το "πειράξουμε" και να μπορέσουμε να αλλάξουμε τους βασικούς διάυλους επικοινωνίας και αρκετά ακόμη, αλλά στην προκειμένη περίπτωση δεν χρειάζεται λόγω της τοπολογίας και των θυρών που επιλέξαμε.

Ο κάθε όροφος συνδέεται άμεσα με τον/τους γειτονικό/κούς του, αλλά μέσω μίας Fast Ethernet θύρας. Από εκεί και πέρα, ο κάθε όροφος, συνδέεται και στο Main Switch, μέσω όμως μίας Gigabit Ethernet θύρας. Αυτό πρακτικά σημαίνει, πως μέσω του Main Switch αν ένας κόμβος του 1^{ου} ορόφου, θέλει να επικοινωνήσει με ένα κόμβο του ισογείου, μπορεί να περάσει από ένα switch ακόμα, αλλά αυτό θα γίνει πολύ πιο γρήγορα, γιατί οι διαφορές ταχύτητας του καναλιού είναι μεγάλες. Έτσι είναι καλύτερο και πιο "άνετο" για το δίκτυο το να χρειάζεται μία πληροφορία να περνάει μέσα από περισσότερα μέσα (switches, routers κτλ), για να φτάσει στον τελικό προορισμό της, αν οι ταχύτητες είναι καλύτερες από την απευθείας αποστολή των δεδομένων μέσω ενός hop.

Έτσι με την προσθήκη του switch που ονομάσαμε Main Switch, έχουμε άμεσα δύο βασικά πλεονεκτήματα. Την εγγυημένη(!) αποφυγή συγκούσεων στο δίκτυο μας και επίσης την ευκολότερη καταγραφή της κίνησης των δεδομένων του.



Εικ. 6.1 Τοπολογία δικτύου μετά την προσθήκη του Main Switch

Σημείωση:

Στο Packet Tracer οι θύρες που είναι απενεργοποιημένες, παρουσιάζονται με κόκκινο χρώμα, οι ενεργές με πράσινο και αυτές που βρίσκονται σε αναμονή (για τον οποιοδήποτε λόγο), με πορτοκαλί.

Έτσι από την παραπάνω εικόνα βλέπουμε ότι οι θύρες από όλα τα switch που συνδέονται στο Main Switch είναι ενεργοποιημένες και λειτουργούν κανονικά, ενώ αυτές που συνδέουν το κάθε switch με τον γειτονικό του όροφο, είναι σε αναμονή.

Η τοποθέτηση του Main Switch μπορεί να είναι ένα θέμα προς συζήτηση. Η τοποθέτησή του χωροταξικά τουλάχιστον. Το υπόγειο είναι μία καλή θέση για να τοποθετηθεί, αφού είναι ένας χώρος που κανένας δεν μπορεί να μπει σ' αυτόν, εκτός από τα άτομα του IT του δήμου. Στο υπόγειο υπάρχει ουσιαστικά μία κλειδωμένη αίθουσα με καλό κλιματισμό που κρατάει τη θερμοκρασία σε χαμηλά επίπεδα (χαμηλή, κάτω από 20°C) και μέσα της υπάρχει, το Main Switch, το switch του υπογείου που έχει πάνω του τους servers του δήμου, το router του δήμου και το dsl modem που συνδέεται πάνω στο router και μέσω αυτού έχουμε πρόσβαση και στο Διαδίκτυο. Εδώ πρέπει να τονίσουμε, πως όλες οι συσκευές του δικτύου, σε όποιο όροφο κι αν βρίσκονται, είναι τοποθετημένες σε σημεία που δεν μπορεί ο οποιοσδήποτε να τις πειράξει. Τα switch του κάθε ορόφου βρίσκονται πάντα κοντά σε κάποιο γραφείο και είναι πάντα κλειδωμένα μέσα στο rack του ορόφου. Τα APs, που βρίσκονται σε "κοινή"

θέα, είναι τοποθετημένα στο ταβάνι του κάθε ορόφου και το καλώδιο που συνδέει το εκάστοτε AP με το switch του ορόφου του, προστατεύεται για λόγους ασφαλείας επίσης.

6.2 Βασική Μεθοδολογία VPN και Ρύθμιση του NAT

Το VPN (Virtual Private Network) μας δίνει τη δυνατότητα ασφαλούς διασύνδεσης κόμβων απομακρυσμένων περιοχών, μέσω του Internet. Το VPN βασίζεται σε τέσσερα (4) πρωτόκολλα. Το πρώτο είναι το PPTP (Point-to-Point Tunneling Protocol) και είναι και το πιο συνηθισμένο. Το δεύτερο είναι το L2TP (Layer 2 Tunneling Protocol) και το τρίτο είναι το IPsec (Internet Protocol Security). Αυτά τα δύο προσφέρουν καλύτερα επίπεδα ασφαλείας από το PPTP, αλλά έχουν πιο περίπλοκη εγκατάσταση .Το τέταρτο και τελευταίο, είναι το πρωτόκολλο ασφαλείας SSL (Secure Sockets Layer) και είναι αυτό που αποκαλείται και "clientless", αφού για αυτήν την υπηρεσία ασφαλείας δεν χρειάζεται να τρέξουμε στον υπολογιστή μας κάποιο ειδικό λογισμικό.

Αυτό που ουσιαστικά γίνεται σε ένα VPN, είναι η επέκταση ενός τοπικού δικτύου για επικοινωνία με κόμβους που βρίσκονται μακριά από αυτό. Έτσι αν για παράδειγμα η ανάγκη για ασφάλεια της επικοινωνίας μας με κόμβους εκτός του δικτύου μας είναι επιτακτική, τότε η χρήση ενός μηχανισμού VPN είναι η καλύτερη και φτηνότερη δυνατή λύση. Στο χώρο της Πληροφορικής υπάρχουν αρκετές VPN υπηρεσίες και προγράμματα που προσφέρουν αυτή τη δυνατότητα δωρεάν, όπως το OpenVPN κ.α.

Στην περίπτωση του δήμου Αμαρουσίου, η ανάγκη για εγκατάσταση ενός VPN υπάρχει, αλλά όχι για όλο το δίκτυο. Πιο συγκεκριμένα, οι πιο σοβαρές επικοινωνίες αφορούν τα δεδομένα που ανταλλάσει ο δήμαρχος της περιοχής με τους συνεργάτες του από τον υπολογιστή που έχει στο γραφείο του. Αν θυμηθούμε από προηγούμενο κεφάλαιο, το subnet της διοίκησης χρειάζεται 10 IPs. Μία από αυτές ανήκει και στον δήμαρχο. Επειδή όμως και κάποιος από τους συνεργάτες του, όπως ο αντιδήμαρχος ή η γραμματέας του, μπορεί να θέλουν να επικοινωνήσουν μαζί του, ασφαλίζουμε και την δικιά τους επικοινωνία. Έτσι δεν επικεντρωνόμαστε μόνο στην IP που ανήκει στον υπολογιστή του δημάρχου, αλλά σε όλο το subnet της διοίκησης.

Το στήσιμο του VPN δεν είναι κάποια αρκετά πολύπλοκη διαδικασία. Αρκεί μόνο να γίνουν μερικές παραμετροποιήσεις στις συσκευές που θα συνδέονται σ' αυτό. Στην περίπτωση του δήμου δηλαδή, που θα καλύπτουμε με ασφαλή σύνδεση εικονικού δικτύου μόνο την διοίκηση, θα πρέπει να παραμετροποιήσουμε τους υπολογιστές που ανήκουν στο υποδίκτυο αυτό και τις συσκευές που θα επικοινωνούν με αυτούς (τους υπολογιστές), οι οποίοι μπορεί και να βρίσκονται εκτός δικτύου. Μετά από την παραμετροποίηση αυτή, ουσιαστικά το σετάρισμα των προγραμμάτων που προσφέρονται από την εκάστοτε VPN υπηρεσία, τότε μας μένει μόνο ένα σετάρισμα για την δρομολόγηση των πακέτων που θα έρχονται εκτός δικτύου (από το Διαδίκτυο) και θα θέλουν να "μιλήσουν" με το subnet που ανήκει το VPN.

Μία καλή τακτική για την αποφυγή προβλημάτων επικοινωνίας μέσω VPN, είναι να αποφεύγονται διευθύνσεις κλάσης C (IP), γιατί υπάρχουν μεγάλες πιθανότητες, αν για παράδειγμα χρησιμοποιούμε στην εταιρεία μας την IP 192.168.1.0 /24 για το δίκτυο μας και θέλουμε να συνδεθούμε από ένα καφέ από μία άλλη περιοχή, το καφέ, να έχει την ίδια IP για το δίκτυο του και ουσιαστικά να μην μπορεί ο απομακρυσμένος υπολογιστής να επικοινωνήσει με το δίκτυο της εταιρείας. Έτσι αν ο Α έχει την IP

192.168.1.13 και θέλει να στείλει μέσω VPN στον Β ο οποίος έχει την IP 192.168.1.136, όταν το router του δικτύου που βρίσκεται ο Α, διαβάσει στο πεδίο του destination IP την διεύθυνση 192.168.1.136, τότε θα ψάξει μέσα στο δικτυό του να τη βρει μέσω ARP request και αν αποτύχει, τότε το πακέτο θα απορριφθεί (drop). Αλλά και σε περίπτωση που στο LAN που βρίσκεται ο Α, υπάρχει αυτή η IP και πάλι θα απορριφθεί το πακέτο (αυτή την φορά από τον υπολογιστή με αυτή την IP), αφού δεν τον αφορά η πληροφορία αυτή. Βέβαια υπάρχουν διάφοροι τρόποι για να μην πέσουμε σε τέτοιες παγίδες. Ένας από αυτούς είναι να χρησιμοποιήσουμε κάποια IP πάνω στην οποία θα στήσουμε το δίκτυο μας, την οποία να μη την συναντάμε συχνά σε τοπικά δίκτυα. Ένας από τους λόγους που χρησιμοποιήσαμε την 10.10.10.0 /24 IP για το δίκτυο του δήμου Αμαρουσίου είναι αυτός.

Αναφέρουμε ότι βάσει IANA (Internet Assigned Numbers Authority), ένα εύρος διευθύνσεων IP έχει καταχωρηθεί ως ιδιωτικό (private) και καλύπτει τις ανάγκες IP που υπάρχουν για το κάθε LAN, λόγω έλλειψης διευθύνσεων στη γενιά IPv4. Και στη γενιά IPv6 υπάρχουν private διευθύνσεις, αλλά το πλήθος των IP που μπορούν να παραχθούν (2^128) είναι τόσο μεγάλο, που τις περισσότερες φορές δεν χρησιμοποιούνται.

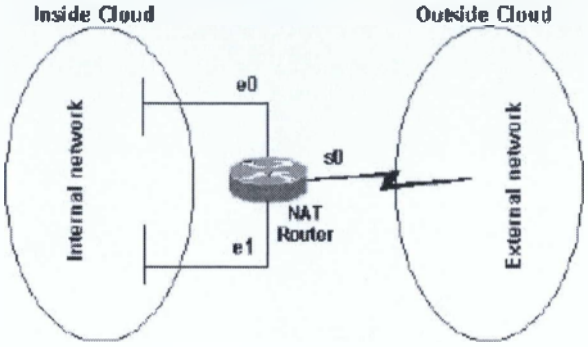
Πίνακας private IP διευθύνσεων της IPv4:

ΑΠΟ	ΕΩΣ	PREFIX - CLASS
10.0.0.0	10.255.255.255	10 /8 – CLASS A
172.16.0.0	172.31.255.255	172.16 /12 – CLASS B
192.168.0.0	192.168.0.0	192.168 /16 – CLASS C

Μία private διεύθυνση μπορεί να χρησιμοποιείται σε όλα τα τοπικά δίκτυα ανά τον κόσμο, χωρίς όμως να προκύπτει κάποιο πρόβλημα, αφού ποτέ(!) ένας υπολογιστής ή οποιαδήποτε συσκευή που μπορεί να συνδεθεί στο Διαδίκτυο, δεν χρησιμοποιεί μία private IP. Για να είμαστε πιο ακριβείς, δεν μπορεί να χρησιμοποιήσει μία τέτοια διεύθυνση. Η διαδικασία για την μετατροπή αυτή, δηλαδή η μετάφραση μίας οποιασδήποτε private IP, ενός οποιουδήποτε τοπικού δικτύου, σε μία IP η οποία μπορεί να χρησιμοποιηθεί στο Internet (public IP), γίνεται μέσω του NAT (Network Address Translation).

Θα ακολουθήσουμε την μέθοδο που χρησιμοποιεί το SSL, αλλά πριν από αυτό, θα πρέπει να πούμε δύο λόγια για τον τρόπο που θα περνάμε τα δεδομένα που αφορούν το VPN μέσα από το Cisco router. Για να το επιτύχουμε αυτό, θα χρησιμοποιήσουμε το NAT. Με το NAT μπορούμε να κάνουμε δύο (2) βασικά πράγματα σε ένα δρομολογητή. Το ένα είναι να μεταφράζουμε τις εσωτερικές IP του δικτύου (private) σε μία ή περισσότερες εξωτερικές IP (public), αφού οι πρώτες δεν μπορούν να βγουν εκτός LAN. Το δεύτερο που μπορούμε να κάνουμε είναι η προώθηση πακέτων βάσει πρωτοκόλλων, θυρών κτλ. Στην περίπτωση μας, που θα παίξουμε με VPN στο δίκτυο του δήμου, πρέπει να καλύψουμε αυτό το κενό, αφού αν στήσιμουμε το VPN, στη συνέχεια δεν θα μπορούμε να έχουμε επικοινωνία με αυτό από υπολογιστές που βρίσκονται εκτός δικτύου, γιατί θα έρχονται πακέτα στο δρομολογητή, αλλά αυτός δεν θα ξέρει πως να τα διαχειριστεί. Για να ρυθμίσουμε το NAT, πρέπει πρώτα να καταλάβουμε τη διαφορά του NAT inside και του NAT outside. Ουσιατικά με αυτές τις δύο (2) παραμέτρους, δίνουμε στο NAT να καταλάβει στις θύρες που το ενεργοποιούμε, αν αυτές οι θύρες ανήκουν στο LAN ή στο

εξωτερικό δίκυο (Internet). Έτσι μία θύρα Fa που ανήκει στο LAN, θα πάρει την παράμετρο NAT inside, ενώ αντίστοιχα μία θύρα Se, που ανήκει εκτός του κομματιού του LAN, θα πάρει την παράμετρο NAT outside.

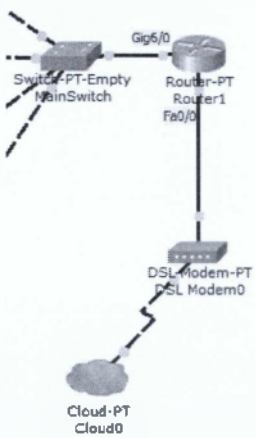


Εικ. 6.2 e0 & e1 NAT inside, s0 NAT outside

Έτσι και στο παραπάνω σχήμα, βλέπουμε πως οι δύο Ethernet θύρες που ανήκουν στο εσωτερικό δίκτυο, παίρνουν την παράμετρο inside, ενώ η μοναδική Serial θύρα που συνδέει το εσωτερικό δίκτυο με το Internet, παίρνει την παράμετρο outside.

