ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΕΡΕΥΝΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ
ΙΝΣΤΙΤΟΥΤΟ ΕΚΠΑΙΔΕΥΤΙΚΗΣ ΠΟΛΙΤΙΚΗΣ

Βασιλάκης Β., Δρακόπουλος Ι., Θεμελής Θ., Κωνσταντοπούλου Μ.

ΕΙΔΙΚΑ ΘΕΜΑΤΑ ΣΤΟ ΥΛΙΚΟ ΚΑΙ ΣΤΑ ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

Γ΄ Τάξη ΤΟΜΕΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΕΠΑ.Λ.

ΣΗΜΕΙΩΣΕΙΣ ΜΑΘΗΤΗ

ΙΝΣΤΙΤΟΥΤΟ ΤΕΧΝΟΛΟΓΙΑΣ ΥΠΟΛΟΓΙΣΤΩΝ & ΕΚΔΟΣΕΩΝ
«ΔΙΟΦΑΝΤΟΣ»

ΙΝΣΤΙΤΟΥΤΟ ΕΚΠΑΙΔΕΥΤΙΚΗΣ ΠΟΛΙΤΙΚΗΣ
Πρόεδρος: **Γκλαβάς Σωτήριος**

ΓΡΑΦΕΙΟ ΕΡΕΥΝΑΣ, ΣΧΕΔΙΑΣΜΟΥ ΚΑΙ ΕΦΑΡΜΟΓΩΝ Β΄
Προϊστάμενος: **Μάραντος Παύλος**
Επιστημονικά Υπεύθυνος: **Δρ. Τσαπέλας Θεοδόσιος,** Σύμβουλος Β΄ Πληροφορικής ΙΕΠ

ΣΥΓΓΡΑΦΙΚΗ ΟΜΑΔΑ:
Βασιλάκης Βασίλειος, MSc, Εκπαιδευτικός Πληροφορικής
Δρακόπουλος Ιωάννης, MSc, Εκπαιδευτικός Πληροφορικής
Θεμελής Θεόδωρος, MSc, Εκπαιδευτικός Πληροφορικής
Κωνσταντοπούλου Μαρία-Δήμητρα, MSc, MEd, Εκπαιδευτικός Πληροφορικής

ΕΠΙΜΕΛΕΙΑ – ΣΥΝΤΟΝΙΣΜΟΣ ΟΜΑΔΑΣ:
Κωτσάκης Σταύρος, Σχολικός Σύμβουλος Πληροφορικής

ΕΠΙΤΡΟΠΗ ΚΡΙΣΗΣ:
Αράπογλου Αριστείδης, Εκπαιδευτικός Πληροφορικής
Μπόγρης Αντώνιος, Αναπληρωτής Καθηγητής Τ.Ε.Ι. Αθηνών
Σπανουδάκης Εμμανουήλ, Εκπαιδευτικός Πληροφορικής.

ΦΙΛΟΛΟΓΙΚΗ ΕΠΙΜΕΛΕΙΑ
Γιακουμής Φώτιος, Εκπαιδευτικός Φιλόλογος

ΠΡΟΕΚΤΥΠΩΤΙΚΕΣ ΕΡΓΑΣΙΕΣ: ΔΙΕΥΘΥΝΣΗ ΕΚΔΟΣΕΩΝ/Ι.Τ.Υ.Ε. «ΔΙΟΦΑΝΤΟΣ»

Περιεχόμενα

Πρόλογος

Το παρόν σύνολο σημειώσεων έχει ως σκοπό οι μαθητές να εμβαθύνουν σε προχωρημένα θέματα του υλικού και των δικτύων υπολογιστών και να αποκτήσουν εξειδικευμένες γνώσεις και δεξιότητες πάνω στα θέματα που πραγματεύονται, μέσω της μελέτης και της εκτέλεσης των προτεινόμενων ασκήσεων σε κάθε κεφάλαιο.

Ο εργαστηριακός προσανατολισμός τους ενισχύει την εξοικείωση με την πρακτική εφαρμογή της θεωρίας του υλικού και των δικτύων των υπολογιστικών συστημάτων και παράλληλα αποζητά την ουσιαστική επαφή των μαθητών με τον εξοπλισμό και τις ρυθμίσεις που απαιτούνται από τη θεματολογία που καλύπτουν τα επιμέρους κεφάλαια.

Επιπροσθέτως, το μάθημα στοχεύει στην ανάπτυξη της κριτικής, συνθετικής και αναλυτικής σκέψης των μαθητών, αλλά και στην εξοικείωση και αρμονική συνεργασία ομάδων και στη σύνθεση των απόψεων των μελών τους, μέσω της εφαρμογής των προτεινόμενων εργαστηριακών και ομαδοσυνεργατικών ασκήσεων.

Από τους Συγγραφείς

Κεφάλαιο 1ο

Μέθοδοι Αύξησης των Επιδόσεων ενός Υπολογιστικού Συστήματος

Εισαγωγή

Η αύξηση των επιδόσεων ενός υπολογιστικού συστήματος μπορεί να πραγματοποιηθεί είτε με αλλαγή μονάδων υλικού, είτε με τροποποίηση των τιμών λειτουργίας τους, διαδικασία που ονομάζεται υπερχρονισμός. Ο υπερχρονισμός εξαρτάται από τα κατασκευαστικά χαρακτηριστικά μιας μονάδας υλικού και τα αποτελέσματά του είναι μοναδικά για κάθε σύστημα. Είναι μια διαδικασία που κερδίζει συνεχώς οπαδούς ανά τον κόσμο, καθώς επιφέρει σημαντικά πλεονεκτήματα απόδοσης, όμως έχει και σημαντικούς κινδύνους αν δεν εφαρμοστεί σωστά, λόγω της αυξημένης θερμότητας που παράγεται από τις υπερχρονισμένες μονάδες.

Διδακτικοί Στόχοι

Με την ολοκλήρωση του 1ου κεφαλαίου οι μαθητές θα πρέπει να είναι σε θέση να:

- Αναγνωρίζουν την ανάγκη για αύξηση των επιδόσεων ενός συστήματος.
- Περιγράφουν τους τρόπους αναβάθμισης ενός συστήματος.
- Επιλέγουν το κατάλληλο υλικό για αναβάθμιση ενός συστήματος.
- Εξοικειωθούν με τις τεχνικές υπερχρονισμού της ταχύτητας της Κεντρική Μονάδας Επεξεργασίας, της Κύριας Μνήμης και της Κάρτας Γραφικών ενός συστήματος.
- Εξηγούν τους κινδύνους που προκαλούνται από ενέργειες υπερχρονισμού.

Διδακτικές Ενότητες

1.1 Μέθοδοι αναβάθμισης μονάδων υλικού υπολογιστικού συστήματος.
1.2 Υπερχρονισμός μονάδων υλικού.
1.3 Αύξηση Επιδόσεων Κάρτας Γραφικών.
1.4 Πλεονεκτήματα και κίνδυνοι.

1.1 Μέθοδοι αναβάθμισης μονάδων υλικού υπολογιστικού συστήματος

Η αναβάθμιση του υλικού ενός ηλεκτρονικού υπολογιστή (Η/Υ) μπορεί να πραγματοποιηθεί με δύο τρόπους:

- Με **αντικατάσταση μερών του υλικού με άλλα υψηλότερων επιδόσεων**. Σε αυτή την περίπτωση απαιτείται προμήθεια νέου εξοπλισμού, συνήθως ακριβότερου σε κόστος από τον ήδη υπάρχοντα και αντικατάσταση και απόρριψη του παλιού. Επιπρόσθετα, πρέπει να είμαστε σίγουροι ότι το νέο υλικό μπορεί να προσαρμοστεί στον υπάρχοντα εξοπλισμό και μπορεί να συνεργάζεται αρμονικά με το υπόλοιπο σύστημα.
- Με **τροποποίηση των τιμών των παραμέτρων** των ήδη υπαρχόντων μονάδων υλικού, διαδικασία που ονομάζεται υπερχρονισμός υλικού. Στον υπερχρονισμό με τη χρήση ειδικού λογισμικού μπορεί ένας χρήστης να αυξήσει τις επιδόσεις του συστήματος, χωρίς να αντικαταστήσει μονάδες υλικού. Είναι πιθανό όμως να χρειαστεί να ενισχύσει το σύστημα ψύξης του Η/Υ με προσθήκη ανεμιστήρων ή αντικατάσταση των παλιών με μεγαλύτερους.

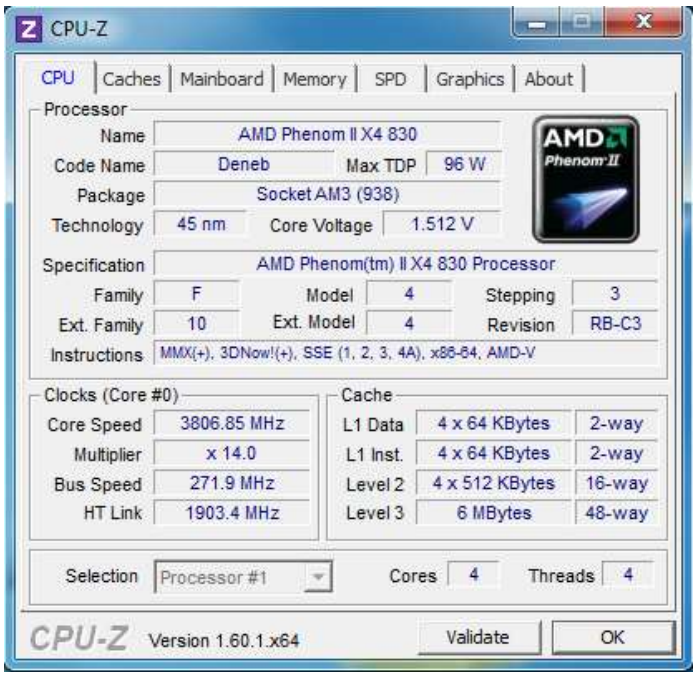
1.2 Υπερχρονισμός μονάδων υλικού

Ο υπερχρονισμός (overclocking) είναι η διαδικασία που αναγκάζει έναν υπολογιστή ή μια μονάδα υλικού του, να λειτουργήσουν ταχύτερα από τη συχνότητα χρονισμού που ορίζει ο κατασκευαστής τους. Η διαδικασία αυτή μπορεί επίσης να περιλαμβάνει την αύξηση της τάσης του ηλεκτρικού ρεύματος μιας μονάδας υλικού, η οποία αυξάνει την ταχύτητα λειτουργίας έως του βαθμού όπου το σύστημα εξακολουθεί να ανταποκρίνεται με σταθερότητα. Η τεχνική αυτή μπορεί να βελτιώσει σημαντικά την απόδοση του Η/Υ, όμως μπορεί παράλληλα να προκαλέσει ζημιά στο υλικό του, αν δεν γίνει με το σωστό τρόπο.

Η δυνατότητα υπερχρονισμού μιας μονάδας υλικού οφείλεται στο γεγονός ότι οι κατασκευαστές υλικού συνήθως ορίζουν τη λειτουργία των μονάδων που κατασκευάζουν σε χαμηλότερα επίπεδα απόδοσης από αυτά που πραγματικά μπορούν να επιτύχουν. Αυτό συμβαίνει είτε γιατί επιλέγουν να προσαρμόσουν τις μονάδες υλικού σε στάνταρ που επιτρέπουν χαμηλότερη κατανάλωση ενέργειας, μικρότερες ανάγκες ψύξης, αθόρυβη λειτουργία και μεγαλύτερη διάρκεια ζωής των μπαταριών του συστήματος.

Ο υπερχρονισμός βασίζεται στις πραγματικές επιδόσεις κατασκευής του υλικού. Ωστόσο είναι αξιοσημείωτο ότι αν δύο συστήματα έχουν ακριβώς το ίδιο υλικό, ο υπερχρονισμός δεν θα αποφέρει και για τα δύο όμοια αποτελέσματα. Αυτό οφείλεται στο γεγονός ότι η διαδικασία αυτή επηρεάζεται σε σημαντικό βαθμό από τις μικρές αποκλίσεις κατά τη φάση κατασκευής του υλικού. Επομένως δεν μπορούν να υπάρχουν σταθερές μετρήσεις ή διεθνείς τυποποιήσεις για τον υπερχρονισμό, καθώς κάθε μονάδα υλικού συμπεριφέρεται μοναδικά κατά την εφαρμογή της διαδικασίας αύξησης επιδόσεων.

Για την πραγματοποίηση της διαδικασίας υπερχρονισμού είναι απαραίτητη η εγκατάσταση ειδικών προγραμμάτων μέτρησης επιδόσεων (benchmark programs) και παρακολούθησης (monitoring programs) που ελέγχουν τις επιδόσεις των επιμέρους μονάδων του συστήματος και μας βοηθούν στον έλεγχο των τιμών των παραμέτρων που πρέπει να επηρεαστούν, όπως τα CPU-Z, Prime95, Heaven, 3DMark κ.α. για τα Windows και c2ctl (Intel), k10ctl (AMD), TurionPowerContol (AMD) για Linux.



Εικόνα 1.1: Πρόγραμμα παραμετροποίησης των τιμών ενός επεξεργαστή AMD Phenom II.

Τέλος, οι μονάδες υλικού ενός Η/Υ, οι οποίες συνήθως επιδέχονται αύξηση της επίδοσής τους με τη βοήθεια της διαδικασίας του υπερχρονισμού είναι η Κεντρική Μονάδα Επεξεργασίας, η Κύρια Μνήμη, η Κάρτα Γραφικών και το σύνολο ολοκληρωμένων κυκλωμάτων (chipset) της Μητρικής Πλακέτας.

1.2.1 Υπερχρονισμός Κεντρική Μονάδας Επεξεργασίας (Κ.Μ.Ε.)

Ο υπερχρονισμός της Κεντρικής Μονάδας Επεξεργασίας (Κ.Μ.Ε.) είναι μια διαδικασία κατά την οποία αυξάνεται η ταχύτητα με την οποία λειτουργεί η Κ.Μ.Ε. και επιτρέπεται η μεγιστοποίηση της απόδοσης ενός Η/Υ. Όπως προαναφέραμε, πριν την έναρξη της διαδικασίας είναι απαραίτητη η εγκατάσταση ειδικών προγραμμάτων που επιτρέπουν την αλλαγή των παραμέτρων λειτουργίας της Κ.Μ.Ε.

Στη διαδικασία του υπερχρονισμού αυξάνουμε κατ' ουσία σταδιακά την τάση του ηλεκτρικού ρεύματος και την ταχύτητα του ρολογιού της Κ.Μ.Ε. και παράλληλα ελέγχουμε τη σταθερότητα του Η/Υ, ώστε να εξασφαλίσουμε ότι η θερμοκρασία της Κ.Μ.Ε. δεν είναι υψηλή. Τα βήματα είναι τα εξής:

- Κάθε φορά που αυξάνουμε την ταχύτητα του ρολογιού-πολλαπλασιαστή της Κ.Μ.Ε. (CPU multiplier), ελέγχουμε τη θερμοκρασία της Κ.Μ.Ε.
- Σταματούμε τη διαδικασία όταν η λειτουργία του Η/Υ γίνεται ασταθής ή η Κ.Μ.Ε. θερμαίνεται πολύ. Συνήθως προτείνεται η θερμοκρασία του συστήματος να παραμένει χαμηλότερη των 80°C, ενώ το όριο συνήθως είναι οι 90°C.
- Στην περίπτωση που η Κ.Μ.Ε. θερμανθεί πολύ, τότε πρέπει να μειώσουμε την ταχύτητα του ρολογιού στην προηγούμενη τιμή της, κατά την οποία η θερμοκρασία της Κ.Μ.Ε. ήταν σε αποδεκτά επίπεδα.
- Στην περίπτωση που η Κ.Μ.Ε. δεν θερμαίνεται πολύ, αλλά η λειτουργία του Η/Υ γίνεται ασταθής, τότε πρέπει είτε να αυξήσουμε την τάση του ηλεκτρικού ρεύματος που δέχεται η Κ.Μ.Ε. (CPU Vcore), είτε να μειώσουμε την ταχύτητα του ρολογιού στην προηγούμενη τιμή της, κατά την οποία ο Η/Υ λειτουργούσε φυσιολογικά.

Σε αυτό το σημείο πρέπει να τονίσουμε ότι η αύξηση της τάσης της Κ.Μ.Ε., οδηγεί στην αύξηση της ποσότητας θερμότητας που παράγεται από την Κ.Μ.Ε. Επομένως η υψηλή τάση στη λειτουργία της Κ.Μ.Ε., με υψηλές τιμές θερμοκρασίας, για παρατεταμένη περίοδο μπορεί να οδηγήσουν στην οριστική βλάβη της Κ.Μ.Ε.

1.2.2 Υπερχρονισμός Κύριας Μνήμης

Η διαδικασία του υπερχρονισμού της κύριας μνήμης ενός Η/Υ έχει αρκετά κοινά στοιχεία με τον υπερχρονισμό της Κ.Μ.Ε., όμως τα αποτελέσματα της δεν μπορούν να συγκριθούν με αυτά του υπερχρονισμού της Κ.Μ.Ε., ο οποίος έχει καλύτερη απόδοση. Ωστόσο, έχει και αυτή πλεονεκτήματα που δεν θεωρούνται αμελητέα.

Τα βήματα για τον υπερχρονισμό της μνήμης είναι τα εξής:

- Πριν από οποιαδήποτε προσπάθεια υπερχρονισμού απαραίτητος είναι ο έλεγχος της κατάστασης και της σταθερότητας της μνήμης με κατάλληλο λογισμικό (πχ. Windows Memory Diagnostic ή MemTest86).
- Αν τα αποτελέσματα του ελέγχου εμφανίσουν λάθη, τότε οφείλουμε να ελέγξουμε αν λειτουργεί η μνήμη με το χρονισμό και την τάση που προτείνει ο κατασκευαστής της.
- Αν η μνήμη δεν εμφανίζει προβλήματα κατά τον προηγούμενο έλεγχο, μπορούμε να αυξήσουμε αρχικά το χρονισμό της μνήμης αυξάνοντας της τιμή της και δοκιμάζοντας τα αποτελέσματα με τη χρήση ειδικού λογισμικού (πχ. SiSoft Sandra).

- Στη συνέχεια μπορούμε να αυξήσουμε την ταχύτητα στη μέγιστη τιμή χρονισμού του Βασικού Ρολογιού (Base Clock ή BCLK) που επιτρέπει το BIOS του Η/Υ, το οποίο επηρεάζει και την απόδοση της μνήμης. Αυτό μπορεί να γίνει είτε αυξάνοντας τον πολλαπλασιαστή μνήμης (memory multiplier), είτε μειώνοντας την αναλογία του χρονισμού. Η μέθοδος που θα χρησιμοποιηθεί εξαρτάται από το συγκεκριμένο BIOS.
- Τέλος μπορούμε να μειώσουμε το χρόνο που παρεμβάλλεται ανάμεσα στην αίτηση της Κ.Μ.Ε. για δεδομένα και στην αποστολή τους από τη μνήμη (CAS latency).

Η διαδικασία του υπερχρονισμού της κύριας μνήμης, συνήθως γίνεται συνδυαστικά με τη διαδικασία υπερχρονισμού της ΚΜΕ και επιφέρει μεγάλη διαφορά στην αύξηση των επιδόσεων κατά τη χρήση στην επιφάνεια εργασίας ενός λειτουργικού συστήματος και στη διαχείριση των αρχείων. Άλλωστε το Βασικό Ρολόι επηρεάζει εκτός από τη συχνότητα λειτουργίας της Κύριας Μνήμης, τη συχνότητα της Κ.Μ.Ε. και άλλες μονάδες.

Ουσιαστικά ο υπερχρονισμός συνδυαστικά Μνήμης και Κ.Μ.Ε. μπορεί να γίνει με δυο τρόπους. Είτε με αύξηση της τιμής του Πολλαπλασιαστή Κ.Μ.Ε. και μείωση της τιμής του Βασικού Ρολογιού, είτε με το αντίθετο, δηλαδή την αύξηση της τιμής του Βασικού Ρολογιού και μείωση της τιμής του Πολλαπλασιαστή Κ.Μ.Ε. Συνήθως η χρυσή τομή της καλύτερης απόδοσης του υπερχρονισμού βρίσκεται αυξομειώνοντας τις τιμές και δοκιμάζοντας την απόδοση ώστε να βρεθεί το καλύτερο σημείο αυτής.

1.3 Αύξηση Επιδόσεων Κάρτας Γραφικών

1.3.1 Διαδικασία Υπερχρονισμού Κάρτας Γραφικών

Για την εφαρμογή του υπερχρονισμού στις κάρτες γραφικών, η διαδικασία είναι περίπου όμοια με τις προηγούμενες περιπτώσεις που αναφέρθηκαν. Για την πραγματοποίηση του υπερχρονισμού της κάρτας γραφικών μπορεί να χρησιμοποιηθεί ειδικό λογισμικό (overclocking utilities) που παρέχουν οι κατασκευαστές της, αλλά και λογισμικό παραμετροποίησης που είναι συμβατό με τις πιο γνωστές κάρτες γραφικών, όπως το MSI Afterburner.

Τα βήματα για τον υπερχρονισμό μιας κάρτας γραφικών είναι τα εξής:

- Αρχικά πρέπει να γίνει ενημέρωση του οδηγού της κάρτας γραφικών, ώστε να έχει την πιο πρόσφατη ενημέρωση του κατασκευαστή. Συνήθως οι νεότεροι οδηγοί εξασφαλίζουν τη σταθερότητα λειτουργίας της μονάδας και αυξάνουν την απόδοση της.
- Στη συνέχεια προτείνεται η ρύθμιση των γραφικών και της ανάλυσης στα επίπεδα που είναι επιθυμητά από το χρήστη του συστήματος.
- Τροποποιούμε τις τιμές της ηλεκτρικής τάσης και παράλληλα ελέγχουμε την αύξηση της θερμοκρασίας, ώστε να μην ξεπεράσει τα αποδεκτά όρια 90oC. Η ενίσχυση της ψύξης τόσο της Κ.Μ.Ε., όσο και της κάρτας γραφικών, είναι μια λύση που προτείνεται ώστε να έχει καλύτερα αποτελέσματα η διαδικασία του υπερχρονισμού.
- Αν μετά την ολοκλήρωση του υπερχρονισμού δεν διαφαίνονται αποδεκτά επίπεδα βελτίωση του συστήματος, τότε μπορούμε να τροποποιήσουμε τις αρχικές ρυθμίσεις των γραφικών και της ανάλυσης και να επαναλάβουμε τη διαδικασία.

Οι διαδικασίες υπερχρονισμού της κάρτας γραφικών, αλλά και της Κ.Μ.Ε. και της Κύριας Μνήμης μπορεί να γίνουν παράλληλα. Μάλιστα συνήθως ο υπερχρονισμός και μόνο της Κ.Μ.Ε. μπορεί να αυξήσει τις επιδόσεις και των υπόλοιπων μονάδων υλικού. Ωστόσο αν ο χρήστης δεν έχει εμπειρία στην εφαρμογή της διαδικασίας, καλό είναι να προχωρήσει βήμα-βήμα στον υπερχρονισμό κάθε μονάδας ξεχωριστά.

1.3.2 Τεχνολογίες πολλαπλών καρτών γραφικών

Η αύξηση των επιδόσεων στην επεξεργασία γραφικών μπορεί να επιτευχθεί και με την τεχνολογία των πολλαπλών καρτών γραφικών, με πιο συνηθισμένη αυτή της διπλής εγκατάστασης. Οι πιο γνωστές τεχνολογίες που υποστηρίζουν την πολλαπλή εγκατάσταση και λειτουργία καρτών γραφικών είναι η **Crossfire της AMD** και η **SLI (Scalable Link Interface) της NVIDIA**. Σε ορισμένες μητρικές πλακέτες υπάρχει η δυνατότητα να τοποθετηθεί και μια δεύτερη κάρτα γραφικών, η οποία λειτουργεί παράλληλα με την αρχική, αυξάνοντας την ταχύτητα επεξεργασίας γραφικών. Προϋπόθεση εκμετάλλευσης αυτής της τεχνικής είναι το εγκατεστημένο λειτουργικό σύστημα να υποστηρίζει την τεχνολογία αυτή, όπως είναι τα Λ.Σ MS Windows Vista, 7, 8 και Linux. Μάλιστα οι παραπάνω εκδόσεις των Λ.Σ MS Windows υποστηρίζουν την εγκατάσταση τριών ή και τεσσάρων καρτών γραφικών στο ίδιο σύστημα.

Εικόνα 1.2: Εγκατάσταση διπλών καρτών γραφικών τεχνολογίας Crossfire

(Πηγή: http://www.legionhardware.com/articles_pages/nvidia_geforce_8800_gt_sli_vs_amd_radeon_hd_3870_crossfire,1.html)

Εικόνα 1.3: Εγκατάσταση διπλών καρτών γραφικών τεχνολογίας SLI

(Πηγή: http://www.hartware.de/press_2575.html)

Η μητρική πλακέτα που μπορεί να υποστηρίξει αυτή την τεχνολογία πρέπει να έχει πολλαπλές υποδοχές τύπου PCI (PCI Express slots) και τους απαραίτητους αριθμητικά συνδετήρες παροχής ρεύματος, τουλάχιστον των 800 watt, για τις κάρτες γραφικών. Επίσης οι κάρτες γραφικών που θα χρησιμοποιηθούν πρέπει να είναι συμβατές με την τεχνολογία SLI ή Crossfire, να είναι το ίδιο μοντέλο ή και να έχουν την ίδια εσωτερική μνήμη.

Μετά την τοποθέτησή τους στην υποδοχή PCI της μητρικής πλακέτας, τις συνδέουμε με ένα συνδετήρα στην κορυφή τους, που ονομάζεται γέφυρα SLI ή Crossfire (SLI/Crossfire bridge).

Αν και η σύνδεση των καρτών γραφικών μπορεί να γίνει χωρίς την παρουσία της γέφυρας SLI ή Crossfire, με τη χρήση απλά της υποδοχής PCI, τότε όμως υπάρχει μειωμένη απόδοση στο σύστημα γραφικών. Για τη σύνδεση περισσότερων των δύο καρτών γραφικών, αρκεί οι κάρτες που θα εγκατασταθούν να έχουν δύο υποδοχές ακραίων συνδετήρων-γεφυρών SLI/Crossfire αντί του ενός που έχουν οι περισσότερες.

Εικόνα 1.4: Γέφυρες SLI και Crossfire

(Πηγή: http://forum.worldoftanks.com/index.php?/topic/342711-nvidia-geforce-sli/)

Τέλος για την ενεργοποίησης της τεχνολογίας πολλαπλών καρτών γραφικών απαιτείται η **εγκατάσταση των οδηγών και για τις δύο κάρτες γραφικών** και στη συνέχεια η **ενεργοποίηση της από το λογισμικό παραμετροποίησης** (Control Panel) της κάρτας γραφικών που είναι εγκατεστημένο στον Η/Υ. Η παράμετρος που πρέπει να επιλεγεί είναι η για παράδειγμα η Maximize 3D performance ή Enable AMD CrossFireX, ανάλογα με την έκδοση του λογισμικού παραμετροποίησης και του μοντέλου της κάρτας γραφικών

Οι **βασικές διαφορές** των τεχνολογιών SLI NVIDIA και Crossfire AMD είναι οι εξής:

- Οι κάρτες γραφικών SLI που θα χρησιμοποιηθούν πρέπει να έχουν όμοιους επεξεργαστές γραφικών (GPUs) και εσωτερική μνήμη, ενώ αυτές της Crossfire πρέπει απλά να ανήκουν στην ίδια «οικογένεια» μοντέλων και δεν απαιτείται να έχουν τις ίδιες προδιαγραφές εσωτερικής μνήμης.
- Η τεχνολογία Crossfire είναι διαθέσιμη σε περισσότερες μητρικές πλακέτες.
- Οι νεότερες Crossfire συμβατές κάρτες γραφικών δεν απαιτούν συνδετήρες – γέφυρες.
- Σε Crossfire συμβατές κάρτες γραφικών, οι επεξεργαστές γραφικών (GPUs) μπορούν να συνεργαστούν με τις ενσωματωμένες στη μητρική μονάδες επεξεργασίας APUs (AMD-Accelerated Processing Units).

Σε γενικές γραμμές και μέχρι στιγμής, η τεχνολογία SLI είναι λίγο πιο περιοριστική σε σχέση με την τεχνολογία Crossfire, η οποία είναι πιο ευέλικτη.

1.4 Πλεονεκτήματα και κίνδυνοι

Βασικό πλεονέκτημα του υπερχρονισμού είναι ότι μπορούμε να προμηθευτούμε μια σχετικά φθηνή και χαμηλών επιδόσεων μονάδα υλικού και με τον υπερχρονισμό να συναγωνίζεται σε απόδοση μια πιο ακριβή και υψηλότερων επιδόσεων μονάδα υλικού. Με αυτό τον τρόπο παρατείνουμε, επίσης, τη χρηστικότητα παλιού εξοπλισμού, που θα θεωρούνταν παρωχημένης τεχνολογίας. Επιπλέον ορισμένες φορές μπορεί ο υπερχρονισμός μιας μονάδας υλικού να οδηγήσει στη διαπίστωση ότι άλλη συνεργαζόμενη μονάδα υλικού έχει μεγαλύτερες δυνατότητες ή να οδηγήσει στην εκμετάλλευση των ήδη γνωστών δυνατοτήτων της, οι οποίες όμως έμεναν αναξιοποίητές λόγω της χαμηλής απόδοσης του υπόλοιπου εξοπλισμού.

Ο υπερχρονισμός, όμως, περιέχει και κινδύνους για την υγεία του υλικού του Η/Υ, καθώς είναι αρκετός για να οδηγήσει σε προβληματική συμπεριφορά ένα υπολογιστικό σύστημα ή ακόμα και στην καταστροφή υλικού του. Οι περισσότερες τεχνικές υπερχρονισμού αυξάνουν την κατανάλωση ενέργειας και παράγουν περισσότερη θερμότητα, η οποία πρέπει να διασκορπίζεται αν θέλουμε το εξάρτημα να παραμείνει λειτουργικό. Επίσης η αυξημένη θερμότητα μέσα στη θήκη του συστήματος μπορεί να επηρεάσει τη λειτουργία άλλων μονάδων υλικού του Η/Υ. Επομένως είναι σημαντική η εξασφάλιση και εφαρμογή μεγαλύτερου βαθμού ψύξης για να αποφευχθούν οι πιθανοί κίνδυνοι, λόγω της θερμότητας που παράγεται από τα υπερχρονισμένα τμήματα υλικού. Για αυτό το λόγο οι φορητοί υπολογιστές δεν είναι κατάλληλοι για υπερχρονισμό, καθώς έχουν περιορισμένες δυνατότητες ψύξης, σε σχέση με τους σταθερούς υπολογιστές με θήκη στους οποίους μπορούμε να διαχειριστούμε την ψύξη πιο αποτελεσματικά.

Άλλα πιθανά μειονεκτήματα είναι η αύξηση της κατανάλωσης και κατά συνέπεια και του κόστος ηλεκτρικής ενέργειας. Επιπρόσθετα ένα υπερχρονισμένο σύστημα μπορεί να δείχνει σταθερό, ωστόσο μικρά μη ανιχνεύσιμα λάθη αποτελούν σημαντική απειλή για εφαρμογές που πρέπει να είναι αλάνθαστες, όπως για παράδειγμα επιστημονικές ή χρηματοοικονομικές εφαρμογές.

Τέλος, θα πρέπει να τονίσουμε ότι ο υπερχρονισμός μπορεί να μην οδηγεί πάντα σε επιθυμητά αποτελέσματα απόδοσης, καθώς η γενικότερη απόδοση ενός συστήματος μπορεί να επηρεάζεται από τη χαμηλή ταχύτητα πρόσβασης στο σκληρό δίσκο, της σύνδεσης δικτύου/Διαδικτύου και της επεξεργασίας γραφικών από την κάρτα γραφικών. Δηλαδή, ενώ υπερχρονίζουμε ένα σύστημα, αυτό τελικά ενδέχεται να μην έχει εμφανή αποτελέσματα στην τελική απόδοση λειτουργίας του συστήματος ή ορισμένων εφαρμογών που εξαρτώνται από τη λειτουργία και άλλων στοιχείων, όπως το Διαδίκτυο ή τα γραφικά.

Ερωτήσεις Ανακεφαλαίωσης

1. Με ποιους τρόπους μπορεί να γίνει η αναβάθμιση μονάδων υλικού ενός υπολογιστικού συστήματος;
2. Τι είναι ο υπερχρονισμός;
3. Που οφείλεται η δυνατότητα υπερχρονισμού που έχουν κάποιες μονάδες υλικού;
4. Δύο ίδιες μονάδες υλικού έχουν τα ίδια αποτελέσματα μετά την εφαρμογή της διαδικασίας υπερχρονισμού; Ναι ή όχι και γιατί;
5. Ποια είναι τα βασικά βήματα της διαδικασίας του υπερχρονισμού της Κεντρικής Μονάδας Επεξεργασίας;
6. Ποια είναι τα βασικά βήματα της διαδικασίας του υπερχρονισμού της Κύριας Μνήμης;
7. Με ποιο τρόπο μπορούν να υπερχρονιστούν συνδυαστικά η Κεντρική Μονάδα Επεξεργασίας και η Κύρια Μνήμη;
8. Ποια είναι τα βασικά βήματα της διαδικασίας του υπερχρονισμού μιας Κάρτας Γραφικών;
9. Ποιες είναι οι προϋποθέσεις στο υλικό ενός Η/Υ, ώστε να εφαρμοστεί η τεχνολογίας διπλών καρτών γραφικών;
10. Ποια είναι τα στοιχεία/μονάδες υλικού που είναι απαραίτητες για την εφαρμογή της τεχνολογίας διπλών καρτών γραφικών;
11. Ποιες είναι οι βασικές διαφορές των τεχνολογιών SLI NVIDIA και Crossfire AMD;
12. Ποια είναι τα βασικά πλεονεκτήματα του υπερχρονισμού;
13. Ποια είναι τα βασικά μειονεκτήματα του υπερχρονισμού;
14. Για ποιο λόγο οι φορητοί υπολογιστές δεν μπορούν να υπερχρονιστούν;

Ασκήσεις

1η Άσκηση (Σε εργαστηριακό περιβάλλον)

1. Ανοίξτε το BIOS του Η/Υ κατά την εκκίνηση του πατώντας το πλήκτρο που ζητείται (DEL, F2, F10, F12) και προσπαθήστε να εντοπίσετε τις ακόλουθες παραμέτρους:
   - Πίνακας ελέγχου συχνοτήτων: Frequency Control
   - Πίνακας ελέγχου ηλεκτρικής τάσης: Voltage Control
   - Πολλαπλασιαστής Κύριας Μνήμης (RAM) με όνομα: Memory multiplier ή DDR Memory Frequency ή Memory Ratio
   - Βασικό Ρολόι χρονισμού: Base Clock ή BCLK
   - Συχνότητα χρονισμού Κ.Μ.Ε.: CPU frequency.

   Προσοχή! Κατά την έξοδο σας από την οθόνη χειρισμού του BIOS δεν πρέπει να αποθηκεύσετε καμία αλλαγή σε αυτό. Επομένως πρέπει κατά την έξοδο να επιλέξτε **έξοδος χωρίς αποθήκευση αλλαγών**.

2. Χωριστείτε σε ομάδες εργασίας. Κάθε ομάδα να συγκεντρώσει πληροφορίες από το Διαδίκτυο για κάποια ή κάποιες από τις παραπάνω παραμέτρους του BIOS.
3. Παρουσιάστε στην ολομέλεια της τάξης τα ευρήματα από την έρευνα που πραγματοποιήσατε.
4. Συζητείστε στη τάξη και απαντήστε στα ακόλουθα ερωτήματα:
   - Ποιος είναι ο βασικός ρόλος του Βασικού Ρολογιού Χρονισμού της Κ.Μ.Ε;
   - Ποια είναι η σημασία της Συχνότητας Χρονισμού της Κ.Μ.Ε; Τι μπορεί να επηρεάσει η μεταβολή της;

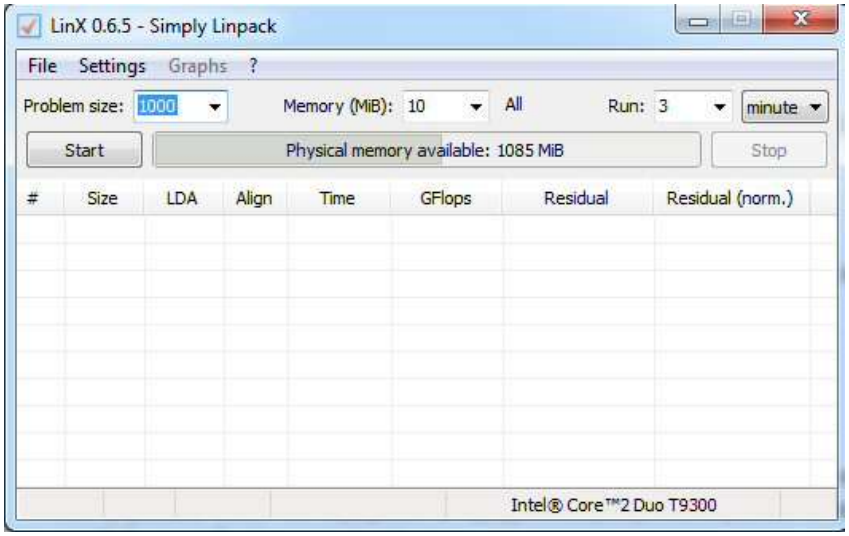
Άσκηση 2η (Σε εργαστηριακό περιβάλλον)

Εκτέλεση Βασικού Στρες-Τεστ σε έναν Η/Υ.

Σημείωση: Για την εκτέλεση της άσκησης απαιτείται η εγκατάσταση του προγράμματος LInX-Simply Linpack (Λήψη από: http://www.softpedia.com/get/System/Benchmarks/LinX-benchmark.shtml), το οποίο πραγματοποιεί επίλυση γραμμικών εξισώσεων δοκιμάζοντας τις αντοχές λειτουργίας ενός Η/Υ. Το βασικό παράθυρο διαχείρισής του επιτρέπει τον ορισμό του μεγέθους των προβλημάτων (problem size) προς επίλυση, τις φορές που θα εκτελεστούν ή το χρονικό διάστημα για το οποίο θα εκτελεστούν κ.α.

Ανοίγουμε το πρόγραμμα παρακολούθησης LinX. Με τη βοήθεια αυτού του λογισμικού θα πραγματοποιήσουμε ένα στρες-τεστ το οποίο θα μας δείξει τη σταθερότητα του συστήματος. Παρατηρήστε το παράθυρο εργασίας του προγράμματος, καταγράψτε τις παραμέτρους που βλέπετε και συζητήστε με τον εκπαιδευτικό σας για το τι συμβολίζει το κάθε ένα από αυτά:

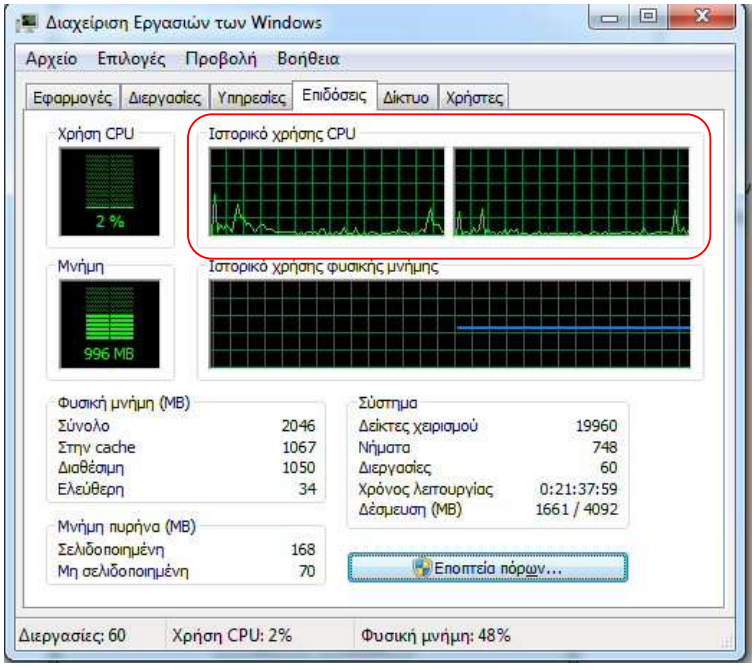
- Μέγεθος Προβλήματος (problem size)
- Μνήμη (Memory)
- Εκτέλεση (Run)



Εικόνα 1.5: Βασικό παράθυρο προγράμματος LinX

1. Ανοίξτε την καρτέλα settings (Παράμετροι). Ορίστε τα νήματα εκτέλεσης (threads) της Κ.Μ.Ε. Για να βρείτε πόσα υπάρχουν πηγαίνετε στη Διαχείριση Εργασιών του Λ.Σ MS Windows, στην καρτέλα επιδόσεις (Ctrl + Shift + Esc).

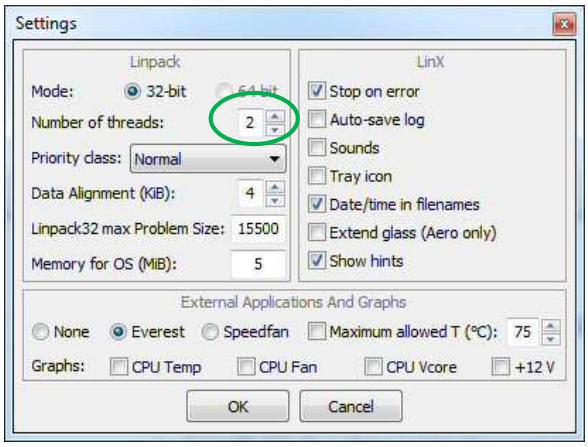
Ένα **νήμα** εκτέλεσης (thread) είναι η μικρότερη ακολουθία προγραμματισμένων εντολών, η οποία μπορεί να υποστεί ανεξάρτητη διαχείριση από το λειτουργικό σύστημα (Λ.Σ.). Μπορούν να υπάρχουν πολλαπλά νήματα μέσα σε μια διεργασία που εκτελείται από το Λ.Σ., τα οποία μπορούν να μοιράζονται πόρους από το σύστημα, όπως ο επεξεργαστής ή η μνήμη. *(Πηγή: el.wikipedia.org)*



Εικόνα 1.6: Παράθυρο Διαχείρισης Εργασιών του Λ.Σ MS Windows.

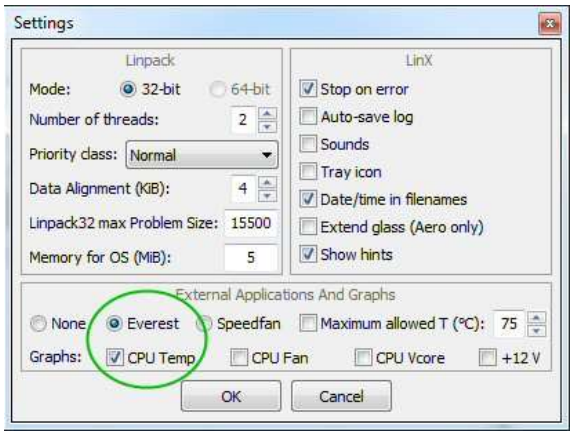
Π.χ. στην εικόνα 1.6 βλέπετε την προβολή των δύο (2) νημάτων της Κ.Μ.Ε. στο παράθυρο Διαχείρισης Εργασιών του Λ.Σ MS Windows (κόκκινο πλαίσιο). Αντίστοιχα

στην εικόνα 1.7 προβάλλονται τα δύο (2) νημάτων (Number of threads) της Κ.Μ.Ε. στο παράθυρο παραμέτρων (settings) προγράμματος LinX (πράσινο πλαίσιο).