Αφού αναλύσαμε με λίγα λόγια το NAT και τη λειτουργία του, πάμε να δούμε το σετ εντολών που χρειάζονται για να το ενεργοποιήσουμε στο router του δήμου. Για να περάσουμε τις εντολές του NAT πρέπει να δούμε σε ποια interfaces θέλουμε να ενεργοποιηθούν.

Στη διπλανή εικόνα βλέπουμε τα δύο ενεργά interfaces του router. Και στα δύο (2) αυτά interfaces θέλουμε να ενεργοποιήσουμε το NAT, αφού το ένα Gig6/0 είναι αυτό που συνδέεται με το δίκτυο του δήμου Αμαρουσίου, ενώ το άλλο, δηλαδή το Fa0/0, είναι αυτό που συνδέεται με το DSL-modem και κατ' επέκταση με το Διαδίκτυο. Οι εντολές που θα χρησιμοποιήσουμε είναι τρεις (3) και είναι οι εξής:



Router(config-if)#ip nat inside

Router(config-if)#ip nat outside

Router(config)#ip nat outside static udp 71.31.200.38 2324 10.10.10.205 1194

Εικ. 6.3 Router interfaces

Την πρώτη εντολή την τρέχουμε στο interface Gig6/0 του router και με αυτό τον τρόπο του γνωστοποιούμε πως για το NAT, αυτή η θύρα συνδέεται στο LAN. Τη δεύτερη εντολή την τρέχουμε στο interface Fa0/0 του router και ορίζουμε στο NAT πως αυτή η θύρα συνδέεται εκτός του LAN. Στην τρίτη και τελευταία εντολή, ορίζουμε πως από την static public IP 71.31.200.38 με αίτημα για πόρτα 2324 (UDP), θα γίνεται μετάφραση αυτής της IP στην 10.10.10.205 στην πόρτα 1194. Γιατί όμως κάνουμε αυτή την μετάφραση; Ο δήμος Αμαρουσίου για λόγους σταθερότητας έχει αγοράσει (ενοικιάσει) μερικές public IP. Μία από αυτές είναι και η 71.31.200.38. Έτσι στην κινητή συσκευή που χρησιμοποιεί ο αντιδήμαρχος και θέλει να επικοινωνεί μέσω αυτής με τον δήμαρχο όταν βρίσκεται εκτός του κτηρίου, ο αντιδήμαρχος έχει σαν IP την 71.31.200.38. Επίσης έχουμε ρυθμίσει το VPN να μην ακολουθεί κάποια standard πόρτα για την υπηρεσία, αλλά μία τυχαία, την 2324, για λόγους ασφαλείας. Έτσι με την τελευταία εντολή, ουσιαστικά ορίζουμε πως σε περίπτωση που έρθει πακέτο από το interface Fa0/0, το οποίο θα έχει σαν IP (source IP) την static public IP που αναφέραμε παραπάνω και επίσης θέλει κάποια υπηρεσία που εξυπηρετείται από την πόρτα 2324, να προωθείται το πακέτο αυτό στον υπολογιστή με IP 10.10.10.205, σε έναν υπολογιστή δηλαδή που υπάρχει στο υποδίκτυο της Διοίκησης και λειτουργεί σαν VPN Server.

6.3 Εγκατάσταση Δικτύου και Παραμετροποίηση Συσκευών

Αφού είδαμε την γενική φιλοσοφία που θα ακολουθήσουμε στο δίκτυο του δήμου Αμαρουσίου, προχωράμε στο σετάρισμα των συσκευών και στο πέρασμα των IP διευθύνσεων στις συσκευές των υπαλλήλων που συνδέονται στα υποδίκτυα των τμημάτων. Έχουμε ήδη δει πως το κάθε υποδίκτυο ανήκει και σε διαφορετικά VLAN και υλοποιήσαμε την τοπολογία Router-on-a-stick. Όταν έχουμε κάποιο δρομολογητή (router) στο δίκτυο μας και αυτό χωρίζεται σε διάφορα υποδίκτυα, μπορούμε να διασυνδέσουμε τα υποδίκτυα αυτά με δύο τρόπους. Ο ένας είναι ο "κλασικός" τρόπος, στον οποίο συνδέουμε ανά interface του router και ένα υποδίκτυο και ο άλλος είναι η τοπολογία Router-on-a-stick. Σ' αυτή την περίπτωση, σε ένα φυσικό interface του δρομολογητή συνδέουμε όλα τα υποδίκτυα. Αυτό γίνεται διαιρώντας το φυσικό interface σε όσα λογικά interfaces θέλουμε (μέχρι 99). Πρακτικά αυτό σημαίνει πως σε μία μόνο θύρα του δρομολογητή, μπορούμε να συνδέσουμε μέχρι και 99 υποδίκτυα. Κάτι τέτοιο βέβαια μπορεί να γίνεται, αλλά πρακτικά ο φόρτος κίνησης θα είναι τόσο μεγάλος που ουσιαστικά η θύρα αυτή θα μπουκώσει και θα έχουμε πολύ μεγάλες καθυστερήσεις. Στη τοπολογία όμως που υλοποιήσαμε και στην μελέτη που κάναμε πριν προχωρήσουμε στο στήσιμο του δικτύου, υπολογίσαμε πως χρειαζόμαστε εννέα (9) VLAN. Αυτό το νούμερο δεν είναι απαγορευτικό για την τοπολογία Router-on-a-stick και έτσι ακολουθήσαμε αυτή την υλοποίηση. Μέσω αυτής της υλοποίησης, γλιτώνουμε και αρκετά χρήματα, αφού αφαιρούμε από τον προϋπολογισμό του δικτύου οχτώ (8) έξτρα interfaces που θα χρειαζόμασταν, σε περίπτωση που υλοποιούσαμε την κλασική τοπολογία που είναι υποδίκτυο ανά θύρα.

Σε ένα Cisco Router για να υλοποιήσουμε το Router-on-a-stick, χρειάζονται οι παρακάτω εντολές:

(config)#interface gig6/0.10

(config-if)#encapsulation dot1Q 10

(config-if)#ip address 10.10.10.206 255.255.255.240

Με την πρώτη εντολή, πηγαίνουμε στο **φυσικό** interface Gigabit6/0 και στο **λογικό** interface .10. Το .10 είναι μία τυπική ονομασία. Η λογική που ακολουθούμε για λόγους ευκολίας στον εντοπισμό του εκάστοτε λογικού interface, είναι το νούμερο που ακολουθεί μετά την τελεία να είναι το ίδιο με το νούμερο που αντιστοιχεί στο VLAN που εκπροσωπεί αυτό το interface. Έτσι στην προκειμένη περίπτωση, παραμετροποιούμε το λογικό interface που αφορά το VLAN 10.

Στη δεύτερη εντολή, δίνουμε τον τύπο του encapsulation (ενθυλάκωσης). Είναι ο τρόπος που ανοίγονται τα πακέτα δεδομένων και στη συνέχεια ο τρόπος με τον οποίο διαβάζονται και στη συνέχεια μετά από μερικές αλλαγές που ενδέχεται να γίνουν, ο δρομολογητής τα "ξαναπακετάρει" και τα στέλνει στη θύρα που πρέπει, για να συνεχίσουν την πορεία τους μέχρι τον τελικό αποστολέα. Το dot1Q είναι το γενικό πρότυπο ενθυλάκωσης που ακολουθείται από όλες τις συσκευές δικτύων (Cisco και μη). Επίσης, στο τέλος της εντολής, βλέπουμε το νούμερο 10. Αυτός ο αριθμός αφορά το VLAN. Οπότε ουσιαστικά ορίζουμε πως για κάθε πακέτο στο VLAN 10, θα ακολουθείται η ενθυλάκωση dot1Q.

Στην τρίτη και τελευταία εντολή, δίνουμε την IP της θύρας και τη μάσκα δικτύου. Ουσιαστικά η IP αυτή είναι η προεπιλεγμένη πύλη (default gateway) που θα ορίσουμε σε όλους τους κόμβους που ανήκουν στο VLAN 10.

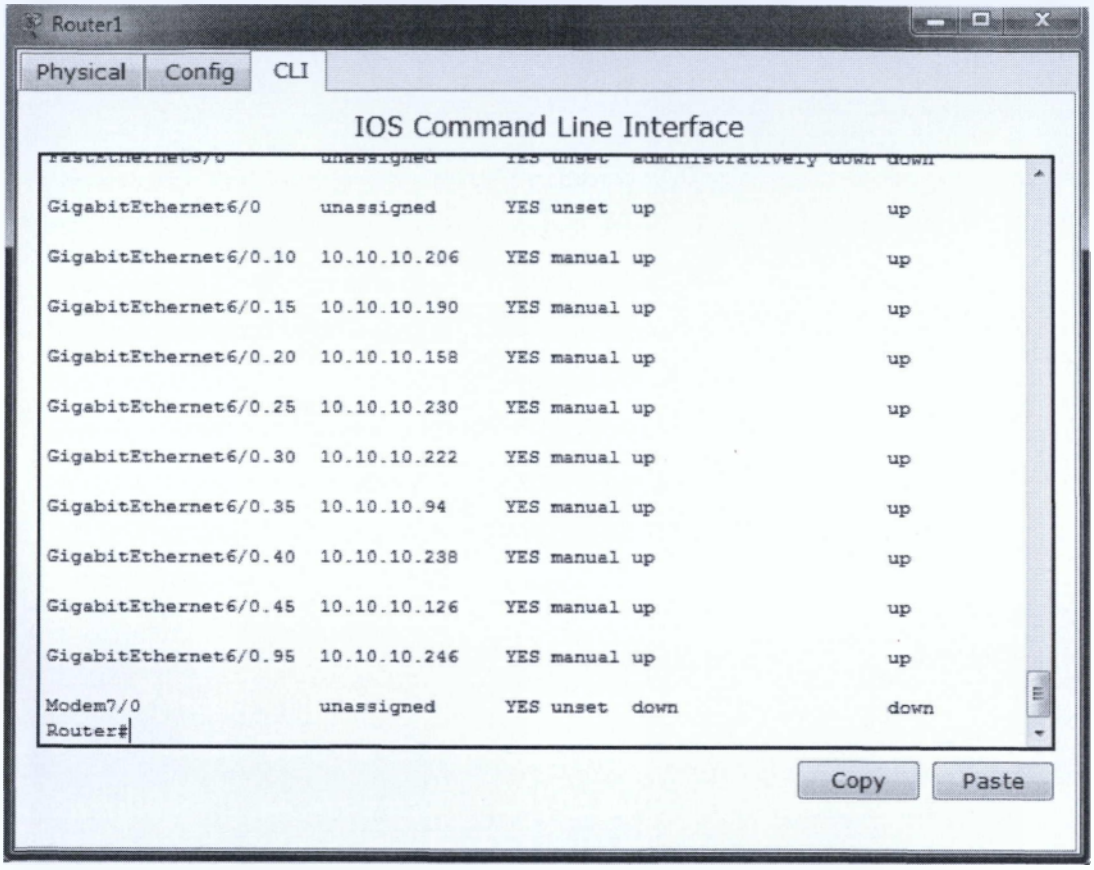
Αναφέρουμε πως για λόγους "αρχιτεκτονικής" του δικτύου και για ευκολότερο troubleshooting σε περίπτωση κάποιου προβλήματος, ακολουθείται κάποια λογική σε όλα τα υποδίκτυα και την διευθυνσιοδότησή τους. Η λογική αυτή λέει, πως σε κάθε υποδίκτυο, σαν default gateway θα ορίζουμε την πρώτη ή την τελευταία IP από τις διαθέσιμες IP που έχουμε. Στην εργασία αυτή, σε κάθε υποδίκτυο ορίζουμε ως προεπιλεγμένη πύλη την τελευταία διαθέσιμη IP του εκάστοτε υποδικτύου.

Στον πίνακα που ακολουθεί, μπορούμε να δούμε την default gateway όλων των υποδικτύων και επίσης και τη μάσκα υποδικτύου.

ΤΜΗΜΑ	ΠΡΟΕΠΙΛΕΓΜΕΝΗ ΠΥΛΗ	ΜΑΣΚΑ ΥΠΟΔΙΚΤΥΟΥ
ΔΙΟΙΚΗΣΗΣ	10.10.10.206	255.255.255.240 /28
ΓΡΑΜΜΑΤΕΙΑΣ	10.10.10.190	255.255.255.224 /27
IT / Τεχνικών	10.10.10.158	255.255.255.224 /27
ΠΡΩΤΟΚΟΛΛΟΥ	10.10.10.230	255.255.255.248 /29
ΛΟΓΙΣΤΗΡΙΟΥ	10.10.10.222	255.255.255.240 /28
ΔΗΜ. ΑΣΤΥΝΟΜΙΑΣ	10.10.10.94	255.255.255.224 /27
ΠΛΗΡΟΦΟΡΙΩΝ	10.10.10.238	255.255.255.248 /29
ΕΞΥΠΗΡΕΤΗΣΗΣ	10.10.10.126	255.255.255.224 /27
SERVERS	10.10.10.246	255.255.255.248 /29

Να αναφέρουμε εδώ, πως τις τρεις (3) εντολές που αναλύσαμε παραπάνω, για τον τρόπο με τον οποίο μπορούμε να δημιουργήσουμε λογικά interfaces σε ένα δρομολογητή για τις ανάγκες της τοπολογίας Router-on-a-stick, πρέπει να τις χρησιμοποιήσουμε για όλα τα VLAN που θέλουμε να "περνάνε" μέσα από το router. Υπενθυμίζουμε, πως τα υποδίκτυα και τα VLAN, σε περίπτωση που δεν υπάρχει

δρομολογητής ή ένα switch L3 (τα Layer 3 switches έχουν δυνατότητες δρομολόγησης), τότε τα υποδίκτυα δεν μπορούν να επικοινωνήσουν μεταξύ τους.

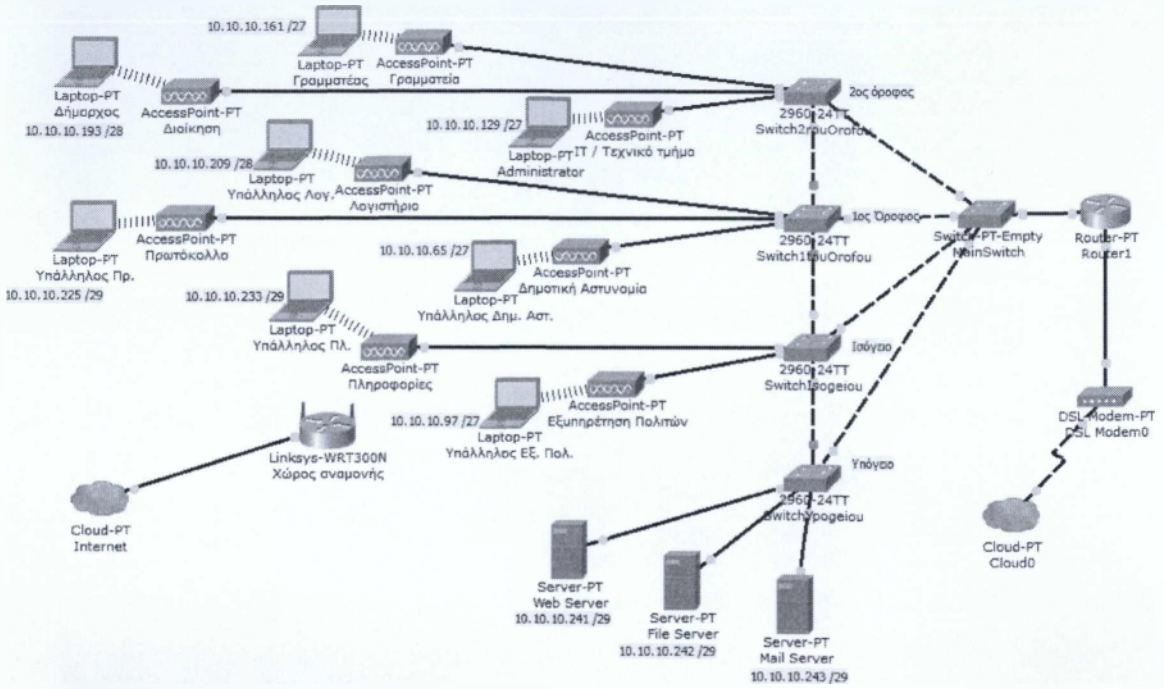


Εικ. 6.4 Εμφάνιση όλως των λογικών θυρών του router με την εντολή #sh ip interface brief

Όπως βλέπουμε παραπάνω, με την εντολή **#show ip interface brief** έχουμε μία πλήρη εικόνα για τις θύρες του δρομολογητή. Επίσης εκτός από τις φυσικές θύρες, βλέπουμε και τα λογικά interfaces που δημιουργήσαμε για τις ανάγκες της τοπολογίας μας. Έτσι έχουμε στη θύρα gig6/0, εννέα λογικά interfaces, για τα οποία λόγω της λογικής ονομασίας που χρησιμοποιήσαμε, μπορούμε εύκολα να καταλάβουμε για ποιο VLAN υπάρχει το κάθε ένα interface. Επίσης, μέσω αυτής της εντολής, βλέπουμε ποια IP έχει το κάθε interface (φυσικό ή λογικό) και αν είναι ενεργοποιημένο. Σημειώνουμε εδώ πως στους δρομολογητές της Cisco, από default, όλες οι θύρες είναι απερνεργοποιημένες (Administratively down).

Αν συνδυάσουμε τα δεδομένα που έχουμε από τον πίνακα με τις προεπιλεγμένες πύλες και τις πληροφορίες που παίρνουμε από το router, όσον αφορά στις θύρες του, τότε βλέπουμε πως όντως, το τμήμα της Διοίκησης, που ανήκει στο VLAN 10, έχει ως default gateway την IP 10.10.10.206, δηλαδή την IP που υπάρχει στο λογικό interface gig6/0.10.

Η εικόνα που ακολουθεί, μας δείχνει την πλήρη επικοινωνία μεταξύ των συσκευών του δικτύου του δήμου Αμαρουσίου.



Εικ. 6.5 Τελική τοπολογία και πλήρης κάλυψη των κόμβων όλων των υποδικτύων

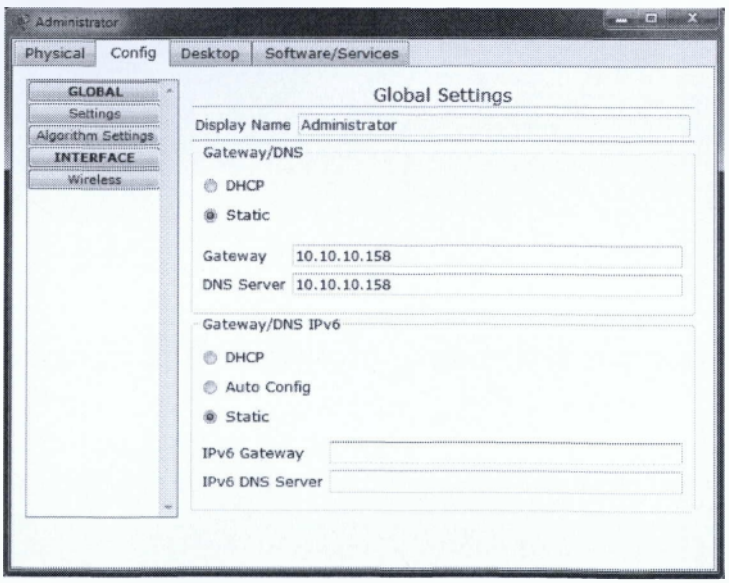
Όπως βλέπετε παραπάνω, όλες οι συσκευές του δήμου συνδέονται κανονικά με τα Access Points που ανήκουν και υπάρχει πλήρης κάλυψη. Για τις ανάγκες της παρουσίασης του δικτύου, προσθέσαμε απλά μία συσκευή ανά VLAN ή μία συσκευή ανά υποδίκτυο ή μία συσκευή ανά Access Point. Επίσης, αν παρατηρήσουμε την εικόνα, βλέπουμε και τη IP που έχουμε δώσει στη κάθε συσκευή και μέσω του πίνακα των IP που δείξαμε στο προηγούμενο υποκεφάλαιο, οι IP που βλέπουμε είναι οι πρώτες IP ελεύθερες προς χρήση, που ανήκουν στο εκάστοτε subnet. Πριν όμως προχωρήσουμε στην ανάλυση της διασύνδεσης των συσκευών καλό θα ήταν να δούμε τις ρυθμίσεις των Access Points. Με την λέξη ρυθμίσεις, εννοούμε το SSID, το κανάλι, την πιστοποίηση, τη μέθοδο κρυπτογράφησης και το κλειδί ασφαλείας. Ακολουθεί πίνακας με όλα αυτά τα δεδομένα.

ACCESS POINT	SSID	ΚΑΝΑΛΙ	ΠΙΣΤΟΠΟΙΗΣΗ	ΚΡΥΠΤΟΓΡΑΦΗΣΗ	ΚΛΕΙΔΙ
ΔΙΟΙΚΗΣΗΣ	Dioikisi	1	WPA2-PSK	AES	*tm1m4Di01ki515!
ΓΡΑΜΜΑΤΕΙΑΣ	Grammateia	6	WPA2-PSK	AES	*gr4mmAt314d1m0U$
IT	IT	11	WPA2-PSK	AES	*tm1m4T3Xn1kWn017#
ΠΡΩΤΟΚΟΛΛΟΥ	Protokollo	6	WPA2-PSK	AES	*prWt0KoLL0d1moU83^

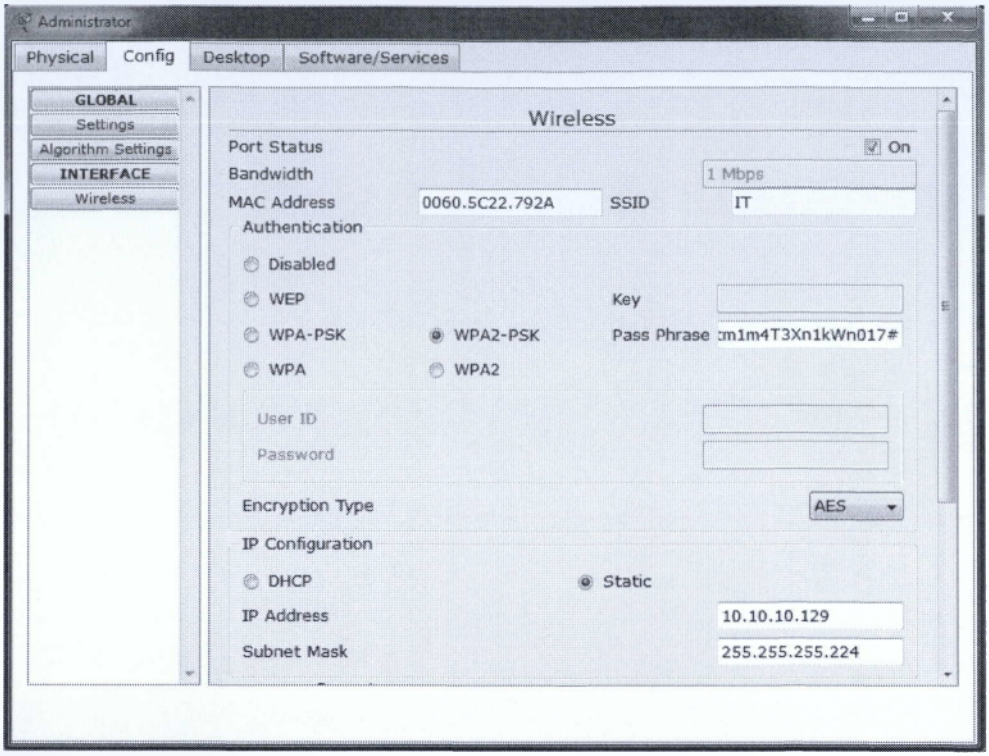
ΛΟΓΙΣΤΗΡΙΟΥ	Logistirio	1	WPA2-PSK	AES	*tM1m4l0G15t1Ri0U19#
ΔΗΜ. ΑΣΤΥΝΟΜΙΑΣ	Dim. Astynomia	11	WPA2-PSK	AES	*mUN1c1P4lp0l1c3D&
ΠΛΗΡΟΦΟΡΙΩΝ	Plirofories	1	WPA2-PSK	AES	*dim051Nf0m4rU5i70@
ΕΞΥΠΗΡΕΤΗΣΗΣ	Eksypiretisi	6	WPA2-PSK	AES	*ek5yp1R3ti51d1M0U?

Όπως βλέπουμε στον πίνακα για τα κλειδιά, χρησιμοποιήσαμε την τεχνική που περιγράψαμε σε προηγούμενο κεφάλαιο. Χρησιμοποιήσαμε πεζά και κεφαλαία γράμματα (όχι στην αρχή της λέξης), νούμερα, ελίτ γραφή και ειδικούς χαρακτήρες στην αρχή και στο τέλος των κωδικών. Επίσης, αν συνδυάσουμε τα κανάλια όπως φαίνονται στον πίνακα αυτό, με την τοποθέτηση των AP στο χώρο, βλέπουμε πως δεν υπάρχουν γειτονικά AP που να λειτουργούν στο ίδιο κανάλι, αλλά ούτε και σε διαφορά καναλιών μικρότερη των πέντε (5). Αυτό σημαίνει πως δεν έχουμε απώλειες σήματος και παρεμβολές. Τέλος, σε όλα τα AP, χρησιμοποιήσαμε σαν μέθοδο πιστοποίησης το WPA2-PSK και σαν μέθοδο κρυπτογράφησης τον AES, καθώς αυτός είναι ο πιο δυνατός συνδιασμός ασφαλείας που μπορούμε να επιτύχουμε, πέραν από ένα αρκετά δυνατό κλειδί.

Για μία καλύτερη εικόνα του στησίματος των συσκευών, παραθέτουμε δύο ενδεικτικά screenshot από τις ρυθμίσεις που πραγματοποιήσαμε σε ένα laptop που συνδέεται στο AP του IT.



Εικ. 6.6 Gateway & DNS του υπολογιστή



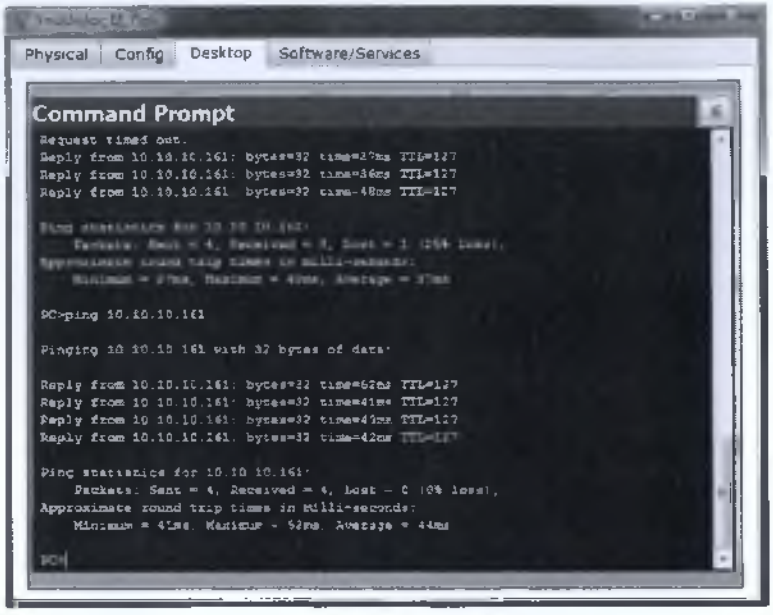
Εικ. 6.7 Ρυθμίσεις σύνδεσης και IP υπολογιστή

Στις εικόνες 6.4 και 6.5 βλέπουμε την παραμετροποίηση των ρυθμίσεων του υπολογιστή του Administrator στο τμήμα του IT που συνδέεται στο αντίστοιχο AP. Στην εικόνα 6.4 βλέπουμε την ρύθμιση του default gateway, που είναι το 10.10.10.158 και του DNS Server που είναι η ίδια IP. Το DNS (Domain Name Translation), είναι η υπηρεσία που μεταφράζει τα URLs στις IP διευθύνσεις που ανήκουν. Στην δεύτερη εικόνα, βλέπουμε πως σαν SSID που θέλει ο υπολογιστής να συνδεθεί, έχουμε ορίσει το "IT", σαν μέθοδο πιστοποίησης το "WPA2-PSK", με κλειδί εισόδου το "*tm1m4T3Xn1kWn017#" και μέθοδο κρυπτογράφησης τον "AES". Τέλος, χειροκίνητα και όχι μέσω DHCP, δώσαμε την IP "10.10.10.129", που είναι η πρώτη διαθέσιμη του συγκεκριμένου subnet και η μάσκα υποδικτύου που δώσαμε είναι η "255.255.255.224", όπως δηλαδή προκύπτει από τη μελέτη VLSM που κάναμε για τη δημιουργία του κάθε υποδικτύου. Ο λόγος που στήνουμε το δίκτυο μας χωρίς DHCP είναι πρώτον, γιατί το πλήθος των υπολογιστών δεν είναι αρκετά μεγάλο και δεύτερον, με στατικές διευθύνσεις μπορούμε να έχουμε και καλύτερη ανάθεση IP διευθύνσεων και καλύτερο έλεγχο (ευκολότερο) για την κίνηση του κάθε υπολογιστή σε περίπτωση έρευνας στο δίκτυό μας.

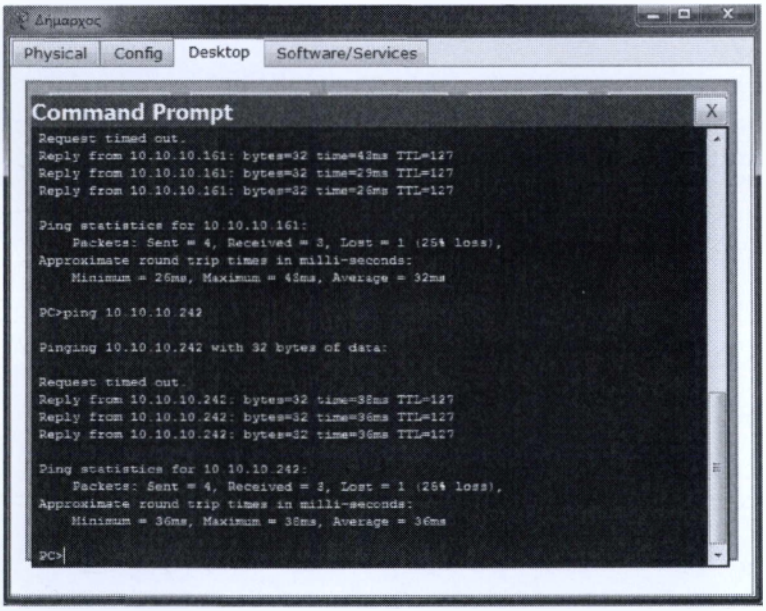
Οι τροποποιήσεις των υπόλοιπων υπολογιστών του δικτύου βασίζονται στις ρυθμίσεις που είδαμε στις δύο (2) παραπάνω εικόνες, με τη διαφορά ότι αλλάζουν φυσικά οι πληροφορίες που βάζουμε. Η λογική παραμένει η ίδια.