Εικόνα 1.7: Παράθυρο παραμέτρων (settings) προγράμματος LinX.

2. Επιλέξτε στην καρτέλα παραμέτρων (settings) την εμφάνιση γραφικών για τον έλεγχο της θερμοκρασίας της Κ.Μ.Ε. (CPU Temp).

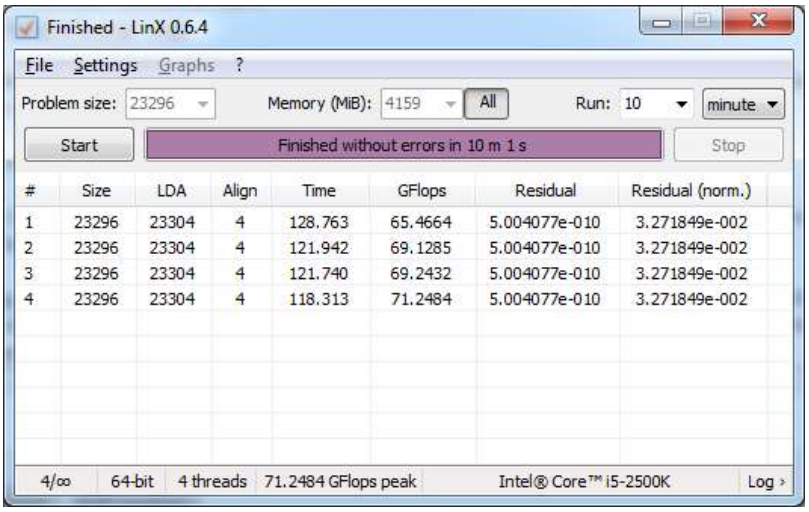


Εικόνα 1.8: Επιλογή παραμέτρου έλεγχου θερμοκρασίας Κ.Μ.Ε. του προγράμματος LinX.

3. Επιλέξτε την παράμετρο **All** (όλα) και εκτέλεση για 10 λεπτά.

Εικόνα 1.9: Επιλογή παραμέτρων All και τρόπου εκτέλεσης στρες-τεστ στο πρόγραμμα LinX.

4. Αν το στρες-τεστ δεν εμφανίσει λάθη, τότε θα ολοκληρωθεί η διαδικασία και θα εμφανιστεί μια εικόνα όπως πιο κάτω. Αν εμφανίσει λάθη, το πρόγραμμα θα διακόψει τον έλεγχο. Σε αυτή την περίπτωση είναι πιθανό η μνήμη (RAM) να έχει ελαττώματα.



Εικόνα 1.10: Προβολή αποτελεσμάτων στρες-τεστ προγράμματος LinX.

5. Τι προτείνετε να γίνει σε αυτή την περίπτωση που εμφανιστούν λάθη; Μπορούμε να προχωρήσουμε σε υπερχρονισμό και γιατί;

Άσκηση 3η (Σε εργαστηριακό περιβάλλον)

Η άσκηση αυτή πραγματοποιείται σε περιβάλλον λειτουργικού συστήματος εκδόσεων Linux. Απαιτεί την εγκατάσταση του Stress tool, το οποίο περιλαμβάνεται με τη διανομή των περισσότερων εκδόσεων Linux.

Σημείωση: Για την εκτέλεση της άσκησης προτείνονται οι εκδόσεις λειτουργικού συστήματος Debian ή Ubuntu Linux. Για την εγκατάσταση του Stress tool σε Debian ή Ubuntu Linux χρησιμοποιείται η εντολή:

apt-get install stress

Για περισσότερες πληροφορίες εγκατάστασης, αλλά και των παραμέτρων των εντολών που εφαρμόζονται στην άσκηση στο http://www.cyberciti.biz/faq/stress-test-linux-unix-server-with-stress-ng/

1. Εκτελέστε την ακόλουθη εντολή για την πραγματοποίηση ενός στρες-τεστ. Τροποποιήστε, αν χρειάζεται, τις παραμέτρους που χρησιμοποιούνται στο παράδειγμα (εκτέλεση για 60 δευτερόλεπτα, με 4 Κ.Μ.Ε. στρεσογόνους και χρησιμοποιώντας 1GB εικονικής μνήμης):

   $ stress-ng --cpu 4 --io 2 --vm 1 --vm-bytes 1G --timeout 60s --metrics-brief

   Το αποτέλεσμα θα είναι περίπου το εξής:

```
(root@cyberciti.biz )# uptime
 03:01:41 up 1 day,  1:32,  1 user,  load average: 0.22, 0.20, 0.22
(root@cyberciti.biz )# ./stress-ng --cpu 4 --io 2 --vm 1 --vm-bytes 1G --timeout 60s --metrics-brief
stress-ng: info: [42203] dispatching hogs: 4 cpu, 2 iosync, 1 vm
stress-ng: info: [42203] successful run completed in 63.15s
stress-ng: info: [42203] stressor      bogo ops real time  usr time  sys time   bogo ops/s   bogo ops/s
stress-ng: info: [42203]                        (secs)    (secs)    (secs)   (real time) (usr+sys time)
stress-ng: info: [42203] cpu              18109     60.01    234.20      0.81       301.75        77.06
stress-ng: info: [42203] iosync            1240     63.10      0.00     51.60        19.65        24.03
stress-ng: info: [42203] vm             1147008     59.99     34.58     21.57     19119.34     20427.57
(root@cyberciti.biz )# uptime
 03:03:33 up 1 day,  1:34,  1 user,  load average: 2.49, 1.32, 0.63
(root@cyberciti.biz )#
```

2. Εκτελέστε την ακόλουθη εντολή. Εκτελεί 2 στρες-τεστ για 10 λεπτά.

   $ stress-ng --all 2 --timeout 10m

3. Τι παρατηρείτε; Συζητήστε τα αποτελέσματα από την εκτέλεση της εντολής.
4. Εκτελέστε την ακόλουθη εντολή για την πραγματοποίηση ελέγχου των θερμοκρασιών:

   $ sensors

   Το αποτέλεσμα θα είναι περίπου το εξής:

   $ sensors
   acpitz-virtual-0
   Adapter: Virtual device
   temp1: +40.5°C (crit = +105.0°C)

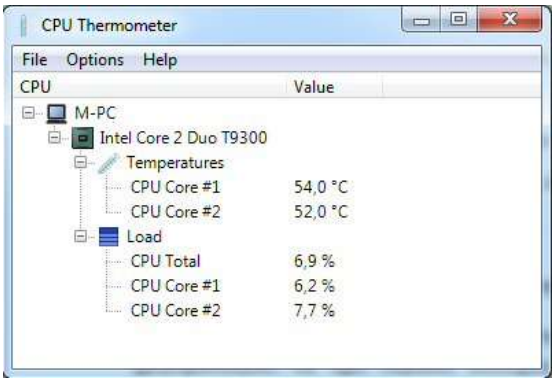
   coretemp-isa-0000
   Adapter: ISA adapter
   Core 0: +35.0°C (crit = +100.0°C)

   coretemp-isa-0001
   Adapter: ISA adapter
   Core 1: +40.0°C (crit = +100.0°C)

Άσκηση 4η (Σε εργαστηριακό περιβάλλον)

Επίδειξη εφαρμογής υπερχρονισμού σε Η/Υ με χρήση του Βασικού Ρολογιού (Base Clock).

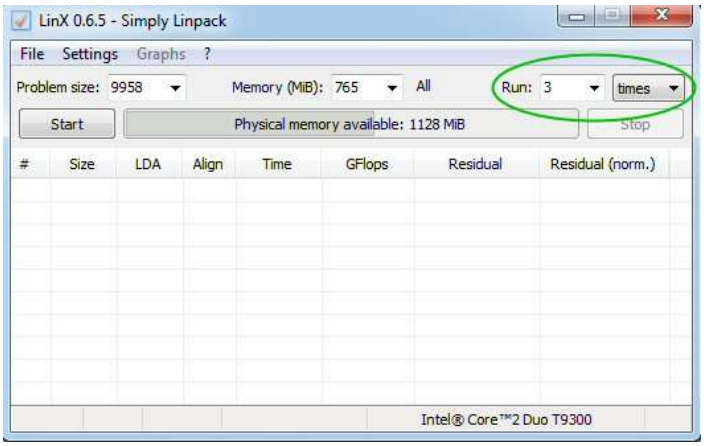
Πριν την έναρξη εκτέλεσης της άσκησης αυτής πρέπει ο υπολογιστής που θα χρησιμοποιηθεί **να έχει περάσει επιτυχώς το στρες-τεστ της 2ης άσκησης** και οι θερμοκρασίες να παρέμειναν κάτω από 70 °C. Για την παρακολούθηση της θερμοκρασίας χρησιμοποιήστε την εφαρμογή CPU Thermometer.



Εικόνα 1.11: Παράθυρο εφαρμογής CPU Thermometer.

1. Είσοδος στο BIOS του Η/Υ όπως στην 1η άσκηση.
2. Μείωση της ταχύτητας του δίαυλου μνήμης (memory bus) για την αποφυγή λαθών προερχόμενα από τη μνήμη. Αναζήτηση της παραμέτρου με όνομα **"Memory Multiplier" ή "DDR Memory Frequency" ή "Memory Ratio"** ή πάτημα Ctrl+Alt+F1 και μείωση της στη χαμηλότερη διαθέσιμη τιμή.
3. Αύξηση του Βασικού Ρολογιού κατά 10%. Αναζήτηση της παραμέτρου με όνομα CPU Base Clock και εφαρμογή της αλλαγής, πχ αν έχει τιμή 100 MHz να γίνει 110 MHz.
4. Επανεκκίνηση του υπολογιστή με αποθήκευση των αλλαγών.

5. Εκτέλεση ξανά του στρες-τεστ της 2ης άσκησης, με τη διαφορά ότι αντί για 10 λεπτά να εκτελεστεί για μερικούς κύκλους.



Εικόνα 1.12: Αλλαγή τρόπου εκτέλεσης στρες-τεστ στο πρόγραμμα LinX.

6. Παρακολούθηση της θερμοκρασίας, ώστε να είναι σε φυσιολογικά ανεκτά επίπεδα (70°C-80°C).
7. Αν δεν εμφανίσει λάθη το στρες-τεστ να επαναληφθούν τα βήματα 2 ως 6 μέχρι να εμφανίσει το τεστ λάθη.
8. Αν το στρες-τεστ εμφανίσει λάθη τότε πρέπει να επιστρέψει το Βασικό Ρολόι στην προηγούμενη τιμή του, με την οποία το τεστ δεν εμφάνισε λάθη.

Άσκηση 5η (Σε εργαστηριακό περιβάλλον)

Επίδειξη εφαρμογής υπερχρονισμού σε Η/Υ με χρήση του Πολλαπλασιαστή της Κ.Μ.Ε.

Πριν την έναρξη εκτέλεσης της άσκησης αυτής πρέπει ο υπολογιστής που θα χρησιμοποιηθεί να έχει περάσει επιτυχώς το στρες-τεστ της 2ης άσκησης και οι θερμοκρασίες να παρέμειναν κάτω από 70 °C. Για την παρακολούθηση της θερμοκρασίας χρησιμοποιήστε την εφαρμογή CPU Thermometer.

1. Είσοδος στο BIOS του Η/Υ όπως στην 1η άσκηση.
2. Εντοπισμός της παραμέτρου του Βασικού Ρολογιού (Base Clock).
3. Μείωση της ταχύτητας του Βασικού Ρολογιού κατά 5% για μεγαλύτερη ακρίβεια στην αύξηση των τιμών του Πολλαπλασιαστή Κ.Μ.Ε.
4. Εντοπισμός του Πολλαπλασιαστή της Κ.Μ.Ε. Η παράμετρος είναι η CPU Multiplier ή CPU Ratio ή κάτι παρόμοιο.
5. Αύξηση του Πολλαπλασιαστή της Κ.Μ.Ε. κατά 0,5. Η παράμετρος είναι η CPU Multiplier ή CPU Ratio ή κάτι παρόμοιο.
6. Επανεκκίνηση του υπολογιστή αποθηκεύοντας τις αλλαγές.
7. Εκτέλεση ξανά του στρες-τεστ της 2ης άσκησης, με τη διαφορά ότι αντί για 10 λεπτά να εκτελεστεί για μερικούς κύκλους.
8. Παρακολούθηση της θερμοκρασίας, ώστε να είναι σε φυσιολογικά ανεκτά επίπεδα (70°C-80°C).
9. Αν δεν εμφανίσει λάθη το στρες-τεστ να επαναληφθούν τα βήματα 2 ως 8 μέχρι να εμφανίσει το τεστ λάθη.
10. Αν το στρες-τεστ εμφανίσει λάθη τότε πρέπει να επιστρέψει ο Πολλαπλασιαστής της Κ.Μ.Ε. στην προηγούμενη τιμή του, με την οποία το τεστ δεν εμφάνισε λάθη.

Άσκηση 6η (Σε εργαστηριακό περιβάλλον)

Επίδειξη εφαρμογής υπερχρονισμού σε Η/Υ με χρήση της τάσης του ηλεκτρικού ρεύματος της Κ.Μ.Ε.

Πριν την έναρξη εκτέλεσης της άσκησης αυτής πρέπει ο υπολογιστής που θα χρησιμοποιηθεί να έχει περάσει επιτυχώς το στρες-τεστ της 2ης άσκησης και οι θερμοκρασίες να παρέμειναν κάτω από 70 °C. Για την παρακολούθηση της θερμοκρασίας χρησιμοποιήστε την εφαρμογή CPU Thermometer.

1. Είσοδος στο BIOS του Η/Υ όπως στην 1η άσκηση.
2. Εντοπισμός της παραμέτρου της τάσης του ηλεκτρικού ρεύματος της Κ.Μ.Ε. Η παράμετρος είναι η Vcore Voltage ή κάτι παρόμοιο.
3. Αύξηση της τάσης του ηλεκτρικού ρεύματος της Κ.Μ.Ε. κατά 0,025.
4. Επανεκκίνηση του υπολογιστή αποθηκεύοντας τις αλλαγές.
5. Εκτέλεση ξανά του στρες-τεστ της 2ης άσκησης, με τη διαφορά ότι αντί για 10 λεπτά να εκτελεστεί για μερικούς κύκλους.
6. Παρακολούθηση της θερμοκρασίας, ώστε να είναι σε φυσιολογικά ανεκτά επίπεδα (70°C-80°C).
7. Αν δεν εμφανίσει λάθη το στρες-τεστ να επαναληφθούν τα βήματα 2 ως 6 μέχρι να εμφανίσει το τεστ λάθη.
8. Αν το στρες-τεστ εμφανίσει λάθη τότε πρέπει να επιστρέψει η τάση του ηλεκτρικού ρεύματος της Κ.Μ.Ε. στην προηγούμενη τιμή της, κατά την οποία το τεστ δεν εμφάνισε λάθη.

Άσκηση 7η (Σε εργαστηριακό περιβάλλον)

1. Αναζητείστε βίντεο που να επιδεικνύουν τρόπους εγκατάστασης των διπλών καρτών γραφικών με χρήση τεχνολογιών SLI/Crossfire.

   Προτείνονται επίσης οι παρακάτω σύνδεσμοι με σχετικά βίντεο:

   - Για εγκατάσταση SLI τεχνολογίας: https://www.youtube.com/watch?v=--Wc0yppvCI
   - Για εγκατάσταση Crossfire τεχνολογίας: https://www.youtube.com/watch?v=kHqSAcLpHcs
2. Παρακολουθήσετε τον τρόπο εγκατάστασης των διπλών καρτών γραφικών στις υποδοχές PCI, της γέφυρας σύνδεσης τους στις υποδοχές SLI/Crossfire και της τροποποίησης των παραμέτρων μέσω λογισμικού για την ενεργοποίηση της τεχνολογίας SLI/Crossfire.
3. Συζητήστε ομαδικά και απαντήστε στο ακόλουθο ερώτημα:
   - Τι ομοιότητες και τις διαφορές παρατηρείτε ανάμεσα στις δύο αυτές εγκαταστάσεις διπλών καρτών γραφικών διαφορετικών τεχνολογιών;

Άσκηση 8η (Σε εργαστηριακό Περιβάλλον)

Αν υπάρχει διαθέσιμος εξοπλισμός στο σχολικό εργαστήριο, να γίνει επίδειξη του τρόπου εφαρμογής διπλών καρτών γραφικών σε ένα σύστημα.

Δικτυογραφία

Domingo, J. S. (2013, Ιούλιος 2). *How to Overclock Your CPU*. Retrieved from PC Magazine: http://www.pcmag.com/article2/0,2817,2421233,00.asp

Gite, V. (2015, Ιανουάριος 29). *How To Stress Test CPU and Memory (VM) On a Linux and Unix With Stress-ng*. Ανάκτηση από nixCraft: http://www.cyberciti.biz/faq/stress-test-linux-unix-server-with-stress-ng/

Gordon, W. (2014, Ιανουάριος 13). *A Beginner's Introduction to Overclocking Your Intel Processor*. Ανάκτηση από LifeHacker: http://lifehacker.com/a-beginners-introduction-to-overclocking-your-intel-pr-5580998

Iwaniuk, P. (2011, Οκτώβριος 02). *How to overclock your RAM*. Ανάκτηση από Tech Radar: http://www.techradar.com/news/computing-components/upgrades/how-to-overclock-your-ram-1030286

Wiki Ubuntu. (2015, Νοέμβριος 03). *Overclocking CPU on Ubuntu*. Ανάκτηση από Wiki Ubuntu: https://wiki.ubuntu.com/OverclockingCpu

Κεφάλαιο 2ο

Απαγωγή θερμότητας από Υπολογιστικά Συστήματα

Εισαγωγή

Κάθε ένα υπολογιστικό σύστημα αποτελείται από ηλεκτρονικά εξαρτήματα όπως η Κ.Μ.Ε., η μνήμη RAM, ο σκληρός δίσκος κλπ. Για να λειτουργήσουν χρειάζονται ηλεκτρικό ρεύμα, το οποίο περνώντας μέσα από τα κυκλώματα συναντά κάποια αντίσταση. Αυτή η αντίσταση είναι ο λόγος που παράγεται θερμότητα κατά τη λειτουργία ενός υπολογιστικού συστήματος. Σ' αυτό το κεφάλαιο θα μελετήσουμε τους τρόπους απαγωγής αυτής της παραγόμενης θερμότητας.

Διδακτικοί Στόχοι

Με την ολοκλήρωση του 2ου κεφαλαίου οι μαθητές θα πρέπει να είναι σε θέση να:

- Περιγράφουν τις βασικές αρχές της αερόψυξης και της υδρόψυξης.
- Απαριθμούν πλεονεκτήματα και μειονεκτήματα της κάθε μεθόδου ψύξης.
- Επεξηγούν το ρόλο των θερμοαγώγιμων παστών και το ρόλο των θερμοαγωγών.

Διδακτικές Ενότητες

2.1 Μέθοδοι ψύξης Υπολογιστικών Συστημάτων.
2.2 Ο Ρόλος των θερμοαγώγιμων παστών.
2.3 Ο Ρόλος των θερμοαγωγών (heatpipes).

2.1 Μέθοδοι ψύξης Υπολογιστικών Συστημάτων

Μια σημαντική παράμετρος για τη σωστή λειτουργία ενός υπολογιστικού συστήματος είναι η θερμοκρασία, η οποία θα πρέπει να διατηρείται κάτω από ένα όριο. Αν η θερμοκρασία μέσα στο κουτί του υπολογιστικού συστήματος, αλλά και στα επιμέρους εξαρτήματα ξεπεράσει αυτό το όριο τότε τα αποτελέσματα θα είναι:

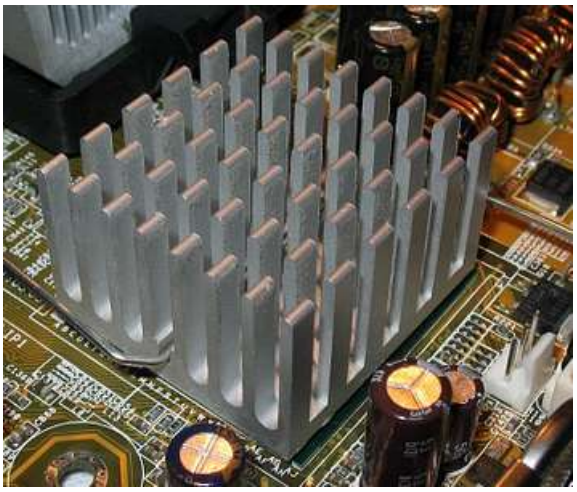
- Αστάθεια στη λειτουργία του υπολογιστικού συστήματος (κολλήματα, επανεκκινήσεις)
- Μείωση της διάρκειας ζωής των ηλεκτρονικών εξαρτημάτων
- Καταστροφή των ηλεκτρονικών εξαρτημάτων, αν η θερμοκρασία ξεπεράσει κατά πολύ τα όρια (εικόνα 2.1).

Τα εξαρτήματα που παράγουν την περισσότερη θερμότητα είναι η Κ.Μ.Ε., η κάρτα γραφικών, η μνήμη RAM, τα σύνολα ολοκληρωμένων κυκλωμάτων (chipset) και οι σκληροί δίσκοι.

Εικόνα 2.1: Κατεστραμμένη Κ.Μ.Ε., λόγω υπερθέρμανσης

2.1.1 Παθητική ψύξη

Στην παθητική ψύξη χρησιμοποιούνται ψύκτρες, οι οποίες ουσιαστικά προσθέτουν επιφάνεια ψύξης στο ηλεκτρονικό εξάρτημα.

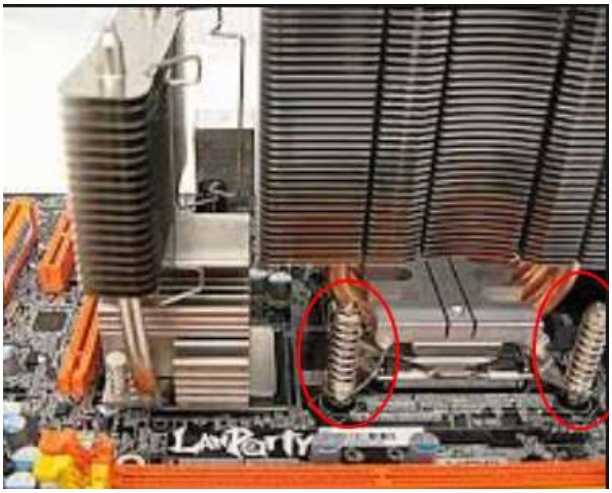


Εικόνα 2.2: Ψύκτρα

Η μία πλευρά της ψύκτρας είναι επίπεδη και εφάπτεται στον ηλεκτρονικό εξάρτημα, ενώ η άλλη πλευρά έχει πτερύγια τα οποία είναι σχετικά μεγάλα και ο ρόλος τους είναι να επεκτείνουν την επιφάνεια ψύξης. Επίσης, μεταξύ των πτερυγίων υπάρχει κενό για να κυκλοφορεί ο αέρας και να μειώνει τη θερμοκρασία της ψύκτρας.

Οι ψύκτρες μπορεί να είναι πολύ βαριές και να χρειάζονται ειδικούς μηχανισμούς στήριξης πάνω στη μητρική πλακέτα.

Οι απλές ψύκτρες είναι σχετικά φθηνές, δεν καταναλώνουν ενέργεια, δεν χρειάζονται συντήρηση. Το μεγάλο τους μειονέκτημα είναι ότι δεν μπορούν να ανταποκριθούν σε περιπτώσεις που χρειάζεται να ψυχθεί ένα εξάρτημα που παράγει μεγάλη ποσότητα θερμότητας.



Εικόνα 2.3: Ψύκτρα με μηχανισμό στήριξης

2.1.2 Αερόψυξη

Σ' αυτή τη μέθοδο ψύξης χρησιμοποιούνται ψύκτρες σε συνδυασμό με ανεμιστήρα. Η αρχή λειτουργίας τους είναι ίδια με τις απλές ψύκτρες, μόνο που σ' αυτήν την περίπτωση η κυκλοφορία του αέρα ανάμεσα στα πτερύγια γίνεται βεβιασμένα με τη χρήστη ανεμιστήρα. Με αυτόν τον τρόπο αυξάνεται η δυνατότητα απαγωγής θερμότητας συγκριτικά με τις απλές ψύκτρες.

Εικόνα 2.4: Ψύκτρα με ανεμιστήρα

Οι ψύκτρες με τη χρήση ανεμιστήρα είναι συνήθως πιο ακριβές από τις απλές ψύκτρες, απάγουν περισσότερη θερμότητα καταναλώνοντας ενέργεια (από την περιστροφή του ανεμιστήρα) και χρειάζονται κάποια συντήρηση. Συντήρηση χρειάζεται ο ανεμιστήρας ο οποίος με τον καιρό μπορεί να μαζεύει σκόνη και να μην λειτουργεί κανονικά.

2.1.3 Απαγωγή θερμότητας από το κουτί του υπολογιστικού συστήματος

Όλα τα κουτιά υπολογιστικών συστημάτων έχουν οπές σε κατάλληλα σημεία έτσι ώστε να υπάρχει παθητική ροή αέρα για την απαγωγή της πλεονάζουσας θερμότητας.

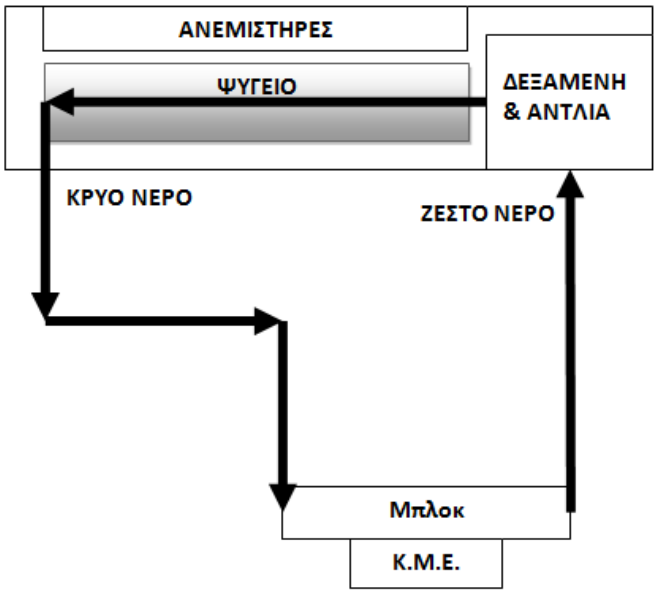
Στα σύγχρονα κουτιά υπολογιστικών συστημάτων, για να διευκολυνθεί ή να αυξηθεί η ροή του αέρα έχουμε τη δυνατότητα να τοποθετήσουμε ανεμιστήρες. Με αυτόν τον τρόπο μπορούμε να κρατήσουμε τη θερμοκρασία ακόμα πιο χαμηλά.

Σ' αυτό το σημείο θα πρέπει να επισημάνουμε ότι οι ανεμιστήρες ελκύουν σκόνη, η οποία εμποδίζει τη σωστή λειτουργία τους (μειωμένη ροή αέρα, αυξημένος θόρυβος). Για αυτό το λόγο, θα πρέπει να ελέγχουμε τα πτερύγιά τους και αν χρειάζεται να απομακρύνουμε την σκόνη με χρήση φυσητήρα.

Εικόνα 2.5: Ροή αέρα

2.1.4 Υδρόψυξη

Η υδρόψυξη είναι ένας σχετικά καινούριος τρόπος ψύξης κυρίως της Κ.Μ.Ε., η οποία παράγει μεγάλη ποσότητα θερμότητας. Η λειτουργία της στηρίζεται στο γεγονός ότι το νερό είναι πολύ καλός αγωγός της θερμότητας. Δηλαδή, απορροφά και απελευθερώνει πολύ γρήγορα τη θερμότητα.



Εικόνα 2.6: Βασική λειτουργία υδρόψυξης

Ένα σύστημα υδρόψυξης αποτελείται από ένα τουλάχιστον μπλοκ, το οποίο τοποθετείται στο εξάρτημα που θέλουμε να ψύξουμε, μια δεξαμενή νερού, μια αντλία (κυκλοφορητής) και ένα ψυγείο. Οι ανεμιστήρες που διακρίνονται στο παραπάνω σχήμα δεν χρησιμοποιούνται συχνά.

Η αντλία αναλαμβάνει την κυκλοφορία του νερού από το ψυγείο στο μπλοκ ψύξης και στη συνέχεια στη δεξαμενή. Αυτός ο κύκλος επαναλαμβάνεται, με αποτέλεσμα το νερό να θερμαίνεται όταν περνάει από το μπλοκ ψύξης και να κρυώνει όταν περνάει μέσα από το ψυγείο.

Η απαγωγή της θερμότητας που επιτυγχάνει ένα σύστημα υδρόψυξης είναι πολύ μεγάλη, αλλά έχει μεγάλο κόστος αγοράς και συντήρησης. Επίσης, στα αρνητικά μπορούμε να συμπεριλάβουμε το γεγονός ότι καταναλώνει επιπλέον ενέργεια και η τοποθέτησή της δεν είναι απλή.

2.2 Ο Ρόλος των θερμοαγώγιμων παστών

Πριν τοποθετήσουμε την ψύκτρα στην Κ.Μ.Ε. θα πρέπει να απλώσουμε στην επιφάνεια του επεξεργαστή μια θερμοαγώγιμη πάστα. Ο ρόλος της είναι πολύ σημαντικός, γιατί αφενός μεγιστοποιεί την επαφή της ψύκτρας με την Κ.Μ.Ε., αφετέρου ελαχιστοποιεί τα κενά αέρα (τα οποία δρουν αρνητικά) μεταξύ των δύο επιφανειών.

Η σύνθεση της είναι τέτοια που επιτρέπει την εύκολη μεταφορά θερμότητας, αλλά και την ηλεκτρική μόνωση.

Για την εφαρμογή της θερμοαγώγιμης πάστας ακολουθούμε τα παρακάτω βήματα:

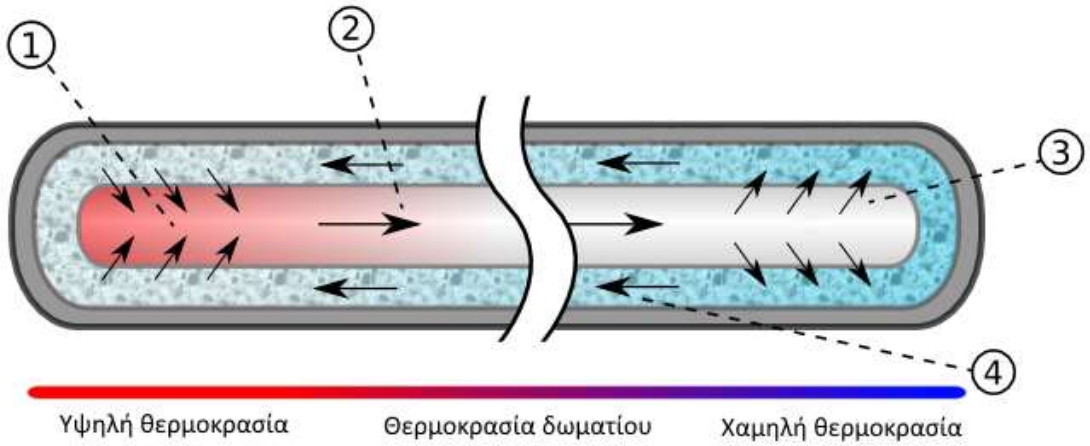
1. Καθαρίζουμε πολύ καλά τις επιφάνειες της ψύκτρας και της Κ.Μ.Ε.
2. Τοποθετούμε μια μικρή ποσότητα θερμοαγώγιμης πάστας (όσο ένας κόκκος ρυζιού) στο κέντρο της επιφάνειας της Κ.Μ.Ε.
3. Με ένα πλατύ αντικείμενο απλώνουμε την πάστα στην επιφάνεια της Κ.Μ.Ε.
4. Τοποθετούμε την ψύκτρα.

Εικόνα 2.7: Εφαρμογή θερμοαγώγιμης πάστας

2.3 Ο Ρόλος των θερμοαγωγών (heatpipes)

Ένας θερμοαγωγός είναι ένας κλειστός σωλήνας από τον οποίο έχει αφαιρεθεί ο αέρας και έχει προστεθεί ένα υγρό. Στην μια άκρη του θερμοαγωγού, στην οποία υπάρχει μεγάλη

θερμοκρασία, το υγρό απορροφά θερμότητα και μετατρέπεται σε αέριο (Σημείο 1 στην εικόνα 2.8). Καθώς το αέριο οδεύει προς την άλλη άκρη του αγωγού, μειώνεται η θερμοκρασία του και απελευθερώνει θερμότητα (Σημείο 2 στην εικόνα 2.8). Μέχρι να φτάσει το αέριο στο άλλο άκρο του αγωγού (Σημείο 3 στην εικόνα 2.8), έχει μετατραπεί σε πάλι υγρό και αρχίζει να ταξιδεύει προς την αντίθετη άκρη του (Σημείο 4 στην εικόνα 2.8). Σε αυτήν την άκρη του αγωγού τοποθετούμε μια ψύκτρα για την απαγωγής της θερμότητας.



Εικόνα 2.8: Αρχή λειτουργίας θερμοαγωγού
(Πηγή: https://en.wikipedia.org/wiki/Heat_pipe)

Ένας θερμοαγωγός έχει μεγάλη ικανότητα μεταφοράς θερμότητας από τη μια άκρη του στην άλλη. Για αυτό το λόγο, πολλές σύγχρονες ψύκτρες συμπεριλαμβάνουν και θερμοαγωγούς.

Εικόνα 2.9: Σύγχρονη ψύκτρα με θερμοαγωγούς

Ερωτήσεις Ανακεφαλαίωσης

1. Για ποιους λόγους επιβάλλεται η σωστή απαγωγή της θερμότητας από το κουτί του υπολογιστή;
2. Για ποιους λόγους είναι απαραίτητη η εφαρμογή θερμοαγώγιμης πάστας μεταξύ της ΚΜΕ και της ψύκτρας της;
3. Ποια είναι η βασική αρχή λειτουργίας των θερμοαγωγών;
4. Ποια είναι τα πλεονεκτήματα και ποια τα μειονεκτήματα της παθητικής ψύξης;

Ασκήσεις

1η Άσκηση (Σε εργαστηριακό περιβάλλον)

Για την υλοποίηση της άσκησης προτείνεται να χρησιμοποιηθεί παλαιό ή κατεστραμμένο υλικό υπολογιστών.

1. Να γίνει αφαίρεση της ψύκτρας της ΚΜΕ.
2. Να καθαριστεί επιμελώς η επιφάνεια της ΚΜΕ και στη συνέχεια να εφαρμοστεί ικανή ποσότητα θερμοαγώγιμης πάστας.
3. Να τοποθετηθεί στη θέση της η ψύκτρα της ΚΜΕ.

2η Άσκηση (Σε εργαστηριακό περιβάλλον)

1. Να γίνει έλεγχος του ανεμιστήρα της ΚΜΕ και του ανεμιστήρα του τροφοδοτικού του υπολογιστικού συστήματος.
2. Με τη χρήση φυσητήρα να απομακρυνθεί η σκόνη που τυχόν υπάρχει.

Βιβλιογραφία

Heatpipe.nl. (2010). *HeatPipe.nl.* Ανάκτηση από http://www.heatpipe.nl/index.php?page=heatpipe&lang=EN.

Lazaridis, G. (2009, April 9). *PC Cooling Methods.* Ανάκτηση από http://www.pcbheaven.com/blogpages/PC_Cooling_Methods/.

Wikipedia. (2015, August 6). *Heat pipe.* Ανάκτηση από https://en.wikipedia.org/wiki/Heat_pipe.

Κεφάλαιο 3ο

Συστοιχίες Δίσκων - RAID

Εισαγωγή

Το παρόν κεφάλαιο αποτελεί μια εισαγωγή στις συστοιχίες δίσκων, τις διάφορες μορφές τους και τους τρόπους με τους οποίους μπορούν να αξιοποιηθούν για την αύξηση της ταχύτητας μεταφοράς και της ασφάλειας των δεδομένων ενός υπολογιστικού συστήματος.

Διδακτικοί Στόχοι

Με την ολοκλήρωση του 3ου κεφαλαίου οι μαθητές θα πρέπει να είναι σε θέση να:

- Προσδιορίζουν τη δομή Συστοιχιών Δίσκων.
- Αναφέρουν τις συνηθισμένες μορφές συστοιχιών.
- Εντοπίζουν τα βασικά στοιχεία υλικού και λογισμικού που είναι απαραίτητα για την υλοποίηση μιας Συστοιχίας Δίσκων.
- Υλοποιούν μια δομή Συστοιχίας Δίσκων σε εικονική μηχανή.

Διδακτικές Ενότητες

3.1. Εισαγωγή στις Συστοιχίες Δίσκων (RAID)

Η λέξη RAID προκύπτει από τα αρχικά των λέξεων Redundant Array of Independent Disks (Πλεονάζουσα Συστοιχία Ανεξάρτητων Δίσκων). Πρόκειται για συνδυασμό δύο ή περισσότερων σκληρών δίσκων (κατά προτίμηση ίσης χωρητικότητας) που ο υπολογιστής τους αντιλαμβάνεται σαν ένα ενιαίο δίσκο. Ανάλογα με το πλήθος, αλλά και τον τρόπο με τον οποίο χρησιμοποιούνται οι δίσκοι υπάρχουν συγκεκριμένα πλεονεκτήματα σε σχέση με τη χρήση ενός μεμονωμένου δίσκου.

3.1.1 Μορφές

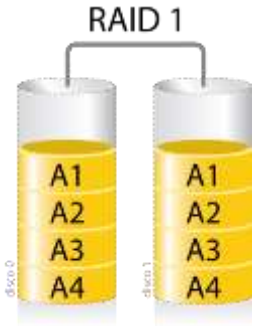
Υπάρχουν αρκετές μορφές RAID. Οι περισσότερο συνηθισμένες πάντως είναι οι ακόλουθες:

- **RAID 0:** Η διάταξη αυτή που είναι γνωστή και ως striping (διαγράμμιση) χρησιμοποιεί δύο ή περισσότερους ίδιας χωρητικότητας δίσκους στους οποίους κατανέμονται ταυτόχρονα τα δεδομένα. Αυτό έχει σαν αποτέλεσμα αύξηση της απόδοσης στις εργασίες ανάγνωσης/εγγραφής, με ταυτόχρονη όμως μείωση της ασφάλειας των δεδομένων, αφού η αστοχία ακόμη και ενός δίσκου αχρηστεύει όλη τη συστοιχία. Οι κίνδυνοι μάλιστα για την ασφάλεια των δεδομένων αυξάνονται (αντίστοιχα όμως και οι επιδόσεις) όσο αυξάνεται το πλήθος των δίσκων που συμμετέχουν στη συστοιχία. Το συνολικό μέγεθος της συστοιχίας είναι το άθροισμα του μεγέθους των δίσκων που την αποτελούν.

Εικόνα 3.1. Συστοιχία RAID 0 (stripping).

(Πηγή: http://www.easynas.org/wp-content/uploads/2014/05/raid0.png)

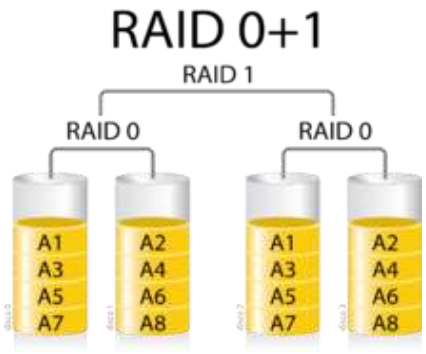
RAID 1: Γνωστό και σαν mirroring (κατοπτρισμός), χρησιμοποιεί τους επιπλέον δίσκους για την αποθήκευση των ίδιων δεδομένων, κάνοντας έτσι τους επιπλέον δίσκους αντίγραφα του πρώτου. Με τον τρόπου αυτό επιτυγχάνεται αύξηση της ασφάλειας, αλλά και αύξηση της ταχύτητας των εργασιών ανάγνωσης (αφού δεδομένα μπορούν να διαβάζονται ταυτόχρονα από όλους τους δίσκους). Είναι ωστόσο η πιο «ακριβή» λύση, αφού οι επιπλέον δίσκοι δεν αυξάνουν τη χωρητικότητα της συστοιχίας.



Εικόνα 3.2. Συστοιχία RAID 0 (mirroring).

(Πηγή: http://www.easynas.org/wp-content/uploads/2014/05/raid1.png)

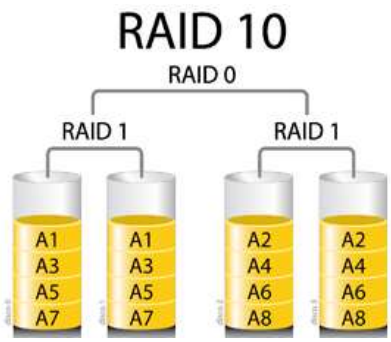
- **RAID 0+1:** Αποτελεί συνδυασμό των παραπάνω δύο ειδών, που υπόσχεται ταχύτητα και ασφάλεια. Αυτό που στην πράξη γίνεται είναι να έχουμε δύο συστοιχίες RAID 0 που ενώνονται μεταξύ τους σε συστοιχία RAID 1, δηλ. η δεύτερη συστοιχία γίνεται αντίγραφο της πρώτης. Χρειάζεται τέσσερις ίδιας χωρητικότητας δίσκους για να υλοποιηθεί, το μέγεθος της συστοιχίας είναι το μισό του συνολικού μεγέθους των δίσκων και η μόνη περίπτωση να καταρρεύσει είναι να χαλάσουν δύο δίσκοι ταυτόχρονα, ένας από κάθε υπο-συστοιχία RAID 0.



Εικόνα 3.3. Συστοιχία RAID 0+1.

(Πηγή: https://upload.wikimedia.org/wikipedia/commons/thumb/c/c4/Raid0mas1.png/1024px-Raid0mas1.png)

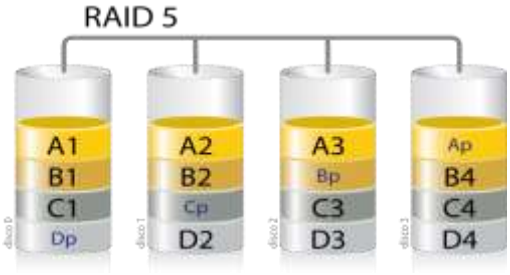
- **RAID 1+0:** Το αντίστροφο από το προηγούμενο. Δύο συστοιχίες RAID 1 που ενώνονται σε συστοιχία RAID 0. Εδώ για να υπάρξει αστοχία θα πρέπει να χαλάσουν και οι δύο δίσκοι μιας υπο-συστοιχίας. Για τον αριθμό των δίσκων και τη συνολική χωρητικότητα ισχύει ότι και στην περίπτωση του 0+1.



Εικόνα 3.4. Συστοιχία RAID 1+0.