Αφού είδαμε και το στήσιμο των AP που υπάρχουν στον κάθε όροφο, πλέον μπορούμε να τσεκάρουμε αν όντως όλα αυτά λειτουργούν. Θεωρητικά, το δίκτυό μας, πρέπει να λειτουργεί κανονικά. Για να

ελέγξουμε με τον πιο εύκολο τρόπο αν οι συσκευές βλέπουν η μία την άλλη στο δίκτυο, το πιο απλό πράγμα που μπορούμε να κάνουμε είναι να αρχίσουμε να κάνουμε διάφορα pings.



Εικ. 6.8 Ping από υπολογιστή υπαλλήλου Εξυπηρέτησης στον υπολογιστή της γραμματέως



Εικ. 6.9 Ping από τον υπολογιστή του Δημάρχου στο File Server

Όπως μπορούμε να δούμε στις δύο αυτές εικόνες τα pings που δοκιμάσαμε λειτουργούν κανονικά. Επίσης για να σιγουρέψουμε πως και η τοπολογία Router-on-a-stick, λειτουργεί κι αυτή κανονικά, φροντίσαμε να κάνουμε ping από ξεχωριστά subnets, ώστε η κίνηση να χρειαστεί να περάσει μέσα και

από το router. Όταν μιλάμε για το ίδιο VLAN, τότε το πακέτο δεν χρειάζεται να επεξεργαστεί από το δρομολογητή. Έτσι, αν για παράδειγμα ο υπολογιστής ενός υπαλλήλου από την Εξυπηρέτηση, έκανε ένα ping σε έναν άλλο υπολογιστή που ανήκει κι αυτός στο VLAN της εξυπηρέτησης, τότε το πακέτο θα έφτανε μέχρι το switch, θα γινόταν decapsulate, θα έλεγχε τη destination mac address, θα την έβρισκε στο ARP table που υπάρχει στο switch και έτσι θα ήξερε σε ποιο port θα έπρεπε να αποστείλει το πακέτο. Εκτός από αυτό, θα έβλεπε επίσης και σε ποιο VLAN ανήκει ο αποστολέας και σε ποιο VLAN θέλει να στείλει το πακέτο του. Με αυτό τον συνδυασμό δεν χρειαζόταν το πακέτο να μεταφερθεί σε συσκευή ανώτερου layer (router layer 3 device), αφού το switch (layer 2 device), θα ήξερε πως να διαχειριστεί το πακέτο που έλαβε από τον συγκεκριμένο υπολογιστή. Τώρα όμως, από την στιγμή που δεν έχει κάποια mac address καταχωρημένη στο ARP table του και το VLAN που θέλει να σταλεί το πακέτο, δεν έχει κάποιο ενεργό port πάνω σε αυτό το switch, τότε περνάει την πληροφορία στο router και εκείνο μετά από τους ελέγχους που κάνει, προωθεί ή καταστρέφει (drop) το πακέτο. Από τη στιγμή που τα pings που κάναμε παραπάνω λειτουργούν κανονικά και δεν έχουμε κάποιο time out ή αδυναμία απάντησης, αυτό σημαίνει πως το δίκτυό μας λειτουργεί κανονικά και η δρομολόγηση των πακέτων γίνεται σωστά.

6.4 Εγκατάσταση IDS - IPS

Όπως αναφέραμε και στο προηγούμενο κεφάλαιο, μία ακόμη καλή μέθοδος προστασίας του δικτύου μας είναι η εγκατάσταση ενός IDP ή ενός IPS συστήματος. Αυτό μπορεί να γίνει είτε μέσω hardware είτε μέσω software. Στην περίπτωση του δήμου, θα τοποθετήσουμε ένα IDS/IPS σύστημα σε έναν υπολογιστή που βρίσκεται στο τμήμα του IT ή μπορούμε να συνδέσουμε κάποιο laptop στο Main Switch (απ' όπου δηλαδή περνάει όλη η κίνηση του δικτύου). Αυτό το μηχάνημα ουσιαστικά μπορούμε να του ορίσουμε να διαβάζει την κίνηση του δικτύου σε όποια κομμάτια θέλουμε και βάσει όποιων πρωτοκόλλων θέλουμε και να προχωράει στις ενέργειες που θα του δώσουμε. Μία καλή λύση, για την οποία επίσης δεν χρειάζεται να γίνουν κάποια οικονομικά έξοδα, είναι το SNORT. Το συγκεκριμένο εργαλείο μπορούμε να το κατεβάσουμε ελεύθερα και να το διαχειριστούμε όπως θέλουμε. Το μεγάλο του πλεονέκτημα επίσης, είναι πως μπορεί να λειτουργήσει και ως IDS αλλά και ως IPS. Υπενθυμίζουμε πως τα IDS συστήματα, απλά εμφανίζουν κάποια alerts και δεν κάνουν κάτι παραπάνω, ενώ τα IPS συστήματα μπορούμε να τα ρυθμίσουμε στο να προχωρήσουν ένα βήμα παρακάτω, όπως π.χ. να κλείσουν την κίνηση από κάποια IP κτλ. Η διαδικασία παραμετροποίησης του SNORT είναι λίγο περίπλοκη, αφού για να περάσουμε τις παραμέτρους που θέλουμε για τον έλεγχο του δικτύου μας και να υποδείξουμε τις κινήσεις που θέλουμε να ακολουθήσουν σε περίπτωση παραβίασης ή επίθεσης στο δίκτυο μας, πρέπει να διαβάσουμε αρκετά καλά το manual του προγράμματος και θα χρειαστεί να επεξεργαστούμε συγκεκριμένα αρχεία. Δεν υπάρχει κάποιο GUI (Graphical User Interface) που να μας βοηθάει στο να κάνουμε αυτές τις ενέργειες. Ας δούμε τα βασικά της παραμετροποίησης του συγκεκριμένου εργαλείου.

Το βασικό του SNORT, είναι ότι μπορούμε να δημιουργήσουμε τους δικούς μας κανόνες. Έτσι δεν ακολουθούμε κάποια standards που μπορεί να επιβαρύνουν είτε το δίκτυο μας, είτε να είναι περιττά για τις ανάγκες μας. Εμάς, όπως περιγράψαμε και σε προηγούμενο κεφάλαιο, μας ενδιαφέρει να μπλοκάρουμε και να ελέγχουμε τις προσπάθειες για TELNET συνδέσεις εκτός και εντός του δικτύου. Είναι βέβαια ένας εύκολος τρόπος να παραμετροποιήσουμε συσκευές από απόσταση, αλλά κάτι τέτοιο

μας είναι ανούσιο στην περίπτωση του δήμου, αφού τα περισσότερα άτομα που εργάζονται στο IT, παραμένουν στο κτήριο όλες τις ώρες λειτουργίας του δημαρχείου. Έτσι προτιμούμε να εφαρμόσουμε μια πολιτική ασφαλείας που θα αφήνει εκτός τις TELNET συνδέσεις και έτσι θα κλείνουμε μία πιθανή τρύπα ασφαλείας για το δίκτυο μας. Στο παράρτημα των εντολών και των configuration των δικτυακών Cisco συσκευών, θα δούμε πώς μπορούμε να απενεργοποιήσουμε τις TELNET συνδέσεις και άλλες οι οποίες αν δεν τις χρησιμοποιούμε είναι περιττό να είναι ανοιχτές, και επίσης πώς μπορούμε να συνδεόμαστε μέσω SSH για απομακρυσμένη σύνδεση.

Δημιουργία κανόνων στο SNORT:

Για τη δημιουργία ενός κανόνα στο SNORT, χρησιμοποιούμε την εξής εντολή:

**alert tcp any any -> 192.168.1.0/24 111 **
(content:"|00 01 86 a5|"; msg:"mountd access";)

Με την εντολή αυτή ορίζουμε πως οποιοδήποτε TCP πακέτο έχει προορισμό το δίκτυο 192.168.1.0 /24, να ενεργοποιεί ένα alert με το μήνυμα "mountd access". Η πρώτη λέξη της εντολής αυτής είναι "alert" και ουσιαστικά προσδιορίζει τι πρέπει να γίνει με την εκάστοτε περίπτωση πακέτου. Αντί αυτής της λέξης μπορούμε να ορίσουμε πολλά πράγματα που μπορεί να μας ενδιαφέρουν και διαφορετικές μεθόδους και τρόπους αντίδρασης. Στην περίπτωση που θέλουμε να απενεργοποιήσουμε τα ping που μπορεί να θέλει να κάνει κάποιος επιτιθέμενος προς οποιονδήποτε σταθμό του δικτύου μας, πακέτα δεδομένων που βασίζονται στο ICMP (Internet Control Message Protocol), μπορούμε να βάλουμε την ακόλουθη εντολή:

**reject udp any any -> 10.10.10.240/29 111 **

Έτσι με αυτή την εντολή, σε περίπτωση που κάποιος θέλει να κάνει κάποιο ping στις συσκευές που βρίσκονται στο υποδίκτυο των Servers, θα σταλεί μήνυμα στον αποστολέα (πιθανός επιτιθέμενος) με το ICMP message "port unreachable". Έτσι μπορεί να υποθέσει πως ο υπολογιστής είναι εκτός λειτουργίας ή δεν χρησιμοποιείται η IP που χρησιμοποιήσε. Οπότε την παραπάνω εντολή θα την χρησιμοποιήσουμε για όλους τους κόμβους που βρίσκονται στο δίκτυο μας. Θα χρειαστεί δηλαδή να τη συντάξουμε εννέα (9) φορές, μία δηλαδή για κάθε υποδίκτυο. Έτσι θα αποκλείσουμε κάποια DDoS (Distributed-Denial-of-Service) επίθεση. Οι DDoS επιθέσεις έχουν να κάνουν με καταιγισμό αιτημάτων σε έναν υπολογιστή, που λόγω των πολλών αυτών αιτημάτων δεν προλαβαίνει να ανταποκριθεί και έτσι κάποιος που θα προσπαθήσει να συνδεθεί αργότερα δεν θα μπορεί γιατί ο υπολογιστής θα ασχολείται ακόμη με τα προηγούμενα αιτήματα που έχουν γίνει προς αυτόν, και η υπηρεσία θα φαίνεται κλειστή. Με απλά λόγια, όλα αυτά τα πακέτα που έχουν σταλεί από ένα πλήθος υπολογιστών, μπλοκάρουν την είσοδο σε άλλους υπολογιστές. Βέβαια κάτι τέτοιο δεν μπορεί να αποκλειστεί σαν πιθανότητα επίθεσης από κάποιον, απλά μειώνει τις πιθανότητες εύκολης εύρεσης της IP που θέλει να βρει ο επιτιθέμενος. Επίσης, με όλα αυτά τα "port unreachable" μηνύματα που θα λάβει, θα χρειαστεί κι άλλο χρόνο μέχρι να βρει το τι φταίει. Έτσι αν προσθέσουμε την εντολή του reject σε συνδυασμό με το alert, το τμήμα του IT θα δει ότι γίνονται αρκετές προσπάθειες μέσω pings και έτσι θα μπορέσει να πάρει τα κατάλληλα μέτρα.

Οπότε ουσιαστικά με τον συνδυασμό των δύο (2) παραπάνω εντολών μπορούμε να έχουμε μία βασική ειδοποίηση και μία μέθοδο που θα ακολουθείται σε προσπάθειες ping για εντοπισμούς των IP που χρησιμοποιούνται στο δίκτυο. Με αυτό τον απλό τρόπο, μπορούμε να συμβάλουμε αισθητά στην καλύτερη ασφάλεια του δικτύου μας. Το laptop που θα σετάρουμε με το SNORT, θα το τοποθετήσουμε στο Main Switch και από εκεί θα φιλτράρουμε όλα τα πακέτα που περνάνε από το δίκτυό μας. Αυτό που μόλις κάναμε με το συγκεκριμένο εργαλείο, θα μπορούσαμε απλά να το μπλοκάρουμε μέσω κάποιας ACL που θα τοποθετούσαμε στο δρομολογητή του δικτύου μας, αλλά σε εκείνη την περίπτωση η ανάγνωση των log files που παράγονται, γίνεται πολύ πιο σπάνια και έτσι θα μπορούσε το δίκτυο να τεθεί σε κίνδυνο εισβολής και να μην το γνωρίζει κανείς. Ποτέ δεν πρέπει να ξεχνάμε τον ανθρώπινο παράγοντα, που ειδικά σε θέματα ασφαλείας παίζει αρκετά μεγάλο ρόλο, όπως τονίσαμε τόσες φορές και στα προηγούμενα κεφάλαια της εργασίας.

7. Συμπεράσματα

7.1 Αποτελέσματα Εργασίας

Με την ολοκλήρωση αυτής της εργασίας έχουμε συλλέξει κάποιες πληροφορίες οι οποίες πρέπει να αναφερθούν. Πρώτον, η ασφάλεια ενός δικτύου και ενός Πληροφοριακού Συστήματος βασίζεται και στο προσωπικό που εργάζεται σ' αυτό και πρέπει να είναι πάντα ενημερωμένο.

Δεύτερον, η ασφάλεια του δικτύου βασίζεται και στις παραμέτρους και στα μέτρα που ορίζουμε για το δίκτυο μας ως κάποια έξτρα ασφάλεια. Έτσι εκτός από ένα μεγάλο κωδικό π.χ. που μπορεί να ορίσουμε για διάφορα κομμάτια του δικτύου μας, πρέπει να ακολουθούνται κάποιες πολιτικές γι' αυτό, ώστε να μην μπορεί να παραβιαστεί εύκολα.

Τρίτον, ο κάθε επιτιθέμενος συνήθως κάνει κάποια έρευνα για το δίκτυο που θέλει να επιτεθεί και καλό θα είναι οι πληροφορίες που δίνονται προς τα έξω να είναι ελάχιστες και σε καμία περίπτωση να μην δίνονται κρίσιμα δεδομένα που μπορούν να χρησιμοποιηθούν εναντίον του δικτύου μας.

Τέταρτον, κανένα σύστημα δεν μπορεί να είναι 100% ασφαλές και πρέπει πάντα να γίνονται έλεγχοι από το προσωπικό, ώστε σε περίπτωση ευπάθειας του συστήματος ή του δικτύου, να γίνουν άμεσες αλλαγές.

Πέμπτον, η κάθε εταιρεία καλό είναι να επενδύσει κάποιο κομμάτι του προϋπολογισμού της για την ασφάλεια των πληροφοριών της. Έτσι, μία καλή μέθοδος για να υπάρξει κάποια ισοστάθμιση μεταξύ κέρδους και σπατάλης για την εταιρεία, είναι να γίνει κάποια μελέτη ώστε να τοποθετηθούν κάποια συστήματα που είναι πιο αξιόπιστα (όπως συσκευές της εταιρείας Cisco) και παράλληλα να μειωθούν τα έξοδα από τα κλειδιά που πληρώνονται σε εταιρείες όπως η Microsoft και να χρησιμοποιηθούν Λειτουργικά Συστήματα ανοιχτού κώδικα, όπως το Linux, τα οποία μάλιστα μας παρέχουν και μεγαλύτερη ασφάλεια των δεδομένων μας.

Έκτον, οι πληροφορίες που είναι αρκετά σημαντικές για το δίκτυο μας, είναι καλό να μεταφέρονται μέσω εικονικών δικτύων (VPN). Τα εικονικά δίκτυα είναι ένα έξτρα επίπεδο ασφαλείας για τα δεδομένα μας και μπορούμε να το χρησιμοποιήσουμε αρκετά εύκολα.

7.2 Ανακεφαλαίωση

Στο πρώτο κεφάλαιο είδαμε τη γέννηση των Ασύρματων Δικτύων και πως αυτά εξελίχθηκαν στο χρόνο. Στο δεύτερο κεφάλαιο είχαμε μία ανάλυση των πρωτοκόλλων που χρησιμοποιούνται στο τοπικά Ασύρματα Δίκτυα της οικογένειας του IEEE 802.11. Στο τρίτο κεφάλαιο, είχαμε μία αναφορά σχετικά με την ασφάλεια των πληροφοριών μας σε ένα ασύρματο δίκτυο και είδαμε τις μεθόδους πιστοποίησης που υπάρχουν. Επίσης κάναμε μία επισκόπηση των παραπάνω δεδομένων που παράχθηκαν. Στο τέταρτο κεφάλαιο κάναμε μερικές επιθέσεις σε Ασύρματα Δίκτυα και είδαμε τους χρόνους που χρειάζονται για το σπάσιμο ενός δικτύου. Επίσης είδαμε μερικά εργαλεία που χρησιμοποιούνται από τους επιτιθέμενους για παραγωγή λεξικών με λέξεις κλειδιά, δηλαδή υποψήφιους κωδικούς/κλειδιά για πρόσβαση στο εκάστοτε δίκτυο.

Από το πέμπτο κεφάλαιο, αρχίσαμε να ασχολούμαστε με το δίκτυο του δήμου Αμαρουσίου. Στο συγκεκριμένο κεφάλαιο ασχοληθήκαμε με το διαμοιρασμό των υποδικτύων, τη μελέτη του χώρου για την τοποθέτηση των συσκευών σε αυτό και με την εγκατάσταση συστημάτων ασφαλείας (IDS & IPS) που μπορούν να προστατέψουν κι αυτά με τη σειρά τους το δίκτυο. Στο έκτο κεφάλαιο αλλάξαμε λίγο την τοπολογία του δικτύου μας, τοποθετόντας ένα ακόμη switch για την σωστώτερη λειτουργία του δικτύου και την καλύτερη δρομολόγηση των δεδομένων, είδαμε τον τρόπο εγκατάσταση ενός εικονικού δικτύου, τη βασική παραμετροποίηση των δικτυακών συσκευών και τον τρόπο παραμετροποιήσης ενός IDS/IPS.

Ακολουθούν τρία (3) παραρτήματα, στο πρώτο έχουμε τα δεδομένα των ρυθμίσεων των συσκευών έτσι όπως τις παραμετροποιήσαμε, στο δεύτερο παράρτημα βρίσκουμε μία προσθήκη εντολών για να αυξήσουμε την ασφάλεια στις δικτυακές συσκευές του κτηρίου του δήμου, ενώ στο τρίτο και τελευταίο έχουμε τον τρόπο εγκατάστασης του OpenVPN στο ΛΣ Linux και πιο συγκεκριμένα στην έκδοση Fedora 18.

ΠΑΡΑΡΤΗΜΑ Α (Configuration Συσκευών Δικτύου)

Configuration Των Switches

Σε αυτό το παράρτημα θα δούμε όλα τα configuration files των Cisco Catalyst Switches που έχουμε εγκαταστήσει στο δίκτυο του δήμου Αμαρουσίου. Σε αυτά τα αρχεία βλέπουμε συγκεντρωτικά όλες τις ρυθμίσεις που περιγράψαμε στα δύο τελευταία κεφάλαια, που έχουν να κάνουν με τις θύρες και τις παραμέτρους που ορίσαμε σε αυτές, τα πρωτόκολλα που είναι ενεργά και άλλες πληροφορίες. Να σημειωθεί εδώ πως στα configuration files που ακολουθούν, δεν θα δούμε αρκετές ρυθμίσεις ασφαλείας, αλλά επικεντρωνόμαστε στη διασυνδεσιμότητα μεταξύ των συσκευών του δικτύου και των κόμβων αυτού. Στο Παράρτημα Β, θα δούμε κάποιες έξτρα εντολές με τις οποίες μπορούμε να αυξήσουμε την ασφάλεια του δικτύου μας και των συσκευών. Οι εντολές αυτές αφορούν στην απενεργοποίηση υπηρεσιών των δικτυακών συσκευών που δεν τις χρησιμοποιούμε, στην προσθήκη κωδικών ασφαλείας στις συσκευές (για log in κτλ) και στην απενεργοποίηση υπηρεσιών TELNET.

Switch 2ου Ορόφου

Switch2rouOrofou#sh start *//Εντολή show startup-config*

Using 1446 bytes *//Μέγεθος αρχείου αποθηκευμένων ρυθμίσεων*

!

version 12.2 *//Έκδοση ΛΣ Cisco OS*

no service timestamps log datetime msec *//Μη ενεργοποιημένη υπηρεσία καταγραφής log in στη συσκευή*

no service timestamps debug datetime msec *//Μη ενεργοποιημένη υπηρεσία καταγραφής ώρας και ημ/νίας*

no service password-encryption *//Μη ενεργοποιημένη υπηρεσία κρυπτογράφησης των κωδικών ασφαλείας*

!

hostname Switch2rouOrofou *//Όνομα συσκευής*

!

!

spanning-tree mode pvst *//Default STP πρωτόκολλο (Per VLAN Spanning Tree Protocol)*

!

interface FastEthernet0/1 *//Interface Fa0/1*

switchport access vlan 10 *//Ανήκει στο VLAN 10 (Διοίκησης)*

!

```
interface FastEthernet0/2 //Interface Fa0/2
 switchport access vlan 15 //Ανήκει στο VLAN 15 (Γραμματείας)
!
interface FastEthernet0/3 //Interface Fa0/3
 switchport access vlan 20 //Ανήκει στο VLAN 20 (IT/Τεχνικοί)
!
interface FastEthernet0/4 //Interface Fa0/4
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/5 //Interface Fa0/5
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/6 //Interface Fa0/6
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/7 //Interface Fa0/7
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/8 //Interface Fa0/8
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/9 //Interface Fa0/9
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/10 //Interface Fa0/10
```

```
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/11 //Interface Fa0/11
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/12 //Interface Fa0/12
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/13 //Interface Fa0/13
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/14 //Interface Fa0/14
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/15 //Interface Fa0/15
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/16 //Interface Fa0/16
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/17 //Interface Fa0/17
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/18 //Interface Fa0/18
 shutdown //Απενεργοποιημένο
```

```
!
interface FastEthernet0/19 //Interface Fa0/19
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/20 //Interface Fa0/20
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/21 //Interface Fa0/21
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/22 //Interface Fa0/22
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/23 //Interface Fa0/23
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/24 //Interface Fa0/24
 switchport trunk native vlan 87 //Native VLAN 87
 switchport mode trunk //Ορίζουμε τη θύρα ως trunk
!
interface GigabitEthernet1/1 //Interface Gig1/1
 switchport trunk native vlan 87 //Native VLAN 87
 switchport mode trunk //Ορίζουμε τη θύρα ως trunk
!
interface GigabitEthernet1/2 //Interface Gig1/2
```

shutdown *//Απενεργοποιημένο*

!

interface Vlan1 *//Default VLAN1*

no ip address *//Δεν έχει κάποια IP*

shutdown *//Δεν λειτουργεί κάποια θύρα του switch που να ανήκει στο VLAN1*

!

!

line con 0 *//Θύρα κονσόλας*

!

line vty 0 4 *//Θύρες 0 – 4 (λογικές) για απομακρυσμένη σύνδεση TELNET/SSH*

login *//Απαιτεί log in*

line vty 5 15 *//Θύρες 5 - 15 (λογικές) για απομακρυσμένη σύνδεση TELNET/SSH*

login *//Απαιτεί log in*

!

!

end *//Τέλος αρχείου ρυθμίσεων (startup-configuration file)*

Switch 1ου Ορόφου

Switch1ouOrofou#sh start *//Εντολή show startup-config*

Using 1862 bytes *//Μέγεθος αρχείου αποθυκευμένων ρυκθίσεων*

!

version 12.2 *//Εκδοση ΛΣ Cisco OS*

no service timestamps log datetime msec *//Μη ενεργοποιημένη υπηρεσία καταγραφής log in στη συσκευή*

no service timestamps debug datetime msec *//Μη ενεγοποιημένη υπηρεσία καταγραφής ώρας και ημ/νίας*

no service password-encryption *//Μη ενεργοποιημένη υπηρεσία κρυπτογράφησης των κωδικών ασφαλείας*

!

```
hostname Switch1ouOrofou //Όνομα συσκευής
!
!
spanning-tree mode pvst //Default STP πρωτόκολλο (Per VLAN Spanning Tree Protocol)
!
interface FastEthernet0/1 //Interface Fa0/1
 description Access Point Protokollou. Dinamiko 5 IPs. //Περιγραφή θύρας
 switchport access vlan 25 //Ανήκει στο VLAN 25 (Πρωτόκολλο)
!
interface FastEthernet0/2 //Interface Fa0/2
 description Access Point Logistiriou. Dynamiko 10 IPs. //Περιγραφή θύρας
 switchport access vlan 30 //Ανήκει στο VLAN 30 (Λογιστήριο)
!
interface FastEthernet0/3 //Interface Fa0/3
 description Access Point Dym. Astynomias. Dynamiko 25 IPs. //Περιγραφή θύρας
 switchport access vlan 35 //Ανήκει στο VLAN 30 (Δημοτικής Αστυνομίας)
!
interface FastEthernet0/4 //Interface Fa0/4
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/5 //Interface Fa0/5
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/6 //Interface Fa0/6
 shutdown //Απενεργοποιημένο
```

```
!
interface FastEthernet0/7 //Interface Fa0/7
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/8 //Interface Fa0/8
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/9 //Interface Fa0/9
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/10 //Interface Fa0/10
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/11 //Interface Fa0/11
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/12 //Interface Fa0/12
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/13 //Interface Fa0/13
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/14 //Interface Fa0/14
 shutdown //Απενεργοποιημένο
!
```

```
interface FastEthernet0/15 //Interface Fa0/15
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/16 //Interface Fa0/16
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/17 //Interface Fa0/17
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/18 //Interface Fa0/18
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/19 //Interface Fa0/19
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/20 //Interface Fa0/20
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/21 //Interface Fa0/21
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/22 //Interface Fa0/22
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/23 //Interface Fa0/23
```

```
 switchport trunk native vlan 87 //Native VLAN 87
 switchport mode trunk //Ορίζουμε τη θύρα ως trunk
!
interface FastEthernet0/24 //Interface Fa0/24
 switchport trunk native vlan 87 //Native VLAN 87
 switchport mode trunk //Ορίζουμε τη θύρα ως trunk
!
interface GigabitEthernet1/1 //Interface Gig1/1
 description Trunk thyra, epikoinonia me Switch2rouOrofou. Allowed VLANs ALL! //Περιγραφή θύρας
 switchport trunk native vlan 87 //Native VLAN 87
 switchport mode trunk //Ορίζουμε τη θύρα ως trunk
!
interface GigabitEthernet1/2 //Interface Gig1/2
 description Trunk thyra, epikoinonia me SwitchIsogeiou. Allowed VLANs ALL! //Περιγραφή θύρας
 switchport trunk native vlan 87 //Native VLAN 87
 switchport mode trunk //Ορίζουμε τη θύρα ως trunk
!
interface Vlan1 //Default VLAN
 no ip address //Δεν έχει κάποια IP
 shutdown //Δεν λειτουργεί κάποια θύρα του switch που να ανήκει στο VLAN 1
!
!
line con 0 //Θύρα κονσόλας
!
line vty 0 4 //Θύρες 0 – 4 (λογικές) για απομακρυσμένη σύνδεση TELNET/SSH
```

login *//Απαιτεί log in*

line vty 5 15 *//Θύρες 5 – 15 (λογικές) για απομακρυσμένη σύνδεση TELNET/SSH*

login *//Απαιτεί log in*

!

!

end *//Τέλος αρχείου ρυθμίσεων (startup-configuration file)*

Switch Ισογείου

SwitchIsogeiou#sh start *//Εντολή show startup-config*

Using 1329 bytes *//Μέγεθος αρχείου αποθηκευμένων ρυθμίσεων*

!

version 12.2 *//Εκδοση ΛΣ Cisco OS*

no service timestamps log datetime msec *//Μη ενεργοποιημένη υπηρεσία καταγραφής log in στη συσκευή*

no service timestamps debug datetime msec *//Μη ενεγοποιημένη υπηρεσία καταγραφής ώρας και ημ/νίας*

no service password-encryption *//Μη ενεργοποιημένη υπηρεσία κρυπτογράφησης των κωδικών ασφαλείας*

!

hostname SwitchIsogeiou *//Όνομα συσκευής*

!

!

spanning-tree mode pvst *//Default STP πρωτόκολλο (Per VLAN Spanning Tree Protocol)*

!

interface FastEthernet0/1 *//Interface Fa0/1*

switchport access vlan 40 *//Ανήκει στο VLAN 40 (Πληροφορίες)*

!

interface FastEthernet0/2 *//Interface Fa0/2*

switchport access vlan 45 *//Ανήκει στο VLAN 45 (Εξυπηρέτηση Δημοτών)*

!

```
interface FastEthernet0/3 //Interface Fa0/3
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/4 //Interface Fa0/4
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/5 //Interface Fa0/5
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/6 //Interface Fa0/6
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/7 //Interface Fa0/7
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/8 //Interface Fa0/8
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/9 //Interface Fa0/9
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/10 //Interface Fa0/10
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/11 //Interface Fa0/11
```

shutdown *//Απενεργοποιημένο*

!

interface FastEthernet0/12 *//Interface Fa0/12*

shutdown *//Απενεργοποιημένο*

!

interface FastEthernet0/13 *//Interface Fa0/13*

shutdown *//Απενεργοποιημένο*

!

interface FastEthernet0/14 *//Interface Fa0/14*

shutdown *//Απενεργοποιημένο*

!

interface FastEthernet0/15 *//Interface Fa0/15*

shutdown *//Απενεργοποιημένο*

!

interface FastEthernet0/16 *//Interface Fa0/16*

shutdown *//Απενεργοποιημένο*

!

interface FastEthernet0/17 *//Interface Fa0/17*

shutdown *//Απενεργοποιημένο*

!

interface FastEthernet0/18 *//Interface Fa0/18*

shutdown *//Απενεργοποιημένο*

!

interface FastEthernet0/19 *//Interface Fa0/19*

shutdown *//Απενεργοποιημένο*

```
!
interface FastEthernet0/20 //Interface Fa0/20
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/21 //Interface Fa0/21
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/22 //Interface Fa0/22
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/23 //Interface Fa0/23
 switchport trunk native vlan 87 //Native VLAN 87
 switchport mode trunk //Ορίζουμε τη θύρα ως trunk
!
interface FastEthernet0/24 //Interface Fa0/24
 switchport trunk native vlan 87 //Native VLAN 87
 switchport mode trunk //Ορίζουμε τη θύρα ως trunk
!
interface GigabitEthernet1/1 //Interface Gig1/1
 switchport trunk native vlan 87 //Native VLAN 87
 switchport mode trunk //Ορίζουμε τη θύρα ως trunk
!
interface GigabitEthernet1/2 //Interface Gig1/2
 switchport trunk native vlan 87 //Native VLAN 87
 switchport mode trunk //Ορίζουμε τη θύρα ως trunk
```

!

interface Vlan1 *//Default VLAN1*

no ip address *//Δεν έχει κάποια IP*

shutdown *//Δεν λειτουργεί κάποια θύρα του switch που να ανήκει στο VLAN1*

!