(Πηγή: http://www.easynas.org/wp-content/uploads/2014/05/Raid10-300x262.png)

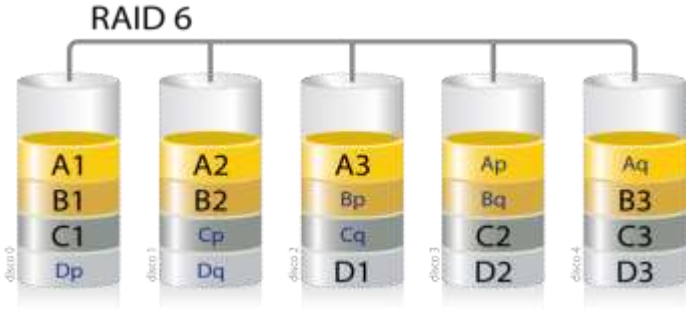
- **RAID 5:** Η διάταξη αυτή υλοποιείται με τρεις τουλάχιστον ίδιους δίσκους. Το RAID 5 μοιράζει τα δεδομένα ανάμεσα στους δίσκους της συστοιχίας με τρόπο ανάλογο του RAID 0 (παρέχοντας αυξημένες ταχύτητες ανάγνωσης), με τη βασική όμως διαφορά ότι μαζί με τα δεδομένα αποθηκεύονται και δυαδικά ψηφία ισοτιμίας (parity) που επιτρέπουν την ανάκτηση των δεδομένων στην περίπτωση που χαλάσει ένας από τους δίσκους. Σε περίπτωση που χαλάσουν πάνω από ένας δίσκος (ανεξάρτητα του πόσους χρησιμοποιούσε η συστοιχία) τα δεδομένα δεν μπορούν να ανακτηθούν. Η συνολική χωρητικότητα της συστοιχίας είναι κατά έναν δίσκο μικρότερη από το σύνολο των δίσκων που είναι συνδεδεμένοι σε αυτήν. Θεωρείται η χρυσή τομή ανάμεσα στην ταχύτητα, την ασφάλεια και τη χωρητικότητα.



Εικόνα 3.5. Συστοιχία RAID 5.

(Πηγή:: http://www.easynas.org/wp-content/uploads/2014/05/raid5.png)

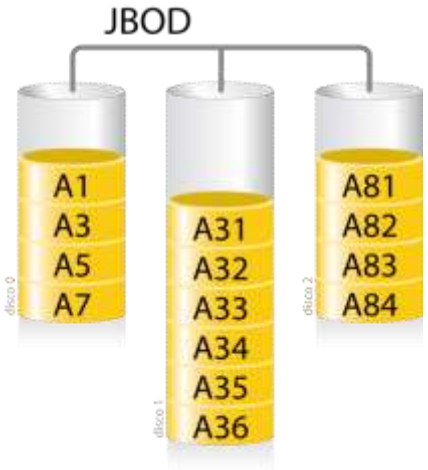
- **RAID 6:** Όπως και το RAID 5, αποθηκεύει όμως διπλάσια ψηφία ισοτιμίας. Αυτό σημαίνει ότι χρειάζεται τέσσερις τουλάχιστον δίσκους, μπορεί όμως να ανταπεξέλθει στην απώλεια δύο δίσκων, έναντι ενός του RAID 5, αυξάνοντας έτσι την ασφάλεια των δεδομένων.



Εικόνα 3.6. Συστοιχία RAID 6.

(Πηγή: http://www.easynas.org/wp-content/uploads/2014/05/raid6.png)

- **RAID JBOD:** Το όνομά του προέρχεται από τα αρχικά των λέξεων Just a Bunch Of Disks (ένα σύνολο δίσκων). Στην υλοποίηση αυτοί οι διαθέσιμοι δίσκοι (που μπορεί να είναι οποιασδήποτε χωρητικότητας) συνενώνονται απλά σε μια συστοιχία με χωρητικότητα το σύνολο των επιμέρους δίσκων. Δεν παρέχει αύξηση ταχύτητας, ούτε ενισχύει την ασφάλεια, όμως σε περίπτωση βλάβης ενός δίσκου χάνονται μόνο τα δεδομένα που αυτός περιέχει και όχι ολόκληρη η συστοιχία.



Εικόνα 3.7. Συστοιχία RAID JBOD.

(Πηγή: http://www.easynas.org/wp-content/uploads/2014/05/jbod.png)

3.1.2 Ασφάλεια και επιδόσεις

Ο ακόλουθος πίνακας συνοψίζει την κατάσταση για τις μορφές του RAID που παρουσιάστηκαν:

	0	**1**	**0+1**	**1+0**	**5**	**6**	**JBOD**
Ελάχιστος # δίσκων	2	2	4	4	3	4	2
Ανοχή σε Βλάβες Δίσκων	-	1	2 στην ίδια υπο-συστοιχία	1 από κάθε υπο-συστοιχία	1	2	-
Ταχύτητα Ανάγνωσης	Υψηλή	Υψηλή	Υψηλή	Υψηλή	Υψηλή	Υψηλή	Τυπική
Ταχύτητα Εγγραφής	Υψηλή	Τυπική	Τυπική	Τυπική	Τυπική	Τυπική	Τυπική
Αξιοποίηση Χωρητικότητας	100%	50%	50%	50%	67%	50%	100%

Πίνακας 3.1. Σύγκριση Υλοποιήσεων RAID

3.2. Τρόποι Υλοποίησης

Οι συστοιχίες RAID μπορούν να υλοποιηθούν είτε με χρήση εξειδικευμένου υλικού (RAID Controllers) ή με χρήση λογισμικού (υποστήριξη από το λειτουργικό σύστημα ή οδηγούς συσκευών). Κάθε μία υλοποίηση έχει πλεονεκτήματα και μειονεκτήματα που θα συζητηθούν παρακάτω.

3.2.1. RAID μέσω Λογισμικού (Software RAID)

Πρόκειται για συστοιχίες RAID που υλοποιούνται αποκλειστικά με λογισμικό, συνήθως λόγω υποστήριξης από το λειτουργικό σύστημα του υπολογιστή. Είναι η πιο οικονομική λύση, καθώς το μόνο που χρειάζεται είναι οι δίσκοι που θα συμμετέχουν στη συστοιχία. Ωστόσο προκαλεί επιβάρυνση του επεξεργαστή του υπολογιστή, ειδικά στις περιπτώσεις των RAID 5 και 6 όπου θα πρέπει να γίνει υπολογισμός των πλεοναζόντων δυαδικών ψηφίων που θα αποθηκευτούν. Εξαρτάται ακόμη σε μεγάλο βαθμό από το λειτουργικό σύστημα που χρησιμοποιείται, πράγμα που σημαίνει ότι η συστοιχία δεν μπορεί εύκολα να μεταφερθεί σε υπολογιστή με άλλο λειτουργικό, ενώ δεν εξασφαλίζεται πάντα η δυνατότητα εκκίνησης του συστήματος από μια τέτοια συστοιχία. Χρησιμοποιείται κυρίως σε οικιακά συστήματα.

3.2.2. RAID μέσω Υλικού (Hardware RAID)

Η υλοποίηση αυτή προϋποθέτει την ύπαρξη μιας ειδικής κάρτας που λέγεται Ελεγκτής RAID (RAID Controller) και περιέχει δικό του επεξεργαστή, μνήμη, αλλά και υποδοχές για τη σύνδεση των δίσκων που θα συμμετέχουν στη συστοιχία. Εφόσον η κάρτα έχει το δικό της επεξεργαστή όλοι οι απαραίτητοι υπολογισμοί γίνονται εκεί, χωρίς να επιβαρύνεται ο υπολογιστής και με αύξηση των επιδόσεων. Από την άλλη, το κόστος απόκτησης ενός τέτοιου ελεγκτή είναι υψηλό, ενώ αρκετοί από αυτούς δέχονται μόνο δίσκους SAS ή SSD που είναι

σημαντικά πιο ακριβοί από τους κλασικούς δίσκους. Χρησιμοποιείται σε συστήματα server και για πολύπλοκες διατάξεις RAID.

Εικόνα 3.8. Ελεγκτής για δημιουργία RAID.

(Πηγή: http://www.iocrest.com/uploadfiles/20140404/20140404153901797 7.jpg)

3.2.3. Υβριδικό RAID (Hybrid RAID)

Πρόκειται για την υλοποίηση που ακολουθείται στους ενσωματωμένους σε μητρικές πλακέτες ελεγκτές και στις χαμηλού κόστους κάρτες. Στην πράξη πρόκειται για οικονομικές υλοποιήσεις που διαχειρίζονται τη συστοιχία κατά τη διάρκεια της εκκίνησης του υπολογιστή, ενώ μετά ο έλεγχος περνά στο λειτουργικό σύστημα μέσω κατάλληλων οδηγών, ενδεχομένως με κάποια μικρή υποβοήθηση από το υλικό. Αυτό βέβαια σημαίνει ότι η συστοιχία δεν θα μπορεί να λειτουργήσει αν δεν υπάρχουν οι κατάλληλοι οδηγοί για το λειτουργικό σύστημα. Συνήθως υποστηρίζουν μόνο τους τύπους 0, 1 και 0+1. Ένα ακόμα μειονέκτημα είναι ότι η συστοιχία είναι στενά συνδεδεμένη με τον ελεγκτή, άρα αν αυτός χαλάσει θα πρέπει να βρούμε μια ίδια μητρική ή κάρτα για να ανακτήσουμε τα δεδομένα μας. Χρησιμοποιείται σε οικιακά συστήματα.

3.3. Συμπεράσματα

Η τεχνολογία RAID είναι πλέον ώριμη και οι διαθέσιμες υλοποιήσεις πολλές. Είναι επίσης σχετικά εύκολο ο καθένας να φτιάξει τη δική του συστοιχία RAID και να επωφεληθεί από τα πλεονεκτήματα σε ασφάλεια και ταχύτητα. Ειδικά με τη χρήση των γρήγορων δίσκων SAS και SSD οι ταχύτητες μιας συστοιχίας μπορούν να αυξηθούν θεαματικά.

Πρέπει ωστόσο να γίνει κατανοητό πως παρά το ότι υπάρχουν υλοποιήσεις RAID που αυξάνουν την ασφάλεια των δεδομένων, αυτό δεν υποκαθιστά την τακτική λήψη εφεδρικών αντιγράφων ασφαλείας, που είναι η πλέον αξιόπιστη μέθοδος για την εξασφάλιση της ακεραιότητας των δεδομένων, αλλά και τη γρήγορη ανάκαμψη μετά από αστοχία υλικού.

Ερωτήσεις Ανακεφαλαίωσης

1. Στον παρακάτω πίνακα επισημάνετε με το σύμβολο ✓ τα χαρακτηριστικά που ισχύουν σε κάθε έναν από τους τύπους RAID που αναφέρονται στην 1η στήλη.

Τύπος RAID	Αύξηση Ταχύτητας Ανάγνωσης	Αύξηση Ταχύτητας Εγγραφής	Πλήρης αξιοποίηση της χωρητικότητας των δίσκων
0			
1			
0+1			
1+0			
5			
6			
JBOD			

2. Ποια υλοποίηση RAID έχει το μικρότερο κόστος (εκτός του κόστους των δίσκων);
3. Ποια τα πλεονεκτήματα του RAID μέσω υλικού;
4. Ποια τα μειονεκτήματα του υβριδικού RAID;

Ασκήσεις

1η Άσκηση

Στην άσκηση αυτή θα φτιάξετε μια συστοιχία RAID 0 μέσω λογισμικού στο Λ.Σ MS Windows 7. Για την πραγματοποίηση της άσκησης θα αξιοποιήσετε την τεχνολογία των εικονικών μηχανών.

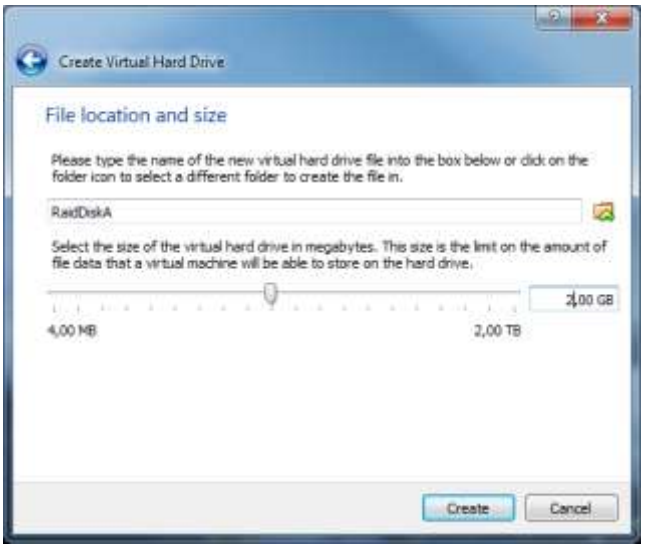
Η **τεχνολογία των εικονικών μηχανών** είναι λογισμικό που δίνει τη δυνατότητα σε ένα φυσικό υπολογιστή να δημιουργηθούν ένας ή περισσότεροι εικονικοί-ιδεατοί (virtual) υπολογιστές. Στους εικονικούς αυτούς υπολογιστές μπορεί να εγκατασταθεί λειτουργικό σύστημα και εφαρμογές, που θα λειτουργούν και θα συμπεριφέρονται σαν να εκτελούνταν σε ένα κανονικό σύστημα. Το σημαντικό είναι ότι οι ιδεατοί υπολογιστές υλοποιούνται εξ' ολοκλήρου από λογισμικό και δεν εγκυμονούν κινδύνους για την διαμόρφωση του φυσικού υπολογιστή. Έτσι, η τεχνολογία αυτή είναι ιδανική για την ασφαλή πραγματοποίηση δοκιμών με πολλά και διαφορετικά περιβάλλοντα.

Το Oracle Virtual Box (https://www.virtualbox.org/) είναι ελεύθερο λογισμικό ανοιχτού κώδικα που χρησιμοποιείται για τη δημιουργία εικονικών μηχανών. Χαρακτηρίζεται από μεγάλη ευελιξία και υψηλά επίπεδα συμβατότητας με λειτουργικά συστήματα και εφαρμογές και μπορεί να αξιοποιηθεί σε μια πληθώρα διαφορετικών περιπτώσεων.

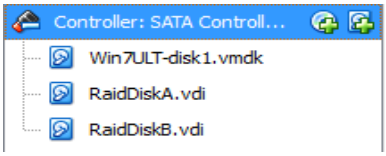
1. Ξεκινήστε το Oracle Virtual Box, εντοπίστε την εικονική μηχανή με το Λ.Σ MS Windows 7 και ανοίξτε τις ιδιότητές της.
2. Στην ενότητα Storage και πατήστε πάνω στον SATA Controller που εμφανίζεται στην ενότητα Storage Tree στη μέση του παραθύρου. Θέλουμε να προσθέσουμε δύο ακόμα σκληρούς δίσκους SATA στην εικονική μας μηχανή. Ποιο από τα εικονίδια που εμφανίζονται στα δεξιά πιστεύετε ότι πρέπει να χρησιμοποιήσουμε; Αν δεν σας είναι προφανές από το εικονίδιο, αφήστε για λίγο το ποντίκι πάνω από κάθε εικονίδιο και δείτε την περιγραφή που εμφανίζεται.

3. Πατήστε το κατάλληλο κουμπί για να προσθέσετε τον πρώτο SATA δίσκο. Στο παράθυρο που θα εμφανισθεί πατήστε στο [Create new disk]. Με τι θα ισοδυναμούσε η ενέργεια αυτή σε ένα κανονικό υπολογιστή;

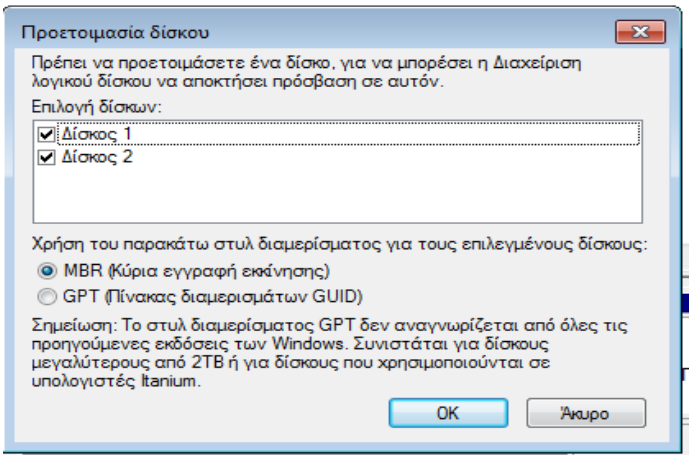
4. Στο επόμενο παράθυρο πατήστε [Next].
5. Στη συνέχεια αφήστε την επιλογή για δυναμικό δίσκο και πατήστε [Next]
6. Αλλάξτε το όνομα του δίσκου σε RaidDiskA και άντε το μέγεθος του δίσκου να είναι 2GB.



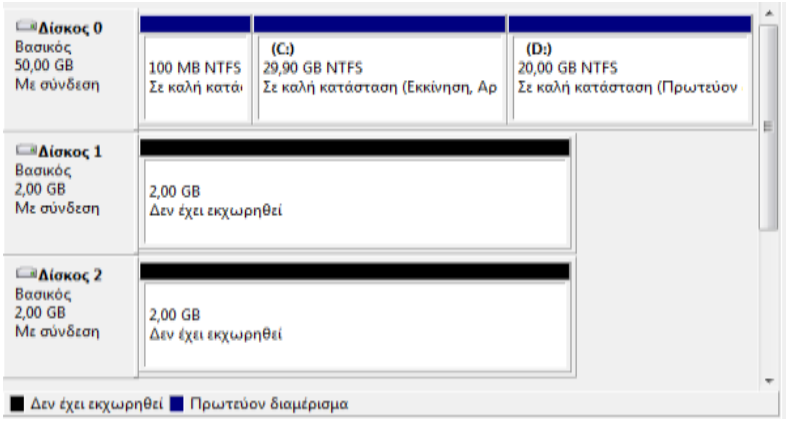
7. Με τον ίδιο τρόπο δημιουργήστε και έναν δεύτερο δίσκο με όνομα RaidDiskB και ίδια χωρητικότητα.



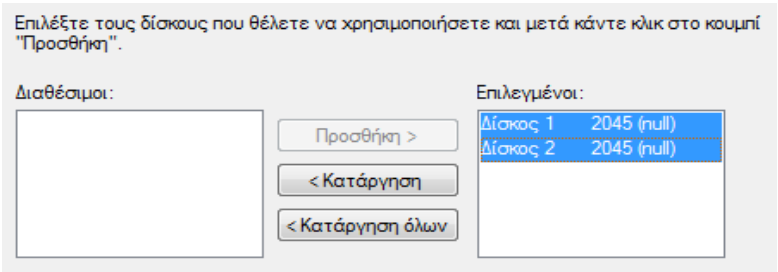
8. Πατήστε [OK] και ξεκινήστε την εικονική μηχανή. Όταν ξεκινήσει το λειτουργικό σύστημα συνδεθείτε με λογαριασμό διαχειριστή.
9. Ανοίξτε τη Διαχείριση του υπολογιστή. Τι θα πρέπει να επιλέξετε στα αριστερά για να κάνετε ενέργειες στους διαθέσιμους δίσκους;
10. Οι δίσκοι που εισαγάγατε χρειάζονται προετοιμασία για να αναγνωριστούν από τα Windows. Κατά τη διαδικασία αυτή θα δημιουργηθεί το Master Boot Record (MBR) όπου κρατούνται οι πληροφορίες για τα διαμερίσματα στα οποία είναι χωρισμένος ένας δίσκος και απ' όπου ξεκινάει η διαδικασία εκκίνησης του ή των λειτουργικών συστημάτων που περιέχει ένας δίσκος. Διαβάστε τη σημείωση που βρίσκεται στο κάτω μέρος του παραθύρου και επιλέξτε τον τύπο του στυλ διαμερίσματος που θα πρέπει να δώσετε για τους δίσκους.



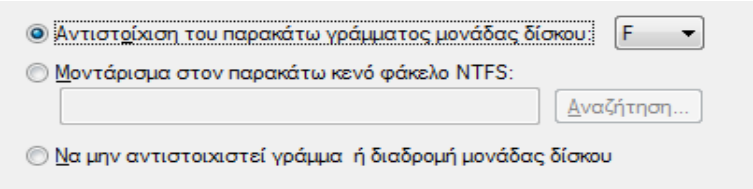
11. Επιλέξτε και πατήστε [OK]. Οι μονάδες δίσκων θα φανούν στο κάτω μέρος της Διαχείρισης δίσκων.



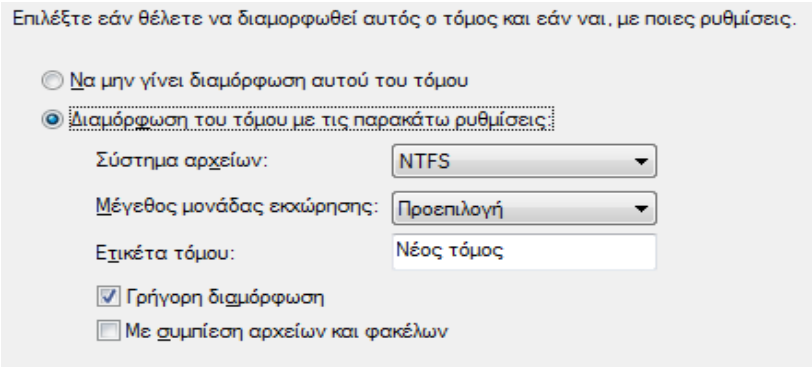
12. Κάντε δεξί-click σε κάποιον από τους δύο δίσκους που φτιάξατε και εξετάστε τις επιλογές που βλέπετε εκεί. Καταγράψτε τις επιλογές που βλέπετε και αντιστοιχίστε τις με αυτές που συζητήθηκαν στη θεωρία. Χρησιμοποιείστε το Διαδίκτυο για βοήθεια.
13. Ποια από τις επιλογές πρέπει να χρησιμοποιήσετε για να δημιουργήσετε μια συστοιχία RAID 0; Αν δεν μπορείτε να αποφασίσετε ανατρέξετε στο κομμάτι της θεωρίας. Δώστε την επιλογή σας και πατήστε [OK].
14. Στην εισαγωγική οθόνη του οδηγού πατήστε [Επόμενο].
15. Στην επόμενη οθόνη συμπεριλάβετε και το δεύτερο δίσκο στη συστοιχία. Ελέγξτε στο κάτω μέρος του παραθύρου το συνολικό μέγεθος της συστοιχίας. Είναι το αναμενόμενο για τον τύπο συστοιχίας που θέλετε να φτιάξετε; Αν όχι ίσως κάνατε λάθος επιλογή, την οποία μπορείτε να διορθώσετε επιστρέφοντας σε προηγούμενα βήματα. Αν όλα είναι εντάξει πατήστε [Επόμενο].



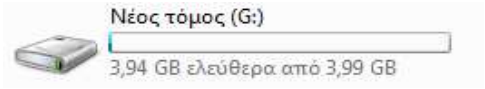
16. Στη συνέχεια μπορείτε να δώσετε το γράμμα οδηγού με το οποίο θα είναι γνωστός στο Λ.Σ MS Windows ο δίσκος RAID (δώστε ένα γράμμα που δεν χρησιμοποιείται ήδη) και πατήστε [Επόμενο].



17. Προχωρήστε στη μορφοποίηση του νέου δίσκου κρατώντας τις προεπιλεγμένες τιμές.



18. Στην τελευταία οθόνη του οδηγού σας δίνεται μια περίληψη των επιλογών σας. Πατήστε [Τέλος]. Στην προειδοποίηση που σας δίνεται πατήστε [ΟΚ].
19. Ανοίξτε το [Υπολογιστής] και εξετάστε το νέο δίσκο που δημιουργήθηκε. Έχει τη χωρητικότητα που πρέπει;



20. Σε ένα υπολογιστικό σύστημα με το οποίο δεν είστε εξοικειωμένοι πως μπορείτε να καταλάβετε αν μία μονάδα σκληρού δίσκου είναι όντως ένα αυτούσιος δίσκος, ένα διαμέρισμα ενός δίσκου ή μια συστοιχία RAID;

Βιβλιογραφία

Ξενόγλωσση

Bott E., Siechert C., Stinson C. (2011). *Windows 7 Inside Out Deluxe Edition*. Redmond, Washinghton, Microsoft Press

Stanek W. (2010). *Windows 7: The Definitive Guide*. Sebastopol, O'Reilly Media Inc.

Δικτυογραφία

Τι είναι το RAID: Η Μέγιστη Ασφάλεια και Ταχύτητα Δίσκου, http://www.pcsteps.gr/60129-τι-είναι-το-raid-ασφάλεια-ταχύτητα-δίσκου/

Wikipedia (RAID), https://en.wikipedia.org/wiki/RAID

Συστοιχίες Σκληρών Δίσκων (RAID), http://www.codeland.net63.net/2013/02/02/sistixies-skliron-diskon-raid

Κεφάλαιο 4ο

Συστοιχίες Υπολογιστών (Computer Clusters)

Εισαγωγή

Παρά τη διαρκή και αλματώδη αύξηση της ταχύτητας της ταχύτητας των υπολογιστικών συστημάτων, πάντα υπήρχαν πολύπλοκοι υπολογισμοί για εκτέλεση και ανάγκη για ακόμα μεγαλύτερες ταχύτητες επεξεργασίας. Η ανάγκη αυτή καλύφθηκε με δύο βασικές τεχνολογίες. Η μία ήταν οι υπερυπολογιστές και η άλλη οι συστοιχίες υπολογιστών.

Σημείωση: Στο κεφάλαιο αυτό περιέχονται τα συμπεράσματα του προγράμματος «*Δημιουργία Συστοιχίας Υπολογιστών Υψηλής Απόδοσης για Παράλληλη Επεξεργασία Δεδομένων*» που εκπονήθηκε στα πλαίσια του προγράμματος ΤΕΧΝΟΜΑΘΕΙΑ V από ομάδα μαθητών του 1ου ΕΠΑΛ Αργυρούπολης, υπό την επίβλεψη των καθηγητών Βασιλάκη Βασίλειου και Καλούτση Δημήτριου. Για περισσότερες πληροφορίες, το πλήρες κείμενο της εργασίας και τα ονόματα των συμμετεχόντων μαθητών δείτε: http://1epal-argyroupolis.eu/index.php/to-sxoleio-mas/δραστηριότητες/πρόγραμμα-τεχνομάθεια/συστοιχία-υπολογιστών

Διδακτικοί Στόχοι

Με την ολοκλήρωση του 4ου κεφαλαίου οι μαθητές θα πρέπει να είναι σε θέση να :

- Ορίζουν τι είναι μια συστοιχία υπολογιστών.
- Διακρίνουν τα διαφορετικά είδη συστοιχιών.
- Ονομάζουν τα πλεονεκτήματα των συστοιχιών υπολογιστών.
- Επιλέγουν το κατάλληλο υλικό και λογισμικό για την υλοποίηση μιας συστοιχίας υπολογιστών.
- Υλοποιούν μια συστοιχία υπολογιστών χρησιμοποιώντας εργαλεία ανοιχτού κώδικα.

Διδακτικές Ενότητες

4.1 Βασικά χαρακτηριστικά Συστοιχιών Υπολογιστών

Μια συστοιχία υπολογιστών (computer cluster) είναι δύο ή περισσότεροι υπολογιστές, όχι αναγκαστικά ίδιου τύπου ή δυνατοτήτων, που συνδέονται μεταξύ τους (συνήθως μέσω τοπικού δικτύου ή εικονικού ιδιωτικού δικτύου) προκειμένου να εκμεταλλευθούμε τη δυνατότητα παράλληλης επεξεργασίας που αυτοί παρέχουν. Οι υπολογιστές που απαρτίζουν μια συστοιχία καλούνται κόμβοι (nodes) ή μέλη (members).

4.2 Είδη Συστοιχιών

Σήμερα υπάρχουν αρκετά διαφορετικά είδη συστοιχιών, κάθε ένα από τα οποία προσφέρει διαφορετικά πλεονεκτήματα στους χρήστες του.

- **Συστοιχίες Υψηλής Διαθεσιμότητας (High Availability Clusters):** Οι συστοιχίες αυτές έχουν σχεδιαστεί για να προσφέρουν συνεχή πρόσβαση σε εφαρμογές παροχής υπηρεσιών. Διατηρούν επιπλέον κόμβους που μπορούν να χρησιμοποιηθούν σαν

εφεδρικά συστήματα στην περίπτωση αστοχίας των κύριων κόμβων. Ο ελάχιστος αριθμός κόμβων σε μία τέτοια συστοιχία είναι δύο (ένας κύριος και ένας εφεδρικός), παρόλο που η συντριπτική πλειοψηφία χρησιμοποιεί περισσότερους κόμβους.

- **Συστοιχίες Εξισορρόπησης Φορτίου (Load Balancing Clusters):** Οι συστοιχίες αυτού του τύπου, προσπαθούν να εξισορροπήσουν το φόρτο εργασίας μεταξύ των ενεργών κόμβων. Για το σκοπό αυτό μεταφέρουν διεργασίες από τον ένα κόμβο στον άλλο, ανάλογα με το φόρτο που έχει το κάθε σύστημα. Οι συστοιχίες εξισορρόπησης φορτίου είναι ιδιαίτερα χρήσιμες σε αυτούς που δουλεύουν με περιορισμένο προϋπολογισμό, γιατί φροντίζουν για την όσο το δυνατό αποδοτικότερη εκμετάλλευση του υπάρχοντος εξοπλισμού.
- **Συστοιχίες Υψηλής Απόδοσης (High Performance Clusters):** Οι συστοιχίες υψηλής απόδοσης σχεδιάστηκαν για να εκμεταλλευτούν την επεξεργαστική ισχύ πολλαπλών κόμβων. Χρησιμοποιούνται συνήθως σε εφαρμογές στις οποίες οι κόμβοι χρειάζεται να επικοινωνούν μεταξύ τους κατά τη διάρκεια της λειτουργίας τους, όταν π.χ. τα αποτελέσματα των υπολογισμών ενός κόμβου χρησιμοποιούνται από κάποιον άλλο.

4.3 Πλεονεκτήματα

- **Μείωση Κόστους:** Η τιμή των προσωπικών υπολογιστών έχει μειωθεί σημαντικά τα τελευταία χρόνια, και η μείωση αυτή συνοδεύεται από εκρηκτική αύξηση των επιδόσεων και της υπολογιστικής ισχύος τους. Ένα σημερινό μεσαίων δυνατοτήτων επιτραπέζιο σύστημα είναι πολλές φορές ισχυρότερο από τους πρώτους μεγάλους υπολογιστές.
- **Υπολογιστική Ισχύς:** Η συνδυασμένη υπολογιστική ισχύς μιας συστοιχίας υψηλής απόδοσης μπορεί σε πολλές περιπτώσεις να αποδειχθεί αποτελεσματικότερη, σε σχέση με το κόστος, από αυτήν ενός μεγάλου υπολογιστή παρόμοιων δυνατοτήτων. Με τον τρόπο αυτό η επιχείρηση αξιοποιεί καλύτερα τον εξοπλισμό της.
- **Επεκτασιμότητα:** Το σημαντικότερο πλεονέκτημα των συστοιχιών υπολογιστών είναι οι δυνατότητες επέκτασης που προσφέρουν. Ενώ οι μεγάλοι υπολογιστές έχουν συγκεκριμένη και σταθερή απόδοση, οι συστοιχίες μπορούν να επεκταθούν κατά βούληση με την απλή προσθήκη περισσότερων κόμβων στο δίκτυο.
- **Διαθεσιμότητα:** Όταν ένας μεγάλος υπολογιστής τίθεται εκτός λειτουργίας, καταρρέει όλο το σύστημα. Αν όμως χαλάσει ένας κόμβος μιας συστοιχίας, οι λειτουργίες που εκτελούσε θα μεταφερθούν σε κάποιον άλλο κόμβο, εξασφαλίζοντας την αδιάκοπη παροχή υπηρεσιών.

4.4 Υλικό και Λογισμικό υλοποίησης Συστοιχιών Υπολογιστών

Υλικό: Οι μεγάλες συστοιχίες υπολογιστών αποτελούνται από εκατοντάδες ή και χιλιάδες κόμβους με ισχυρούς επεξεργαστές και μεγάλα ποσά μνήμης. Ωστόσο κάθε υπολογιστής παλιός ή σύγχρονος μπορεί να αξιοποιηθεί σαν μέλος μιας συστοιχίας υπολογιστών.

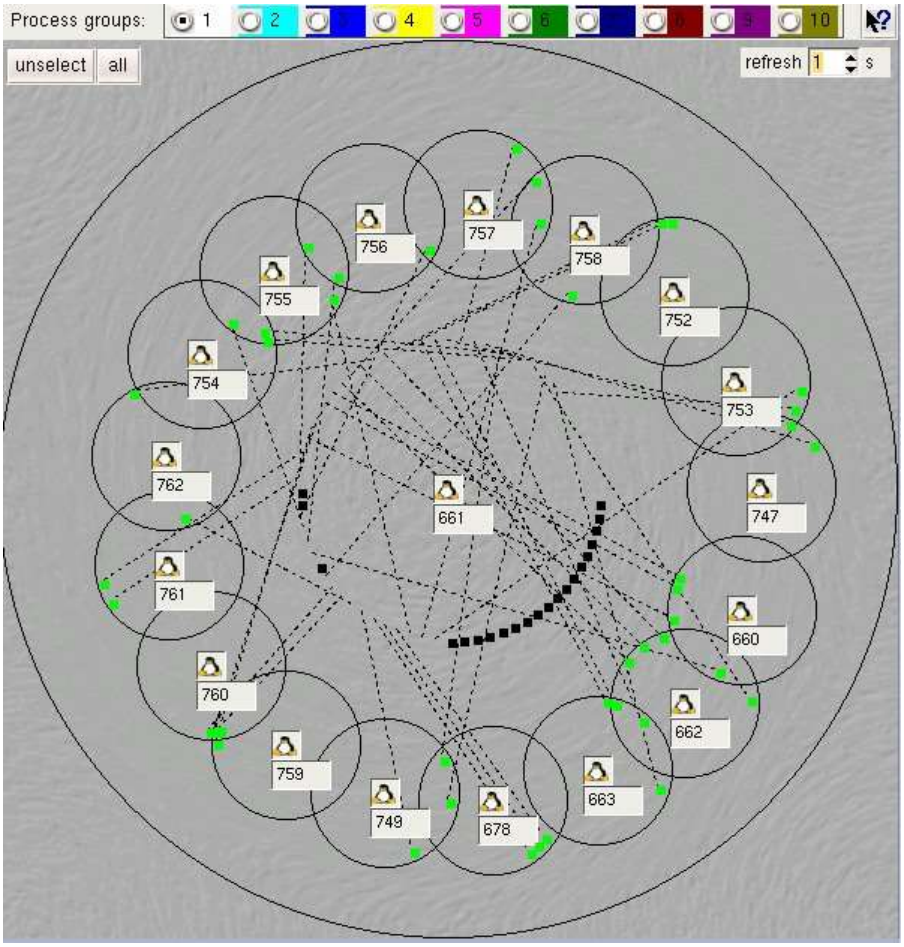
Εικόνα 4.1. Η συστοιχία 16 υδρόψυκτων υπολογιστών που κατασκευάστηκε στο Εργαστήριο Πειραματικής Φυσικής Υψηλών Ενεργειών της Σχολής Εφαρμοσμένων Μαθηματικών και Φυσικών Επιστημών του ΕΜΠ

Έτσι λοιπόν αν υπάρχουν διαθέσιμοι δύο ή περισσότεροι υπολογιστές αυτοί μπορούν να δημιουργήσουν μια συστοιχία, αρκεί να διαθέτουν κάρτα δικτύου και να υπάρχει ένα switch πάνω στο οποίο να μπορούν συνδεθούν.

Εικόνα 4.2. Η συστοιχία υπολογιστών που έφτιαξαν οι μαθητές του 1^{ου} ΕΠΑΛ Αργυρούπολης αποτελείται από 6 υπολογιστές με διπύρηνο επεξεργαστή και 2 GB RAM.

Λογισμικό: Το λογισμικό που μπορεί να χρησιμοποιηθεί εξαρτάται από το λειτουργικό σύστημα που χρησιμοποιούν οι υπολογιστές μας, αλλά και από είδος της συστοιχίας που θέλουμε να φτιάξουμε:

- Στα **Windows Server 2012** υπάρχει ενσωματωμένη η δυνατότητα δημιουργίας συστοιχίας Υψηλής Διαθεσιμότητας (Failover Cluster).
- Στο ίδιο λειτουργικό σύστημα μπορεί να δημιουργηθούν συστοιχίες υψηλής απόδοσης (HPC Clusters) με χρήση του επιπλέον λογισμικού **Microsoft HPC Pack 2012**.
- Στο Linux μπορούν να φτιαχτούν συστοιχίες υψηλής απόδοσης χρησιμοποιώντας λογισμικό ανοιχτού κώδικα όπως το **PVM** (Parallel Virtual Machine) και το **Open MPI** (Message Passing Interface). Τα λογισμικά αυτά επιτρέπουν την επικοινωνία και ανταλλαγή μηνυμάτων μεταξύ των κόμβων της συστοιχίας, επιτρέποντας έτσι την παράλληλη επεξεργασία. Οι συστοιχίες αυτού του είδους συνήθως περιλαμβάνουν ένα κύριο (master) κόμβο που ελέγχει ένα πλήθος από δευτερεύοντες (slave) κόμβους και ονομάζονται **Beowulf Clusters**.
- Σε μια διαφορετική υλοποίηση για Linux μπορεί να χρησιμοποιηθεί το σύστημα διαχείρισης συστοιχίας **OpenMosix**, προκειμένου να δημιουργηθεί μία συστοιχία εξισορρόπησης φορτίου με ομότιμους κόμβους. Στις συστοιχίες αυτού του είδους οι εργασίες κατανέμονται εξίσου στους κόμβους, ανεξάρτητα από το από ποιόν κόμβο προήλθαν. Με κατάλληλο προγραμματισμό οι συστοιχίες αυτές μπορούν να λειτουργήσουν και σαν συστοιχίες υψηλής απόδοσης.



Εικόνα 4.3. Συστοιχία δεκαοκτώ υπολογιστών βασισμένη στο OpenMosix. Οι πράσινες κουκκίδες είναι διεργασίες που έχουν μεταφερθεί για εκτέλεση σε διαφορετικό κόμβο από αυτόν απ' όπου προήλθαν.

Ερωτήσεις Ανακεφαλαίωσης

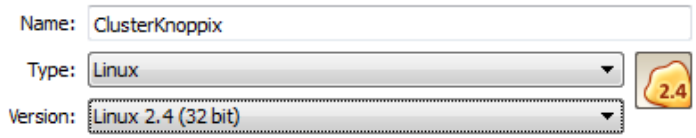
1. Τι είναι μια συστοιχία υπολογιστών;
2. Ποια είδη συστοιχιών μπορούν να χρησιμοποιηθούν για την επιτάχυνση της εκτέλεσης πολύπλοκων υπολογισμών;
3. Αναφέρετε και αναπτύξτε δύο πλεονεκτήματα της χρήσης συστοιχίας υπολογιστών, αντί ενός μεγάλου υπολογιστή.

Ασκήσεις

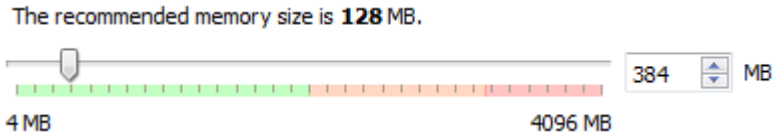
1η Άσκηση

Στην άσκηση αυτή θα φτιάξετε τη δική σας συστοιχία χρησιμοποιώντας εικονικές μηχανές. Για τη δημιουργία της συστοιχίας θα χρησιμοποιήσετε μια έκδοση του Linux που λέγεται ClusterKnoppix και διανέμεται σε live-cd με όλα τα απαραίτητα ενσωματωμένα.

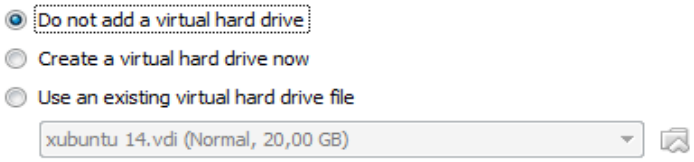
1. Ανοίξτε το Oracle VirtualBox και δημιουργείστε μια νέα εικονική μηχανή δίνοντας τις ακόλουθες τιμές στα βήματα του οδηγού:
   1.1. Name: ClusterKnoppix, Type: Linux, Version: Linux 2.4 (32bit)



   1.2. Memory Size: 384 MB



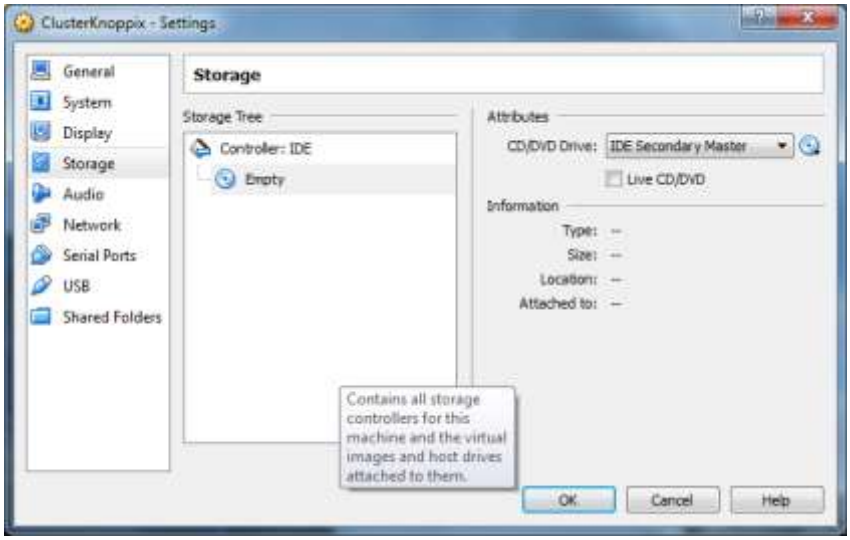
   1.3. Hard Drive: Do not add a virtual hard drive (Γιατί δεν είναι απαραίτητο να έχει σκληρό δίσκο ο εικονικός υπολογιστής;)



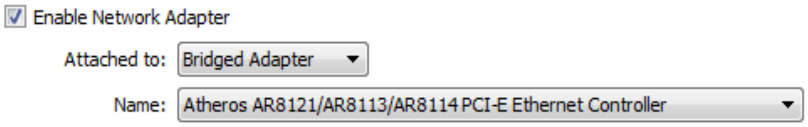
   1.4. Δημιουργείστε την εικονική μηχανή και πατήστε [Continue] στην προειδοποίηση ότι δεν υπάρχει σκληρός δίσκος

2. Πατήστε πάνω στο όνομα της εικονικής μηχανής που δημιουργήσατε και ανοίξτε τις ιδιότητές της πατώντας στο εικονίδιο με το γρανάζι 

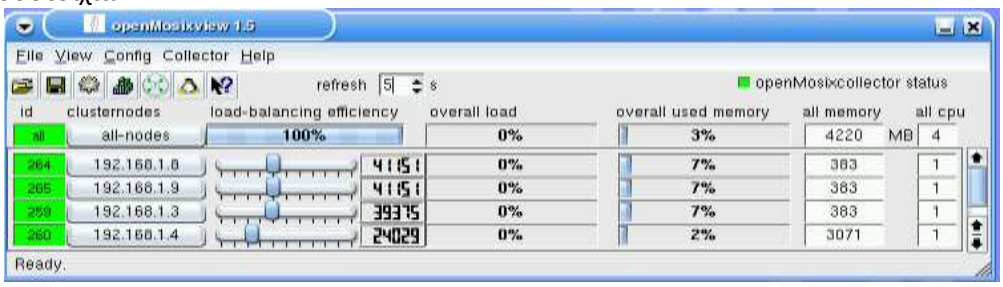
2.1. Στην ενότητα [*Storage*] πατήστε πάνω στο εικονίδιο του CD (στη μέση) που γράφει [*Empty*] και στη συνέχεια πατήστε στο εικονίδιο του CD στα δεξιά. Από το μενού που θα εμφανιστεί επιλέξτε [*Choose a virtual CD/DVD disk file…*] και επιλέξτε το αρχείο **clusterKNOPPIX_PI.iso**.