!

line con 0 *//Θύρα κονσόλας*

!

line vty 0 4 *//Θύρες 0 – 4 (λογικές) για απομακρυσμένη σύνδεση TELNET/SSH*

login *//Απαιτεί log in*

line vty 5 15 *//Θύρες 5 – 15 (λογικές) για απομακρυσμένη σύνδεση TELNET/SSH*

login *//Απαιτεί log in*

!

!

end *//Τέλος αρχείου ρυθμίσεων (startup-configuration file)*

Switch Υπογείου

SwitchYpogeiou#sh start *//Εντολή show startup-config*

Using 1490 bytes *//Μέγεθος αρχείου αποθηκευμένων ρυθμίσεων*

!

version 12.2 *//Εκδοση ΛΣ Cisco OS*

no service timestamps log datetime msec *//Μη ενεργοποιημένη υπηρεσία καταγραφής log in στη συσκευή*

no service timestamps debug datetime msec *//Μη ενεγοποιημένη υπηρεσία καταγραφής ώρας και ημ/νίας*

no service password-encryption *//Μη ενεργοποιημένη υπηρεσία κρυπτογράφησης των κωδικών ασφαλείας*

!

hostname SwitchYpogeiou *//Όνομα συσκευής*

```
!
!
spanning-tree mode pvst //Default STP πρωτόκολλο (Per VLAN Spanning Tree Protocol)
!
interface FastEthernet0/1 //Interface Fa0/1
 switchport access vlan 95 //Ανήκει στο VLAN 95 (Servers)
!
interface FastEthernet0/2 //Interface Fa0/2
 switchport access vlan 95 //Ανήκει στο VLAN 95 (Servers)
!
interface FastEthernet0/3 //Interface Fa0/3
 switchport access vlan 95 //Ανήκει στο VLAN 95 (Servers)
!
interface FastEthernet0/4 //Interface Fa0/4
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/5 //Interface Fa0/5
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/6 //Interface Fa0/6
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/7 //Interface Fa0/7
 shutdown //Απενεργοποιημένο
!
```

```
interface FastEthernet0/8 //Interface Fa0/8
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/9 //Interface Fa0/9
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/10 //Interface Fa0/10
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/11 //Interface Fa0/11
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/12 //Interface Fa0/12
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/13 //Interface Fa0/13
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/14 //Interface Fa0/14
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/15 //Interface Fa0/15
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/16 //Interface Fa0/16
```

```
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/17 //Interface Fa0/17
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/18 //Interface Fa0/18
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/19 //Interface Fa0/19
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/20 //Interface Fa0/20
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/21 //Interface Fa0/21
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/22 //Interface Fa0/22
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/23 //Interface Fa0/23
 shutdown //Απενεργοποιημένο
!
interface FastEthernet0/24 //Interface Fa0/24
 switchport trunk native vlan 87 //Native VLAN 87
```

```
 switchport mode trunk //Ορίζουμε τη θύρα ως trunk
!
interface GigabitEthernet1/1 //Interface Gig1/1
 switchport trunk native vlan 87 //Native VLAN 87
 switchport mode trunk //Ορίζουμε τη θύρα ως trunk
!
interface GigabitEthernet1/2 //Interface Gig1/2
 switchport trunk native vlan 87 //Native VLAN 87
 switchport mode trunk //Ορίζουμε τη θύρα ως trunk
!
interface Vlan1 //Default VLAN1
 no ip address //Δεν έχει κάποια IP
 shutdown //Δεν λειτουργεί κάποια θύρα του switch που να ανήκει στο VLAN1
!
!
line con 0 //Θύρα κονσόλας
!
line vty 0 4 //Θύρες 0 – 4 (λογικές) για απομακρυσμένη σύνδεση TELNET/SSH
 login //Απαιτεί log in
line vty 5 15 //Θύρες 5 – 15 (λογικές) για απομακρυσμένη σύνδεση TELNET/SSH
 login //Απαιτεί log in
!
!
end //Τέλος αρχείου ρυθμίσεων (startup-configuration file)
```

Main Switch

```
MainSwitch#sh start //Εντολή show startup-config
```

```
Using 690 bytes //Μέγεθος αρχείου αποθηκευμένων ρυθμίσεων
!
version 12.1 //Έκδοση ΛΣ Cisco OS
no service timestamps log datetime msec //Μη ενεργοποιημένη υπηρεσία καταγραφής log in στη συσκευή
no service timestamps debug datetime msec //Μη ενεγοποιημένη υπηρεσία καταγραφής ώρας και ημ/νίας
no service password-encryption //Μη ενεργοποιημένη υπηρεσία κρυπτογράφησης των κωδικών ασφαλείας
!
hostname MainSwitch //Όνομα συσκευής
!
!
spanning-tree mode pvst //Default STP πρωτόκολλο (Per VLAN Spanning Tree Protocol)
!
interface GigabitEthernet0/1 //Interface Gig0/1
 switchport trunk native vlan 87 //Native VLAN 87
 switchport mode trunk //Ορίζουμε τη θύρα ως trunk
!
interface GigabitEthernet1/1 //Interface Gig1/1
 switchport trunk native vlan 87 //Native VLAN 87
 switchport mode trunk //Ορίζουμε τη θύρα ως trunk
!
interface GigabitEthernet2/1 //Interface Gig2/1
 switchport trunk native vlan 87 //Native VLAN 87
 switchport mode trunk //Ορίζουμε τη θύρα ως trunk
!
interface GigabitEthernet3/1 //Interface Gig3/1
```

```
 switchport trunk native vlan 87 //Native VLAN 87
 switchport mode trunk //Ορίζουμε τη θύρα ως trunk
!
interface GigabitEthernet4/1 //Interface Gig4/1
 switchport mode trunk //Ορίζουμε τη θύρα ως trunk
!
interface Vlan1 //Default VLAN
 no ip address //Δεν έχει κάποια IP
shutdown //Δεν λειτουργεί κάποια θύρα του switch που να ανήκει στο VLAN1
!
!
line con 0 //Θύρα κονσόλας
!
line vty 0 4 //Θύρες 0 – 4 (λογικές) για απομακρυσμένη σύνδεση TELNET/SSH
 login //Απαιτεί log in
line vty 5 15 //Θύρες 5 – 15 (λογικές) για απομακρυσμένη σύνδεση TELNET/SSH
 login //Απαιτεί log in
!
!
end //Τέλος αρχείου ρυθμίσεων (startup-configuration file)
```

Configuration του Router

Στην τοπολογία που δημιουργήσαμε για το κτήριο του δήμου Αμαρουσίου, έγινε η εγκατάσταση ενός μόνο δρομολογητή. Ο δρομολογητής αυτός συνδέει όλα τα υποδίκτυα του δήμου μεταξύ τους και επίσης συνδέει το εσωτερικό δίκτυο με το Internet. Στο configuration file που ακολουθεί βλέπουμε όλες τις ρυθμίσεις που είναι αποθηκευμένες στο router και για ακόμη μια φορά βασιζόμαστε στις εντολές και τις ρυθμίσεις που αφορούν την διασυνδεσιμότητα των συσκευών και των κόμβων μεταξύ τους. Οι εντολές που αφορούν την έξτρα ασφάλεια, περιγράφονται στο Παράρτημα Β.

Router Κτηρίου

Router#sh start *//Εντολή show startup-config*

Using 1647 bytes *//Μέγεθος αρχείου αποθηκευμένων ρυθμίσεων*

!

version 12.2 *//Έκδοση ΛΣ Cisco OS*

no service timestamps log datetime msec *//Μη ενεργοποιημένη υπηρεσία καταγραφής log in στη συσκευή*

no service timestamps debug datetime msec *//Μη ενεγοποιημένη υπηρεσία καταγραφής ώρας και ημ/νίας*

no service password-encryption *//Μη ενεργοποιημένη υπηρεσία κρυπτογράφησης των κωδικών ασφαλείας*

!

hostname Router *//Όνομα συσκευής*

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

```
!
!
interface FastEthernet0/0 //Inteface Fa0/0
 no ip address //Δεν έχει οριστεί κάποια IP
 duplex auto //Αυτόματη αναγνώριση half-duplex/full-duplex
 speed auto //Αυτόματη αναγνώριση ταχύτητας που υποστηρίζεται από το μέσο
!
interface FastEthernet1/0 //Inteface Fa1/0
 no ip address //Δεν έχει οριστεί κάποια IP
 duplex auto //Αυτόματη αναγνώριση half-duplex/full-duplex
 speed auto //Αυτόματη αναγνώριση ταχύτητας που υποστηρίζεται από το μέσο
 shutdown //Απενεργοποιημένο
!
interface Serial2/0 //Interface Se2/0
 no ip address //Δεν έχει οριστεί κάποια IP
 clock rate 2000000 //Ταχύτητα συγχρονισμού μετάδοσης δεδομένων (DTE/DCE)
 shutdown //Απενεργοποιημένο
!
interface Serial3/0 //Interface Se3/0
 no ip address //Δεν έχει οριστεί κάποια IP
 clock rate 2000000 //Ταχύτητα συγχρονισμού μετάδοσης δεδομένων (DTE/DCE)
 shutdown //Απενεργοποιημένο
!
interface FastEthernet4/0 //Inteface Fa4/0
 no ip address //Δεν έχει οριστεί κάποια IP
```

```
 shutdown //Απενεργοποιημένο
!
interface FastEthernet5/0 //Inteface Fa5/0
 no ip address //Δεν έχει οριστεί κάποια IP
 shutdown //Απενεργοποιημένο
!
interface GigabitEthernet6/0 //Interface Gig6/0 (Router-on-a-stick)
 no ip address //Δεν έχει οριστεί κάποια IP στο φυσικό αυτό interface
 duplex auto //Αυτόματη αναγνώριση half-duplex/full-duplex
 speed auto //Αυτόματη αναγνώριση ταχύτητας που υποστηρίζεται από το μέσο
!
interface GigabitEthernet6/0.10 //Interface Gig6/0.10
 encapsulation dot1Q 10 //Ενεργοποίηση πρωτοκόλλου 802.1Q για το VLAN 10
 ip address 10.10.10.206 255.255.255.240 //Ορισμός IP διεύθυνσης (default gateway υποδικτύου)
!
interface GigabitEthernet6/0.15 //Interface Gig6/0.15
 encapsulation dot1Q 15 //Ενεργοποίηση πρωτοκόλλου 802.1Q για το VLAN 15
 ip address 10.10.10.190 255.255.255.224 //Ορισμός IP διεύθυνσης (default gateway υποδικτύου)
!
interface GigabitEthernet6/0.20 //Interface Gig6/0.20
 encapsulation dot1Q 20 //Ενεργοποίηση πρωτοκόλλου 802.1Q για το VLAN 20
 ip address 10.10.10.158 255.255.255.224 //Ορισμός IP διεύθυνσης (default gateway υποδικτύου)
!
interface GigabitEthernet6/0.25 //Interface Gig6/0.25
 encapsulation dot1Q 25 //Ενεργοποίηση πρωτοκόλλου 802.1Q για το VLAN 25
```

```
 ip address 10.10.10.230 255.255.255.248 //Ορισμός IP διεύθυνσης (default gateway υποδικτύου)
!
interface GigabitEthernet6/0.30 //Interface Gig6/0.30
 encapsulation dot1Q 30 //Ενεργοποίηση πρωτοκόλλου 802.1Q για το VLAN 30
 ip address 10.10.10.222 255.255.255.240 //Ορισμός IP διεύθυνσης (default gateway υποδικτύου)
!
interface GigabitEthernet6/0.35 //Interface Gig6/0.35
 encapsulation dot1Q 35 //Ενεργοποίηση πρωτοκόλλου 802.1Q για το VLAN 35
 ip address 10.10.10.94 255.255.255.224 //Ορισμός IP διεύθυνσης (default gateway υποδικτύου)
!
interface GigabitEthernet6/0.40 //Interface Gig6/0.40
 encapsulation dot1Q 40 //Ενεργοποίηση πρωτοκόλλου 802.1Q για το VLAN 40
 ip address 10.10.10.238 255.255.255.248 //Ορισμός IP διεύθυνσης (default gateway υποδικτύου)
!
interface GigabitEthernet6/0.45 //Interface Gig6/0.45
 encapsulation dot1Q 45 //Ενεργοποίηση πρωτοκόλλου 802.1Q για το VLAN 45
 ip address 10.10.10.126 255.255.255.224 //Ορισμός IP διεύθυνσης (default gateway υποδικτύου)
!
interface GigabitEthernet6/0.95 //Interface Gig6/0.95
 encapsulation dot1Q 95 //Ενεργοποίηση πρωτοκόλλου 802.1Q για το VLAN 95
 ip address 10.10.10.246 255.255.255.248 //Ορισμός IP διεύθυνσης (default gateway υποδικτύου)
!
interface Modem7/0 //Interface Mod7/0
 no ip address //Δεν έχει οριστεί κάποια IP
!
```

ip classless *//Λειτουργία ανάγνωσης της route list του δρομολογητή*

!

!

!

no cdp run *//Απενεργοποιημένο CDP (Cisco Descovery Protocol) για την συσκευή αυτή*

!

!

!

!

!

line con 0 *//Θύρα κονσόλας*

line vty 0 4 *//Θύρες 0 – 4 (λογικές) για απομακρυσμένη σύνδεση TELNET/SSH*

login *//Απαιτεί log in*

!

!

!

end *//Τέλος αρχείου ρυθμίσεων (startup-configuration file)*

ΠΑΡΑΡΤΗΜΑ Β (Έξτρα Παράμετροι Ασφαλείας)

Στο Παράρτημα Α, είδαμε τα configuration files των συσκευών που έχουμε εγκαταστήσει στο δίκτυο του δήμου Αμαρουσίου. Όλες οι εντολές που παρουσιάστηκαν σ' εκείνο το παράρτημα, αφορούσαν καθαρά την διασυνδεσιμότητα των συσκευών και όχι την ασφάλεια του δικτύου και των συσκευών. Εδώ λοιπόν θα δούμε κάποιες έξτρα παράμετρους/εντολές που μπορούμε να χρησιμοποιήσουμε για να ενδυναμώσουμε την ασφάλεια του δικτύου.

Προσθήκη Κωδικών Ασφαλείας

Οι συσκευές του δικτύου πρέπει πάντα να προστατεύονται όσο το δυνατόν καλύτερα. Η πρώτη κίνηση που πρέπει να γίνει γι' αυτό, είναι η προσθήκη κωδικών στην συσκευή. Έτσι σε περίπτωση που κάποιος μπορέσει να αποκτήσει πρόσβαση (φυσική ή απομακρυσμένη) στο εκάστοτε μηχάνημα, να πρέπει να έχει και τον κωδικό για να αποκτήσει πρόσβαση σ' αυτό.