2.2. Στην ενότητα [*Network*] αλλάξτε τη ρύθμιση [*Attached to:*] σε [*Bridged Adapter*]. Με τη ρύθμιση αυτή εξασφαλίζουμε ότι η εικονική μηχανή θα φαίνεται στο δίκτυο σαν ένας ανεξάρτητος υπολογιστής

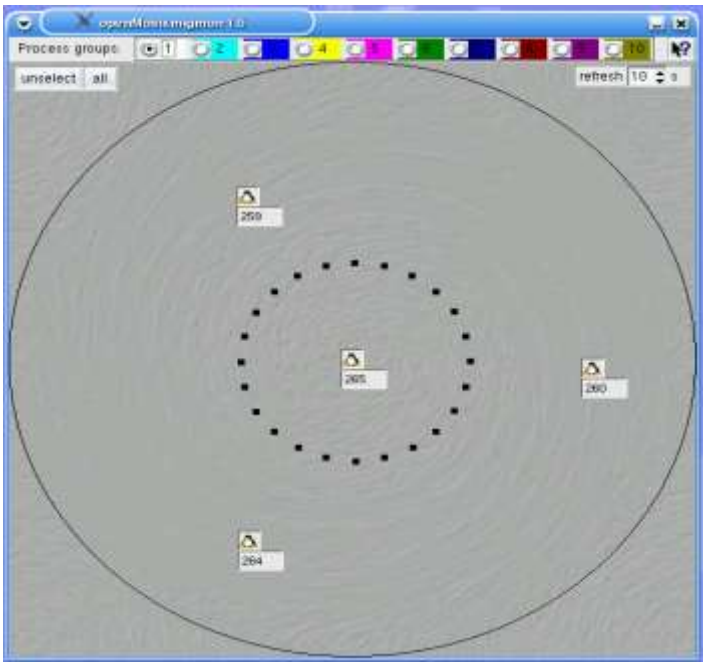


3. Ξεκινήστε την εικονική μηχανή πατώντας στο  .
4. Στην προτροπή boot: του λειτουργικού συστήματος πατήστε [*Enter*].
5. Όταν ξεκινήσει το γραφικό περιβάλλον πατήστε στη γραμμή εργασιών το εικονίδιο με τον πιγκουΐνο  για να ξεκινήσει η εφαρμογή **OpenMosixView** που διαχειρίζεται τη συστοιχία. Αν όλα πήγαν καλά θα πρέπει στο παράθυρο να εμφανίζονται τόσες καταχωρήσεις όσοι οι υπολογιστές (εικονικές μηχανές) που συμμετέχουν στη συστοιχία.



6. Κάθε κόμβος της συστοιχίας παίρνει έναν αύξοντα αριθμό που εμφανίζεται στην πρώτη στήλη. Μπορείτε να πείτε τι αντιπροσωπεύουν οι αριθμοί της 2ης στήλης;

7. Στην 3η στήλη φαίνεται η ισχύς του κάθε υπολογιστή που συμμετέχει στη συστοιχία, ενώ στην 4η το φορτίο του κάθε κόμβου. Σκοπός της συστοιχίας είναι να εξισορροπεί το φορτίο αυτό. Εξετάστε την 4η και την 5η στήλη και σημειώστε τι πληροφορίες μας δίνει κάθε μία από αυτές.
8. Αλλάξτε το ρυθμό ανανέωσης (refresh) των περιεχομένων του παραθύρου σε 1s.
9. Πατήστε στο εικονίδιο . Θα ανοίξει το παράθυρο **OpenMosixMon** που θα απεικονίζει τους υπολογιστές της συστοιχίας. Κάθε πιγκουίνος είναι ένας υπολογιστής. Ο υπολογιστής στο κέντρο είναι αυτός στον οποίο εργάζεστε. Οι κουκκίδες γύρω του είναι οι διεργασίες που εκτελούνται σε αυτόν. Τα υπόλοιπα εικονίδια αντιπροσωπεύουν τους υπόλοιπους υπολογιστές της συστοιχίας. Αλλάξτε και εδώ το χρόνο ανανέωσης σε 1s.



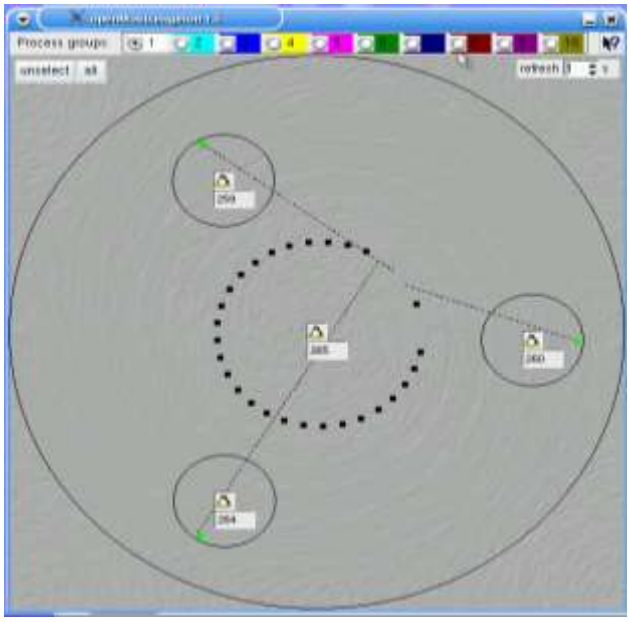
10. Βάλτε τη συστοιχία να δουλέψει. Στη γραμμή εργασιών πατιέστε στο κουμπί για να ανοίξετε ένα παράθυρο γραμμής εντολών. Δώστε την εντολή **ls** για να δείτε τα αρχεία που υπάρχουν στο φάκελο.
11. Το αρχείο με όνομα pi υπολογίζει την τιμή του π (3,14159…) σαν ένα άθροισμα όρων μιας σειράς. Όσο περισσότερους όρους αθροίζουμε, τόσο μεγαλύτερη ακρίβεια σε δεκαδικά ψηφία παίρνουμε, αλλά και ο υπολογισμός κρατά περισσότερο.
12. Βρείτε στο internet σελίδες που να δίνουν την τιμή του π με πολλά δεκαδικά ψηφία. Καταγράψτε τον αριθμό με τα 20 πρώτα δεκαδικά του.
13. Ο αλγόριθμος που θα χρησιμοποιήσετε συγκλίνει πολύ αργά. Αυτό σημαίνει ότι πρέπει να γίνουν πολλές πράξεις για να πάρουμε το π με ακρίβεια αρκετών δυαδικών ψηφίων. Επίσης η εφαρμογή επιτρέπει το σπάσιμο των υπολογισμών σε κομμάτια (διεργασίες) που θα μοιραστούν στους υπολογιστές της συστοιχίας για να γίνουν οι πράξεις πιο γρήγορα. Ξεκινήστε με μία διεργασία, δίνοντας την εντολή: **pi 100000000 1**. Η εφαρμογή θα υπολογίσει την τιμή του π προσθέτοντας 100 εκατομμύρια όρους της σειράς σε 1 διεργασία. Θα εμφανίσει την ώρα έναρξης, τερματισμού (δεν πειράζει αν δεν είναι οι σωστές, αυτό που μας ενδιαφέρει είναι η διαφορά), την τιμή του π, την ακρίβεια σε δεκαδικά ψηφία και το συνολικό χρόνο που χρειάστηκε. Από το παράθυρο **openmosixview** μπορείτε να δείτε το φορτίο του υπολογιστή σας να αυξάνεται. Αν στη συστοιχία υπάρχει συνδεδεμένος γρηγορότερος υπολογιστής η

διεργασία θα “μεταναστεύσει” (migrate) στο μηχάνημα αυτό ώστε να εκτελεστεί πιο γρήγορα.

```
knoppix@ttyp0[knoppix]$ pi 100000000 1
EKKINHSH 09:28:00
TERMATISMOS 09:28:25
pi (ETOIMO) = 3.14159265358979323846264338327795
pi (YPOLOG) = 3.14159264358936862748805651790 46
AKRIBEIA  7 DEKADIKA PSIFIA
XRONOS EKTELESIS 0:0:25
```

Παρατηρείστε ότι με 100 εκατομμύρια όρους πετύχατε ακρίβεια μόλις 7 δεκαδικών ψηφίων. Ο ακριβής χρόνος εκτέλεσης εξαρτάται από την ισχύ του μηχανήματος.

14. Δώστε τώρα την εντολή, χωρίζοντας τους υπολογισμού σε 4 κομμάτια. Τι θα πρέπει να αλλάξετε στη σύνταξη της εντολής; Δείτε στο παράθυρο **openmosixmon** τις διεργασίες να μεταναστεύουν σε άλλα μηχανήματα προκειμένου να εξισορροπηθεί το φορτίο της συστοιχίας. Θα διαπιστώσετε ακόμη ότι για την ολοκλήρωση της διαδικασίας απαιτήθηκε μικρότερος χρόνος.



15. Υπολογίστε την τιμή του π χρησιμοποιώντας 1 δις όρους της σειράς. Σε πόσες διεργασίες πρέπει να μοιράσετε τους υπολογισμούς ώστε να έχετε την καλύτερη δυνατή απόδοση της συστοιχίας;

Βιβλιογραφία

Ξενόγλωσση

Granneman S. (2006). *Hacking Knoppix*. Redmond, Washinghton, Indianapolis. Wiley Publishing Inc.

Spector D. (2000). *Building Linux Clusters*. Sebastopol, O’Reilly Media Inc.

Δικτυογραφία

Σπιτικό Clustering με Linux…: http://dimitris.apeiro.gr/2008/12/24/σπιτικό-clustering-με-linux/

Περιβάλλον παράλληλου προγραμματισμού για την εκπαίδευση: http://users.sch.gr/delistavrou/.dimiourgies/clusterhowto.pdf

The openMosix HOWTO: http://www.tldp.org/HOWTO/openMosix-HOWTO/index.html

Wikipedia (Computer Clusters): https://en.wikipedia.org/wiki/Computer_cluster

Building your own Super Computer: http://www.webstreet.com/super_computer.htm

Δημιουργία Failover Cluster σε Windows 2012 Server: http://windowsitpro.com/windows-server-2012/windows-server-2012-building-two-node-failover-cluster

Οδηγός δημιουργίας συστοιχίας υψηλής απόδοσης σε Windows Server: http://social.technet.microsoft.com/wiki/contents/articles/2539.diy-supercomputing-how-to-build-a-small-windows-hpc-cluster.aspx

Κεφάλαιο 5ο

Βασικές Εντολές Δικτύωσης

Εισαγωγή

Για τη ρύθμιση και εξασφάλιση της ομαλής επικοινωνία μιας δικτυακής συσκευής είναι απαραίτητη η γνώση των βασικών ρυθμίσεων που απαιτούνται για την παραμετροποίηση της κάρτας δικτύου, βασικής μονάδας σύνδεσης της με ένα δίκτυο δεδομένων. Επίσης η χρήση βασικών εντολών δικτύωσης επιτρέπει τον έλεγχο της ύπαρξης επικοινωνίας με το δίκτυο, την εύρεση IP διεύθυνσης μιας συσκευής κ.α., ενώ με ειδικό λογισμικό μπορεί να γίνει παρακολούθηση πακέτων για την εξαγωγή συμπερασμάτων σχετικά με τα στοιχεία επικοινωνίας αλλά και την ποιότητα της σύνδεσης.

Διδακτικοί Στόχοι

Με την ολοκλήρωση του 5ου κεφαλαίου οι μαθητές θα πρέπει να είναι σε θέση να :

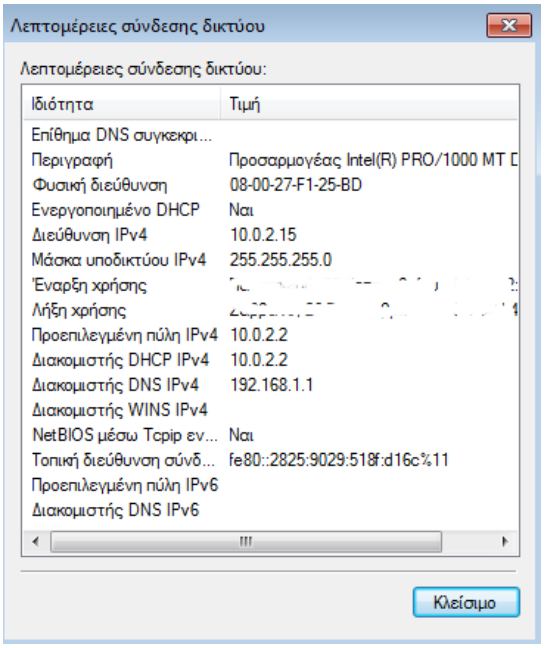
- Εντοπίζουν τη διεύθυνση MAC της κάρτας δικτύου.
- Ρυθμίζουν τη διεύθυνση IP, τη μάσκα υποδικτύου, την πύλη εξόδου και το διακομιστή DNS της κάρτας δικτύου (Στο γραφικό περιβάλλον και σε περιβάλλον εντολών).
- Χρησιμοποιούν βασικές εντολές δικτύωσης για να αναγνωρίζουν την ύπαρξη ή την απουσία επικοινωνίας μεταξύ των υπολογιστών ενός δικτύου.
- Ελέγχουν αν υπάρχει αντιστοίχιση μιας διεύθυνσης IP με ένα όνομα.
- Ελέγχουν τις ενεργές συνδέσεις δικτύου.
- Εφαρμόζουν λογισμικό για την παρακολούθηση των πακέτων που αποστέλλονται/ λαμβάνονται.

Διδακτικές Ενότητες

5.1 Παραμετροποίηση κάρτας δικτύου

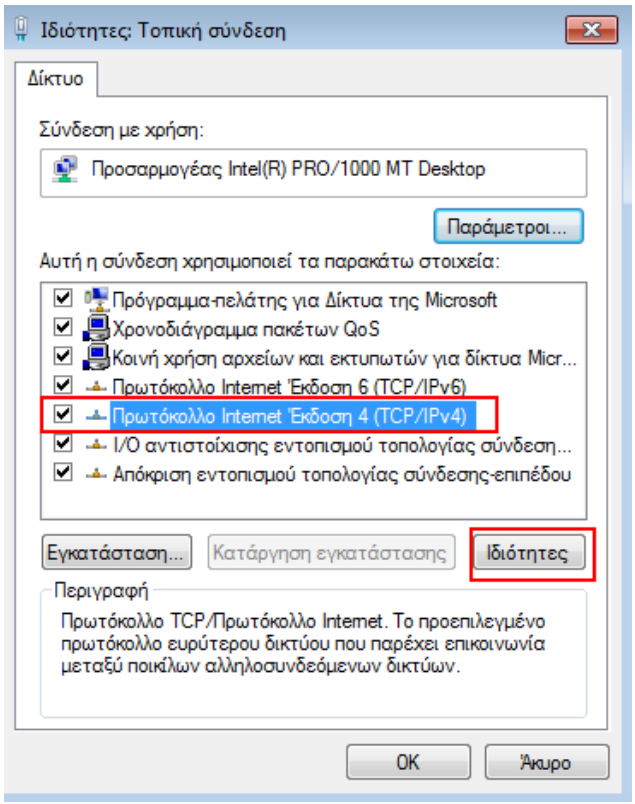
5.1.1 Ενέργειες για λειτουργικό σύστημα Windows

Για τον εντοπισμό των γενικών χαρακτηριστικών της κάρτας δικτύου στο γραφικό περιβάλλον των Windows 7, αρχικά θα πρέπει να ανοίξουμε τον **Πίνακα Ελέγχου**. Στη συνέχεια, ανοίγουμε το **Κέντρο Δικτύωσης και κοινής χρήσης** και επιλέγουμε από την πλευρική στήλη **Αλλαγή ρυθμίσεων προσαρμογέα**. Τέλος, αφού πατήσουμε δεξί κλικ στην **Τοπική σύνδεση** επιλέγουμε διαδοχικά **Κατάσταση** και **Λεπτομέρειες**.

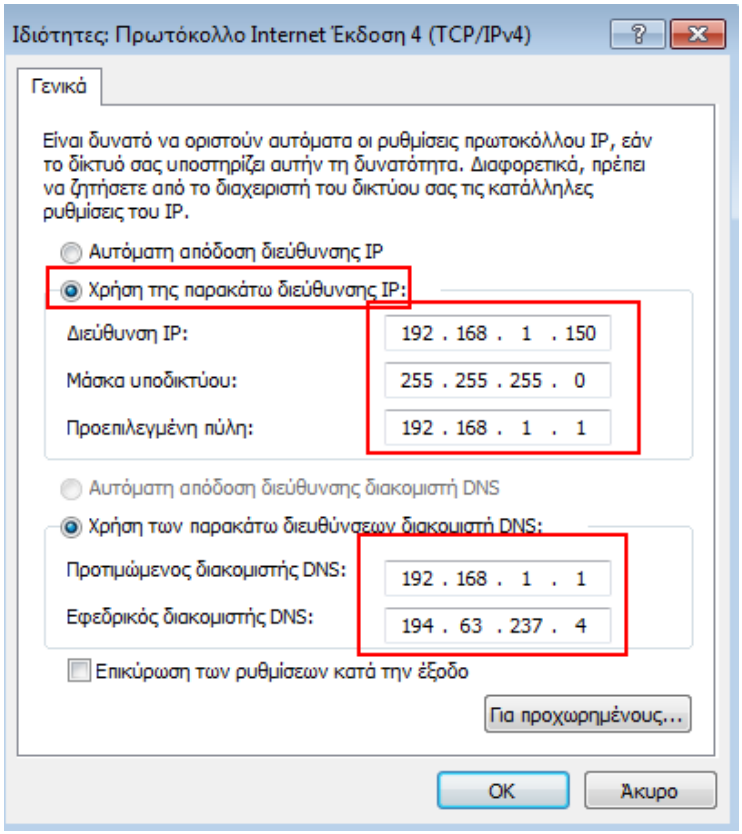


Εικόνα 5.1: Προβολή χαρακτηριστικών κάρτας δικτύου

Για να θέσουμε στατική διεύθυνση IP, πύλη εξόδου και DNS χειροκίνητα, ακολουθούμε όλα τα βήματα ακολουθήσαμε για την προβολή των χαρακτηριστικών της κάρτας δικτύου εκτός από το τελευταίο. Εκεί, αντί να επιλέξουμε **Λεπτομέρειες** επιλέγουμε **Ιδιότητες**. Στη συνέχεια επιλέγουμε **Πρωτόκολλο Internet Έκδοση 4 (TCP/IPv4)** και πατάμε το κουμπί **Ιδιότητες.**



Εικόνα 5.2: Τροποποίηση ιδιοτήτων Πρωτοκόλλου IPv4



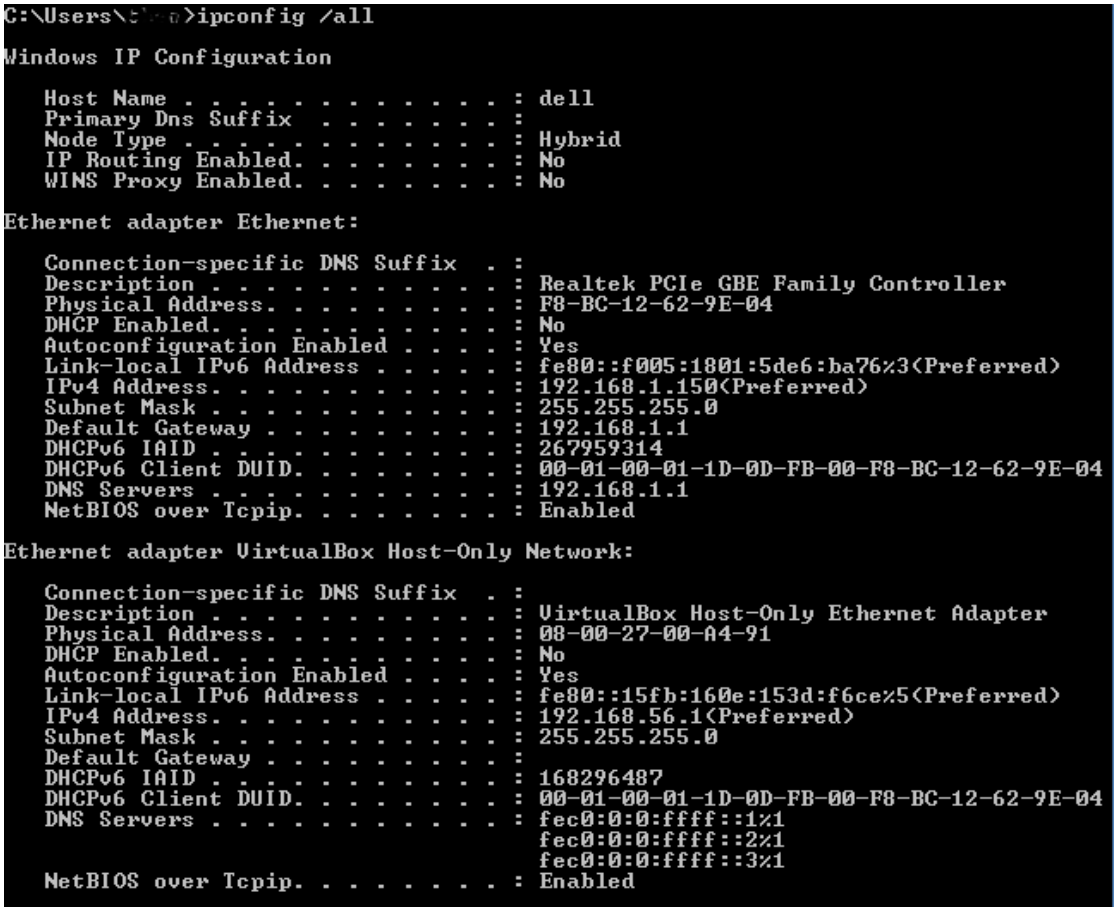
Εικόνα 5.3: Ρυθμίσεις κάρτας δικτύου

Για την προβολή των χαρακτηριστικών της κάρτας δικτύου σε περιβάλλον κειμένου, εκτελούμε την εντολή **ipconfig**. Στο αποτέλεσμα μπορούμε να διακρίνουμε την IP διεύθυνση (IPv4 Address) και την πύλη εξόδου (Default Gateway) για κάθε μία κάρτα δικτύου που υπάρχει στο υπολογιστικό μας σύστημα.

```
C:\Users\[redacted]>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::f005:1801:5de6:ba76%3
   IPv4 Address. . . . . . . . . . . : 192.168.1.150
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::15fb:160e:153d:f6ce%5
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

Εικόνα 5.4: Χαρακτηριστικά κάρτας δικτύου

Για την προβολή όλων των χαρακτηριστικών της κάρτας δικτύου πρέπει να εισάγουμε την παράμετρο **all** στην εντολή **ipconfig.** Έτσι, γράφοντας **ipconfig /all** θα πάρουμε το παρακάτω αποτέλεσμα:



Εικόνα 5.5: Χαρακτηριστικά κάρτας δικτύου

Οι πιο σημαντικές πληροφορίες που μπορούμε να αντλήσουμε από το παραπάνω στιγμιότυπο είναι, το όνομα που έχει ο υπολογιστής στο δίκτυο (**Host Name**), τη φυσική διεύθυνση (**MAC Address)** της κάρτας δικτύου (**Physical Address)**, τη διεύθυνση IP (**IPv4 Address)**, τη μάσκα δικτύου **(Subnet Mask)**, τη διεύθυνση της πύλης εξόδου **(Default Gateway)**, τον τρόπο κτήσης της διεύθυνσης IP – μέσω DHCP ή χειροκίνητα – (**DHCP Enabled)** και τους διακομιστές επίλυσης ονομάτων **(DNS Servers).**

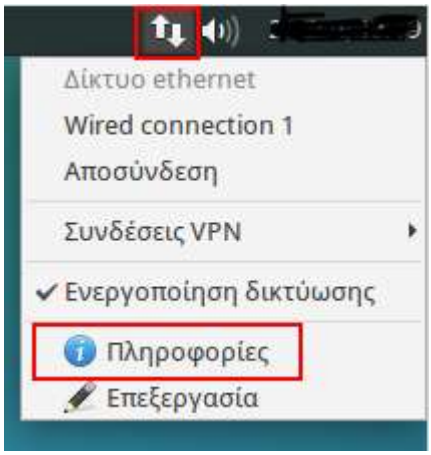
Οι λέξεις ή οι αριθμοί που βρίσκονται στο τέλος μιας εντολής είναι μεταβλητές που χρησιμοποιούνται για την παραμετροποίηση της εντολής. Για αυτό το λόγο ονομάζονται παράμετροι. Για κάθε μια εντολή, οι παράμετροι που μπορεί να δεχτεί είναι διαφορετικές. Για να δούμε τις διαθέσιμες παραμέτρους μιας εντολής στα Windows, αρκεί να γράψουμε το όνομα της εντολής και στη συνέχεια **/?**. Έτσι, αν θέλουμε να δούμε όλες τις παραμέτρους που μπορεί να δεχθεί η εντολή ipconfig θα γράψουμε **ipconfig /?**

Σε περιβάλλον κειμένου, για τη ρύθμιση στατικής διεύθυνση IP, μάσκας δικτύου και πύλης γράφουμε την εντολή **sudo netsh interface ipv4 set address “Ethernet” static 192.168.1.150 255.255.255.0 192.168.1.1**. Το κείμενο μέσα στα εισαγωγικά είναι το όνομα που έχει η κάρτα δικτύου (Εικόνα 5.5).

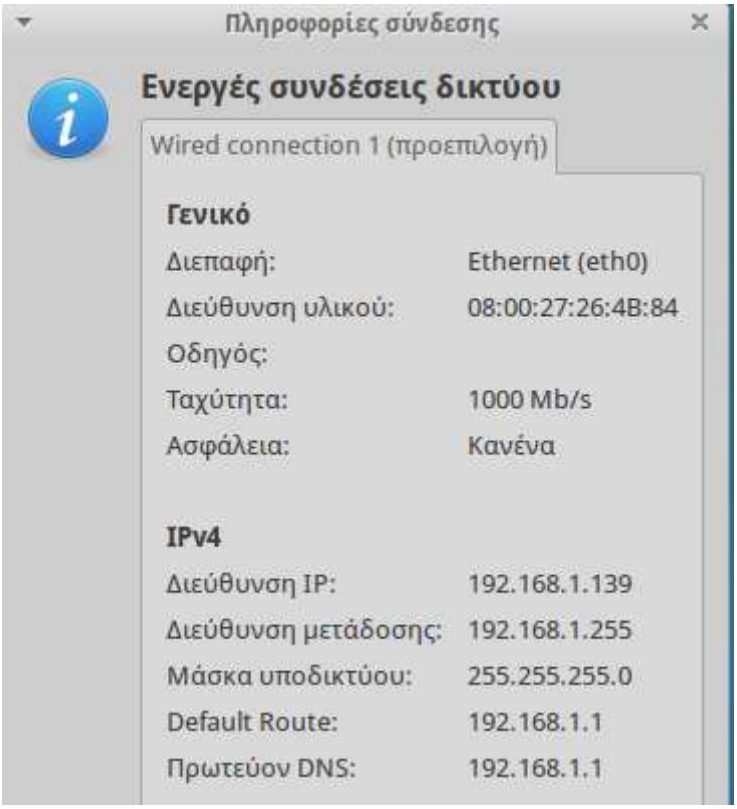
Στη συνέχεια πρέπει να ορίσουμε το διακομιστή επίλυσης ονομάτων (DNS server) με την εντολή **sudo netsh interface ipv4 set dnsservers “Ethernet” static 192.168.1.1.** Αν θέλουμε να προσθέσουμε ακόμα ένα DNS server θα γράψουμε **sudo netsh interface ipv4 set dnsservers “Ethernet” static 19463.237.4 index=2**

5.1.2 Ενέργειες για λειτουργικό σύστημα Xubuntu

Για τον εντοπισμό των γενικών χαρακτηριστικών σε γραφικό περιβάλλον, πατάμε το εικονίδιο με τα δύο βέλη που βρίσκεται στη γραμμή εργασιών και στη συνέχεια επιλέγουμε **Πληροφορίες**.

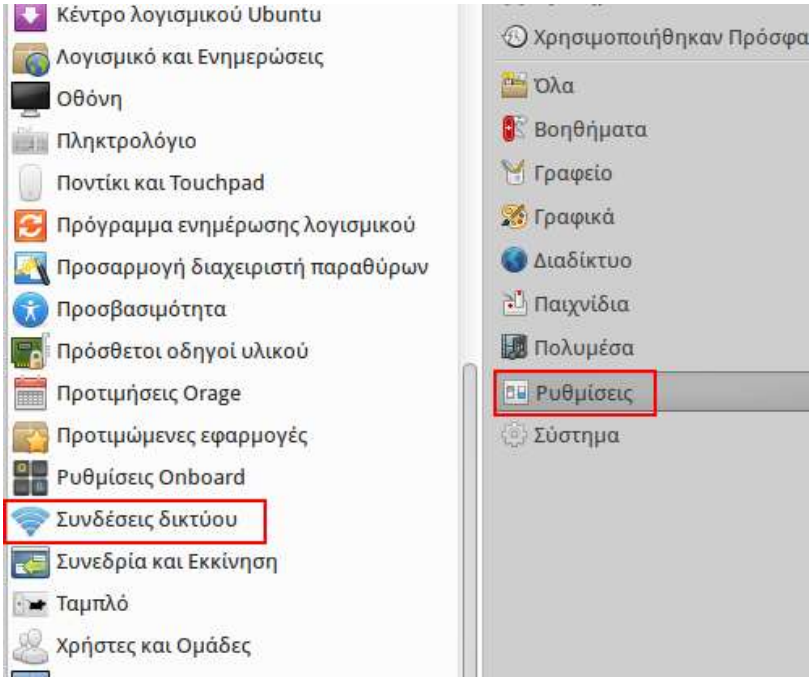


Εικόνα 5.6: Προβολή πληροφοριών κάρτας δικτύου



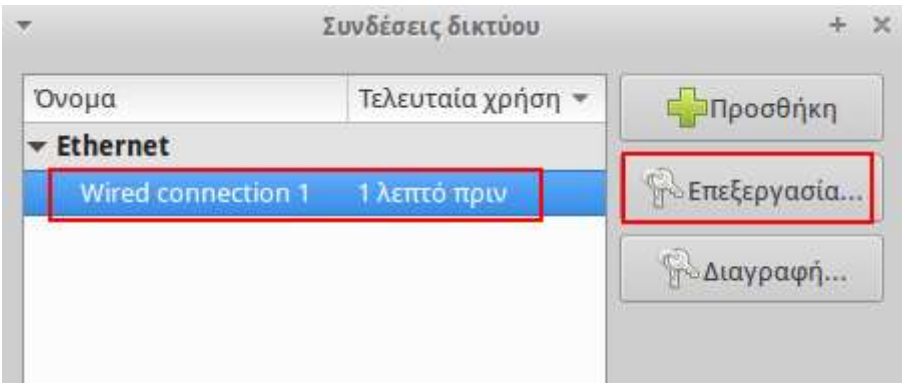
Εικόνα 5.7: Πληροφορίες κάρτας δικτύου

Για να θέσουμε στατική διεύθυνση IP, πύλη εξόδου και DNS χειροκίνητα, πατάμε αρχικά το εικονίδιο στην επάνω αριστερή γωνία και στη συνέχεια επιλέγουμε **Ρυθμίσεις.** Τέλος, επιλέγουμε **Συνδέσεις δικτύου.**



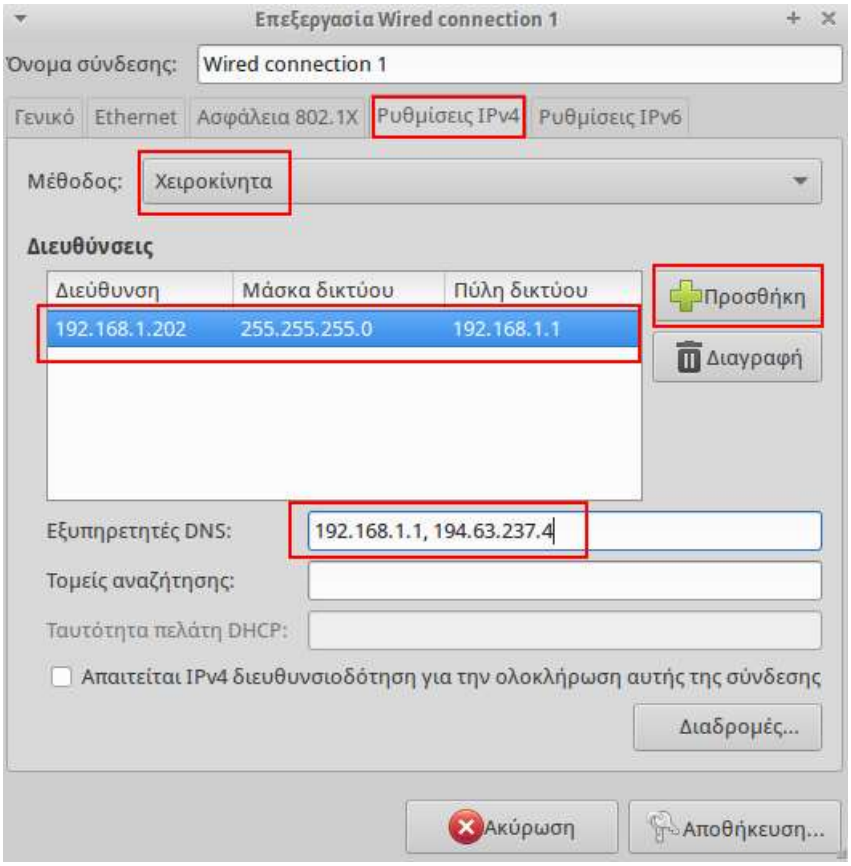
Εικόνα 5.8: Συνδέσεις δικτύου

Στη συνέχεια επιλέγουμε την κάρτα δικτύου **Wired connection 1** και πατάμε το κουμπί **Επεξεργασία.**



Εικόνα 5.9: Ιδιότητες κάρτας δικτύου

Επιλέγουμε την καρτέλα **Ρυθμίσεις IPv4** και από το πεδίο **Μέθοδος** επιλέγουμε **Χειροκίνητα.** Πατάμε το κουμπί **Προσθήκη** και εισάγουμε τη διεύθυνση IP, τη μάσκα δικτύου και την πύλη εξόδου. Επίσης, εισάγουμε στο πεδίο **Εξυπηρετητές DNS** τις διευθύνσεις των διακομιστών επίλυσης ονομάτων. Τέλος, πατάμε το κουμπί **Αποθήκευση**.



Εικόνα 5.10: Ορισμός χαρακτηριστικών κάρτας δικτύου χειροκίνητα

Σε περιβάλλον κειμένου, για τη ρύθμιση στατικής διεύθυνση IP και μάσκας δικτύου γράφουμε την εντολή **sudo ifconfig eth0 192.168.1.203 netmask 255.255.255.0**. Για τον ορισμό της πύλης εξόδου γράφουμε **sudo route add default gw 192.168.1.1**.

5.2 Έλεγχος επικοινωνίας δικτύου μέσω εντολών δικτύωσης

5.2.1 Εντολή ping

Η εντολή **ping** χρησιμοποιεί το πρωτόκολλο ICMP (αποστολή πακέτων και αναμονή για λήψη) για να διαπιστώσει αν ένας υπολογιστής στο δίκτυο είναι ενεργός ή όχι. Το αποτέλεσμα της εντολής **ping 192.168.1.1** είναι:

```
pc@pc-VirtualBox:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=1.69 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=2.19 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=2.14 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=2.01 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=1.27 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4009ms
rtt min/avg/max/mdev = 1.279/1.865/2.190/0.341 ms
```

Εικόνα 5.11: Αποτέλεσμα εντολής ping

Στο παραπάνω παράδειγμα η εντολή **ping** έστειλε 5 πακέτα δεδομένων στον υπολογιστή με διεύθυνση IP 192.168.1.1 και όπως παρατηρούμε επέστρεψαν όλα.

Αν γράψουμε την εντολή ping **192.168.1.25**, το αποτέλεσμα είναι:

```
pc@pc-VirtualBox:~$ ping 192.168.1.25
PING 192.168.1.25 (192.168.1.25) 56(84) bytes of data.
From 192.168.1.203 icmp_seq=1 Destination Host Unreachable
From 192.168.1.203 icmp_seq=2 Destination Host Unreachable
From 192.168.1.203 icmp_seq=3 Destination Host Unreachable
From 192.168.1.203 icmp_seq=4 Destination Host Unreachable
From 192.168.1.203 icmp_seq=5 Destination Host Unreachable
From 192.168.1.203 icmp_seq=6 Destination Host Unreachable
^C
--- 192.168.1.25 ping statistics ---
8 packets transmitted, 0 received, +6 errors, 100% packet loss, time 7010ms
```

Εικόνα 5.12: Αποτέλεσμα εντολής ping

Το συμπέρασμα που μπορούμε να βγάλουμε από το παραπάνω αποτέλεσμα είναι ότι δεν υπάρχει υπολογιστής με τη διεύθυνση 192.168.1.25 στο δίκτυο μας.

Στην περίπτωση που ο συγκεκριμένος υπολογιστής έχει ενεργό τοίχος προστασίας το οποίο απορρίπτει τα πακέτα ICMP το αποτέλεσμα θα ήταν το παρακάτω:

```
pc@pc-VirtualBox:~$ ping 192.168.1.150
PING 192.168.1.150 (192.168.1.150) 56(84) bytes of data.
```

Εικόνα 5.13: Αποτέλεσμα εντολής ping

Φυσικά, έχουμε τη δυνατότητα να ελέγξουμε αν ένας υπολογιστή που βρίσκεται στο Διαδίκτυο είναι ενεργός ή όχι. Για παράδειγμα γράφοντας **ping www.google.gr** θα πάρουμε το παρακάτω αποτέλεσμα:

```
pc@pc-VirtualBox:~$ ping www.google.gr
PING www.google.gr (64.233.167.94) 56(84) bytes of data.
64 bytes from wl-in-f94.1e100.net (64.233.167.94): icmp_seq=1 ttl=45 time=65.2 ms
64 bytes from wl-in-f94.1e100.net (64.233.167.94): icmp_seq=2 ttl=45 time=64.1 ms
64 bytes from wl-in-f94.1e100.net (64.233.167.94): icmp_seq=3 ttl=45 time=64.6 ms
64 bytes from wl-in-f94.1e100.net (64.233.167.94): icmp_seq=4 ttl=45 time=64.4 ms
64 bytes from wl-in-f94.1e100.net (64.233.167.94): icmp_seq=5 ttl=45 time=64.2 ms
^C
--- www.google.gr ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 64.143/64.537/65.204/0.413 ms
```

Εικόνα 5.14: Αποτέλεσμα εντολής ping

5.2.2 Εντολή arp

Η εντολή arp μας δείχνει έναν πίνακα ο οποίος σε κάθε μια γραμμή του περιέχει μια διεύθυνση IP και την αντίστοιχή διεύθυνση MAC.

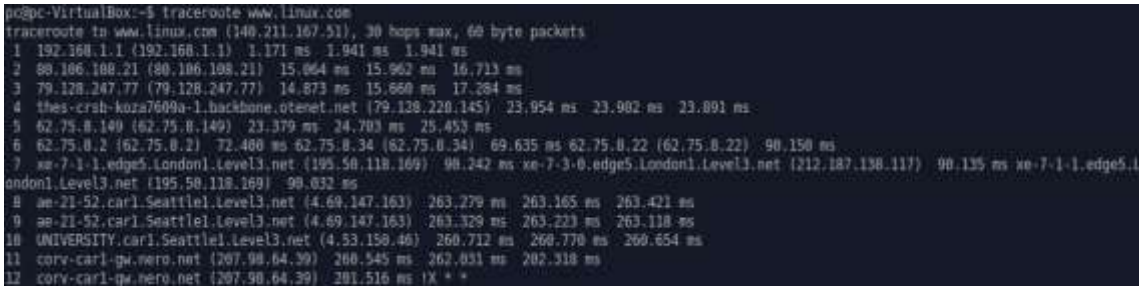
```
Interface: 192.168.1.150 --- 0x3
  Internet Address      Physical Address      Type
  192.168.1.1           00-23-48-77-5f-ff     dynamic
  192.168.1.200         08-00-27-28-ae-45     dynamic
  192.168.1.201         08-00-27-45-12-2b     dynamic
  192.168.1.203         08-00-27-26-4b-84     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
```

Εικόνα 5.15: Πίνακας ARP

Με αυτόν τον τρόπο μπορούμε να δούμε ποιες διευθύνσεις IP του εσωτερικού δικτύου χρησιμοποιούνται.

5.2.3 Εντολή traceroute (tracert)

Η εντολή **traceroute** μας επιτρέπει να δούμε την πορεία που ακολουθεί ένα πακέτο μέχρι να φτάσει στον προορισμό του. Το αποτέλεσμα της εντολής **traceroute www.linux.gr** είναι το παρακάτω:

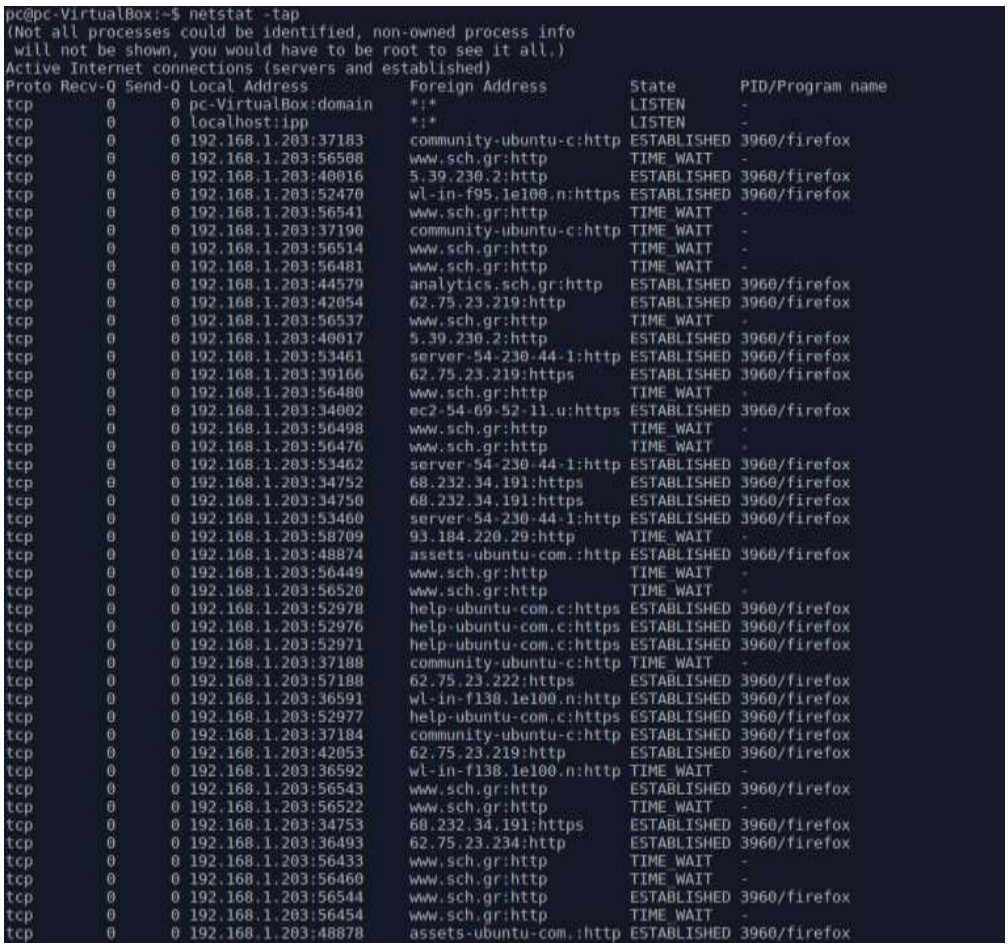


Εικόνα 5.16: Αποτέλεσμα εντολής traceroute

Παρατηρούμε ότι το πακέτο δεδομένων φεύγει από το δρομολογητή μας (1η γραμμή) και ταξιδεύει από κόμβο σε κόμβο στο Διαδίκτυο μέχρι να φτάσει στον προορισμό του.

5.2.4 Εντολή netstat

Η εντολή **netstat** μας δείχνει στατιστικά για όλες τις ενεργές συνδέσεις δικτύου όπως επίσης και τα πρωτόκολλα που χρησιμοποιούνται. Έχοντας ενεργό ένα τερματικό, ανοίγουμε μια ιστοσελίδα μέσω ενός φυλλομετρητή. Αν γράψουμε την εντολή **netstat –tap** στο τερματικό, το αποτέλεσμα θα μοιάζει με την παρακάτω εικόνα:



Εικόνα 5.17: Αποτέλεσμα εντολής netstat

Οι πληροφορίες που μπορούμε να δούμε είναι το πρωτόκολλο που χρησιμοποιείται **(Proto)**, η τοπική διεύθυνση **(Local Address)**, η διεύθυνση του απομακρυσμένου υπολογιστή **(Remote Address)** καθώς και η κατάσταση της σύνδεσης **(State)**.

5.2.5 Εντολή nslookup

Την εντολή nslookup τη χρησιμοποιούμε για να αντλήσουμε πληροφορίες από έναν διακομιστή επίλυσης ονομάτων (DNS Server). Για παράδειγμα, αν θέλουμε να δούμε σε ποια διεύθυνση IP αντιστοιχεί το όνομα www.sch.gr θα γράψουμε **nslookup www.sch.gr**.

```
pc@pc-VirtualBox:~$ nslookup www.sch.gr
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
Name:   www.sch.gr
Address: 194.63.235.170
```

Εικόνα 5.18: Αποτέλεσμα εντολής nslookup

Έχουμε τη δυνατότητα να κάνουμε και αντίστροφη αναζήτηση, εισάγοντας τη διεύθυνση IP για να βρούμε το όνομα. Για παράδειγμα:

```
pc@pc-VirtualBox:~$ nslookup 194.63.235.170
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
170.235.63.194.in-addr.arpa     name = www.sch.gr.

Authoritative answers can be found from:
```

Εικόνα 5.19: Αποτέλεσμα εντολής nslookup

5.3 Παρακολούθηση Πακέτων

Η χρήση εργαλείων ανάλυσης δικτύου αποτελεί βασικό μέρος της διαχείρισης ενός δικτύου, αφού αυτά επιτρέπουν την παρακολούθηση των σημείων που μπορεί να υπάρχει δυσλειτουργία της απόδοσης του δικτύου. Είναι θεμιτό να υπάρχει η δυνατότητα να μετρούνται μερικά χαρακτηριστικά της επίδοσης του δικτύου και να αποθηκεύονται αυτές οι μετρήσεις για μελλοντική επεξεργασία. Οι διαχειριστές του δικτύου θα πρέπει να αναλύουν τις μετρήσεις και να μπορούν να εντοπίσουν σημεία συμφόρησης ή προβληματικής λειτουργίας του δικτύου. Με βάση τα συμπεράσματα από την ανάλυση των μετρήσεων θα μπορούν να λάβουν αποφάσεις για ανασχεδιασμό του δικτύου ή απλά παρεμβάσεις στα προβληματικά σημεία.

Στο πλαίσιο της ανάλυσης δικτύου υπάρχουν εργαλεία, όπως το wireshark, που επιτρέπουν τη σύλληψη των πακέτων που κυκλοφορούν μέσα στο δίκτυο σε πραγματικό χρόνο σε μορφότυπο που επιτρέπει την ανάγνωση τους.

Ερωτήσεις Ανακεφαλαίωσης

1. Με ποιον τρόπο μπορούμε να δούμε το όνομα που έχει ένας υπολογιστής στο δίκτυο (hostname) σε περιβάλλον κειμένου στα Windows;
2. Με ποιον τρόπο μπορούμε να δούμε τη διεύθυνση IP του υπολογιστή σε γραφικό περιβάλλον στα Windows;
3. Πώς μπορούμε να διαπιστώσουμε αν η διεύθυνση IP είναι στατική ή γίνεται ανάκτηση μέσω διακομιστή DHCP σε περιβάλλον κειμένου στα Windows;
4. Με ποια εντολή μπορούμε να δούμε σε ποια διεύθυνση IP αντιστοιχεί το λεκτικό www.ntua.gr;

5. Με ποια εντολή μπορούμε να δούμε την πορεία που ακολουθούν τα πακέτα από τον υπολογιστή μας μέχρι το διακομιστή με διεύθυνση www.auth.gr;
6. Ποιο θα είναι το αποτέλεσμα της απόρριψης των πακέτων ICMP από το τείχος προστασίας ενός υπολογιστή;
7. Με ποια εντολή μπορούμε να δούμε τις ενεργές συνδέσεις δικτύου του υπολογιστή μας;

Άσκηση

Παράδειγμα παρακολούθησης πακέτων με χρήση της εφαρμογής wireshark.

Εκτελέστε τα ακόλουθα βήματα της άσκησης:

1. Να εκτελέσετε το wireshark.
2. Στην αρχική οθόνη της εφαρμογής, να διαλέξετε τον προσαρμογέα δικτύου για τον οποίο θέλετε να ξεκινήσει η διαδικασία καταγραφής των πακέτων.
3. Να ξεκινήσετε την καταγραφή πατώντας το αντίστοιχο κουμπί που βρίσκεται στην εργαλειοθήκη του wireshark.
4. Να σταματήσετε την καταγραφή όταν θέλετε, πατώντας το αντίστοιχο κουμπί που βρίσκεται στην εργαλειοθήκη του wireshark. Τι έχει καταγραφεί μέχρι εκείνη τη στιγμή;
5. Να εντοπίσετε ένα πακέτο για το TCP πρωτόκολλο εφαρμόζοντας φίλτρο αναζήτησης και θέτοντας σαν φίλτρο το TCP.
6. Να εντοπίσετε για αυτό το πακέτο τη διεύθυνση πηγής και τη διεύθυνση προορισμού.
7. Να εντοπίσετε ένα πακέτο για το HTTP πρωτόκολλο.
8. Για το συγκεκριμένο πακέτο να καταγράψετε την «συνομιλία» ανάμεσα στον πελάτη και στον εξυπηρετητή.
9. Να αποθηκεύσετε την καταγραφή των πακέτων που μόλις κάνατε σε αρχείο για μελλοντική επεξεργασία.

Βιβλιογραφία

Wikipedia. (2014, September 15). *ICMP.* Ανάκτηση από https://el.wikipedia.org/wiki/ICMP.

Wikipedia. (2013, November 23). Address Resolution Protocol. Ανάκτηση από https://el.wikipedia.org/wiki/Address_Resolution_Protocol

Wikipedia. (2013, March 21). nslookup. Ανάκτηση από https://el.wikipedia.org/wiki/Nslookup

Wireshark .(2015) Ανάκτηση από https://www.wireshark.org

Κεφάλαιο 6ο

Δικτυακά Μέσα Αποθήκευσης

Εισαγωγή

Η παραγόμενη ποσότητα δεδομένων αυξάνεται με εκρηκτικό ρυθμό από χρόνο σε χρόνο και προβλέπεται ότι το 2020 θα είναι πενήντα φορές μεγαλύτερη από ότι το 2011. Κάτω από αυτές τις συνθήκες, η πρόκληση είναι να μπορούμε να προτείνουμε την καλύτερη λύση για την αποθήκευση και πρόσβαση στα δεδομένα, ανάλογα με τις ανάγκες μας. Αυτό όμως προϋποθέτει την κατανόηση των διαφόρων τεχνολογιών αποθήκευσης που υπάρχουν. Σ' αυτό το κεφάλαιο θα επικεντρωθούμε στα δικτυακά μέσα αποθήκευσης, ενώ θα κάνουμε και μια μικρή αναφορά στα αποθηκευτικά μέσα με απ' ευθείας σύνδεση.

Διδακτικοί Στόχοι

Με την ολοκλήρωση του 6ου κεφαλαίου οι μαθητές θα πρέπει να είναι σε θέση να :

- Περιγράφουν τι είναι ένα Δικτυακό Μέσο Αποθήκευσης.
- Εγκαθιστούν και να ρυθμίζουν έναν Εξυπηρετητή Δικτυακού Μέσου Αποθήκευσης.
- Απαριθμούν τα πλεονεκτήματα των δικτυακών μέσων αποθήκευσης.
- Προτείνουν λύσεις για τον τύπο του συστήματος αρχείων που πρέπει να χρησιμοποιηθεί στο Δικτυακό Μέσο Αποθήκευσης, ανάλογα με τη χρήση του.
- Εγκαθιστούν και να χρησιμοποιούν έναν προσωπικό αποθηκευτικό χώρο σε εφαρμογή Σύννεφου (Cloud).

Διδακτικές Ενότητες

6.1 Τρόπος σύνδεσης αποθηκευτικών μέσων.
6.2 Πλεονεκτήματα – Μειονεκτήματα.
6.3 Εγκατάσταση και ρύθμιση Δικτυακού Μέσου Αποθήκευσης.

6.1 Τρόπος σύνδεσης αποθηκευτικών μέσων

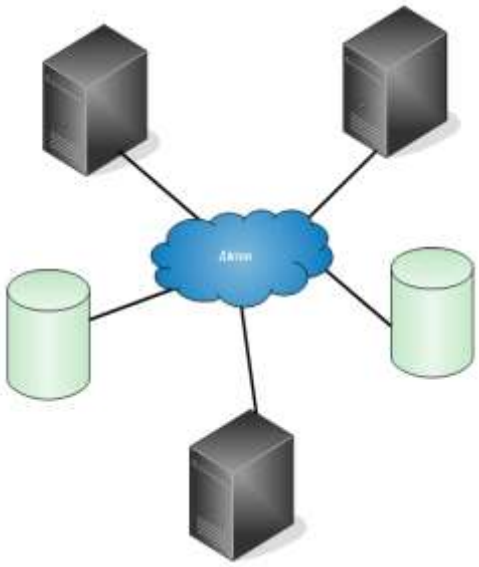
Ο απλούστερος τρόπος σύνδεσης ενός αποθηκευτικού μέσου με ένα υπολογιστικό σύστημα είναι η απ' ευθείας ή άμεση σύνδεση (DAS – Direct Attached Storage). Σ' αυτήν την περίπτωση το αποθηκευτικό μέσο (σκληρός δίσκος, συστοιχία δίσκων, USB Flash κλπ) συνδέεται στο υπολογιστικό σύστημα μέσω ενός καλωδίου.

Μερικά από τα πρωτόκολλα επικοινωνίας που χρησιμοποιούνται στην απ' ευθείας σύνδεση είναι τα SCSI, SAS, SATA, PATA.

Εικόνα 6.1: Απ' ευθείας σύνδεση

Όταν θέλουμε να διαμοιράσουμε τα δεδομένα ενός αποθηκευτικού μέσου σε ένα δίκτυο υπολογιστών χρησιμοποιούμε τη σύνδεση μέσω δικτύου. Ένα δικτυακό μέσο αποθήκευσης (Network Attached Storage, NAS) συνήθως είναι ένα αυτόνομο υπολογιστικό σύστημα που αφιερώνεται στην αποθήκευση και ανάκτηση των δεδομένων των υπολογιστών του δικτύου στο οποίο είναι συνδεδεμένο. Επειδή προορίζεται να αποθηκεύσει δεδομένα πολλών υπολογιστών, εφοδιάζεται με ικανό αριθμό σκληρών δίσκων οι οποίοι ανάλογα με τις ανάγκες μας μπορεί να διαμορφωθούν σε κάποια διάταξη RAID.

Μερικά από τα πρωτόκολλα επικοινωνίας που χρησιμοποιούνται είναι το NFS (Network File System) και το CIFS (Common Internet File System), τα οποία μας δίνουν τη δυνατότητα πρόσβασης και διαμοιρασμού αρχείων και εκτυπωτών σε ένα δίκτυο.



Εικόνα 6.2: Σύνδεση μέσω δικτύου

6.2 Πλεονεκτήματα – Μειονεκτήματα

Τα αποθηκευτικά μέσα με απ' ευθείας πρόσβαση αποτελούν μια σχετικά φθηνή λύση αποθήκευσης με ταυτόχρονα μεγάλη ταχύτητα μετάδοσης δεδομένων. Η εγκατάσταση και ρύθμισή τους είναι μια απλή υπόθεση. Από την άλλη ο διαμοιρασμός των δεδομένων σ' αυτήν την περίπτωση είναι περιορισμένος λόγω της φύσης της σύνδεσης. Τέλος, η αύξηση της χωρητικότητάς τους δεν είναι μια εύκολη υπόθεση.

Τα δικτυακά μέσα αποθήκευσης προσφέρουν έναν σχετικά εύκολο τρόπο να διαμοιράσουμε δεδομένα, με τα κατάλληλα δικαιώματα, σε ένα δίκτυο πολλών υπολογιστών και χρηστών. Έχουν τη δυνατότητα εύκολης διαμόρφωσης συστοιχιών δίσκων ανάλογα με τις ανάγκες μας (RAID-0, RAID-1, RAID-10 κλπ) και αύξησης της διαθέσιμης χωρητικότητας με την προσθήκη επιπλέον δίσκων με εύκολο τρόπο. Επίσης έχουν σχετικά καλή ταχύτητα μετάδοσης δεδομένων, η οποία όμως επηρεάζεται από τις συνθήκες και τον τύπο του δικτύου που χρησιμοποιείται. Για παράδειγμα, η χρήση δικτύου που να υποστηρίζει ταχύτητες μεγαλύτερες ή ίσες από 1 Gbps είναι απαραίτητη.

6.3 Εγκατάσταση και ρύθμιση Δικτυακού Μέσου Αποθήκευσης

Το OpenMediaVault είναι μια διανομή Linux που βασίζεται στο Debian και μας επιτρέπει με εύκολο τρόπο να δημιουργήσουμε ένα NAS που προορίζεται για οικιακή χρήση ή για χρήση σε μια μικρή εταιρεία. Το μεγάλο του πλεονέκτημα είναι η ύπαρξη πολλών πρόσθετων

(plugins) μέσω των οποίων αποκτά επιπλέον λειτουργίες εκτός από τη βασική που είναι φυσικά δικτυακή αποθήκευση δεδομένων.

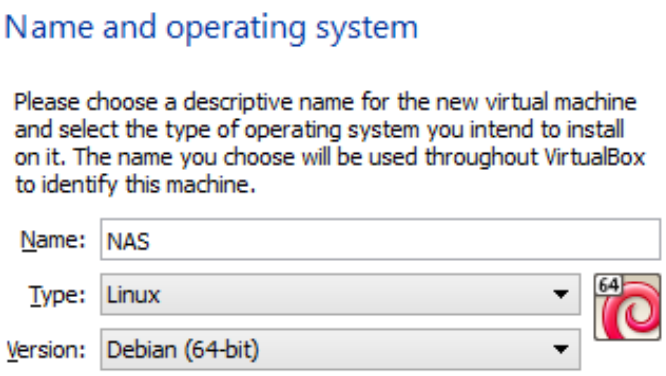
Η εγκατάσταση θα πραγματοποιηθεί σε εικονική μηχανή για λόγους ευκολίας, ακολουθώντας τα παρακάτω βήματα:

Κατεβάζουμε από τον επίσημο δικτυακό τόπο του OpenMediaVault την τελευταία εικόνα του CD εγκατάστασης. Οι ελάχιστες απαιτήσεις υλικού του NAS που προορίζεται για μια μικρή εταιρεία είναι:

Επεξεργαστής	>= Pentium 4 2.6GHz
Μνήμη	>= 1 GBytes
Μέγεθος δίσκου εγκατάστασης	>= 2 GBytes
Μέγεθος δίσκων δεδομένων	Ανάλογα με τον όγκο δεδομένων

Ανοίγουμε το Oracle VirtualBox και δημιουργούμε μια εικονική μηχανή, εισάγοντας τις παρακάτω τιμές στα βήματα του οδηγού:

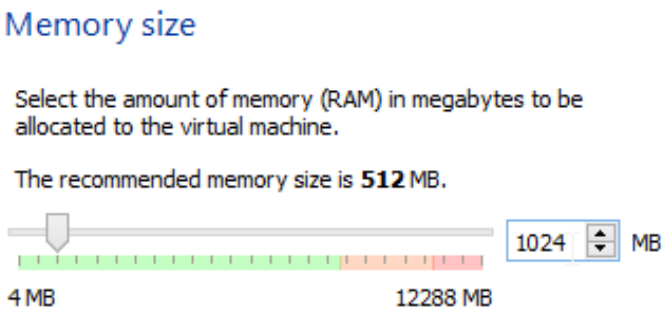
Name: NAS, **Type:** Linux, **Version:** Debian (64-bit)



Εικόνα 6.3: Επιλογή ονόματος και αρχιτεκτονικής εικονικής μηχανής

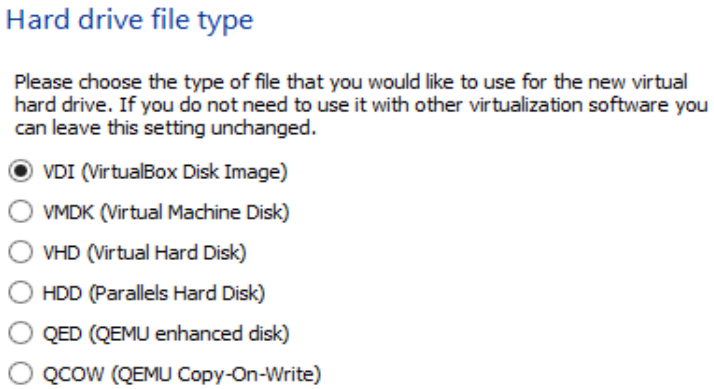
Αν η εγκατάσταση γίνει σε φυσικό υπολογιστικό σύστημα και η αρχιτεκτονική του επεξεργαστή που έχουμε στη διάθεσή μας δεν είναι amd64 τότε στο πεδίο **Version** επιλέγουμε **Debian**.

Memory Size: 1024 MB

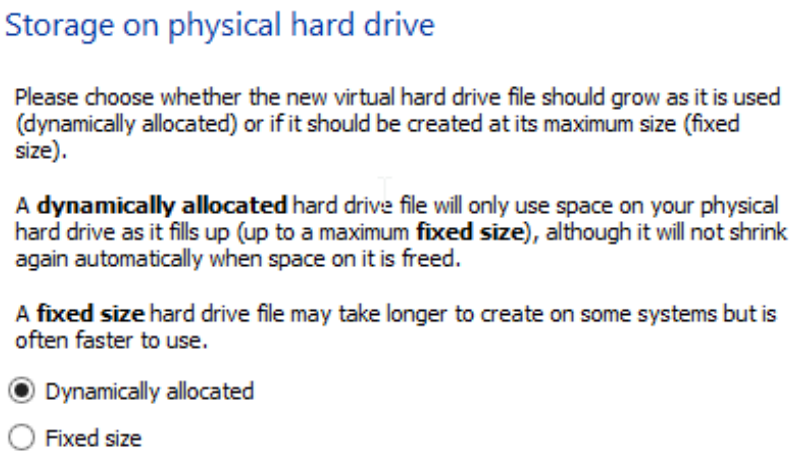


Εικόνα 6.4: Ορισμός μεγέθους μνήμης

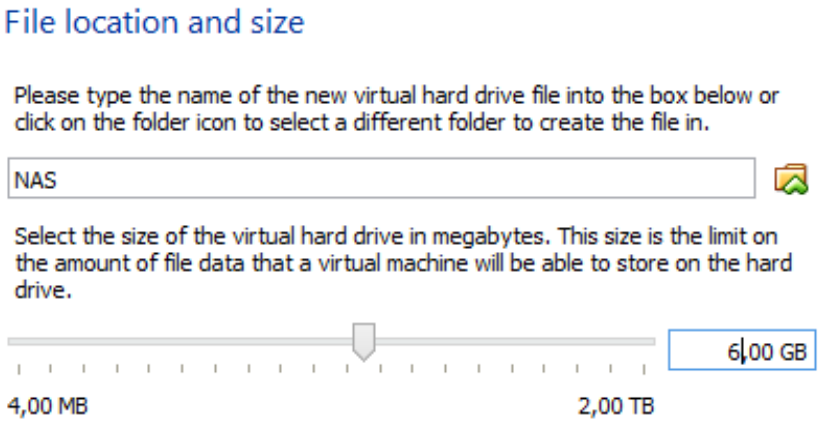
Hard drive: 6GB - Σ' αυτόν το δίσκο θα γίνει μόνο η εγκατάσταση του λειτουργικού συστήματος.



Εικόνα 6.5: Ορισμός τύπου εικονικού δίσκου



Εικόνα 6.6: Επιλογή της μεθόδου αποθήκευσης του εικονικού δίσκου



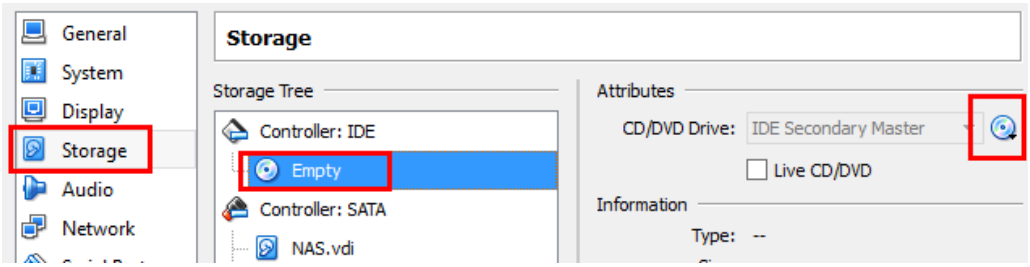
Εικόνα 6.7: Ορισμός ονόματος ε και μεγέθους του εικονικού δίσκου

Πατώντας το κουμπί **Create** θα δημιουργηθεί η εικονική μηχανή.

Πριν προχωρήσουμε στην εγκατάσταση πρέπει να κάνουμε μερικές επιπλέον ρυθμίσεις στην εικονική μηχανή. Για αυτό το λόγο θα πατήσουμε το γρανάζι (**Settings**) που βρίσκεται στη γραμμή εργαλείων, έχοντας επιλέξει πρώτα την εικονική μηχανή που δημιουργήσαμε.

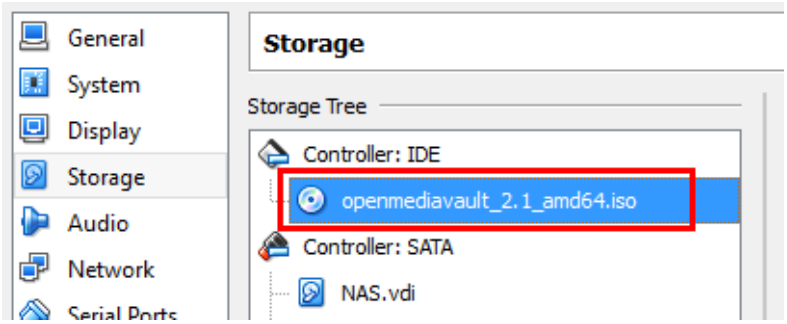
Εικόνα 6.8: Ρυθμίσεις εικονικής μηχανής

Στην ενότητα **Storage** πατάμε στο εικονίδιο του CD που γράφει **Empty** και στη συνέχεια πατάμε το εικονίδιο του CD στο δεξιό τμήμα του παραθύρου. Από το μενού που θα ανοίξει επιλέγουμε **Choose a virtual CD/DVD disk file…**



Εικόνα 6.9: Εισαγωγή εικόνας CD/DVD στην εικονική μηχανή

Επιλέγουμε το αρχείο με την εικόνα εγκατάστασης του OpenMediaVault.

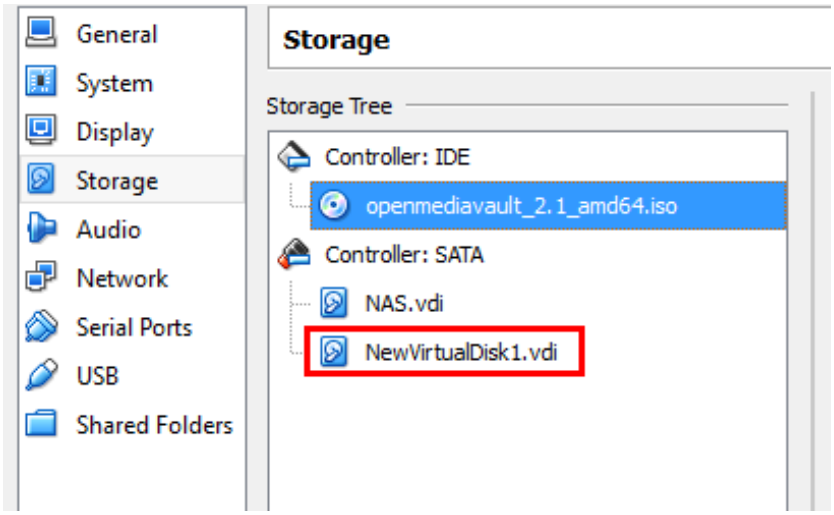


Εικόνα 6.10: Επιλογή του δίσκου εγκατάστασης

Συνεχίζοντας, πατάμε πάνω στο **Controller: SATA** και στη συνέχεια πατάμε το δεύτερο εικονίδιο, από αυτά που θα εμφανιστούν, για να προσθέσουμε ακόμα έναν δίσκο στην εικονική μας μηχανή. Αυτός ο δίσκος θα χρησιμοποιηθεί για την αποθήκευση δεδομένων.

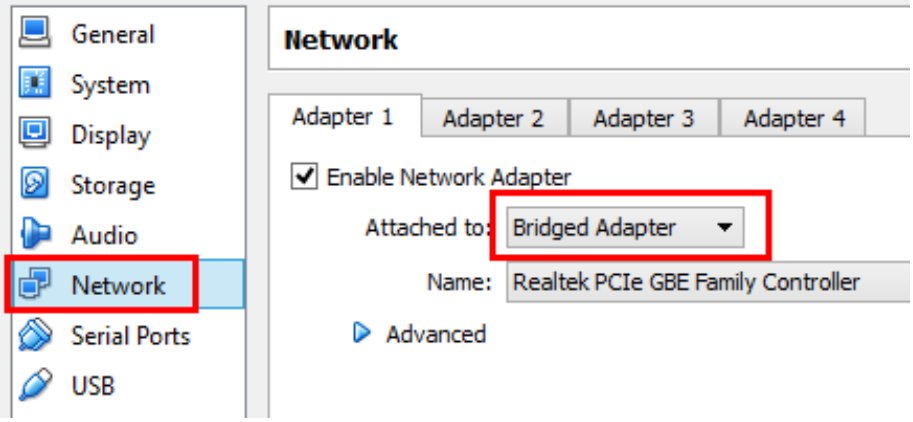
Εικόνα 6.11: Δημιουργία δεύτερου εικονικού δίσκου

Στο παράθυρο που θα εμφανιστεί πατάμε το κουμπί **Create new disk.** Στη συνέχεια επιλέγουμε το μέγεθος του δίσκου εισάγοντας **20GB**.



Εικόνα 6.12: Η εικονική μηχανή με δύο εικονικούς δίσκους

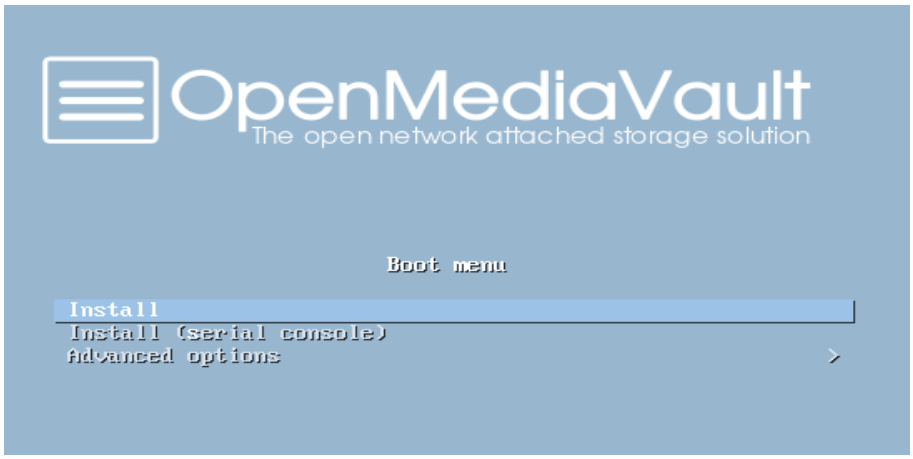
Στην ενότητα ***Network*** αλλάζουμε τη ρύθμιση ***Attached to*** σε ***Bridged Adapter***.



Εικόνα 6.13: Αλλαγή του τρόπου λειτουργίας της εικονικής κάρτας δικτύου

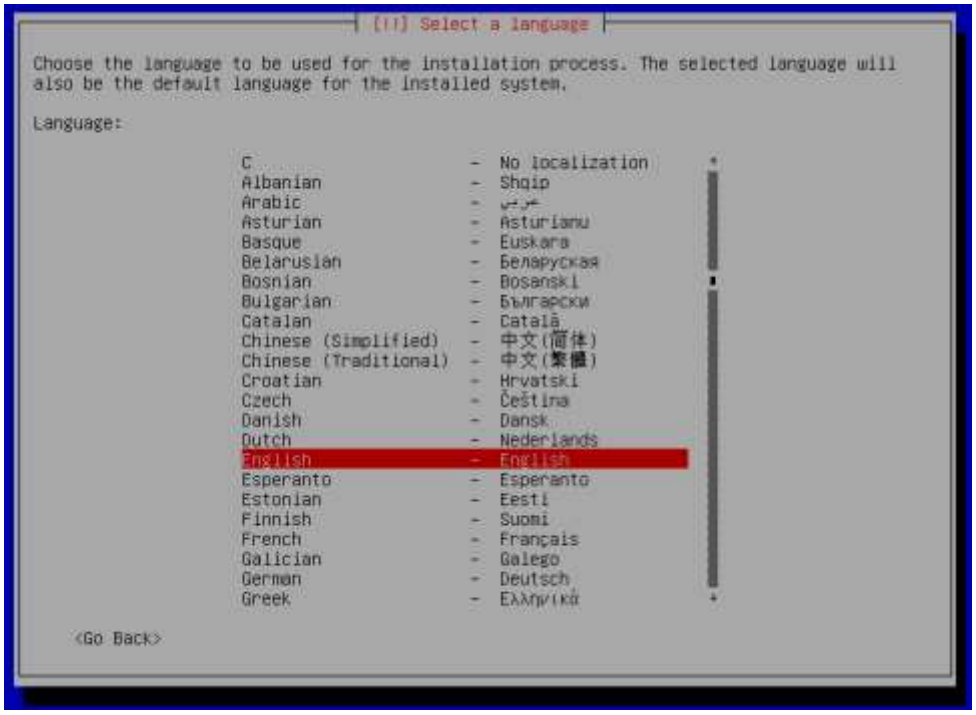
Τέλος, πατάμε **OK** και είμαστε έτοιμοι να ξεκινήσουμε την εικονική μηχανή πατώντας το εικονίδιο **Start**.

Μετά την αρχική εκκίνηση της εικονικής μηχανής, βλέπουμε την παρακάτω εικόνα. Για να αρχίσει η εγκατάσταση του OpenMediaVault πατάμε **Enter** στην επιλογή **Install**.



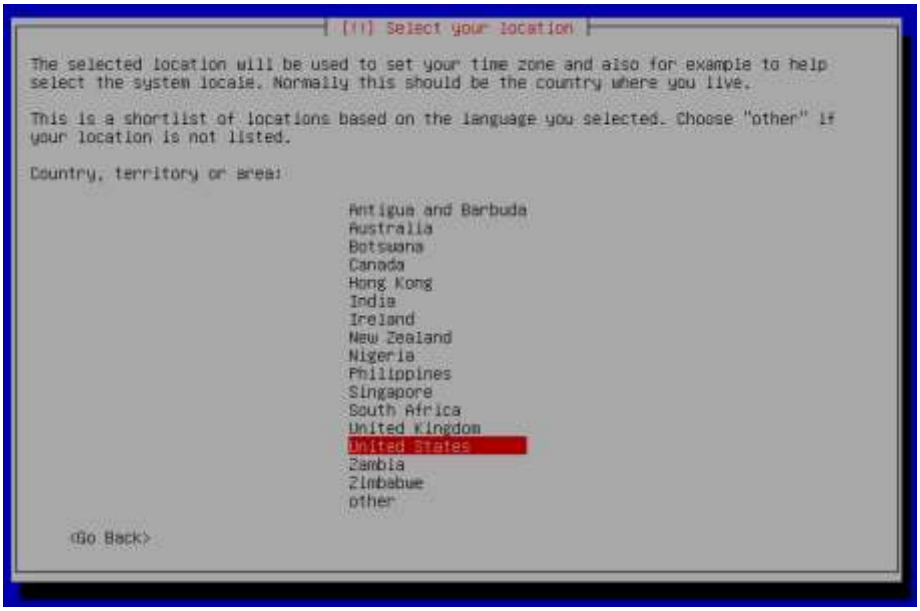
Εικόνα 6.14: Αρχική οθόνη εγκατάστασης του Openmediavault

Επιλέγουμε την γλώσσα που θα χρησιμοποιήσουμε κατά τη διάρκεια της εγκατάστασης **English**.



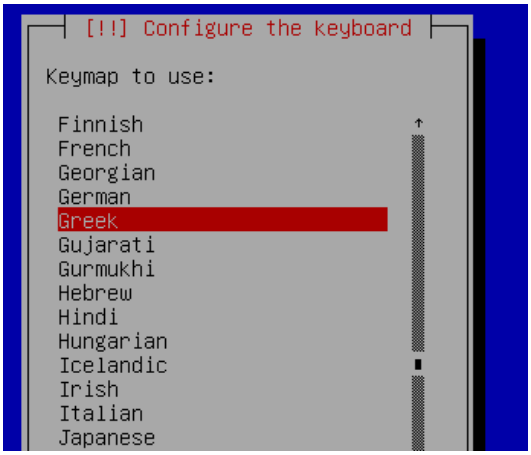
Εικόνα 6.15: Επιλογή γλώσσας εγκατάστασης

Επιλέγουμε τη ζώνη ώρας μέσω της οποίας θα ρυθμιστεί η ώρα του NAS. Επιλέγουμε με τη σειρά **Other - Europe - Greece - United States,** πατώντας ενδιάμεσα **Enter**.



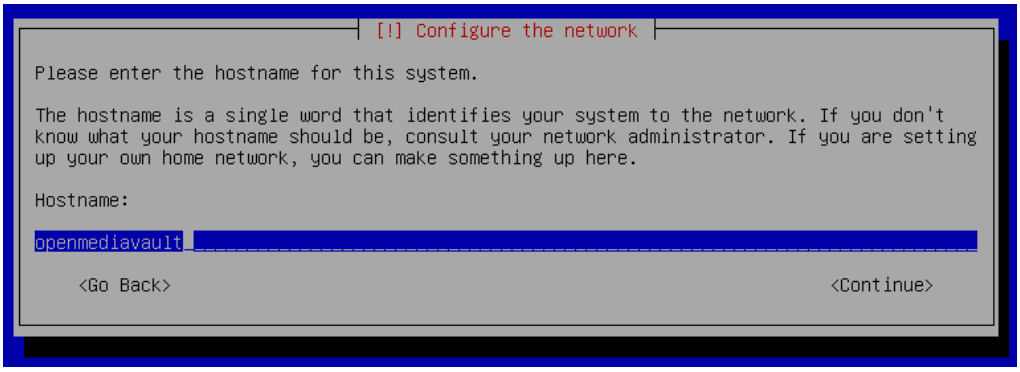
Εικόνα 6.16: Επιλογή τοποθεσίας

Επιλέγουμε **Greek** στη ρύθμιση για το πληκτρολόγιο και **Alt+Shift** για εναλλαγή μεταξύ των γλωσσών



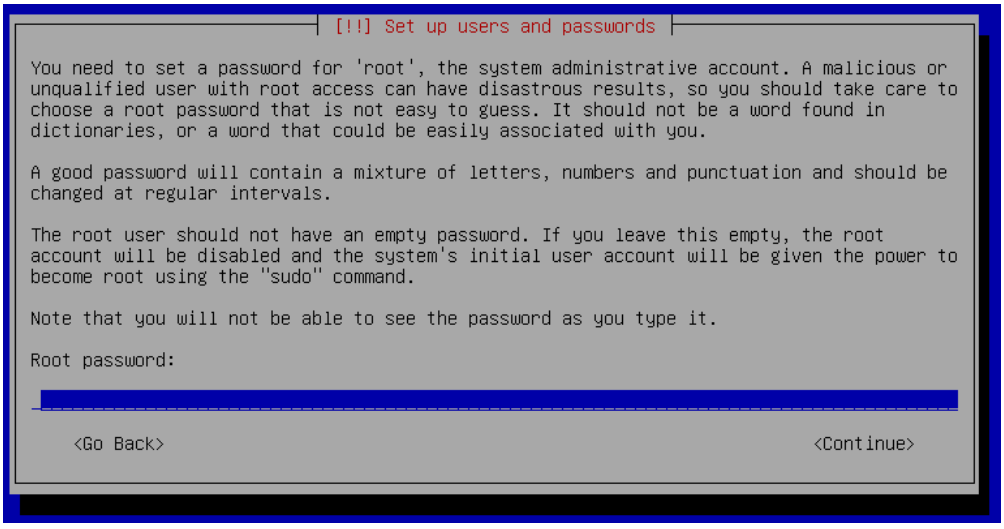
Εικόνα 6.17: Επιλογή υποστήριξης δεύτερης γλώσσας

Αφήνουμε ως έχει το όνομα του υπολογιστή/δέκτη (host name) και το όνομα τομέα (domain name).



Εικόνα 6.18: Ορισμός ονόματος υπολογιστή (hostname)

Εισάγουμε σαν κωδικό πρόσβασης για το διαχειριστή συστήματος (root) το 1234. Προφανώς εισάγουμε έναν τόσο εύκολο κωδικό για λόγους ευκολίας. Σε πραγματικές συνθήκες θα πρέπει να εισάγουμε έναν πολύπλοκο.

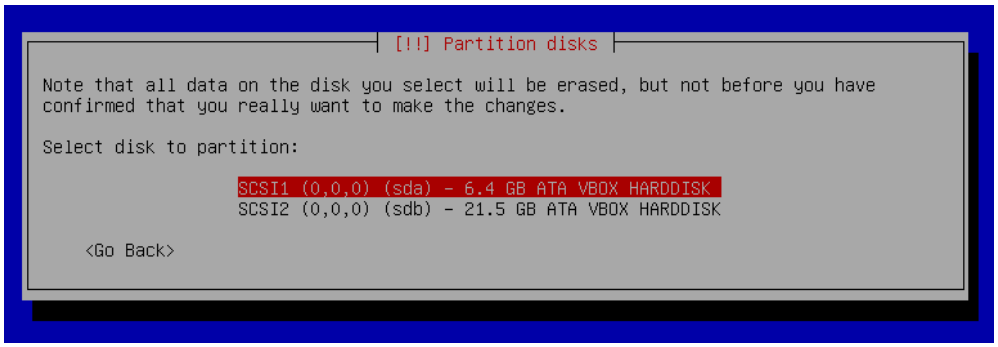


Εικόνα 6.19: Ορισμός κωδικού πρόσβασης διαχειριστή συστήματος

Επειδή υπάρχουν δύο δίσκοι στην εικονική μηχανή θα εμφανιστεί το παρακάτω παράθυρο, στο οποίο πατάμε **Continue**.

Εικόνα 6.20: Προειδοποιητικό ύπαρξης δύο δίσκων

Επιλέγουμε τον πρώτο δίσκο **(sda - 6.4GB)** για την εγκατάσταση του λειτουργικού συστήματος του NAS.

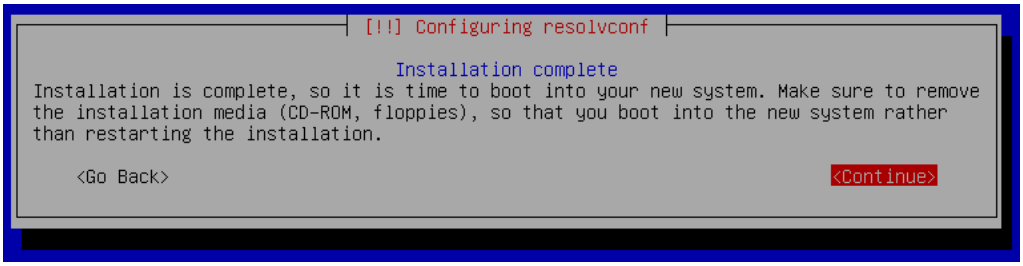


Εικόνα 6.21: Επιλογή του δίσκου εγκατάστασης

Σ' αυτό το βήμα επιλέγουμε την τοποθεσία που βρισκόμαστε με σκοπό να επιλεγεί η κοντινότερη που υπάρχουν τα αρχεία που πρέπει να κατεβάσει το πρόγραμμα εγκατάστασης του OpenMediaVault (OMV). Έτσι επιλέγουμε **Greece** και στη συνέχεια **ftp.gr.debian.or**

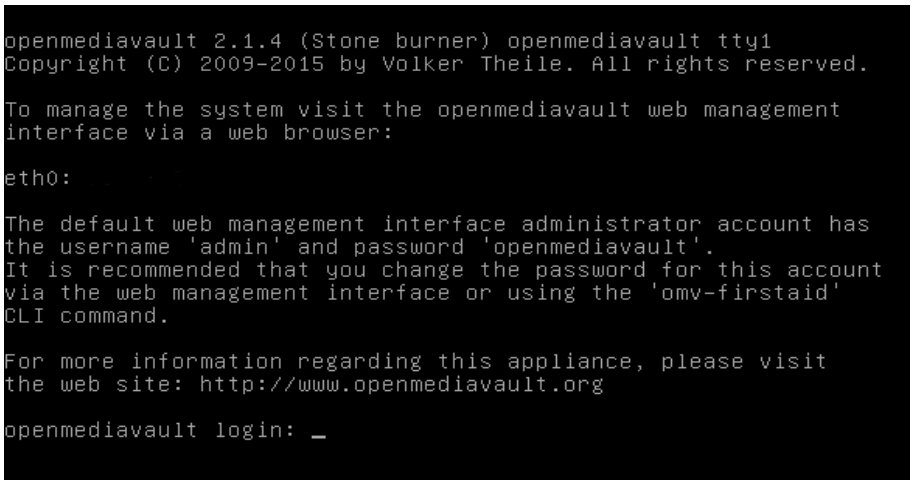
Εικόνα 6.22: Επιλογή του κοντινότερου διακομιστή αρχείων εγκατάστασης

Η εγκατάσταση έφτασε στο τέλος της. Δεν έχουμε να κάνουμε τίποτα άλλο από το να πατήσουμε **Continue.** Η εικονική μηχανή θα κάνει επανεκκίνηση.



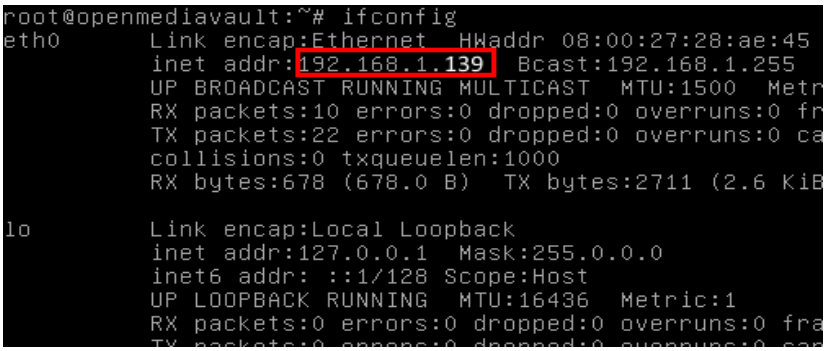
Εικόνα 6.23: Τέλος εγκατάστασης

Μετά την εκκίνηση της εικονικής μηχανής θα δούμε την παρακάτω εικόνα.



Εικόνα 6.24: Οθόνη μετά την πρώτη εκκίνηση

Η διαχείριση του NAS πραγματοποιείται μέσω γραφικού περιβάλλοντος στο οποίο έχουμε πρόσβαση μέσω ενός φυλλομετρητή. Έτσι, για τη διαχείριση του NAS θα πρέπει να γνωρίζουμε τη διεύθυνση IP που έχει. Αυτήν τη στιγμή όμως δεν γνωρίζουμε τη διεύθυνση που έχει δώσει αυτόματα ο δρομολογητής μας στο NAS. Για αυτό το λόγο θα συνδεθούμε σαν διαχειριστές του συστήματος στο περιβάλλον κειμένου. Πληκτρολογούμε **root** στο login και αφού πατήσουμε **Enter** εισάγουμε τον κωδικό πρόσβασης **1234**. Στη συνέχεια, για να δούμε τη διεύθυνση IP πληκτρολογούμε την εντολή **ifconfig** και πατάμε **Enter.**



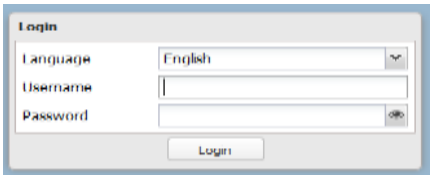
Εικόνα 6.25: Προσωρινή διεύθυνση IP του NAS

Στο κόκκινο πλαίσιο είναι η διεύθυνση IP του NAS. Τώρα είμαστε έτοιμοι να ρυθμίσουμε το NAS μέσω του γραφικού περιβάλλοντος.

6.3.1 Βασικές ρυθμίσεις

Μετά την εγκατάσταση, θα πραγματοποιήσουμε μερικές βασικές ρυθμίσεις και θα δούμε τον τρόπο με τον οποίο τερματίζουμε τη λειτουργία ή κάνουμε επανεκκίνηση το NAS.

Ανοίγουμε έναν φυλλομετρητή και εισάγουμε στη γραμμή διευθύνσεων τη διεύθυνση του NAS που βρήκαμε προηγουμένως. Θα δούμε την παρακάτω οθόνη, μέσω της οποίας θα έχουμε πρόσβαση στο διαχειριστικό περιβάλλον του NAS.



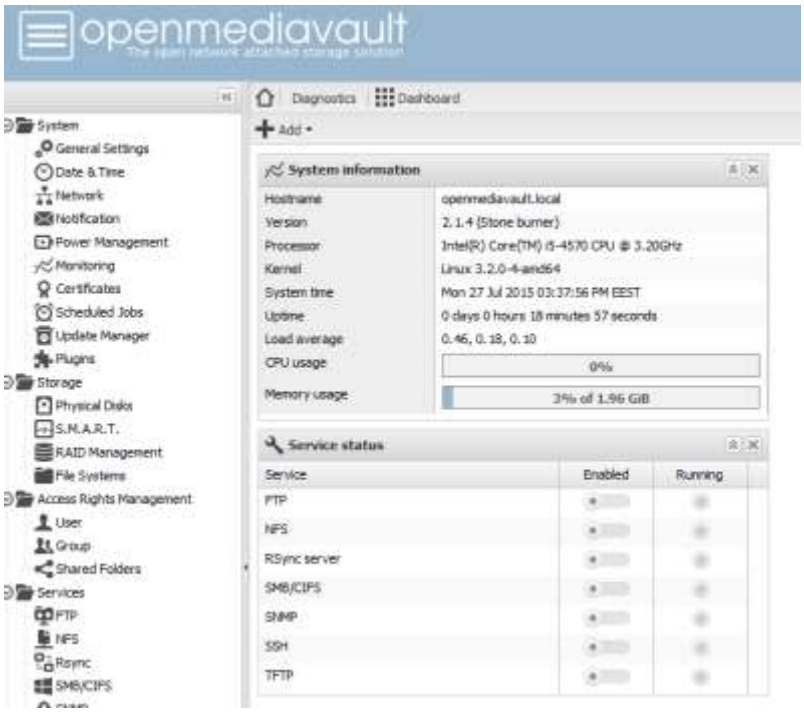
Εικόνα 6.26: Είσοδος στο γραφικό περιβάλλον διαχείρισης

Παρατηρούμε ότι έχουμε τη δυνατότητα να αλλάξουμε τη γλώσσα του περιβάλλοντος διαχείρισης από την επιλογή **Language.** Καλό θα ήταν όμως να κρατήσουμε τα Αγγλικά, γιατί αρκετές επιλογές είτε δεν έχουν ελληνική μετάφραση είτε δεν έχουν μεταφραστεί σωστά.

Για να διαχειριστούμε το NAS θα πρέπει να πληκτρολογήσουμε το όνομα χρήστη και τον κωδικό πρόσβασης του διαχειριστή. Αυτός ο λογαριασμός διαχειριστή δεν είναι ο ίδιος με αυτόν που χρησιμοποιήσαμε για να συνδεθούμε στο περιβάλλον κειμένου του NAS. Έτσι, για τη σύνδεση μας στο γραφικό περιβάλλον διαχείρισης εισάγουμε τα παρακάτω:

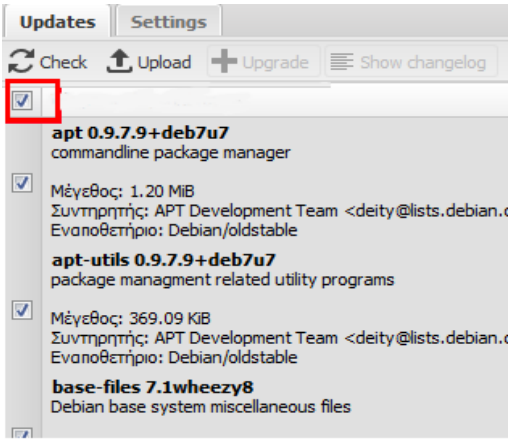
Username	admin
Password	openmediavault

Μετά την επιτυχή εισαγωγή των στοιχείων σύνδεσης θα βρεθούμε στην παρακάτω εικόνα 6.27, η οποία είναι χωρισμένη σε δύο τμήματα. Την αριστερή στήλη στην οποία βρίσκονται οι κατηγορίες των ρυθμίσεων και στην κεντρική περιοχή στην οποία προβάλλονται οι λεπτομέρειες της επιλεγμένης ρύθμισης.



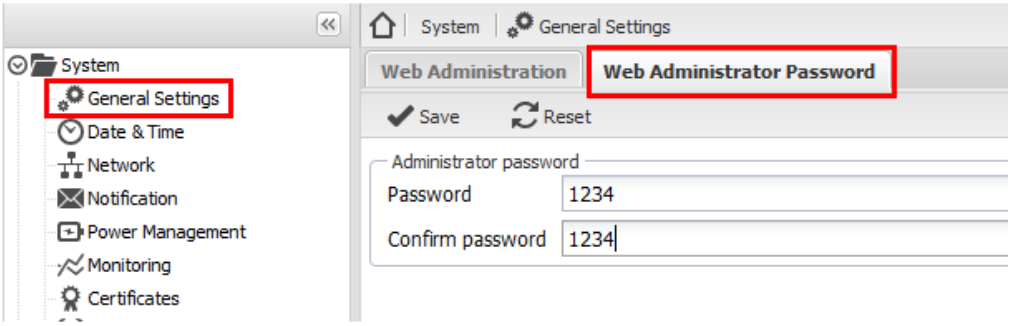
Εικόνα 6.27: Οθόνη διαχείρισης του NAS

Η πρώτη μας ενέργεια είναι να κάνουμε ενημέρωση του λογισμικού. Έτσι, από την πλευρική στήλη αριστερά επιλέγουμε **Update Manager** και στη συνέχεια από την κεντρική περιοχή στην κορυφή **Check**. Για να γίνει εγκατάσταση όλων των ενημερώσεων, αν υπάρχουν, επιλέγουμε το κουτάκι που βρίσκεται στην κορυφή της λίστας και στη συνέχεια πατάμε το κουμπί **Upgrade**.



Εικόνα 6.28: Ενημέρωση του λογισμικού

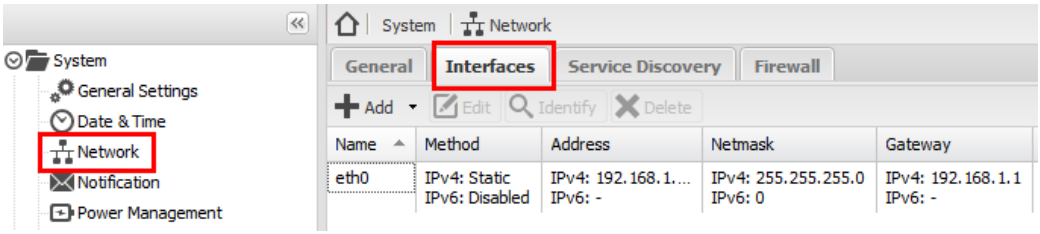
Στη συνέχεια, θα αλλάξουμε τον κωδικό πρόσβασης του διαχειριστή του γραφικού περιβάλλοντος. Από την πλευρική στήλη αριστερά επιλέγουμε **General Settings** και στη συνέχεια από την κεντρική περιοχή στην κορυφή **Web Administrator Password**.



Εικόνα 6.29: Αλλαγή κωδικού πρόσβασης διαχειριστή

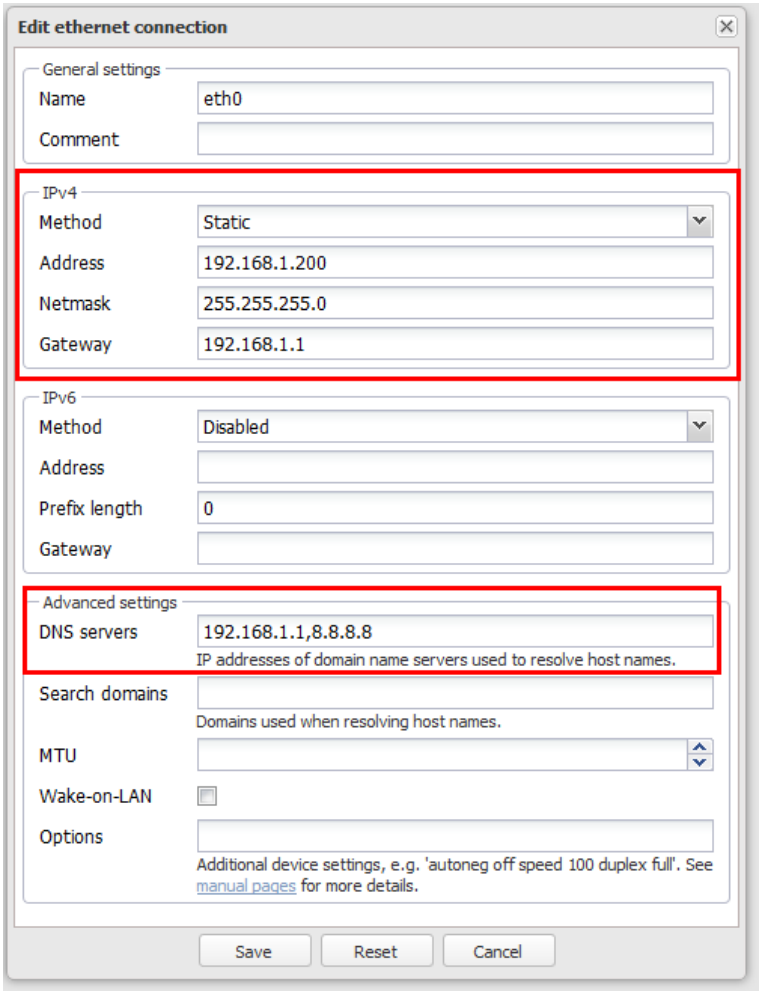
Εισάγουμε τον κωδικό 1234 στα πεδία Password και Confirm Password και στη συνέχεια πατάμε το κουμπί Save.

Η δεύτερη ρύθμιση που θα κάνουμε είναι η εισαγωγή μιας στατικής διεύθυνσης IP, έτσι ώστε το NAS να έχει πάντα την ίδια διεύθυνση μέσα στο δίκτυό μας. Από την πλευρική στήλη αριστερά επιλέγουμε **Network** και στη συνέχεια από την κεντρική περιοχή στην κορυφή **Interfaces**.



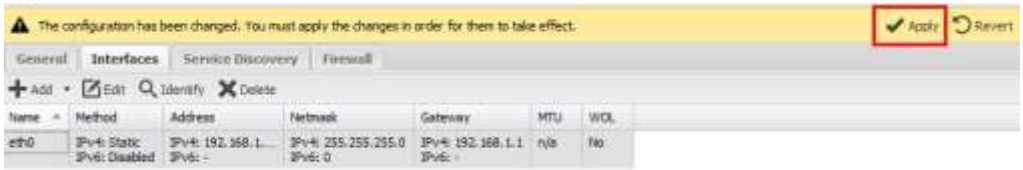
Εικόνα 6.30: Αλλαγή διεύθυνσης IP του NAS

Επιλέγουμε τη διεπαφή και στη συνέχεια πατάμε το κουμπί **Edit**. Θα ανοίξει ένα παράθυρο όπως το παρακάτω. Στην περιοχή IPv4 στο πεδίο Method επιλέγουμε **Static** και στη συνέχεια εισάγουμε μια διεύθυνση από το εσωτερικό δίκτυο που επιθυμούμε να έχει το NAS, τη μάσκα δικτύου και την πύλη πρόσβασης. Επίσης, θα πρέπει να εισαγάγουμε τουλάχιστον έναν DNS server έτσι ώστε το NAS να έχει τη δυνατότητα να κάνει επίλυση διευθύνσεων. Έτσι στο πεδίο **DNS servers** εισάγουμε τουλάχιστον τη διεύθυνση του δρομολογητή (για ταχύτερη επίλυση ονομάτων που έχει στη μνήμη του) και όσες ακόμα διευθύνσεις διακομιστών DNS θέλουμε, χωρισμένες με κόμμα.



Εικόνα 6.31: Εισαγωγή στατικής διεύθυνσης IP και διεύθυνση DNS

Αφού πατήσουμε **Save** θα μας ζητηθεί να επιβεβαιώσουμε την εφαρμογή των καινούριων ρυθμίσεων.

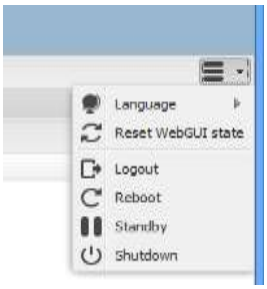


Εικόνα 6.32: Εφαρμογή των ρυθμίσεων

Πατάμε το κουμπί **Apply** και έτσι ολοκληρώνουμε την αλλαγή της διεύθυνσης IP του NAS. Από εδώ και πέρα, για να έχουμε πρόσβαση στο διαχειριστικό του περιβάλλον θα πρέπει να

εισάγουμε στη γραμμή διευθύνσεων του φυλλομετρητή την καινούρια διεύθυνση (στην περίπτωσή μας 192.168.1.200).

Τέλος, θα δούμε τον τρόπο με τον οποίο μπορούμε να κάνουμε επανεκκίνηση όπως επίσης και τερματισμό του NAS. Στο πάνω δεξί τμήμα της οθόνης βρίσκεται ένα κουμπί, που αν το πατήσουμε θα εμφανιστεί το παρακάτω παράθυρο. Ανάλογα με την ενέργεια που θέλουμε να πραγματοποιήσουμε επιλέγουμε την αντίστοιχη επιλογή.



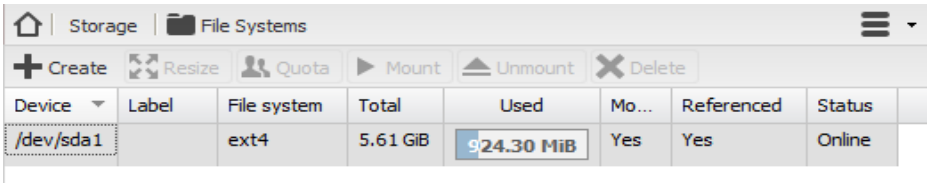
Εικόνα 6.33: Επανεκκίνηση – τερματισμός NAS

Language	Αλλαγή της γλώσσας του γραφικού περιβάλλοντος
Reset WebGUI state	Επαναφορά στις αρχικές ρυθμίσεις
Logout	Έξοδος από το γραφικό περιβάλλον
Reboot	Επανεκκίνηση του NAS
Standby	Το NAS σε κατάσταση αναμονής
Shutdown	Τερματισμός της λειτουργίας του NAS

6.3.2 Μορφοποίηση δίσκου

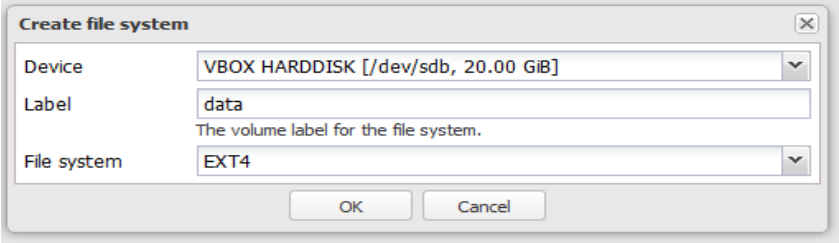
Αυτήν τη στιγμή το NAS μας δεν έχει κάποιον δίσκο στον οποίο έχουμε τη δυνατότητα αποθήκευσης δεδομένων. Για αυτό το λόγο, στο δεύτερο δίσκο που είχαμε δημιουργήσει κατά τη διάρκεια της εγκατάστασης, θα πρέπει να δημιουργήσουμε ένα διαμέρισμα (partition) και να το μορφοποιήσουμε (format).

Αφού έχουμε συνδεθεί στο διαχειριστικό περιβάλλον του NAS, επιλέγουμε από την αριστερή στήλη **File Systems**. Στην κεντρική περιοχή προβάλλονται τα διαθέσιμα διαμερίσματα. Αυτή τη στιγμή υπάρχει μόνο ένα, το οποίο βρίσκεται στο σκληρό δίσκο που έχουμε κάνει την εγκατάσταση. Αν πατήσουμε πάνω του, παρατηρούμε ότι δεν έχουμε τη δυνατότητα να κάνουμε καμία αλλαγή.



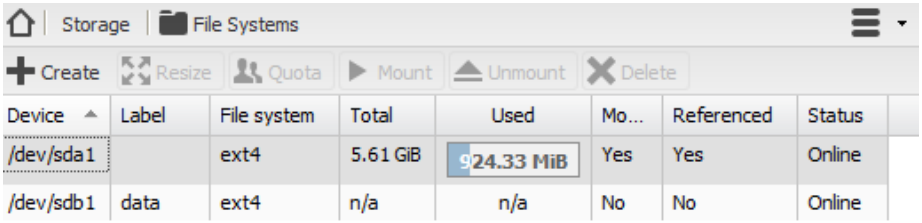
Εικόνα 6.34: Διαχείριση συστημάτων αρχείων

Για να δημιουργήσουμε ένα καινούριο διαμέρισμα θα πατήσουμε το κουμπί **Create**. Αυτό θα έχει σαν αποτέλεσμα να ανοίξει ένα παράθυρο στο οποίο θα κάνουμε τις παρακάτω επιλογές.



Εικόνα 6.35: Δημιουργία διαμερίσματος και μορφοποίησή του

Στο πεδίο **Device** επιλέγουμε το δεύτερο σκληρό δίσκο (/dev/sdb), στο **Label** εισάγουμε ένα όνομα που επιθυμούμε (για παράδειγμα **data**) και στο **File system** αφήνουμε το προεπιλεγμένο **ext4**. Πατώντας **OK** θα ανοίξει ακόμα ένα παράθυρο στο οποίο θα πρέπει να επιβεβαιώσουμε ότι θέλουμε να διαμορφώσουμε το καινούριο διαμέρισμα.



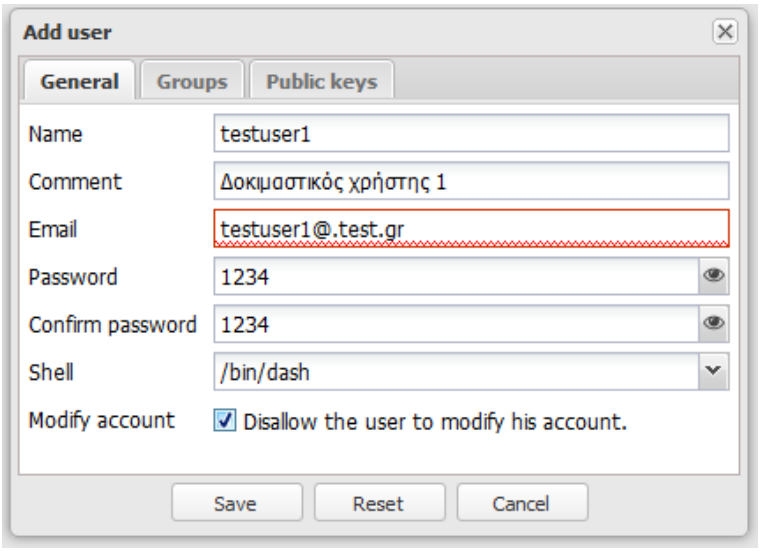
Εικόνα 6.36: Διαθέσιμα διαμερίσματα (partitions)

Για να το χρησιμοποιήσουμε θα πρέπει να το προσαρτήσουμε (mount). Έτσι, επιλέγουμε το σύστημα αρχείων που μόλις δημιουργήσαμε, πατάμε το κουμπί **Mount** και τέλος εφαρμόζουμε τις αλλαγές.

6.3.3 Δημιουργία χρηστών

Για να μπορούμε να ορίζουμε δικαιώματα χρήσης στα αρχεία και τους φακέλους που θα βρίσκονται αποθηκευμένα στο NAS, πρέπει πρώτα να δημιουργήσουμε χρήστες και ομάδες χρηστών.

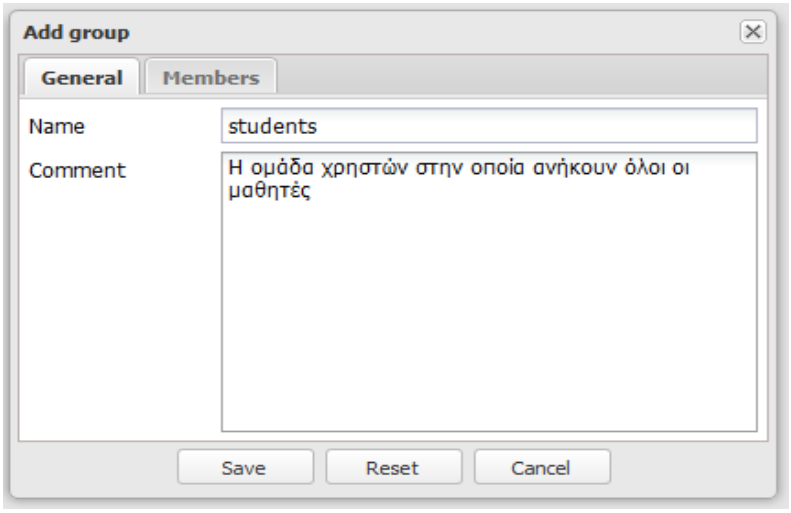
Αφού έχουμε συνδεθεί στο διαχειριστικό περιβάλλον του NAS, επιλέγουμε από την αριστερή στήλη **User** και στη συνέχεια από την κεντρική περιοχή **Add**.



Εικόνα 6.37: Δημιουργία χρήστη

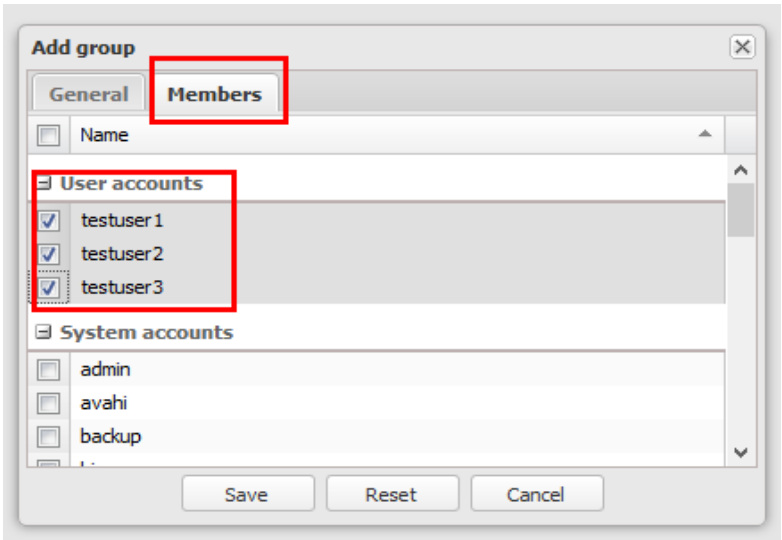
Έχοντας εισάγει τις τιμές στα αντίστοιχα πεδία του παραθύρου, πατάμε το κουμπί **Save** και εφαρμόζουμε τις αλλαγές για να δημιουργηθεί ο καινούριος χρήστης. Όλοι οι καινούριοι χρήστες τοποθετούνται στην ομάδα **Users** και αυτό δεν μπορούμε να το αλλάξουμε.

Για τη δημιουργία ομάδων χρηστών επιλέγουμε από την αριστερή στήλη **Group** και στη συνέχεια από την κεντρική περιοχή **Add**. Εισάγουμε το επιθυμητό όνομα της ομάδας στο πεδίο **Name** και προαιρετικά ένα σχόλιο στο πεδίο **Comment.**



Εικόνα 6.38: Δημιουργία ομάδας χρηστών

Τέλος, επιλέγοντας την καρτέλα **Members** έχουμε τη δυνατότητα να προσθέσουμε μέλη στην ομάδα.

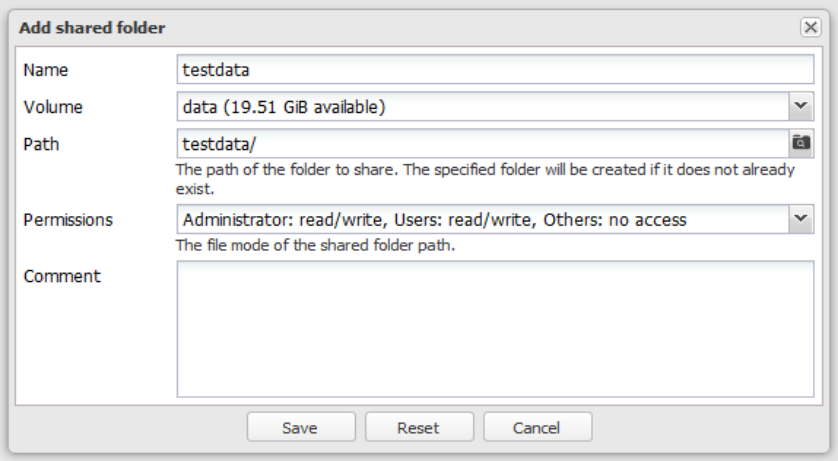


Εικόνα 6.39: Προσθήκη μελών σε ομάδα χρηστών

6.3.4 Δημιουργία φακέλων

Σ' αυτό το σημείο θα δημιουργήσουμε φακέλους στο σύστημα αρχείων και θα ορίσουμε δικαιώματα χρήσης.

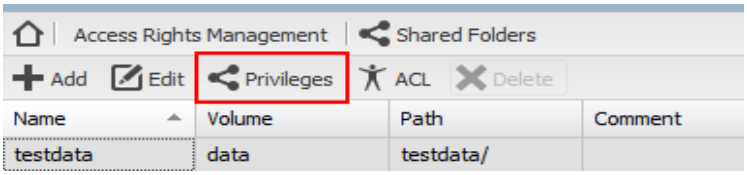
Αφού έχουμε συνδεθεί στο διαχειριστικό περιβάλλον του NAS, επιλέγουμε από την αριστερή στήλη **Shared Folders**.



Εικόνα 6.40: Δημιουργία φακέλου

Αρχικά εισάγουμε ένα όνομα φακέλου (πρέπει να αποτελείται μόνο από λατινικούς χαρακτήρες και να μην περιέχει κενά). Στη συνέχεια στο πεδίο **Volume** επιλέγουμε το διαμέρισμα στο οποίο θέλουμε να δημιουργήσουμε το φάκελο. Στο πεδίο **Permissions** επιλέγουμε ο διαχειριστής και τα μέλη της ομάδας **Users** να έχουν πλήρη πρόσβαση ενώ οι υπόλοιποι (οι χρήστες που δεν είναι μέλη της ομάδας Users) να μην έχουν κανένα δικαίωμα. Τέλος, μπορούμε να εισαγάγουμε και ένα βοηθητικό σχόλιο στο πεδίο **Comment**.

Στη συνέχεια θα ορίσουμε τα δικαιώματα χρήσης του φακέλου με την επιλογή **Privileges**.

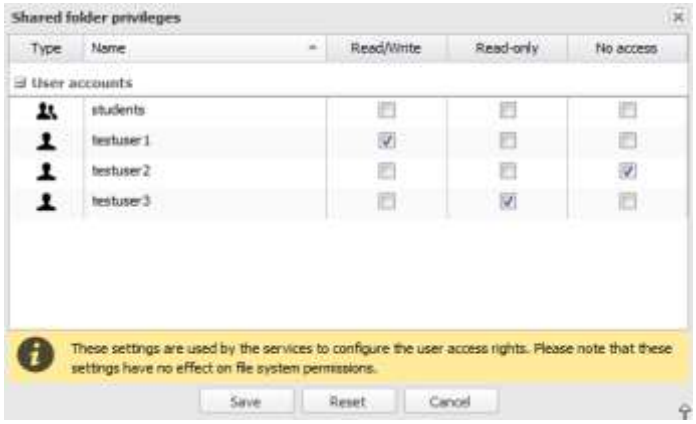


Εικόνα 6.41: Δικαιώματα χρήσης φακέλου

Αν τα δικαιώματα χρήσης του φακέλου **testdata** θέλουμε να είναι τα παρακάτω

testuser1	Εγγραφή και Ανάγνωση
testuser2	Χωρίς πρόσβαση
testuser3	Μόνο Ανάγνωση