Η πρώτη μέθοδος είναι να χρησιμοποιήσουμε την κρυπτογράφηση των κωδικών που θα προσθέσουμε στις συσκευές. Αν έχουμε ήδη κωδικούς στη συσκευή, οι οποίοι μπορεί να διαβαστούν σε plain text αν δει κάποιος το startup-config ή το running-config, μετά την προσθήκη αυτής της εντολής, και οι κωδικοί αυτοί θα κρυπτογραφηθούν. Για την ενεργοποίηση της υπηρεσίας αυτής, χρησιμοποιούμε την ακόλουθη εντολή:

Switch(config)#service password-encryption

Ο πρώτος κωδικός που μπορούμε να προσθέσουμε είναι ο κωδικός που θα απαιτείται όταν ο χρήστης πληκτρολογήσει την εντολή "enable", δηλαδή κατέβει ένα στη συσκευή και πλέον έχει μερικά δικαιώματα παραμετροποίησής της ή προβολής περισσότερων πληροφοριών. Ο κωδικός αυτός μπορεί να ενεργοποιηθεί με δύο τρόπους. Ο πρώτος είναι με το "enable password" και ο δεύτερος (και αυτός που χρησιμοποιήσαμε) με το "enable secret". Η διαφορά των δύο είναι ότι στην πρώτη περίπτωση ο κωδικός δεν κρυπτογραφείτε (σε περίπτωση που δεν έχουμε το password-encryption ενεργοποιημένο), ενώ στη δεύτερη ο κωδικός κρυπτογραφείται και έτσι δεν μπορεί να διαβαστεί σαν plain text. Η εντολή για την ενεργοποίηση του κωδικού είναι η εξής:

Switch(config)#enable secret thisIsMyPassword

Ένας κωδικός ακόμη που μπορούμε να ενεργοποιήσουμε είναι για την κονσόλα. Η κάθε συσκευή Cisco, έχει μία ειδική θύρα μέσω της οποίας μπορούμε να παραμετροποιήσουμε το μηχάνημα αυτό. Για έξτρα προστασία, προσθέτουμε ένα σετ τριών (3) εντολών για να ενεργοποιήσουμε και σ' αυτή την σύνδεση κάποιο κωδικό ασφαλείας. Η πρώτη εντολή,αφορά τη θύρα console 0. Η δεύτερη εντολή αφορά τον κωδικό, ενώ η τρίτη χρησιμοποιείται για να ζητάει από τον χρήστη τον κωδικό. Σε περίπτωση που αγνοήσουμε την τρίτη εντολή, τότε ο κωδικός θα υπάρχει αποθηκευμένος, αλλά δεν θα ζητείται από τον χρήστη(!). Αυτό βέβαια είναι ένα μεγάλο κενό ασφαλείας το οποίο δεν πρέπει να παραληφθεί. Για τον κωδικό αυτό, χρησιμοποιούμε:

Switch(config)#line console 0

Switch(config-line)#password thisIsMyPassword

Switch(config-line)#login

Ο τελευταίος κωδικός που μπορούμε να ενεργοποιήσουμε είναι αυτός της TELNET/SSH απομακρυσμένης σύνδεσης. Να σημειώσουμε εδώ, πως μία Cisco συσκευή μπορεί να υποστηρίξει μέχρι και 15 επιτυχημένες ταυτόχρονες TELNET/SSH συνδέσεις(!). Το σετ των εντολών για την ενεργοποίηση του κωδικού απομακρυσμένης σύνδεσης είναι αντίστοιχο με την ενεργοποίηση του κωδικού για την console θύρα.

Switch(config)#line vty 0 4

Switch(config-line)#password thisIsMyPassword

Switch(config-line)#login

Στο παραπάνω σετ εντολών, ενεργοποιούμε τον κωδικό "thisIsMyPassword" για μέχρι και πέντε (5) επιτυχημένες απομακρυσμένες συνδέσεις (0 – 4). Και πάλι η εντολή "login" είναι υποχρεωτική για να ζητείται από τον χρήστη να εισάγει τον κωδικό. Χωρίς την εντολή αυτή, ο κωδικός θα υπάρχει αποθηκευμένος, αλλά δεν θα ζητείται πουθενά.

Μία ακόμη μέθοδος που αφορά τους κωδικούς, είναι ο ορισμός κάποιου ελάχιστου πλήθους χαρακτήρων. Μία πολιτική που αφορά τους κωδικούς είναι να έχουν μεγάλο μέγεθος. Όσο πιο μεγάλο είναι το μέγεθος ενός κωδικού, τόσο πιο δύσκολο είναι να σπάσει. Για να ορίσουμε το ελάχιστο πλήθος χαρακτήρων για τους κωδικούς που μπορούν να ενεργοποιηθούν στις συσκευές μας, χρησιμοποιούμε την ακόλουθη εντολή (ελάχιστο πλήθος κωδικού οι δέκα χαρακτήρες):

Switch(config)#service passwords ming-length 10

Απενεργοποίηση Υπηρεσιών

Μία ακόμη μέθοδος που προσφέρει έξτρα ασφάλεια στο δίκτυο μας, είναι να απενεργοποιήσουμε τις υπηρεσίες που παρέχονται από τις δικτυακές συσκευές και δεν τις χρησιμοποιούμε. Πολλές φορές ο επιτιθέμενος μπορεί να απωφεληθεί από ξεχασμένες πόρτες συσκευών οι οποίες είναι ανοιχτές για κάποιες υπηρεσίες.

Μία ακόμη θύρα που έχουν οι Cisco συσκευές είναι η auxiliary. Η συγκεκριμένη θύρα υπάρχει για να μπορέσουμε να έχουμε πρόσβαση στη συσκευή εκτός δικτύου και εκτός απομακρυσμένης σύνδεσης. Στη συγκεκριμένη πόρτα συνδέεται ένα RJ-11 καλώδιο (τηλεφωνικό) και έτσι σε περίπτωση που υπάρχει κάποιο πρόβλημα με το δίκτυο, μπορούμε να έχουμε πρόσβαση μέσω αυτής. Στην περίπτωση μας, δεν θα χρησιμοποιείται κάτι τέτοιο, οπότε θα προχωρήσουμε στην απενεργοποίηση αυτής της υπηρεσίας. Για να γίνει αυτό, χρησιμοποιούμε το ακόλουθο σετ εντολών:

Router(config)#line aux 0

Router(config-line)#no password

Router(config-line)#login

Με την χρήση των τριών αυτών εντολών, ουσιαστικά ζητάμε από το router ο χρήστης να πρέπει να κάνει log in στη συσκευή, αλλά δεν έχουμε ορίσει κάποιο κωδικό και έτσι, με τη χρήση αυτών των εντολών, λαμβάνουμε το μήνυμα "%Login disabled, until password is set".

Όπως έχουμε ήδη αναφέρει, οι TELNET συνδέσεις είναι αρκετά αναξιόπιστες, αφού η οποιαδήποτε πληροφορία μεταξύ των δύο συσκευών, μπορεί να διαβαστεί σε plain text. Έτσι η καλύτερη μέθοδος που μπορούμε να ακολουθήσουμε είναι να απενεργοποιήσουμε το TELNET και αν χρειάζεται κάποια απομακρυσμένη σύνδεση αυτή να γίνεται μέσω SSH. Η διαδικασία αυτή είναι πιο περίπλοκη από αυτές που περιγράψαμε παραπάνω, αλλά είναι αρκετά σημαντικό το να γίνει σε περίπτωση που έχουμε TELNET συνδέσεις. Το πρώτο σετ εντολών για να ρυθμίσουμε το SSH με τους κωδικούς που θέλουμε, με την κρυπτογράφηση που θέλουμε να χρησιμοποιεί, με το time-out της σύνδεσης και τις προσπάθειες σύνδεσης, είναι το ακόλουθο:

Router(config)#hostname Thor

Router(config)#ip domain-name myCiscoRouter.com

Router(config)#crypto key generate rsa

Router(config)#username MyMainUser secret MyPassword

Router(config)#line vty 0 4

Router(config-line)#transport input ssh

Router(config-line)#login local

Router(config-line)#ip ssh time-out 15

Router(config-line)#ip ssh authentication-retries 2

Με το παραπάνω σετ εντολών, ορίσαμε σαν hostname του δρομολογητή το όνομα "Thor", το domain με ονομασία "myCiscoRouter.com" και ενεργοποιήσαμε την κρυπτογράφηση RSA. Στη συνέχεια δημιουργήσαμε ένα user με όνομα "MyMainUser" και κωδικό "MyPassword". Μετά ακολούθησε η παραμετροποίηση της απομακρυσμένης σύνδεσης. Σετάραμε τις πρώτες πέντε (5) απομακρυσμένες συνδέσεις (επιτυχημένες) με τα εξής χαρακτηριστικά:

- Ενεργοποίηση του SSH
- Αντιστοιχία των πληροφοριών εισόδου του τοπικού χρήστη για απομακρυσμένη σύνδεση
- Διακοπή της σύνδεσης μετά από πιθανή αδράνεια άνω των δεκαπέντε (15) λεπτών
- Δυνατότητα δύο (2) προσπαθειών για σύνδεση του απομακρυσμένου χρήστη

Αφού έγιναν οι παραπάνω ρυθμίσεις, το επόμενο βήμα είναι η απενεργοποίηση της TELNET υπηρεσίας και ο ορισμός του SSH ως default για απομακρυσμένες συνδέσεις. Για να γίνει αυτό, χρησιμοποιούμε το ακόλουθο σετ εντολών:

Router(config)#line vty 0 4

Router(config-line)#no transport input

Router(config-line)#transport input ssh

Router(config-line)#exit

Μετά το πέρασμα των παραπάνω εντολών, που μέσω των οποίων απενεργοποιούμε το TELNET και ενεργοποιούμε μόνο το SSH, πρέπει να πληκτρολογήσουμε και το τελευταίο σετ εντολών:

Router(config)#line vty 0 4

Router(config-line)#exec-timeout 3

Router(config-line)#exit

Router(config)#service tcp-keepalives-in

Όπως είδαμε το να απενεργοποιήσουμε το TELNET και να ρυθμίσουμε και να ενεργοποιήσουμε το SSH, είναι μια πιο δύσκολη διαδικασία και χρειάζεται περισσότερο χρόνο από τις υπόλοιπες υπηρεσίες. Αυτό βέβαια δεν πρέπει να μας αποθαρρύνει, ούτε να παραλείψουμε κάποια τέτοια ρύθμιση/απενεργοποίηση σε περίπτωση που έχουμε απομακρυσμένες συνδέσεις στο δίκτυο μας.

Μία ακόμη υπηρεσία που μπορεί να απενεργοποιηθεί αν δεν χρησιμοποιείται είναι το CDP. Το CDP χρησιμοποιείται για χαρτογράφηση του δικτύου σε Cisco εξοπλισμό. Είναι ένα πρωτόκολλο που έχει δημιουργηθεί από τη Cisco και ουσιαστικά "μιλάει" με τις γειτονικές συσκευές και μπορεί ο χρήστης να πάρει αρκετές πληροφορίες για τον κάθε γείτονα. Έτσι αν ο επιτιθέμενος έχει πρόσβαση σε μία από τις συσκευές, τότε μέσω εντολών που χρησιμοποιούν το CDP, μπορεί να πηγαίνει από συσκευή σε συσκευή, να δει τα χαρακτηριστικά της κάθε γειτονικής συσκευής και να κάνει μία πλήρη χαρτογράφηση του δικτύου μας. Σε περίπτωση που θέλουμε να απενεργοποιήσουμε το CDP μπορούμε να το κάνουμε με δύο (2) τρόπους. Μπορούμε να το απενεργοποιήσουμε σε κάποια/ες θύρα/ες ή σε ολόκληρη τη συσκευή.

Switch(config)#no cdp run *//Απενεργοποίηση σε όλη τη συσκευή*

Switch(config-if)#no cdp enable *//Απενεργοποίηση σε κάποια θύρα*

ΠΑΡΑΡΤΗΜΑ Γ (Εγκατάσταση OpenVPN)

Εγκατάσταση και Παραμετροποίηση Αρχείου Ρυθμίσεων του OpenVPN

Για την εγκατάσταση του OpenVPN στην έκδοση Fedora 18 χρησιμοποιούμε την εντολή:

$yum install openvpn openvpn-blacklist

Σαν αποτέλεσμα, έχουμε όλα τα πακέτα που χρειαζόμαστε για να εγκαταστήσουμε και να παραμετροποιήσουμε την υπηρεσία VPN. Μετά την εγκατάσταση του προγράμματος, πλοηγούμαστε στον φάκελο "/usr/share/doc/openvpn/examples/sample-config-files/" και αντιγράφουμε το sample config file που υπάρχει με ονομασία "server.conf.gz" στο φάκελο /etc/openvpn, αφού πρώτα το αποσυμπιέσουμε. Το αρχείο μετά την παραμετροποίηση του είναι το ακόλουθο και οι ρυθμίσεις μας είναι αυτές με το κόκκινο χρώμα:

Which TCP/UDP port should OpenVPN listen on?

If you want to run multiple OpenVPN instances

on the same machine, use a different port

number for each one. You will need to

open up this port on your firewall.

port 1194 *//Port που ορίσαμε και στο NAT του δρομολογητή*

TCP or UDP server?

proto udp *//Τύπος πρωτοκόλλου*

"dev tun" will create a routed IP tunnel,

"dev tap" will create an ethernet tunnel.

Use "dev tap0" if you are ethernet bridging

and have precreated a tap0 virtual interface

and bridged it with your ethernet interface.

If you want to control access policies

over the VPN, you must create firewall

rules for the the TUN/TAP interface.

On non-Windows systems, you can give

an explicit unit number, such as tun0.

On Windows, use "dev-node" for this.

```
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
dev tun //Δημιουργία τούνελ μέσω δρομολογητών
# SSL/TLS root certificate (ca), certificate
# (cert), and private key (key).  Each client
# and the server must have their own cert and
# key file.  The server and all clients will
# use the same ca file.
#
# See the "easy-rsa" directory for a series
# of scripts for generating RSA certificates
# and private keys.  Remember to use
# a unique Common Name for the server
# and each of the client certificates.
#
# Any X509 key management system can be used.
# OpenVPN can also use a PKCS #12 formatted key file
# (see "pkcs12" directive in man page).
ca ca.crt //Αρχείο πιστοποίησης
cert server.crt //Αρχείο configuration του server
key server.key  # This file should be kept secret
# Diffie hellman parameters.
# Generate your own with:
#   openssl dhparam -out dh1024.pem 1024
# Substitute 2048 for 1024 if you are using
# 2048 bit keys.
```

dh dh2048.pem *//Αρχείο που περιέχει το κλειδί σύνδεσης μεγέθους 2048 bit*

Configure server mode and supply a VPN subnet

for OpenVPN to draw client addresses from.

The server will take 10.8.0.1 for itself,

the rest will be made available to clients.

Each client will be able to reach the server

on 10.8.0.1. Comment this line out if you are

ethernet bridging. See the man page for more info.

server 10.10.10.193 255.255.255.240 *//Subnet (Διοίκησης) από το οποίο παίρνουν IP οι VPN clients*

Maintain a record of client virtual IP address

associations in this file. If OpenVPN goes down or

is restarted, reconnecting clients can be assigned

the same virtual IP address from the pool that was

previously assigned.

ifconfig-pool-persist ipp.txt *//Αρχείο διατήρησης διευθύνσεων IP των χρηστών του VPN*

Push routes to the client to allow it

to reach other private subnets behind

the server. Remember that these

private subnets will also need

to know to route the OpenVPN client

address pool (10.8.0.0/255.255.255.0)

back to the OpenVPN server.

push "route 10.10.10.193 255.255.255.240" *//Το υποδίκτυο στο οποίο θα έχουν access οι VPN clients*

If enabled, this directive will configure

all clients to redirect their default

network gateway through the VPN, causing

all IP traffic such as web browsing and

and DNS lookups to go through the VPN

(The OpenVPN server machine may need to NAT

or bridge the TUN/TAP interface to the internet

in order for this to work properly).

push "redirect-gateway def1 bypass-dhcp" *//Όλη η κίνηση του κόμβου περνάει μέσα από το server*

Certain Windows-specific network settings

can be pushed to clients, such as DNS

or WINS server addresses. CAVEAT:

http://openvpn.net/faq.html#dhcpcaveats

The addresses below refer to the public

DNS servers provided by opendns.com.

push "dhcp-option DNS 10.13.13.1"

Uncomment this directive to allow different

clients to be able to "see" each other.