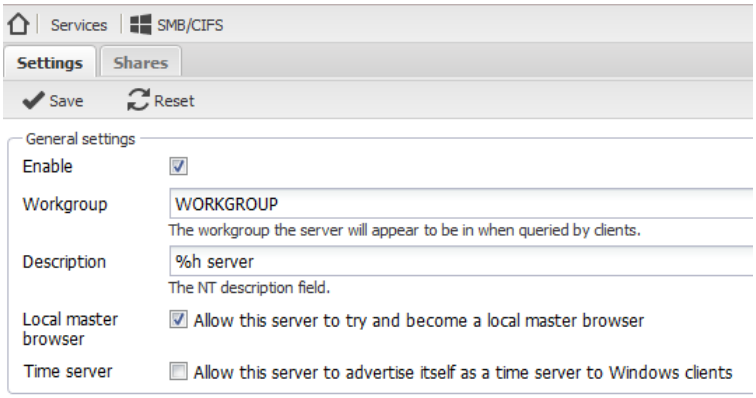
θα πρέπει να κάνουμε τις εξής επιλογές:



Εικόνα 6.42: Ορισμός δικαιωμάτων χρήσης φακέλου

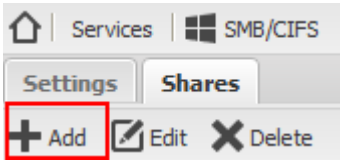
6.3.5 Διαμοιρασμός φακέλων στο δίκτυο

Για να γίνει διαθέσιμος ο φάκελος στους υπόλοιπους υπολογιστές του δικτύου (σε δίκτυο υπολογιστών με λειτουργικό σύστημα Windows ή Linux) απαιτούνται ακόμα δύο βήματα. Το πρώτο είναι να ενεργοποιήσουμε την κατάλληλη υπηρεσία, η οποία είναι η SMB/CIFS. Έτσι, επιλέγουμε από την αριστερή στήλη SMB/CIFS και εμφανίζονται στο κεντρικό τμήμα οι επιλογές της υπηρεσίας.



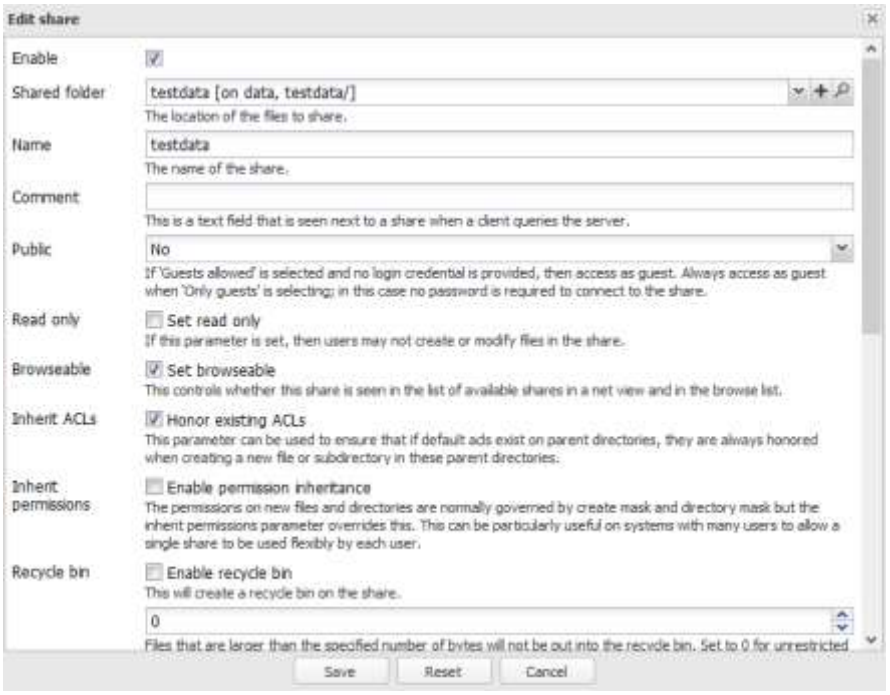
Εικόνα 6.43: Επιλογές υπηρεσίας SMB/CIFS

Ενεργοποιούμε την υπηρεσία επιλέγοντας το πεδίο **Enable** και εισάγουμε το όνομα της ομάδας εργασίας (**Workgroup**) που χρησιμοποιούμε στο δίκτυο μας. Το πιο συνηθισμένο όνομα για ομάδα εργασίας είναι το **WORKGROUP**. Αφού πατήσουμε **Save** και **Apply** θα μπορούμε να μοιράζουμε φακέλους μέσω της επιλογής **Shares**.



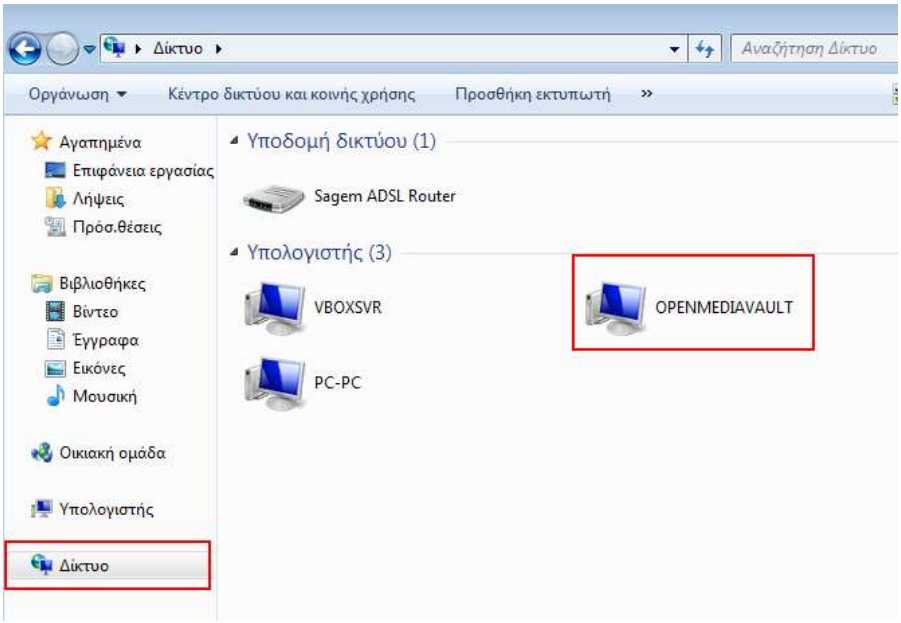
Εικόνα 6.44: Προσθήκη κοινόχρηστου φακέλου

Πατώντας **Add** προβάλλονται οι επιλογές του κοινόχρηστου φακέλου. Το πεδίο **Enable** ενεργοποιεί/ απενεργοποιεί τον κοινόχρηστο φάκελο. Από το πεδίο **Shared Folder** επιλέγουμε έναν φάκελο που έχουμε δημιουργήσει ήδη και θέλουμε να διαμοιράσουμε. Στο πεδίο **Name** εισάγουμε τον όνομα που θέλουμε να έχει ο κοινόχρηστος φάκελος μας (ποιο όνομα θα εμφανίζεται σε αυτούς που θα έχουν πρόσβαση στο NAS). Μέσω του πεδίου **Public** μπορούμε να επιλέξουμε αν ο κοινόχρηστος φάκελος θα είναι δημόσιος (ανοιχτή πρόσβαση) ή όχι. Τέλος, το πεδίο **Recycle Bin** ενεργοποιεί ή όχι τον κάδο ανακύκλωσης για το συγκεκριμένο φάκελο.



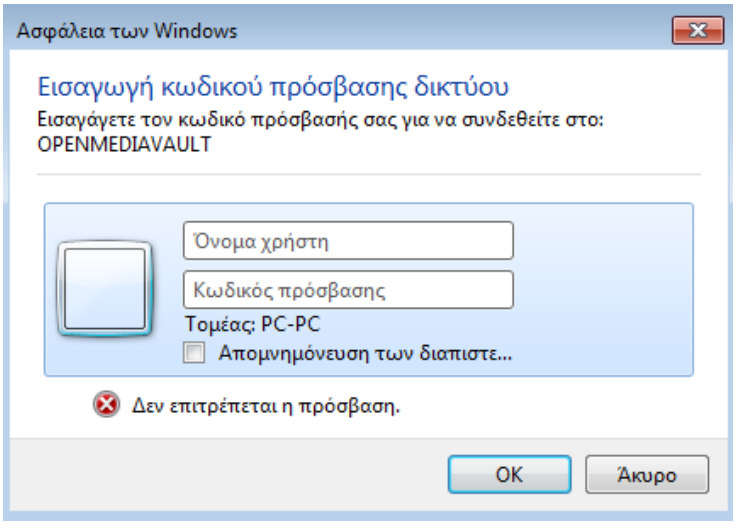
Εικόνα 6.45: Επιλογές κοινόχρηστου φακέλου

Για την πρόσβαση στον παραπάνω φάκελο από έναν υπολογιστή με λειτουργικό σύστημα Windows 7, θα πρέπει να ανοίξουμε το διαχειριστή αρχείων και να επιλέξουμε από την πλευρική στήλη **Δίκτυο**. Αφού δούμε το όνομα του **NAS (OPENMEDIAVAULT)** θα κάνουμε διπλό κλικ πάνω του για να δούμε τα περιεχόμενά του.



Εικόνα 6.46: Πρόσβαση σε κοινόχρηστο φάκελο

Αν προσπαθήσουμε να ανοίξουμε το φάκελο **testdata** θα ανοίξει ένα παράθυρο το οποίο θα ζητάει να εισάγουμε το όνομα χρήστη και τον κωδικό πρόσβασης ενός χρήστη που έχει τα κατάλληλα δικαιώματα πρόσβασης.



Εικόνα 6.47: Εισαγωγή στοιχείων χρήστη για πρόσβαση στο φάκελο

Αν εισαγάγουμε τα στοιχεία του **testuser2** δεν θα επιτραπεί η πρόσβαση. Αν δώσουμε τα στοιχεία του **testuser3** θα έχει πρόσβαση χωρίς όμως να μπορεί να κάνει τροποποιήσεις (διαγραφή αρχείων και δημιουργία νέων αρχείων). Τέλος, αν δώσουμε τα στοιχεία του **testuser1** θα έχουμε πλήρη δικαιώματα στο φάκελο.

Ερωτήσεις Ανακεφαλαίωσης

1. Ποια είναι τα πλεονεκτήματα και ποια τα μειονεκτήματα των δικτυακών μέσων αποθήκευσης;
2. Ποια είναι τα πιο γνωστά πρωτόκολλα που χρησιμοποιούνται για το διαμοιρασμό αρχείων;
3. Ποιοι παράγοντες επηρεάζουν την απόδοση ενός δικτυακού μέσου αποθήκευσης;

Ασκήσεις

Άσκηση 1η

Άσκηση στη διαμόρφωση δίσκου.

Για τη μέγιστη δυνατή ασφάλεια των δεδομένων των χρηστών, καλό θα είναι το NAS να έχει τουλάχιστον δύο δίσκους σε διάταξη εικόνας (RAID-1 mirroring). Με αυτόν τον τρόπο αν χαλάσει ένας δίσκος τα δεδομένα των χρηστών δεν θα χαθούν, αφού βρίσκονται στο δεύτερο δίσκο. Με την αντικατάσταση του χαλασμένου δίσκου και μετά από την αυτόματη διαδικασία συγχρονισμού των δίσκων η κατάσταση ομαλοποιείται πλήρως.

Να δημιουργήσετε και να διαμορφώσετε ένα διαμέρισμα το οποίο θα βρίσκεται σε δύο δίσκους με διάταξη RAID-1.

Άσκηση 2η

Άσκηση στο διαμοιρασμό φακέλων.

Να δημιουργήσετε έναν κοινόχρηστο φάκελο ο οποίος θα είναι δημόσιος. Δηλαδή, θα μπορούν όλοι οι υπολογιστές του δικτύου να έχουν πρόσβαση.

Άσκηση 3η

Άσκηση στη δημιουργία χρηστών.

1. Να δημιουργήσετε 5 χρήστες με όνομα χρήστη **user1, user2, user3, user4** και **user5**

2. Να δημιουργήσετε μια ομάδα χρηστών με όνομα **class1**
3. Να εισάγετε τους καινούριους χρήστες στην ομάδα που δημιουργήσατε στο προηγούμενο βήμα
4. Να δημιουργήσετε ένα κοινόχρηστο φάκελο με όνομα **classfolder** στον οποίο θα έχουν πλήρη δικαιώματα οι χρήστες **user1, user3** και **user5**. Ο φάκελος να δημιουργηθεί στο διαμέρισμα που βρίσκεται στη συστοιχία RAID-1 της προηγούμενης άσκησης
5. Οι χρήστες **user2** και **user4** να έχουν μόνο το δικαίωμα της ανάγνωσης
6. Δοκιμάστε να αντιγράψετε και να προσπαλάσετε δεδομένα στον κοινόχρηστο φάκελο χρησιμοποιώντας διαφορετικούς λογαριασμούς χρηστών

Βιβλιογραφία

Buffalotech. (2010). *http://www.buffalotech.com.* Ανάκτηση από http://www.buffalotech.com/content/files/solutions_articles/DAS_vs_NAS.pdf

Olson, C. (2014, January 23). *Getting started with storage. Understanding SAN vs NAS vs DAS.* Ανάκτηση από https://vanillavideo.com/blog/2014/started-storage-understanding-san-nas-das

Sacks, D. (2001). *Demystifying Storage Networking.* San Jose, California: IBM Corporation.

Surlow, J. (2012, September 26). *Selecting the Optimal Storage Solution.* Ανάκτηση από http://www.viawest.com/sites/default/files/Selecting_the_Optimal_Storage_Solution_-_Data_Storage_Technology.pdf

Theile, V. (2015, July 1). *http://wiki.openmediavault.org/index.php?title=Main_Page*.

Wikipedia. (2015, July 13). *Server Message Block*. Ανάκτηση από https://en.wikipedia.org/wiki/Server_Message_Block.

Wikipedia. (2015, September 13). *Server Network File System*. Ανάκτηση από https://en.wikipedia.org/wiki/Network_File_System.

Κεφάλαιο 7ο

Εγκατάσταση και Διαχείριση Διακομιστή, Απομακρυσμένη Πρόσβαση

Εισαγωγή

Η εγκατάσταση μιας διανομής Linux σε έναν υπολογιστή με σκοπό τη χρήση του σαν διακομιστή μας δίνει τη δυνατότητα πλήρους ελέγχου των δεδομένων μας. Επίσης, μπορούμε να αναπτύσσουμε δικές μας υπηρεσίες , να μαθαίνουμε κάνοντας δοκιμές και όλα αυτά χωρίς ιδιαίτερο κόπο. Σ' αυτό το κεφάλαιο θα εγκαταστήσουμε και θα ρυθμίσουμε το λειτουργικό σύστημα Ubuntu Server. Στη συνέχεια θα ρυθμίσουμε βασικές παραμέτρους του διακομιστή. Τέλος, θα εγκαταστήσουμε μια σειρά από λογισμικά εξυπηρέτησης για ιστοσελίδες, αρχεία, διαμεσολάβηση κλπ..

Διδακτικοί Στόχοι

Με την ολοκλήρωση του 7ου κεφαλαίου οι μαθητές θα πρέπει να είναι σε θέση να :

- Εγκαθιστούν και να παραμετροποιούν λογισμικό διακομιστή ιστοσελίδων για στατικές και δυναμικές ιστοσελίδες.
- Εγκαθιστούν και να παραμετροποιούν λογισμικό διακομιστή αρχείων.
- Εγκαθιστούν και να παραμετροποιούν λογισμικό διακομιστή διαμεσολάβησης.
- Αποκτούν πρόσβαση σε ένα απομακρυσμένο σύστημα, μέσω του δικτύου.
- Χρησιμοποιούν τις υπηρεσίες Telnet και SSH για να συνδεθούν σε έναν απομακρυσμένο Server.
- Εγκαθιστούν και να ρυθμίζουν υπηρεσίες Microsoft Remote Desktop Services.
- Εφαρμόζουν την εφαρμογή teamviewer για να έχουν απομακρυσμένο έλεγχο σε δικτυακούς Η/Υ.
- Εγκαθιστούν και να ρυθμίζουν έναν Εξυπηρετητή και έναν Πελάτη Εικονικού Δικτύου Υπολογιστών.
- Επιτρέπουν την πρόσβαση σε έναν Εξυπηρετητή από το εξωτερικό δίκτυο χρησιμοποιώντας την τεχνική της Προώθησης Θύρας (Port Forwarding).

Διδακτικές Ενότητες

7.1 Εγκατάσταση διανομής Linux (Ubuntu Server).
7.2 Βασικές ρυθμίσεις του λειτουργικού συστήματος.
7.3 Εγκατάσταση και ρύθμιση διακομιστή ιστοσελίδων (Web Server).
7.4 Εγκατάσταση και ρύθμιση διακομιστή αρχείων (FTP Server).
7.5 Εγκατάσταση και ρύθμιση διακομιστή εικονικού δικτύου υπολογιστών (VNC Server).
7.6 Εγκατάσταση και ρύθμιση διακομιστή διαμεσολάβησης (Proxy Server).
7.7 Εφαρμογές Δικτυακών Μέσων Αποθήκευσης (Cloud Computing).

7.1 Εγκατάσταση διανομής Linux (Ubuntu Server)

Η εγκατάσταση του λειτουργικού συστήματος θα πραγματοποιηθεί σε εικονική μηχανή για λόγους ευκολίας, ακολουθώντας τα παρακάτω βήματα:

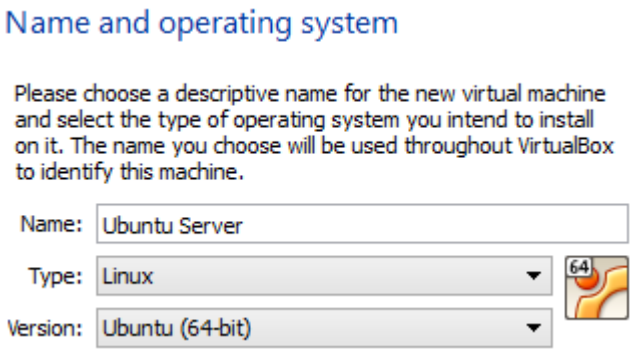
Κατεβάζουμε από τον επίσημο δικτυακό τόπο του Ubuntu την εικόνα δίσκου στην έκδοση διακομιστή (server) – http://www.ubuntu.com/download/server

Οι ελάχιστες απαιτήσεις υλικού είναι:

Επεξεργαστής	>= Pentium 4 2.6GHz
Μνήμη	>= 1 GBytes
Μέγεθος δίσκου εγκατάστασης	>= 1 GBytes
Μέγεθος δίσκων δεδομένων	Ανάλογα με τον όγκο δεδομένων

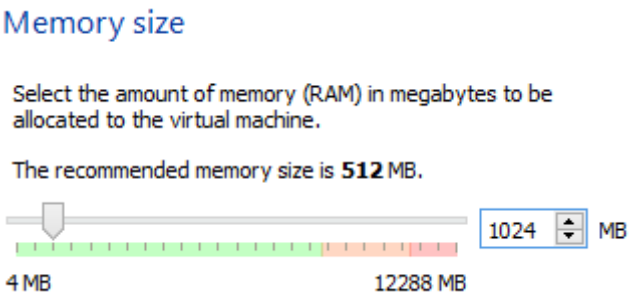
Ανοίγουμε το Oracle VirtualBox και δημιουργούμε μια εικονική μηχανή, εισάγοντας τις παρακάτω τιμές στα βήματα του οδηγού:

Name: Ubuntu Server, **Type:** Linux, **Version:** Ubuntu (64-bit)



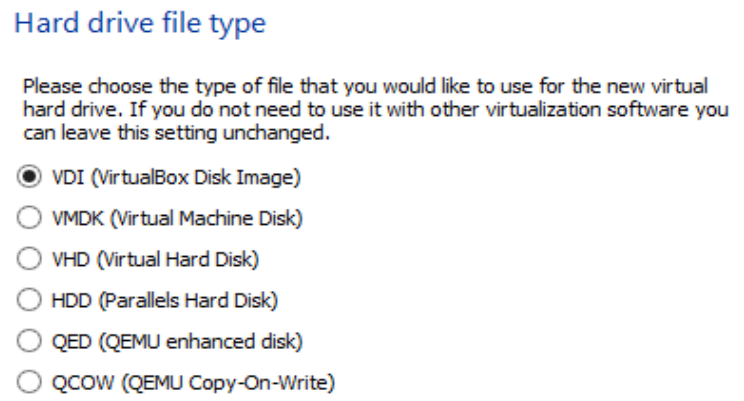
Εικόνα 7.1: Επιλογή ονόματος και αρχιτεκτονικής εικονικής μηχανής

Memory Size: 1024 MB

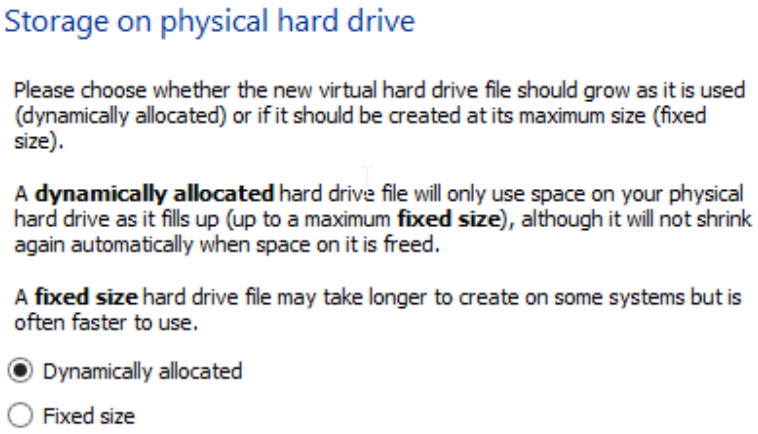


Εικόνα 7.2: Μέγεθος μνήμης εικονικής μηχανής

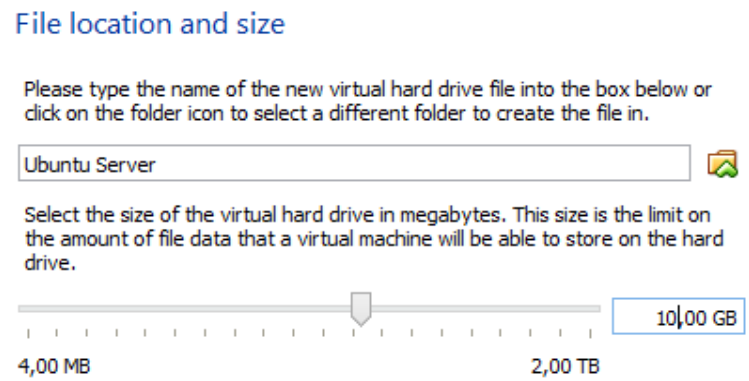
Hard drive: 10GB



Εικόνα 7.3: Ορισμός τύπου εικονικού δίσκου



Εικόνα 7.4: Επιλογή της μεθόδου αποθήκευσης του εικονικού δίσκου



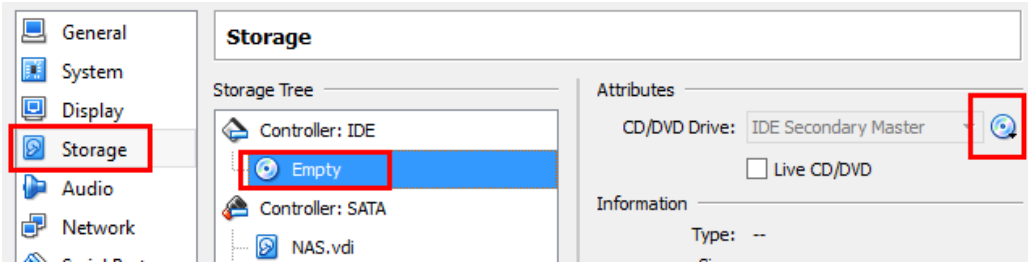
Εικόνα 7.5: Ορισμός ονόματος ε και μεγέθους του εικονικού δίσκου

Πατώντας το κουμπί **Create** θα δημιουργηθεί η εικονική μηχανή.

Πριν προχωρήσουμε στην εγκατάσταση πρέπει να κάνουμε μερικές επιπλέον ρυθμίσεις στην εικονική μηχανή. Για αυτό το λόγο θα πατήσουμε το γρανάζι (**Settings**) που βρίσκεται στη γραμμή εργαλείων, έχοντας επιλέξει πρώτα την εικονική μηχανή που δημιουργήσαμε.

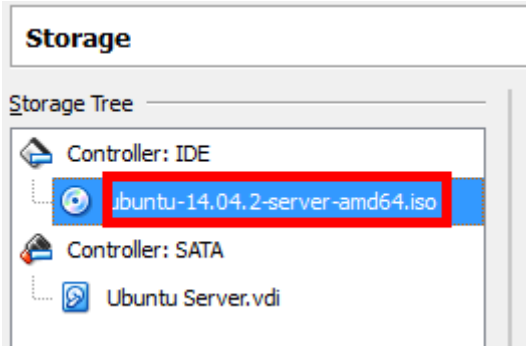
Εικόνα 7.6: Ρυθμίσεις εικονικής μηχανής

Στην ενότητα **Storage** πατάμε στο εικονίδιο του CD που γράφει **Empty** και στη συνέχεια πατάμε το εικονίδιο του CD στο δεξιό τμήμα του παραθύρου. Από το μενού που θα ανοίξει επιλέγουμε **Choose a virtual CD/DVD disk file…**



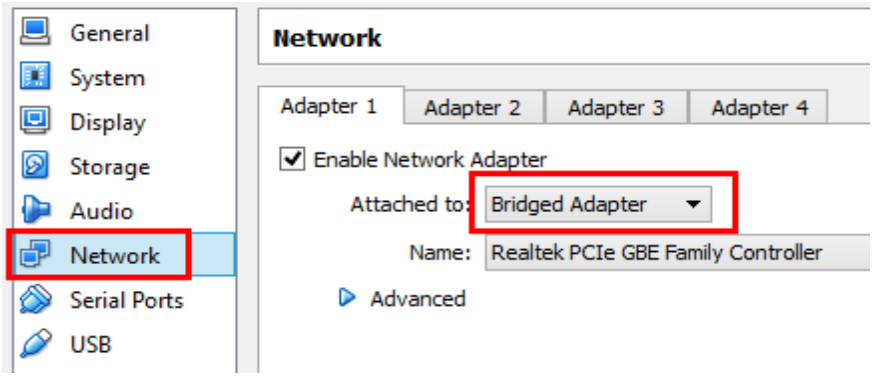
Εικόνα 7.7: Εισαγωγή εικόνας CD/DVD στην εικονική μηχανή

Επιλέγουμε το αρχείο με την εικόνα εγκατάστασης του Ubuntu Server.



Εικόνα 7.8: Επιλογή του δίσκου εγκατάστασης

Στην ενότητα ***Network*** αλλάζουμε τη ρύθμιση ***Attached to*** σε ***Bridged Adapter***.



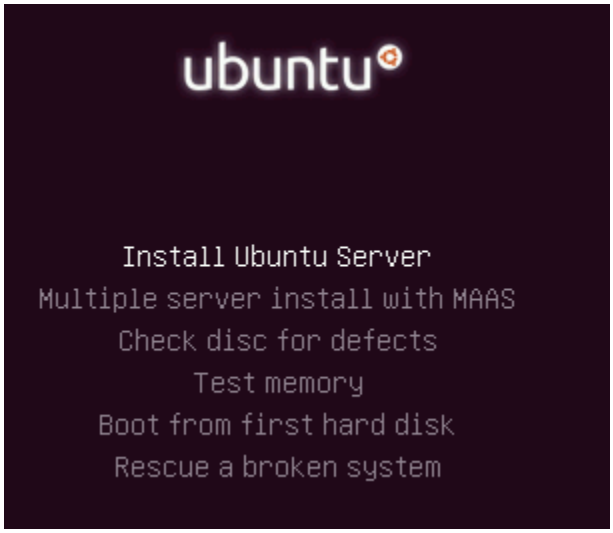
Εικόνα 7.9: Αλλαγή του τρόπου λειτουργίας της εικονικής κάρτας δικτύου

Τέλος, πατάμε **OK** και είμαστε έτοιμοι να ξεκινήσουμε την εικονική μηχανή πατώντας το εικονίδιο **Start**.

Μετά την αρχική εκκίνηση της εικονικής μηχανής, βλέπουμε την παρακάτω εικόνα. Επιλέγουμε τα Αγγλικά και πατάμε **Enter**.

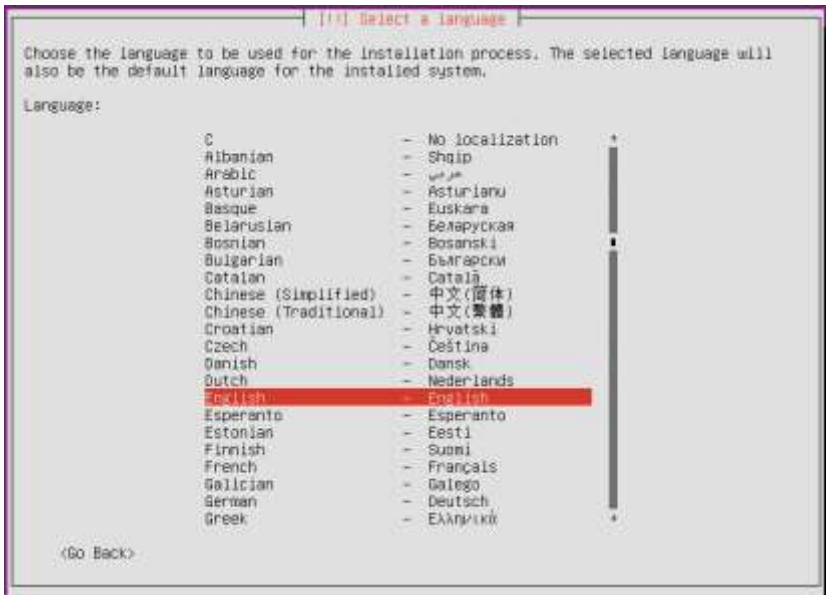
Εικόνα 7.10: Επιλογή γλώσσας εγκατάστασης

Πατάμε ξανά το **Enter** για να αρχίσει η διαδικασία εγκατάστασης του Ubuntu Server.



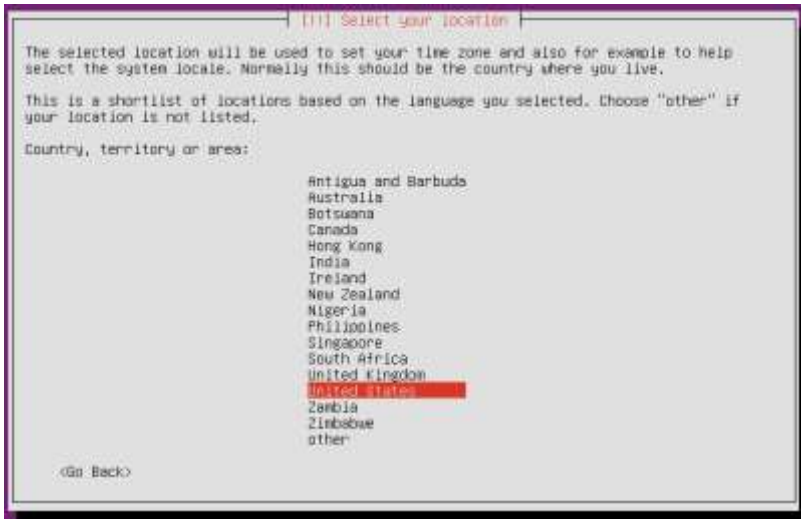
Εικόνα 7.11: Έναρξη εγκατάστασης

Επιλέγουμε τα Αγγλικά ως γλώσσα που θα χρησιμοποιηθεί στα μηνύματα του προγράμματος εγκατάστασης και πατάμε **Enter.**



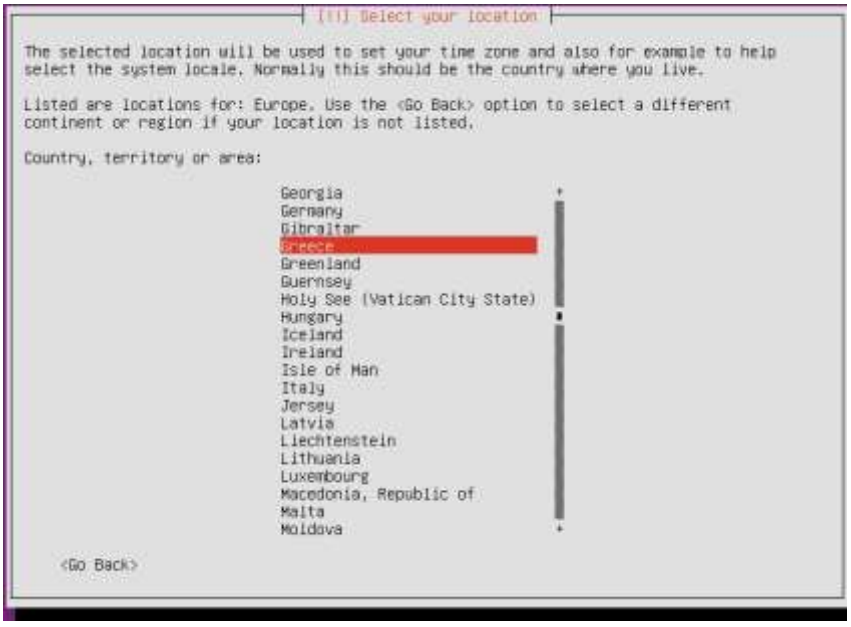
Εικόνα 7.12: Επιλογή γλώσσας εγκατάστασης

Στην επιλογή τοποθεσίας πατάμε διαδοχικά **other – Europe – Greece – United States**



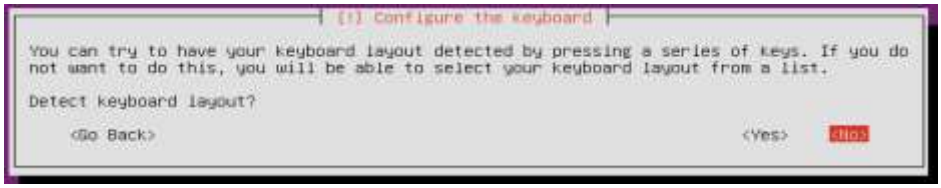
Εικόνα 7.13: Επιλογή τοποθεσίας - Βήμα 1

Εικόνα 7.14: Επιλογή τοποθεσίας - Βήμα 2



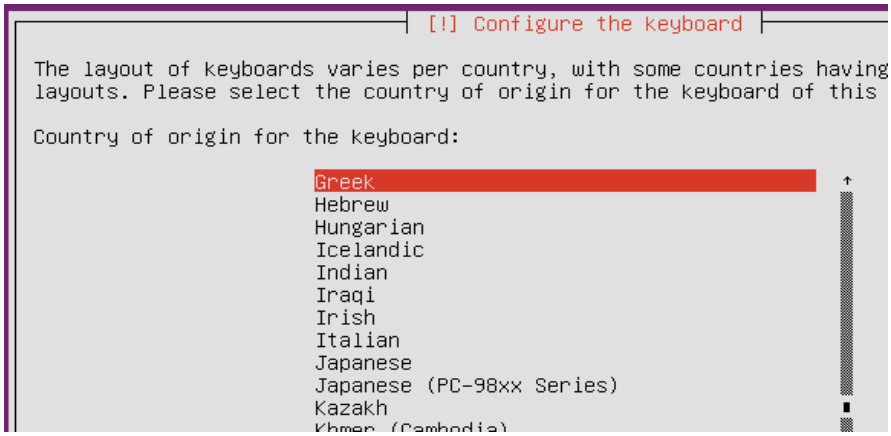
Εικόνα 7.15: Επιλογή τοποθεσίας - Βήμα 3

Επιλέγουμε **No** στην πρόταση αυτόματης αναγνώρισης της διάταξης του πληκτρολογίου.



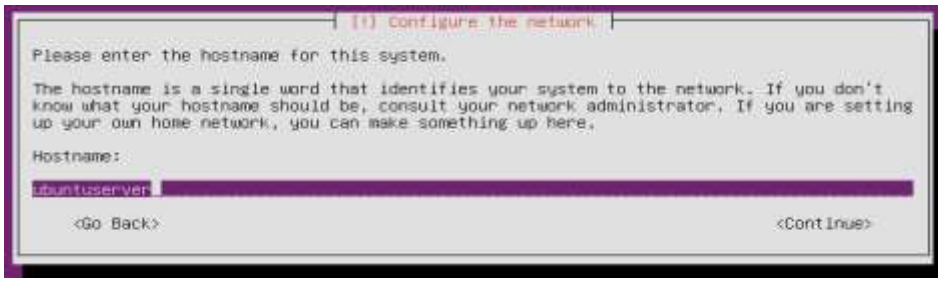
Εικόνα 7.16: Αυτόματη αναγνώριση διάταξης πληκτρολογίου

Επιλέγουμε **Greek** σαν διάταξη πληκτρολογίου και στην επόμενη οθόνη πάλι **Greek**. Σαν συνδυασμό πλήκτρων αλλαγής διάταξης πληκτρολογίου επιλέγουμε **Alt+Shift.**



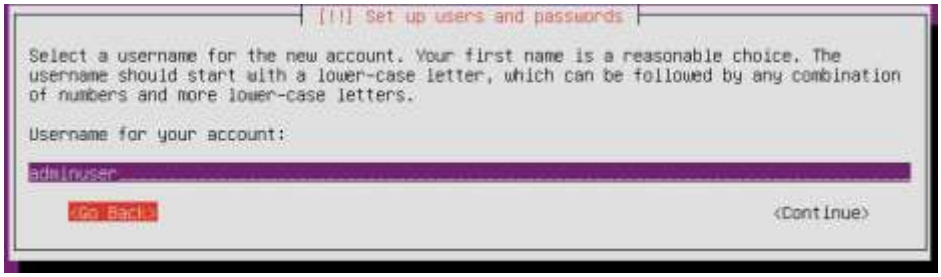
Εικόνα 7.17: Επιλογή ελληνικής διάταξης πληκτρολογίου

Σαν όνομα υπολογιστή (**Hostname**) εισάγουμε ubuntuserver.

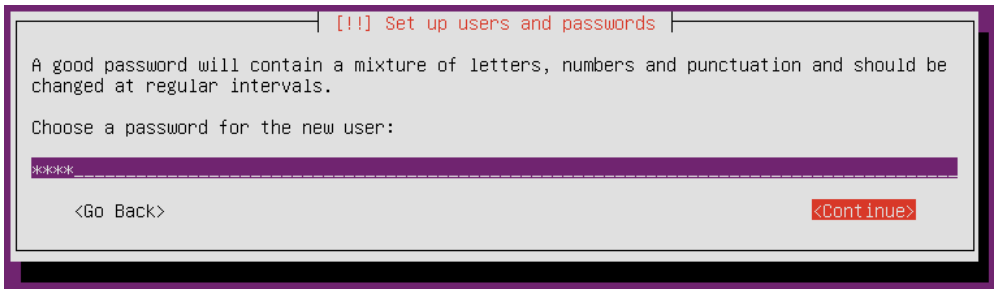


Εικόνα 7.18: Όνομα υπολογιστή

Στην επόμενη οθόνη θα δημιουργήσουμε έναν χρήστη για όλες τις εργασίες που δεν χρειάζονται δικαιώματα διαχειριστή. Για πλήρες όνομα εισάγουμε **Admin User** και σαν **username** το **adminuser.** Σαν κωδικό πρόσβασης θα εισάγουμε έναν εύκολο μόνο για λόγους ευκολίας. Για παράδειγμα 1234. Στην ερώτηση αν θέλουμε να αλλάξουμε τον κωδικό πρόσβασης, γιατί είναι αδύναμος απαντάμε **Yes.**

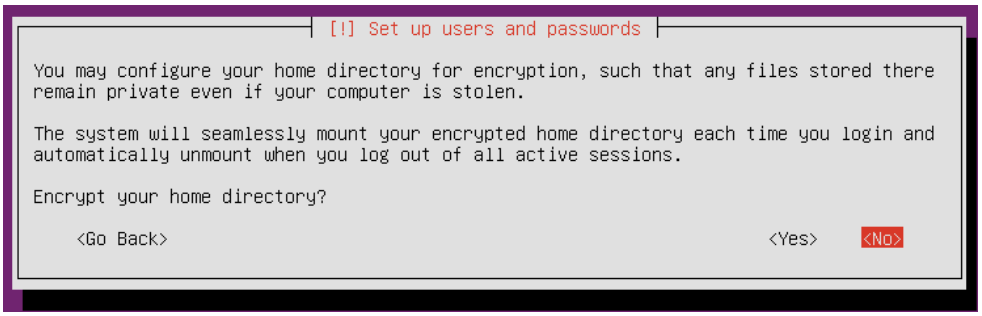


Εικόνα 7.19: Δημιουργία χρήστη



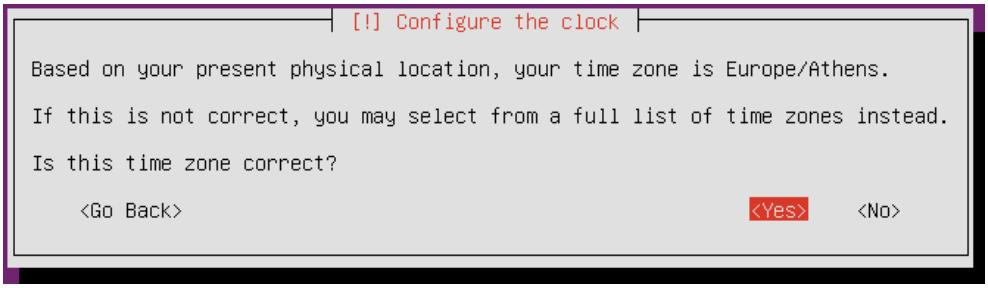
Εικόνα 7.20: Κωδικός πρόσβασης χρήστη

Στην επόμενη ερώτηση που αφορά στην κρυπτογράφηση του προσωπικού φακέλου του χρήστη που μόλις δημιουργήσαμε, απαντάμε **No .**



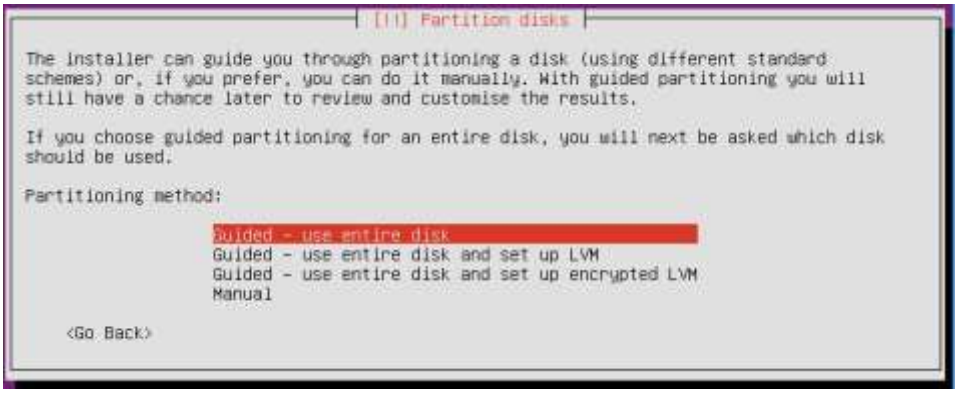
Εικόνα 7.21: Κρυπτογράφηση προσωπικού φακέλου

Η ζώνη ώρας που βρισκόμαστε είναι **Europe/Athens** έτσι απαντάμε **Yes** στην παρακάτω ερώτηση**.**



Εικόνα 7.22: Επιλογή ζώνης ώρας

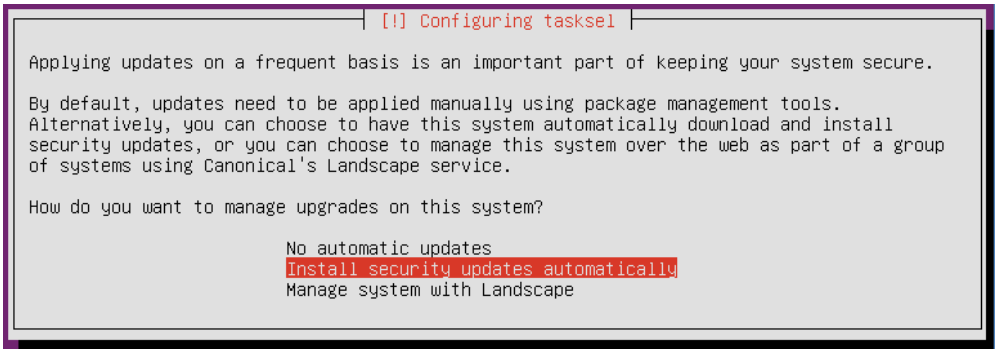
Στην επόμενη ερώτηση για τον τρόπο διαμόρφωσης του δίσκου επιλέγουμε **Guided – use entire disk**. Στη συνέχεια, επιλέγουμε το μοναδικό δίσκο στον οποίο θα γίνει η εγκατάσταση.



Εικόνα 7.23: Επιλογές διαμόρφωσης δίσκου

Σε όλες τις διανομές Linux απαιτείται να υπάρχει τουλάχιστον ένα διαμέρισμα για την εικονική μνήμη (swap) καθώς και ένα διαμέρισμα για τη ρίζα /. Με την επιλογή που κάναμε πιο πάνω, το πρόγραμμα εγκατάστασης δημιούργησε αυτόματα αυτά τα δύο διαμερίσματα.

Κατά διαστήματα υπάρχουν κρίσιμες αναβαθμίσεις που διορθώνουν προβλήματα ασφαλείας του λειτουργικού συστήματος. Έχουμε τη δυνατότητα να επιλέξουμε να εγκαθίστανται τέτοιου είδους αναβαθμίσεις αυτόματα.

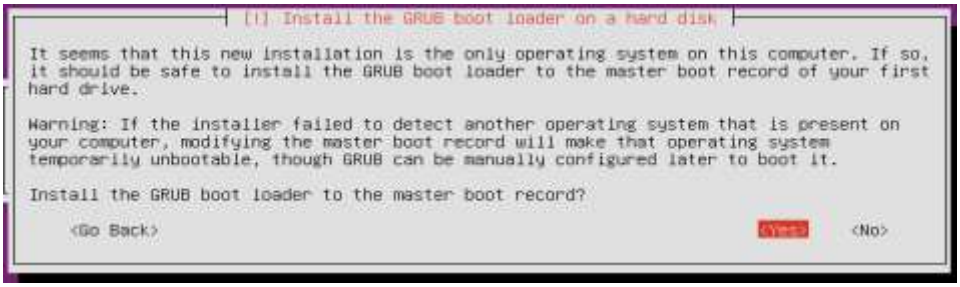


Εικόνα 7.24: Αυτόματη εγκατάσταση κρίσιμων αναβαθμίσεων

Τέλος, μας δίνετε η δυνατότητα εγκατάστασης επιπλέον λογισμικού. Δεν επιλέγουμε τίποτα, γιατί θα κάνουμε τις απαραίτητες εγκαταστάσεις στη συνέχεια χρησιμοποιώντας εντολές.

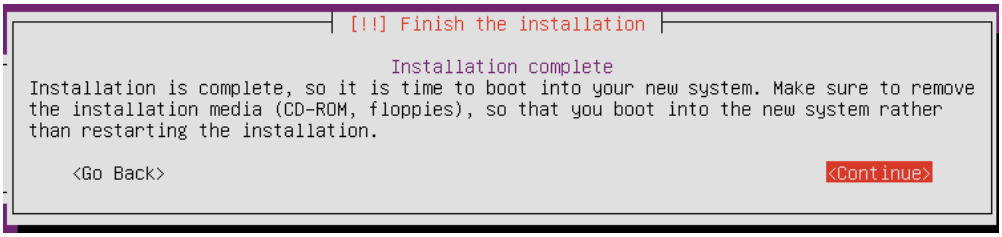
Εικόνα 7.25: Επιλογή εγκατάσταση πρόσθετου λογισμικού

Θα εγκαταστήσουμε το διαχειριστή εκκίνησης στο MBR του δίσκου μας, επιλέγοντας **Yes.**



Εικόνα 7.26: Εγκατάσταση διαχειριστή εκκίνησης

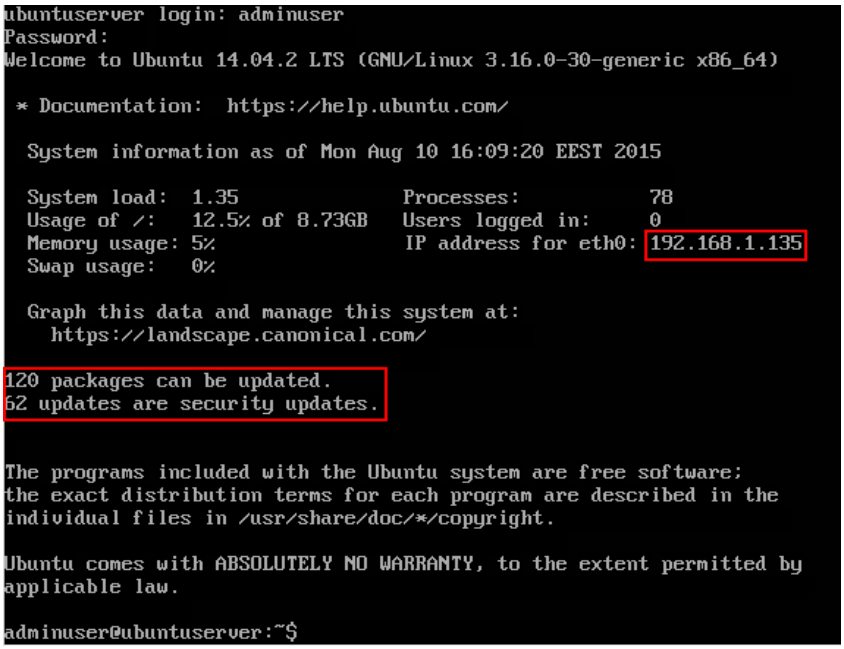
Η εγκατάσταση ολοκληρώθηκε και πατώντας **Continue** θα γίνει επανεκκίνηση της εικονικής μηχανής.



Εικόνα 7.27: Ολοκλήρωση εγκατάστασης

Μετά την επανεκκίνηση της εικονικής μηχανής θα βρεθούμε μπροστά σε μια οθόνη στην οποία θα πρέπει να εισάγουμε τα στοιχεία του λογαριασμού του χρήστη που δημιουργήσαμε κατά τη διάρκεια της εγκατάστασης. Δηλαδή **login: adminuser** και **password**: **1234**

Μετά τη σύνδεσή μας θα δούμε την παρακάτω οθόνη, η οποία μας ενημερώνει εκτός των άλλων για τη διεύθυνση IP που έχει ο διακομιστής, καθώς και για τις αναβαθμίσεις λογισμικού.



Εικόνα 7.28: Οθόνη μετά τη σύνδεση

7.1.1 Γνωριμία με το περιβάλλον κειμένου

Η επικοινωνία με το διακομιστή θα γίνεται αποκλειστικά με εντολές σε περιβάλλον κειμένου, χωρίς τη χρήση κάποιου γραφικού περιβάλλοντος. Στην αρχή ίσως υπάρξει μια σχετική δυσκολία, αλλά με λίγη πρακτική θα υπάρξει γρήγορα βελτίωση. Εξάλλου, όσο δεν χρησιμοποιούμε κάποιον λογαριασμό με διαχειριστικά δικαιώματα, δεν μπορούμε να δημιουργήσουμε σημαντικά προβλήματα στο λειτουργικό σύστημα.

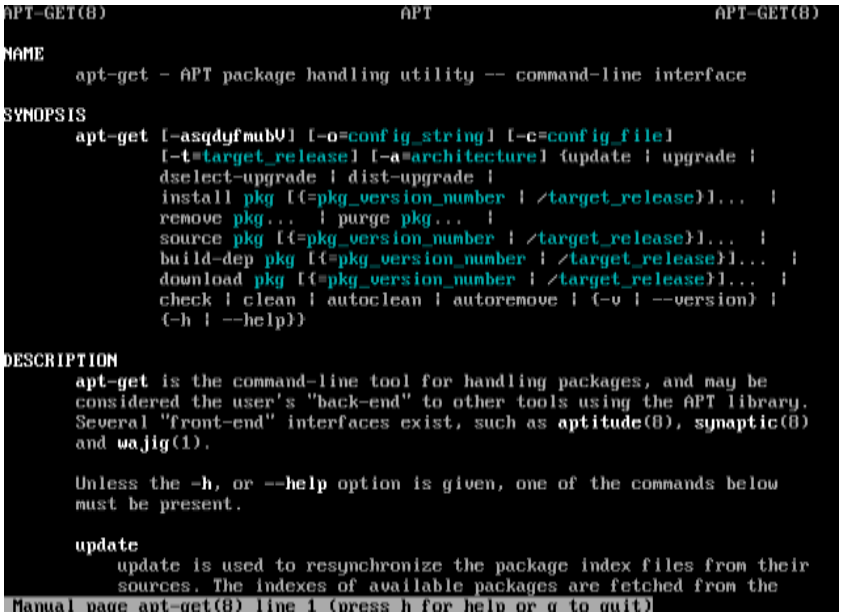
Θα πρέπει να ξέρουμε ότι όλες οι εντολές περιέχουν μόνο πεζούς λατινικούς χαρακτήρες και για την εκτέλεσή τους θα πρέπει να πατήσουμε το πλήκτρο **Enter** στο τέλος. Η γενική σύνταξη μιας εντολής είναι η εξής:

εντολή [επιλογές] [παράμετροι]

Στη θέση **επιλογές** εισάγουμε μια παύλα ακολουθουμένη από ένα γράμμα, όπου ανάλογα με την εντολή και το γράμμα πραγματοποιείται μια ενέργεια.

Στη θέση **παράμετροι** ανάλογα με την εντολή πληκτρολογούμε ένα τμήμα κειμένου που χρησιμοποιείται σαν είσοδος στην εντολή.

Για όλες τις εντολές υπάρχει ένα εγχειρίδιο χρήσης, το οποίο ενεργοποιείται γράφοντας την εντολή **man εντολή.** Αφού μπούμε στο εγχειρίδιο χρήσης μιας εντολής, μπορούμε να περιηγηθούμε χρησιμοποιώντας τα βελάκια ή τα πλήκτρα PgUp – PgDown. Για να βγούμε θα πρέπει να πατήσουμε το πλήκτρο **q**.



Εικόνα 7.29: Εγχειρίδιο χρήσης εντολής apt-get

7.1.2 Διαχείριση συστήματος

Με το χρήστη που έχουμε δημιουργήσει κατά την εγκατάσταση του λειτουργικού συστήματος έχουμε τη δυνατότητα να εκτελούμε κάποιες εντολές, αλλά δεν μπορούμε να πραγματοποιήσουμε ρυθμίσεις που αφορούν στο σύστημα (εγκατάσταση λογισμικού, τροποποίηση αρχείων ρυθμίσεων κλπ). Έτσι, πολλές φορές πριν από κάποιες εντολές θα πρέπει να γράφουμε την εντολή **sudo** μέσω της οποίας θα μπορούμε να εκτελούμε μια εντολή σαν διαχειριστής συστήματος, αφού πρώτα δώσουμε τον κωδικό πρόσβασής μας.

7.1.3 Διαχείριση λογισμικού

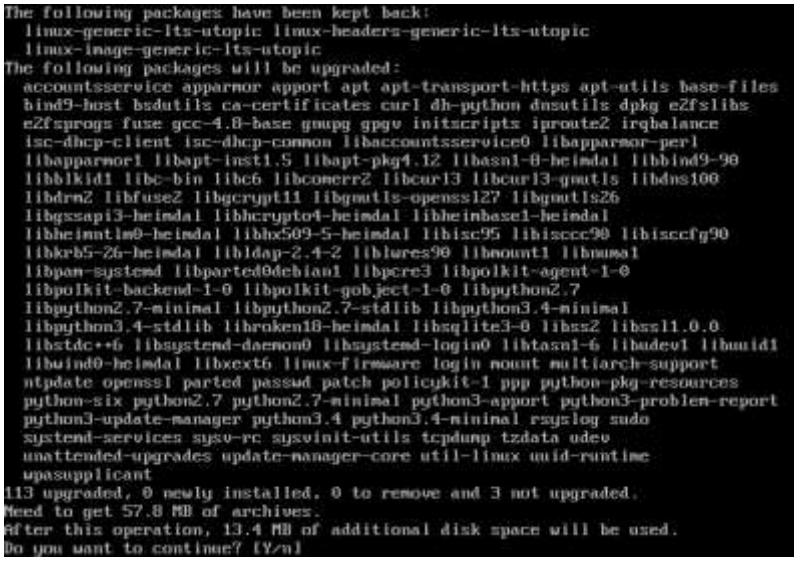
Για την εγκατάσταση και απεγκατάσταση λογισμικού στο διακομιστή μας θα χρησιμοποιήσουμε τις παρακάτω εντολές:

- **dpkg**
  Αυτήν η εντολή μας επιτρέπει να εγκαθιστούμε και να απεγκαθιστούμε λογισμικό το οποίο έχουμε προηγουμένως κατεβάσει από το Διαδίκτυο. Το πακέτο πρέπει να έχει επέκταση .deb δηλαδή να είναι συμβατό πακέτο Debian. Η εντολή dpkg δεν έχει τη δυνατότητα να κατεβάσει αυτόματα από το Διαδίκτυο το λογισμικό που θέλουμε να εγκαταστήσουμε.
  Αν γράψουμε την εντολή **dpkg** χωρίς καμία επιλογή θα παρατηρήσουμε ότι δεν γίνεται καμία ενέργεια (εμφανίζεται απλά ένα τμήμα από τη βοήθεια της εντολής). Έτσι, ανάλογα την ενέργεια που θέλουμε να πραγματοποιήσουμε εισάγουμε και την αντίστοιχη επιλογή. Για παράδειγμα, αν γράψουμε **dpkg –l** θα πάρουμε σαν αποτέλεσμα όλα τα πακέτα που είναι εγκατεστημένα στο διακομιστή. Για εγκατάσταση ενός πακέτου θα πρέπει να γράψουμε **dpkg –i ονομα_λογισμικού.deb**

- **apt-get**
  Η εντολή apt-get είναι πολύ ισχυρή και μας επιτρέπει να εγκαθιστούμε, απεγκαθιστούμε και να αναβαθμίζουμε λογισμικό. Έχει τη δυνατότητα να κατεβάζει αυτόματα από το Διαδίκτυο το πακέτο που θέλουμε να κάνουμε εγκατάσταση καθώς επίσης και τις όποιες εξαρτήσεις του. Μερικές χρήσιμες εκφράσεις της εντολής είναι οι παρακάτω:
    - Εγκατάσταση πακέτου: **sudo apt-get install ονομα_πακέτου**
    - Απεγκατάσταση πακέτου: **sudo apt-get remove ονομα_πακέτου**
    - Αναβάθμιση λογισμικού: **sudo apt-get upgrade**

  Πριν από την αναβάθμιση του λογισμικού καλό θα είναι να έχουμε εκτελέσει την εντολή **sudo apt-get update** η οποία ενημερώνει μια βάση δεδομένων που περιέχει τα διαθέσιμα πακέτα λογισμικού των αποθετηρίων (repositories). Τα αποθετήρια λογισμικού πρακτικά είναι διακομιστές οι οποίοι περιέχουν πακέτα λογισμικού.

  Έτσι αν θέλουμε να αναβαθμίσουμε όλα τα πακέτα του λειτουργικού μας συστήματος θα πρέπει να γράψουμε **sudo apt-get update && sudo apt-get upgrade** και να πατήσουμε το πλήκτρο **y** στην ερώτηση.



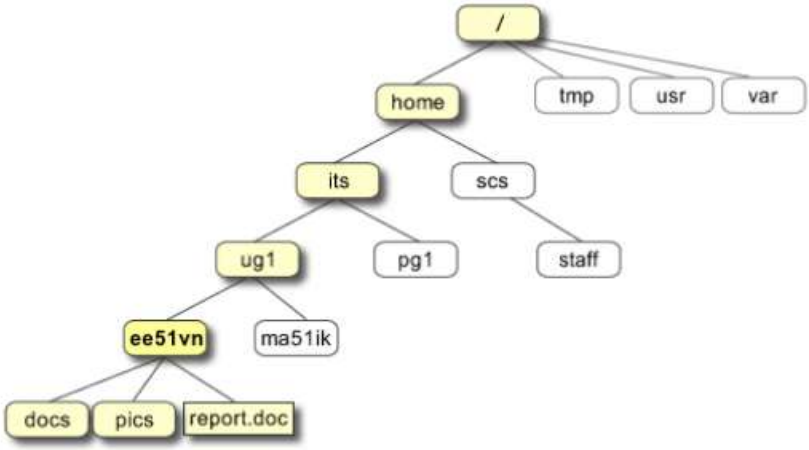
Εικόνα 7.30: Αναβάθμιση λογισμικού

Παρατηρούμε ότι μπορούμε να γράψουμε δύο εντολές σε μία γραμμή χρησιμοποιώντας τον τελεστή **&&** ο οποίος σημαίνει ότι αφού εκτελεστεί η πρώτη εντολή χωρίς σφάλμα στη συνέχεια εκτελείτε και η δεύτερη εντολή.

7.1.4 Σύστημα αρχείων

Γενικά, στον κόσμο του Linux ισχύει: «Σ' ένα σύστημα Linux όλα είναι αρχεία. Αν κάτι δεν είναι αρχείο, τότε είναι διεργασία». Για παράδειγμα, για την πρόσβαση στις συσκευές εισόδου – εξόδου χρησιμοποιούμε αρχεία.

Για τη διαχείριση των αρχείων – φακέλων ακολουθείται μια ιεραρχική δομή (σαν ανάποδο δέντρο), όπου φάκελοι βρίσκονται μέσα σε άλλους φακέλους οι οποίοι μπορεί να περιέχουν αρχεία. Στην κορυφή αυτής της δομής βρίσκεται πάντα ο φάκελος **/** ο οποίος ονομάζεται ρίζα.



Εικόνα 7.31: Ιεραρχική δομή αρχείων και φακέλων

Μέσα σε αυτήν τη δομή υπάρχουν φάκελοι που χρησιμοποιούνται από το λειτουργικό σύστημα και όπου έχει πρόσβαση μόνο ο διαχειριστής συστήματος (root). Βέβαια με τη χρήση της εντολής **sudo** έχει τη δυνατότητα και ένας απλός χρήστης να πάρει προσωρινά τα δικαιώματα του διαχειριστή.

Στο φάκελο **/etc** βρίσκονται σχεδόν όλα τα αρχεία ρυθμίσεων του διακομιστή, ενώ στους φακέλους **/bin** και **/sbin** θα βρούμε σχεδόν όλα τα προγράμματα συστήματος.

7.1.5 Απόλυτη και σχετική διαδρομή (Absolute Path – Relative Path)

Η θέση κάθε ενός αρχείου καθορίζεται από την απόλυτη διαδρομή του, η οποία είναι η διαδρομή που αρχίζει από το ριζικό φάκελο και καταλήγει στο αρχείο περνώντας από όλους τους ενδιάμεσους φακέλους. Ανάμεσα στους φακέλους εισάγουμε σαν διαχωριστικό το χαρακτήρα /. Για παράδειγμα, η απόλυτη διαδρομή του αρχείο **report.doc** είναι **/home/its/ug1/ee51vn/report.doc.** Για κάθε ένα αρχείο υπάρχει μόνο μια απόλυτη διαδρομή.

Η σχετική διαδρομή είναι η διαδρομή ενός αρχείου έχοντας όμως σαν αφετηρία όχι τη ρίζα, αλλά κάποιον άλλο φάκελο. Για παράδειγμα, αν ο τρέχοντας φάκελος είναι ο **/home** η σχετική διαδρομή του αρχείου **report.doc** είναι **its/ug1/ee51vn/report.doc.** Παρατηρήστε ότι η σχετική διαδρομή **δεν** αρχίζει με /.

7.1.6 Βασικές εντολές

Παρακάτω θα κάνουμε μια αναφορά σε μερικές βασικές εντολές:

clear Με αυτήν την εντολή καθαρίζουμε την οθόνη από όλα τα περιεχόμενά της

date Με αυτήν την εντολή προβάλλουμε την ημερομηνία και την ώρα του συστήματος

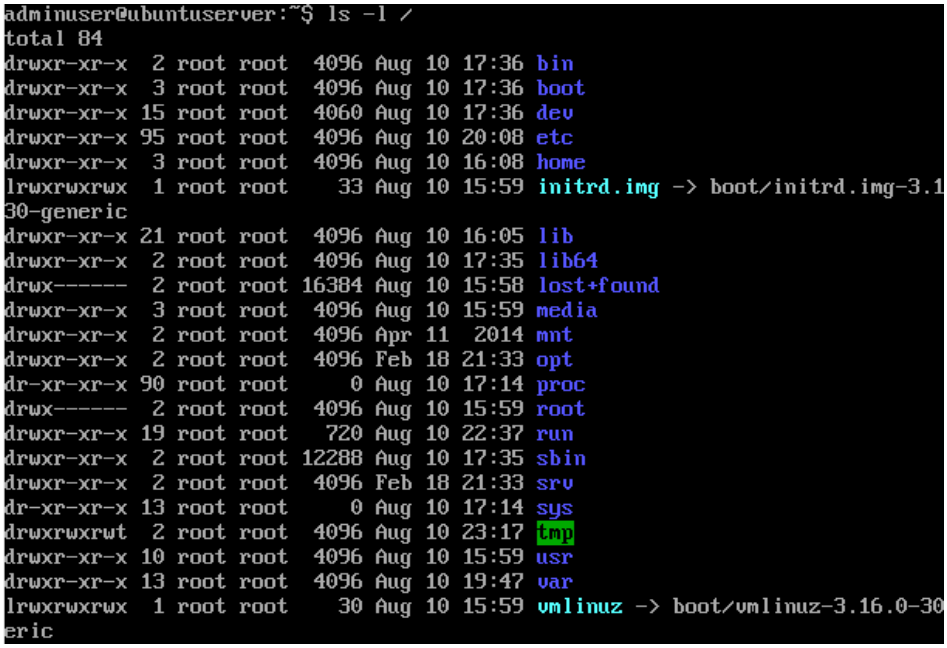
cal Με αυτή την εντολή προβάλλουμε το ημερολόγιο του τρέχοντα μήνα.

Εικόνα 7.32: Ημερολόγιο τρέχοντα μήνα

Αν θέλουμε να προβάλλουμε το ημερολόγιο του Ιανουαρίου του έτους 2010, θα γράφαμε **cal 1 2010**

pwd Χρησιμοποιείται για την προβολή της απόλυτης διαδρομής του τρέχοντα φακέλου

ls Χρησιμοποιείται για την προβολή των περιεχομένων ενός φακέλου. Προαιρετικά δέχεται μια παράμετρο η οποία είναι η διαδρομή του φακέλου τα περιεχόμενα του οποίου θέλουμε να δούμε. Αν δεν εισάγουμε καμία παράμετρο, τότε προβάλλονται τα περιεχόμενα του τρέχοντα φακέλου. Για παράδειγμα, για την προβολή των περιεχομένων του ριζικού φακέλου με λεπτομέρειες, γράφουμε **ls –l /**



Εικόνα 7.33: Περιεχόμενα φακέλου

cd Χρησιμοποιείται για την αλλαγή του τρέχοντα φακέλου. Αν δεν εισάγουμε καμία παράμετρο, το αποτέλεσμα θα είναι να μεταφερθούμε στον προσωπικό μας φάκελο.

mkdir Για τη δημιουργία ενός φακέλου χρησιμοποιούμε την εντολή mkdir, εισάγοντας σαν παράμετρο το όνομα του φακέλου που θέλουμε να δημιουργήσουμε. Για παράδειγμα, γράφοντας **mkdir classroom** θα δημιουργηθεί ένας φάκελος με όνομα **classroom** στον τρέχοντα φάκελο. Σαν απλοί χρήστες έχουμε το δικαίωμα να δημιουργούμε φακέλους μόνο μέσα στον προσωπικό μας φάκελο.

rmdir Χρησιμοποιείται για τη διαγραφή κενών φακέλων.

cp Χρησιμοποιείται για την αντιγραφή φακέλων και αρχείων. Πρέπει να εισάγουμε υποχρεωτικά δύο παραμέτρους. Η μία αντιπροσωπεύει τον αρχείο που θέλουμε να αντιγράψουμε και η δεύτερη τον προορισμό. Για παράδειγμα, αν γράψουμε **cp /home/its/ug1/ee51vn/report.doc /home/its/pg1** θα γίνει αντιγραφή του αρχείου **report.doc** στο φάκελο **/home/its/pg1**

mv Η εντολή χρησιμοποιείται για τη μετακίνηση ή μετονομασία ενός αρχείου ή φακέλου. Για παράδειγμα, αν θέλουμε να μεταφέρουμε το αρχείο **report.doc** στο φάκελο **/tmp** θα γράψουμε **mv /home/its/ug1/ee51vn/report.doc /tmp**

rm Χρησιμοποιείται για τη διαγραφή αρχείων και φακέλων. Για παράδειγμα αν θέλουμε να διαγράψουμε το αρχείο **report.doc** θα γράψουμε **rm /home//its/ug1/ee51vn/report.doc**. Για διαγραφή του φακέλου **ee51vn** και όλων των περιεχομένων του θα γράφαμε **rm –r /home/its/ug1/ee51vn**

7.2 Βασικές ρυθμίσεις του λειτουργικού συστήματος

7.2.1 Ρυθμίσεις δικτύου

Οι κάρτες δικτύου αναγνωρίζονται από το σύστημα σαν **ethX**, όπου Χ είναι ένας αριθμός. Αν το σύστημά μας έχει μια κάρτα δικτύου, το όνομά με το οποίο θα την αναγνωρίζει του λειτουργικό σύστημα θα είναι **eth0**.

Για να δούμε τα βασικά χαρακτηριστικά της κάρτας δικτύου χρησιμοποιούμε την εντολή **ifconfig –a.**

```
adminuser@ubuntuserver:~$ ifconfig -a
eth0      Link encap:Ethernet  HWaddr 08:00:27:45:12:2b
          inet addr:192.168.1.135  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe45:122b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:40576 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22113 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:60563055 (60.5 MB)  TX bytes:1573560 (1.5 MB)
```

Εικόνα 7.34: Χαρακτηριστικά κάρτας δικτύου

Στην παραπάνω εικόνα, βλέπουμε εκτός των άλλων τη διεύθυνση IP, τη μάσκα δικτύου και τη διεύθυνση MAC.

7.2.2 Στατική διεύθυνση IP

Η διεύθυνση IP έχει αποδοθεί αυτόματα από το δρομολογητή μας. Για την εισαγωγή μιας στατικής διεύθυνσης IP θα πρέπει να κάνουμε τις παρακάτω ενέργειες:

- Επεξεργασία του αρχείου κειμένου που περιέχει τις ρυθμίσεις δικτύου με την εντολή **sudo nano /etc/network/interfaces**
- Η παραπάνω εντολή θα ανοίξει το αρχείο **interfaces** το οποίο βρίσκεται στο φάκελο **/etc/network** με τον επεξεργαστή κειμένου **nano**.

- Θα κάνουμε τις αλλαγές σύμφωνα με την παρακάτω εικόνα, έτσι ώστε ο server μας να έχει πάντα τη διεύθυνση IP 192.168.1.201