By default, clients will only see the server.

To force clients to only see the server, you

will also need to appropriately firewall the

server's TUN/TAP interface.

client-to-client *//Οι συσκευές του vpn μπορούν να "βλέπουν" η μία την άλλη*

The keepalive directive causes ping-like

messages to be sent back and forth over

the link so that each side knows when

the other side has gone down.

Ping every 10 seconds, assume that remote

peer is down if no ping received during

a 120 second time period.

keepalive 10 120 *//ping ανά 10 sec και κλείσιμο της σύνδεσης μετά από 120 sec (χωρίς απάντηση)*

```
# For extra security beyond that provided
# by SSL/TLS, create an "HMAC firewall"
# to help block DoS attacks and UDP port flooding.
#
# Generate with:
#   openvpn --genkey --secret ta.key
#
# The server and each client must have
# a copy of this key.
# The second parameter should be '0'
# on the server and '1' on the clients.
tls-auth ta.key 0 # This file is secret
tls-server
# Select a cryptographic cipher.
# This config item must be copied to
# the client config file as well.
cipher AES-256-CBC //Τύπος και μοντέλο κρυπτογράφησης
# Enable compression on the VPN link.
# If you enable it here, you must also
# enable it in the client config file.
comp-lzo //Συμπίεση δεδομένων μέσα στο VPN κανάλι
# The maximum number of concurrently connected
# clients we want to allow.
max-clients 2 //Υποστήριξη μόνο δύο (2) συσκευών (δημάρχου / αντιδημάρχου)
# It's a good idea to reduce the OpenVPN
# daemon's privileges after initialization.
#
```

You can uncomment this out on

non-Windows systems.

user openvpn *//Για δημιουργία χρήστη και*

group openvpn *//group χρηστών σε Linux like ΛΣ*

The persist options will try to avoid

accessing certain resources on restart

that may no longer be accessible because

of the privilege downgrade.

persist-key *//Μέθοδοι ασφαλείας για μη πρόσβαση σε δεδομένα*

persist-tun *//μετά από κάποια πιθανή αφαίρεση δικαιωμάτων*

Output a short status file showing

current connections, truncated

and rewritten every minute.

status /var/log/openvpn/openvpn-status.log *//Δημιουργία log file που ενημερώνεται ανά λεπτό για τις ενεργές συνδέσεις*

By default, log messages will go to the syslog (or

on Windows, if running as a service, they will go to

the "\Program Files\OpenVPN\log" directory).

Use log or log-append to override this default.

"log" will truncate the log file on OpenVPN startup,

while "log-append" will append to it. Use one

or the other (but not both).

log /var/log/openvpn/openvpn.log *//Αλλαγή καταλόγου για την αποθήκευση των log files*

;log-append openvpn.log

Set the appropriate level of log

file verbosity.

#

0 is silent, except for fatal errors

4 is reasonable for general usage

5 and 6 can help to debug connection problems

9 is extremely verbose

verb 4 *//Επίπεδο καταγραφής των δεδομένων του VPN στα log files. Το 4 είναι ένα μέσο επίπεδο το οποίο ενημερώνει τα log files με "λογικούς" ρυθμούς*

Silence repeating messages. At most 20

sequential messages of the same message

category will be output to the log.

mute 20 *//Στα 20 επαναλαμβανόμενα ίδια μηνύματα στο log file, τότε σταματούν να ξαναγράφονται και προσπερνούνται*

Λόγω του ότι από default τα logs αποθηκεύονται στον κατάλογο /etc/openvpn, δημιουργήσαμε τον κατάλογο αυτό και δώσαμε δικαιώματα ιδιοκτησίας αυτού του καταλόγου από τον χρήστη openvpn με τις παρακάτω εντολές:

$mkdir –p /var/log/openvpn

$chown openvpn:openvpn /var/log/openvpn

$chmod 750 /var/log/openvpn

Δημιουργία Κλειδιών για Server και Clients

Αρχικά πλοηγούμαστε στον κατάλογο /usr/share/doc/openvpn/examples/easy-rsa/*version* και αντιγράφουμε τα αρχεία που περιέχει σε έναν άλλο κατάλογο. Στη συνέχεια πηγαίνουμε στον κατάλογο που κάναμε την αντιγραφή αυτή και δημιουργούμε το κλειδί για τον server τρέχοντας το εργαλείο παραγωγής κλειδιών του openvpn με την εντολή:

$./build-key-server server

Στη συνέχεια, αφού ορίσαμε μέχρι δύο clients για το VPN μας, δημιουργούμε τα κλειδιά και για αυτούς με έναν αντίστοιχο τρόπο. Οι εντολές που χρησιμοποιούμε για την παραγωγή των κλειδιών αυτών είναι οι ακόλουθες:

$./build-key client1

$./build-key client2

Για τις παραμέτρους "Diffie Hellman" χρησιμοποιούμε την εξής εντολή (2048 bit για μεγαλύτερη ασφάλεια):

$openssl dhparam –out dh2048.pem 2048

Για έξτρα ασφάλεια εκτός του SSL και προστασία από DDoS επιθέσεις και αποφυγή υπερχείλισης (flooding) UDP πακέτων, τρέχουμε την παρακάτω εντολή:

$openvpn –genkey –secret ta.key

Μετά την διαδικασία που περιγράφτηκε παραπάνω, αντιγράφουμε τα κλειδιά που δημιουργήσαμε στον κατάλογο /etc/openvpn και ελέγχουμε να έχουμε τα σωστά δικαιώματα στα αρχεία αυτά με την εντολή "**$ls –lha**". Επίσης πρέπει να αντιγράψουμε τα κλειδιά των clients στα εκάστοτε μηχανήματα.

Παραμετροποίηση NAT Υπολογιστή

Από την στιγμή που γνωρίζουμε σε ποιο υποδίκτυο ανήκουν όλοι οι clients του VPN, απλά ορίζουμε το NAT στον server ώστε να εξυπηρετεί τις ανάγκες "μετάφρασης". Αρχικά ορίζουμε ένα κανόνα των ip tables για να κάνει τη μετάφραση που αφορά τους πελάτες του VPN με την εξής εντολή:

$iptables –A POSTROUTING –s 10.10.10.193/28 –o wlan0 –j MASQUERADE

και στη συνέχεια αποθηκεύουμε τον κανόνα αυτό με την εντολή:

$iptables-save > /etc/iptables.rules

Μετά επεξεργαζόμαστε το αρχείο /etc/network/interfaces -για να φορτώνεται αυτόματα αυτός ο κανόνας μετά από κάθε εκκίνηση του υπολογιστή- και στην παράμετρο wlan0 προσθέτουμε την ακόλουθη γραμμή:

pre-up iptables-restore < /etc/iptables.rules

Τελευταίο βήμα της εγκατάστασής μας, είναι να ρυθμίσουμε την προώθηση των πακέτων. Η υπηρεσία στο Linux είναι η IP_forward και για να την ενεργοποιήσουμε ώστε να λειτουργεί από default μετά από κάθε εκκίνηση του υπολογιστή, παραμετροποιούμε το αρχείο /etc/sysctl.conf. Ελέγχουμε αν η παράμετρος "net.ipv4.ip_forward" ισοδυναμεί με μηδέν (0) και αν ισχύει κάτι τέτοιο, τότε την αλλάζουμε στις εξής μορφή:

net.ipv4.ip_forward=1

Συντομογραφίες

A

AES: Advanced Encryption Standard

AP: Access Point

ARP: Address Resolution Protocol

B

BCCH: Broadcast Control Channels

BCH: Broadcast Channels

BSS: Basic Service Sets

C

CDM: Code Division Multiplex

CDP: Cisco Descovery Protocol

CDMA: Code Division Multiple Access

CRC: Circle Redundancy Check

CSMA/CA: Carrier Sense Multiple Access / Collision Avoidance

CSMA/CD: Carrier Sense Multiple Access / Collision Detect

D

DES: Data Encryption Standard

DHCP: Dynamic Host Control Protocol

E

ESS: Extended Service Set

ESSID: Ess Service Set Identifier

ETSI: European Telecommunications Standard Institute

F

Fa: Fast Ethernet port

FDD: Frequency Division Duplex

FDMA: Frequency Division Multiple Access

FHSS: Frequency Hopping Spread Spectrum

G

Gig: Gigabit Ethernet port

GUI: Graphical User Interface

I

IP: Internet Protocol

IPsec: Internet Protocol Security

IANA: Internet Assigned Numbers Authority

ICMP: Internet Control Message Protocol

IEEE: Institute for Electrical and Electronic Engineers

ISDN: Integrated Services Digital Networks

ITU: International Telecommunication Union

L

L2TP: Layer 2 Tunneling Protocol

LAC: Link Access Control

LAN: Local Area Network

M

MAC: Media Access Control

MIMO: Multiple Input Multiple Output

N

NAT: Network Address Translation

NIC: Network Interface Controller

O

OFDM: Orthogonal Frequency Division Multiplexing

OSI: Open Systems Interconnection

P

PHY: Physical layer

PPTP: Point-to-Point Tunneling Protocol

Q

QoS: Quality of Service

R

RADIUS: Remote Access Dial-In User Service

RFCs: Request for Comments

S

SCH: Synchronization Channel

SFD: Start Frame Delimiter

SNR: Signal to Noise Ratio

SSD: Shared Secret Data

SSID: Service Set Identifier

STP: Spanning Tree Protocol

T

TCH: Traffic Channel

TCP/IP: Transmission Control Protocol / Internet Protocol

TDD: Time Division Duplex

TDM: Time Division Multiplex

TDMA: Time Division Multiple Access

TKIP: Temporal Key Integrity Protocol

TLS: Transport Layer Security

V

VLAN: Virtual Local Area Network

VPN: Virtual Private Network

VTP: VLAN Trunking Protocol

W

WEP: Wired Equivalent Privacy

Wi-Fi: Wireless - Fidelity

WLAN: Wireless Local Area Network

WPA: Wi-Fi Protected Access

\

Βιβλιογραφία

Βιβλία

[1] Andrew S. Tanenbaum, 2000, **Δίκτυα Υπολογιστών**, Εκδόσεις Παπασωτηρίου (Τρίτη Έκδοση)

[2] David Hucaby, 2010, **CCNP Switch 642-813**, Εκδόσεις ciscopress.com

[3] Wendell Odom, 2010, **CCNP Route 642-902**, Εκδόσεις ciscopress.com

[4] Kevin Wallace, 2010, **CCNP Tshoot 642-832**, Εκδόσεις ciscopress.com

[5] Naomi J. Alpern, 2009, **Cisco Bible**, Εκδόσεις Syngress Publishing

[6] Joel Scambray, Stuart McClure, George Kurtz, 2003, **Χάκερ Επίθεση & Άμυνα**, Εκδόσεις Μ. Γκιούρδας (Τέταρτη Έκδοση)

[7] Jon Erickson, 2008, **Hacking The art of Exploitation**, Εκδόσεις No starch press (Δεύτερη Έκδοση)

[8] Emmanuel Goldstein, 1999, **The best of 2600 [A hacker odyssey]**, Εκδόσεις Wiley

[9] Α. Σουρής, Δ. Πατσός, Ν. Γρηγοριάδης, 2004, **Ασφάλεια της Πληροφορίας**, Εκδόσεις Νέων Τεχνολογιών

[10] Π. Ε. Νάστου, Π. Γ. Σπυράκης, Γ. Κ. Σταματίου, 2003, **Σύγχρονη Κρυπτογραφία, Μια Ξέγνοιαστη διαδρομή στα μονοπάτια της**, Εκδόσεις Ελληνικα γράμματα (Τρίτη Έκδοση)

[11] Α. Πομπορτσής, Α. Τσουλφάς, 2001, **Προσομοίωση Δικτύων Υπολογιστών**, Εκδόσεις Τζιόλα

[12] Θ. Τσιλιγκιρίδης, Γ. Αλεξίου, Χ. Μπουράς, Χ. Μαμαλούκας, Π. Αγγελλοπουλος, 2002, **Μετάδοση Δεδομένων και Δίκτυα Υπολογιστών I & II**, Οργανισμός Εκδόσεως Διδακτικών Βιβλίων

[13] M. Welsh, M. K. Dalheimer, L. Kaufman, 2001, **Ο Οδηγός του Linux**, Εκδόσεις Κλειδάριθμος (Τρίτη Αμερικάνικη Έκδοση)

[14] S. Granneman, 2006, **Linux Phrasebook**, Εκδόσεις Developer's Library

Ιστότοποι – Πηγές

[1] https://www.netacad.com/

[2] http://www.cisco.com/en/US/prod/collateral/routers/ps5855/prod_brochure0900aecd8019dc1f.pdf

[3] http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml

[4] https://en.wikipedia.org/wiki/IEEE_802.11

[5] http://standards.ieee.org/about/get/802/802.11.html

[6] https://en.wikipedia.org/wiki/IEEE_802.11

[7] https://en.wikipedia.org/wiki/Hacker_(computer_security)

[8] https://en.wikipedia.org/wiki/Photophone

[9] http://www.cbtnuggets.com/it-training-videos/series/cisco-ccnp-switch-642-813

[10] https://en.wikipedia.org/wiki/Service_set_(802.11_network)

[11] http://www.ifeed.gr/%CE%B2%CE%B5%CE%BB%CF%84%CE%B9%CF%8E%CF%83%CF%84%CE%B5-%CE%B1%CF%80%CF%8C%CE%B4%CE%BF%CF%83%CE%B7-%CE%B1%CF%83%CF%8D%CF%81%CE%BC%CE%B1%CF%84%CE%BF%CF%85-%CE%B4%CE%B9%CE%BA%CF%84%CF%8D%CE%BF%CF%85/

[12] https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

[13] https://en.wikipedia.org/wiki/Cyclic_redundancy_check

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

[15] https://en.wikipedia.org/wiki/IEEE_802.11i-2004

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

[17] https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Εργασίες – Μελέτες

[1] Α. Κουρμπέλης, Γ. Ψωρομύτης, 2012, **Συγκριτική Μελέτη των Τεχνολογιών και της Ασφάλειας των Ασύρματων και Κινητών Δικτύων Επικοινωνιών**

[2] Π. Παπαδόπουλος, Α. Τριανταφυλλίδης, 2009, **Τα Προτερήματα του Ανοιχτού Λογισμικού Έναντι του Εμπορευματοποιημένου: Χρήση και Εξέλιξη**

Περιοδικά – Δημοσιεύσεις

[1] Δεκέμβριος 2012, **DeltaHacker 015 Bash Commands**

[2] Ιανουάριος 2013, **DeltaHacker 016 Malware**

[3] Φεβρουάριος 2013, **DeltaHacker 017 Πλατφόρμα Metasploit**

[4] Απρίλιος 2013, **DeltaHacker 019 Ανάλυση Πακέτων**