```
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
        address 192.168.1.201
        netmask 255.255.255.0
        broadcast 192.168.1.255
        gateway 192.168.1.1
        dns-nameservers 192.168.1.1 8.8.8.8
```

Εικόνα 7.35: Εισαγωγή στατικής διεύθυνση IP

- Για την αποθήκευση των αλλαγών στο αρχείο θα πρέπει να πατήσουμε το συνδυασμό πλήκτρων **Ctrl+X** και στη συνέχεια **y** για αποδοχή των αλλαγών και κλείσιμο του επεξεργαστή κειμένου.
- Για την ολοκλήρωση της διαδικασίας αλλαγής της διεύθυνσης IP, πρέπει να απενεργοποιήσουμε την κάρτα δικτύου με την εντολή **sudo ifdown eth0** και να τη ενεργοποιήσουμε με την εντολή **sudo ifup eth0.** Τώρα, εισάγοντας την εντολή **ifconfig –a** θα δούμε την καινούρια διεύθυνση IP.

```
adminuser@ubuntuserver:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:45:12:2b
          inet addr:192.168.1.201  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe45:122b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:40607 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22132 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:60566244 (60.5 MB)  TX bytes:1575168 (1.5 MB)
```

Εικόνα 7.36: Χαρακτηριστικά κάρτας δικτύου

7.2.3 Συγχρονισμός ώρας συστήματος

Η εντολή **date** εμφανίζει την τρέχουσα ημερομηνία και ώρα του συστήματος. Για να εξασφαλίσουμε ότι ο server θα έχει πάντα σωστή ημερομηνία και ώρα θα εγκαταστήσουμε μια υπηρεσία η οποία αναλαμβάνει τον αυτόματο συγχρονισμό με έναν διακομιστή ώρας. Έτσι, αν γράψουμε **sudo apt-get install ntp** θα γίνει εγκατάσταση της παραπάνω υπηρεσίας.

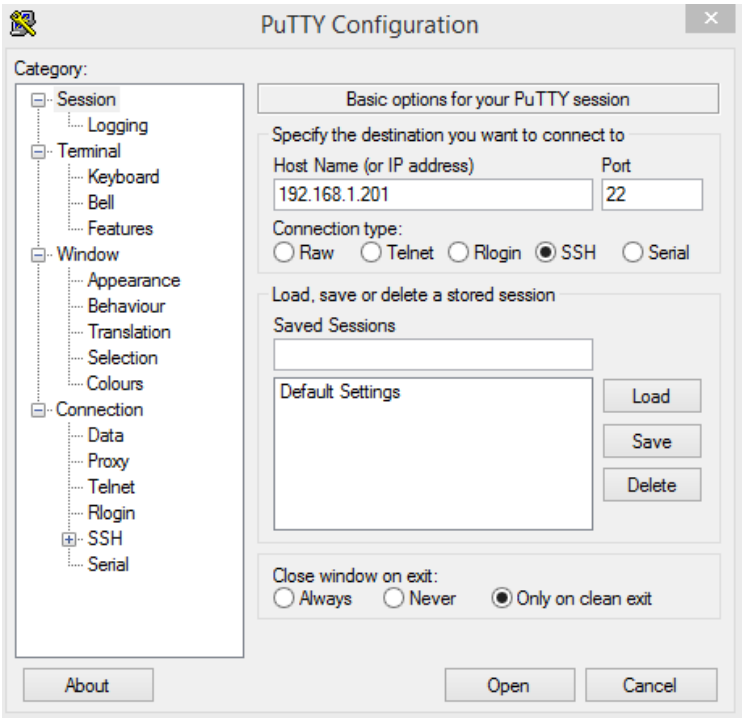
7.2.4 Απομακρυσμένη πρόσβαση

Για να έχουμε τη δυνατότητα να χειριζόμαστε το διακομιστή από μακριά μέσω ενός περιβάλλοντος κειμένου, θα πρέπει να εγκαταστήσουμε το ανάλογο λογισμικό που είναι το **OpenSSH Server.** Το **OpenSSH** είναι μια υλοποίηση του πρωτοκόλλου **Secure Shell (SSH)** για το χειρισμό ενός υπολογιστή εξ αποστάσεως, όπως επίσης και για τη μεταφορά αρχείων. Πλεονεκτεί έναντι του παλαιότερου πρωτοκόλλου **Telnet**, γιατί όλη η επικοινωνία κρυπτογραφείται.

Για την εγκατάσταση γράφουμε **sudo apt-get install openssh-server**. Τώρα, μπορούμε να χειριζόμαστε το διακομιστή από μακριά μέσω ενός περιβάλλοντος κειμένου.

Για να έχουμε απομακρυσμένη πρόσβαση μέσα από το λειτουργικό σύστημα Windows θα πρέπει να κατεβάσουμε και να εκτελέσουμε ένα πρόγραμμα που υλοποιεί το πρωτόκολλο

SSH. Υπάρχουν πολλά διαθέσιμα στο Διαδίκτυο, με πιο γνωστό το putty (http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html). Κατεβάζουμε και εκτελούμε το putty σε έναν υπολογιστή που βρίσκεται μέσα στο δίκτυο που βρίσκεται ο διακομιστής. Εισάγουμε στο πεδίο **Host Name** τη διεύθυνση IP που δώσαμε στο διακομιστή και προσέχουμε το πεδίο **Port** να έχει τιμή 22. Αυτήν η θύρα είναι η προεπιλεγμένη για το πρωτόκολλο SSH.

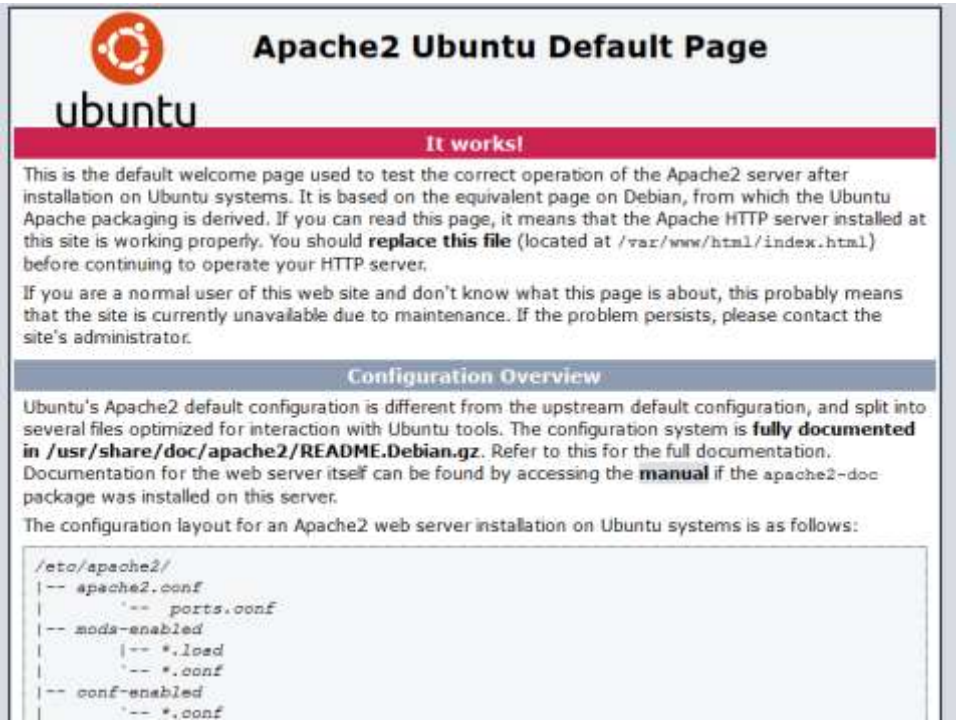


Εικόνα 7.37: Πρόγραμμα απομακρυσμένης σύνδεσης SSH

Αν θέλουμε να έχουμε απομακρυσμένη πρόσβαση στο διακομιστή μας από υπολογιστή που βρίσκεται εκτός του εσωτερικού δικτύου, τότε θα πρέπει να ρυθμίσουμε κατάλληλα το δρομολογητή μας. Δηλαδή, χρησιμοποιώντας την τεχνική της **προώθησης θύρας (Port Forwording)** εισάγουμε τη θύρα 22 να εξυπηρετείται από την εσωτερική διεύθυνση του διακομιστή μας. Θα δούμε τη διαδικασία σε επόμενη παράγραφο του κεφαλαίου.

7.3 Εγκατάσταση και ρύθμιση διακομιστή ιστοσελίδων (Web Server)

Ένας διακομιστής ιστοσελίδων (Web Server) είναι το λογισμικό το οποίο είναι υπεύθυνο για το χειρισμό αιτήσεων HTTP. Με απλά λόγια όταν ένας φυλλομετρητής ζητήσει μια ιστοσελίδα, ο διακομιστής ιστοσελίδων απαντάει με την αποστολή της ιστοσελίδας και των δεδομένων που την αποτελούν στο φυλλομετρητή. Ο πιο γνωστός διακομιστής ιστοσελίδων είναι ο **Apache2 Web Server** τον οποίο θα εγκαταστήσουμε με την εντολή **sudo apt-get install apache2.** Για να ελέγξουμε αν ο διακομιστής ιστοσελίδων λειτουργεί, ανοίγουμε έναν φυλλομετρητή και στη γραμμή διευθύνσεων εισάγουμε τη διεύθυνση του διακομιστή μας (http://192.168.1.201).



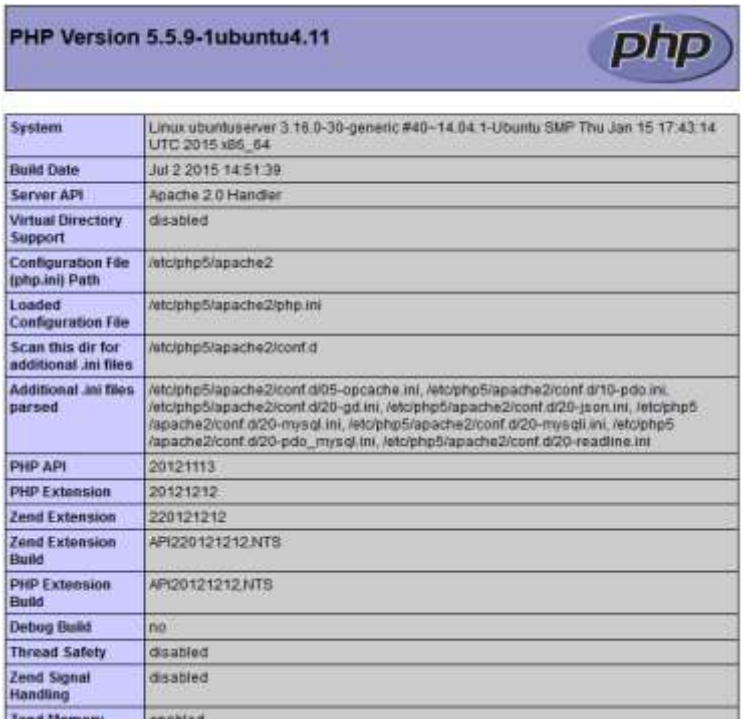
Εικόνα 7.38: Αρχική σελίδα μετά την εγκατάσταση διακομιστή ιστοσελίδων

Αυτή τη στιγμή ο διακομιστής ιστοσελίδων είναι ικανός να χειριστεί μόνο στατικές ιστοσελίδες. Αν θέλουμε όμως να χρησιμοποιήσουμε το διακομιστή ιστοσελίδων για την ανάπτυξη δυναμικών ιστοσελίδων με τη χρήση της γλώσσας PHP και βάσεων δεδομένων με χρήση της MySQL θα πρέπει να εγκαταστήσουμε επιπλέον λογισμικό. Έτσι, γράφουμε **sudo apt-get install php5 libapach2-mod-php5 php5-mysql mysql-server phpmyadmin.** Κατά τη διάρκεια της εγκατάσταση θα εισάγουμε σαν κωδικό πρόσβασης για το διαχειριστή της **MySQL** και του **phpmyadmin** το **1234**. Πλέον ο Apache2 έχει τη δυνατότητα χειρισμού σελίδων γραμμένων σε γλώσσα PHP. Για παράδειγμα:

- Δημιουργούμε μια ιστοσελίδα με την εντολή **sudo nano /var/www/html/index.php** Ο προεπιλεγμένος φάκελος στον οποίο τοποθετούνται οι ιστοσελίδες είναι ο **/var/www/html.**
- Σαν περιεχόμενο εισάγουμε τα παρακάτω:
  <?php

  phpinfo();

  ?>
- Αποθηκεύουμε πατώντας **Ctrl+X** και στη συνέχεια **Y**.
- Ανοίγουμε έναν φυλλομετρητή και εισάγουμε τη διεύθυνση http://192.168.1.201/index.php. Το αποτέλεσμα θα είναι να μας δείξει μια ιστοσελίδα με τις πληροφορίες της γλώσσας PHP που έχουμε εγκαταστήσει.



PHP Version 5.5.9-1ubuntu4.11

System	Linux ubuntuserver 3.16.0-30-generic #40~14.04.1-Ubuntu SMP Thu Jan 15 17:43:14 UTC 2015 x86_64
Build Date	Jul 2 2015 14:51:39
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files parsed	/etc/php5/apache2/conf.d/05-opcache.ini, /etc/php5/apache2/conf.d/10-pdo.ini, /etc/php5/apache2/conf.d/20-gd.ini, /etc/php5/apache2/conf.d/20-json.ini, /etc/php5/apache2/conf.d/20-mysql.ini, /etc/php5/apache2/conf.d/20-mysqli.ini, /etc/php5/apache2/conf.d/20-pdo_mysql.ini, /etc/php5/apache2/conf.d/20-readline.ini
PHP API	20121113
PHP Extension	20121212
Zend Extension	220121212
Zend Extension Build	API220121212,NTS
PHP Extension Build	API20121212,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled

Εικόνα 7.39: Δείγμα δυναμικής ιστοσελίδας

Αν θέλουμε οι ιστοσελίδες που δημιουργούμε στο διακομιστή μας να είναι προσβάσιμες από το Διαδίκτυο θα πρέπει να κάνουμε προώθηση της θύρας 80 από το περιβάλλον διαχείρισης του δρομολογητή προς τη διεύθυνση του διακομιστή.

7.3.1 Ενεργοποίηση φακέλων χρηστών

Αν θέλουμε να δώσουμε τη δυνατότητα στους χρήστες του διακομιστή να δημιουργούν ιστοσελίδες στον προσωπικό τους φάκελο πρέπει να κάνουμε την παρακάτω διαδικασία:

- Να ενεργοποιήσουμε τη δυνατότητα εξυπηρέτησης ιστοσελίδων από τους προσωπικούς φακέλους με την εντολή **sudo a2enmod userdir**
- Να επανεκκινήσουμε το διακομιστή ιστοσελίδων με την εντολή **sudo service apache2 restart**
- Να δημιουργήσουμε ένα φάκελο με όνομα **public_html** μέσα στον προσωπικό φάκελο κάθε ενός χρήστη. Στην περίπτωση μας, δημιουργούμε το φάκελο στο προσωπικό φάκελο του χρήστη **adminuser** με την εντολή **mkdir /home/adminuser/public_html**
- Η πρόσβαση στις ιστοσελίδες του προσωπικού φακέλου γίνεται γράφοντας τη διεύθυνση του διακομιστή και στη συνέχεια εισάγοντας την περισπωμένη ακολουθούμενη από το όνομα χρήστη. Για παράδειγμα **http://192.168.1.201/~adminuser**

7.4 Εγκατάσταση και ρύθμιση διακομιστή αρχείων (FTP Server)

Το File Transfer Protocol (FTP) είναι ένα πρωτόκολλο που επιτρέπει τη μεταφορά αρχείων μεταξύ υπολογιστών. Δυστυχώς, η επικοινωνία μεταξύ των υπολογιστών δεν κρυπτογραφείται με αποτέλεσμα να μην προσφέρει καμία ασφάλεια. Αν θέλουμε να κάνουμε ασφαλείς μεταφορές αρχείων μεταξύ δύο υπολογιστών, είναι προτιμότερο να χρησιμοποιήσουμε το πρωτόκολλο SSH.

Σε ένα διακομιστή αρχείων μπορούμε να έχουμε πρόσβαση είτε με τη χρήση κάποιου λογαριασμού είτε ανώνυμα (χωρίς τη χρήση λογαριασμού).

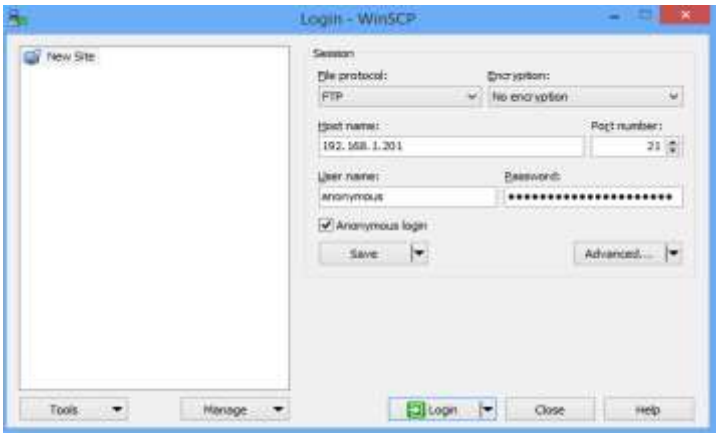
Για την εγκατάσταση ενός από τους πιο δημοφιλής διακομιστές αρχείων που είναι ο vsftpd, γράφουμε **sudo apt-get install vsftpd**.

7.4.1 Πρόσβαση χωρίς λογαριασμό

Για να έχουμε τη δυνατότητα ανώνυμης πρόσβασης πρέπει να κάνουμε μια ρύθμιση στο αρχείο ρυθμίσεων του διακομιστή αρχείων. Γράφουμε λοιπόν **sudo nano /etc/vsftpd.conf** και τροποποιούμε τη γραμμή **anonymous_enable** αλλάζοντας το **No** σε **Yes.** Έτσι θα πρέπει να είναι **anonymous_enable=Yes.** Αποθηκεύουμε πατώντας **Ctrl+X** και **Y.** Για να εφαρμοστούν οι αλλαγές πρέπει να επανεκκινήσουμε το διακομιστή αρχείων με την εντολή **sudo restart vsftpd**

Ο φάκελος στον οποίο αποθηκεύονται τα αρχεία του διακομιστή αρχείων, όταν η σύνδεση είναι ανώνυμη, είναι ο **/srv/ftp**

Τώρα μπορούμε να συνδεθούμε στο διακομιστή αρχείων με ένα πρόγραμμα πελάτη FTP, όπως το WinSCP (http://winscp.net/eng/index.php) ή το Filezilla (https://filezilla-project.org/).



Εικόνα 7.40: Ανώνυμη σύνδεση στο διακομιστή αρχείων με FTP

7.4.2 Πρόσβαση με λογαριασμό

Από προεπιλογή η πρόσβαση στο διακομιστή αρχείου με χρήση λογαριασμού είναι ενεργή. Έτσι, αρκεί να ανοίξουμε έναν πελάτη FTP και να εισάγουμε τα στοιχεία του λογαριασμού και τη διεύθυνση του διακομιστή.

Εικόνα 7.41: Σύνδεση με χρήση λογαριασμού στο διακομιστή αρχείων

Αφού πραγματοποιηθεί η σύνδεση, ο φάκελος στον οποίο θα έχουμε πρόσβασης είναι ο προσωπικός μας φάκελος στο διακομιστή.

7.5 Εγκατάσταση και ρύθμιση διακομιστή εικονικού δικτύου υπολογιστών (VNC Server)

Η εγκατάσταση ενός διακομιστή, τις περισσότερες φορές, δεν περιλαμβάνει την εγκατάσταση γραφικού περιβάλλοντος. Μερικές φορές όμως θέλουμε να έχουμε τη δυνατότητα να συνδεθούμε απομακρυσμένα στο διακομιστή μας σε ένα γραφικό περιβάλλον. Για αυτό το λόγο θα εγκαταστήσουμε ένα μινιμαλιστικό γραφικό περιβάλλον στο διακομιστή μας, καθώς επίσης και το λογισμικό **tightvnc** το οποίο μας επιτρέπει να συνδεόμαστε απομακρυσμένα στο διακομιστή για να τον χρησιμοποιήσουμε μέσω γραφικού περιβάλλοντος. Η εντολή που θα πληκτρολογήσουμε για την εγκατάσταση είναι **sudo apt-get install install xfce4 xfce4-goodies tightvncserver.**

Μετά την εγκατάσταση θα πρέπει να εκτελέσουμε την εντολή **vncserver** για να ολοκληρωθεί η αρχική ρύθμιση του **tightvncserver.** Θα μας ζητήσει να εισάγουμε έναν κωδικό πρόσβασης ο οποίος δεν μπορεί να είναι μικρότερος από 8 χαρακτήρες. Για ευκολία εισάγουμε το 12345678.

Στη συνέχεια θα πρέπει να κάνουμε κάποιες επιπλέον ρυθμίσεις στο διακομιστή VNC. Πρώτα όμως θα πρέπει να σταματήσουμε τη λειτουργία του με την εντολή **vncserver –kill :1**. Θα δημιουργήσουμε ένα αντίγραφο των αρχικών ρυθμίσεων του διακομιστή VNC με την εντολή **mv home/adminuser/.vnc/xstartup /home/adminuser/.vnc/xstartup.bak** σε περίπτωση που το χρειαστούμε αργότερα**.** Θα δημιουργήσουμε ένα καινούριο αρχείο ρυθμίσεων με την εντολή **nano /home/adminuser/.vnc/xstartup** και περιεχόμενο το παρακάτω:

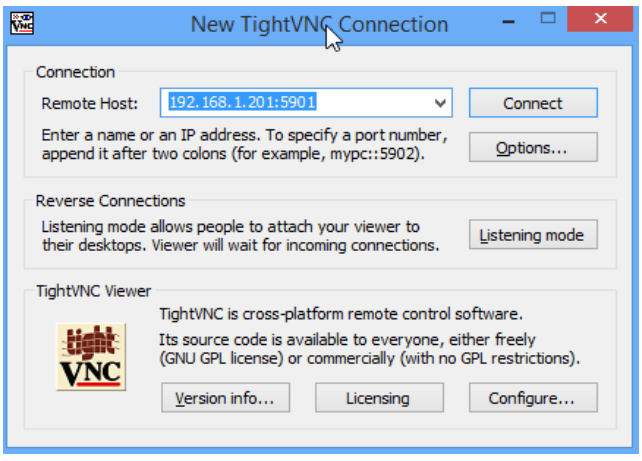
#!/bin/bash

xrdb $HOME/.Xresources

startxfce4 &

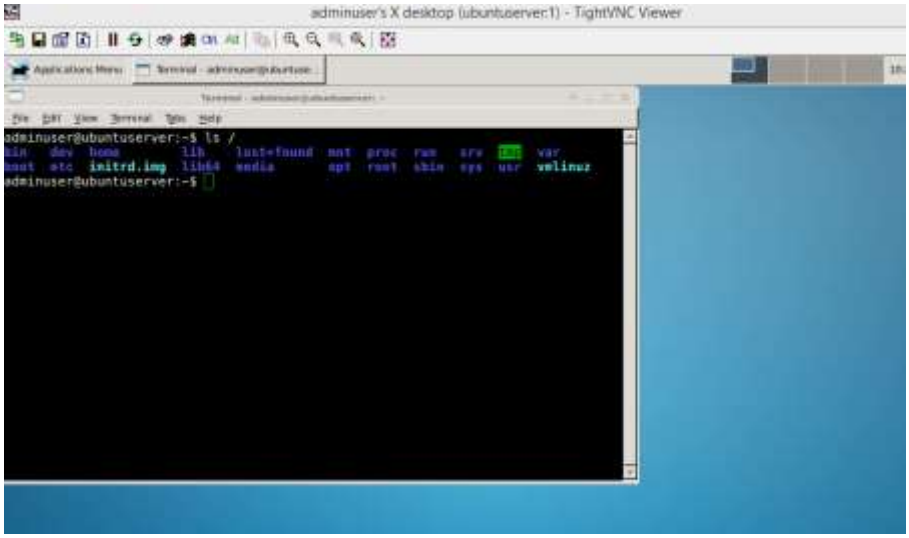
Αποθηκεύουμε πατώντας Ctrl+X και στη συνέχεια Y. Τέλος, θα πρέπει να κάνουμε εκτελέσιμο το παραπάνω αρχείο με την εντολή **sudo chmod +x /home/adminuser/.vnc/xstartup.** Αυτή τη στιγμή είμαστε έτοιμοι να εκτελέσουμε το διακομιστή VNC με την εντολή **vncserver**.

Για τη σύνδεση από έναν υπολογιστή με λειτουργικό σύστημα Windows στο διακομιστή θα πρέπει να εγκαταστήσουμε ένα πρόγραμμα πελάτη VNC. Ένα από τα πιο γνωστά είναι το TightVNC (http://www.tightvnc.com/). Αφού τρέξουμε το TightVNC Viewer θα εισαγάγουμε τη διεύθυνση του διακομιστή και τη θύρα 5901 και θα πατήσουμε το κουμπί **Connect.** Θα μας ζητήσει να εισάγουμε και τον κωδικό πρόσβασης (στην περίπτωση μας 12345678).



Εικόνα 7.42: Σύνδεση στο διακομιστή VNC

Μετά την επιτυχή εισαγωγή του κωδικού πρόσβασης θα ανοίξει ένα παράθυρο μέσω του οποίου μπορούμε να χειριστούμε το διακομιστή με το γραφικό περιβάλλον xfce.



Εικόνα 7.43: Γραφικό περιβάλλον διακομιστή μέσα από τον πελάτη VNC

7.6 Εγκατάσταση και ρύθμιση διακομιστή διαμεσολάβησης (Proxy Server)

Ο διακομιστής διαμεσολάβησης είναι ένα λογισμικό το οποίο επιταχύνει την πρόσβαση σε ιστοσελίδες του Διαδικτύου. Η λειτουργία του βασίζεται στην ύπαρξη ενός προσωρινού αποθηκευτικού χώρου, στον οποία γίνεται αποθήκευση των ιστοσελίδων που έχουν ανακτηθεί πρόσφατα από άλλους χρήστες. Έτσι, αν κάποιος άλλος χρήστης ζητήσει μια ιστοσελίδα που βρίσκεται στην προσωρινή μνήμη, ο διακομιστής διαμεσολάβησης θα τον εξυπηρετήσει και δεν θα χρειαστεί να κατέβει η ιστοσελίδα από το Διαδίκτυο.

Ο διακομιστής διαμεσολάβησης μπορεί να παίξει και το ρόλο του φίλτρου διευθύνσεων Διαδικτύου. Πιο συγκεκριμένα, με κατάλληλες ρυθμίσεις μπορούμε να περιορίσουμε την πρόσβαση σε ορισμένες ιστοσελίδες ή και δίκτυα, κάτι που δεν θα κάνουμε όμως, γιατί είναι μια αρκετά σύνθετη εργασία.

Για την εγκατάσταση του πιο γνωστού διακομιστή διαμεσολάβησης που είναι το Squid γράφουμε την εντολή **sudo apt-get install squid3.**

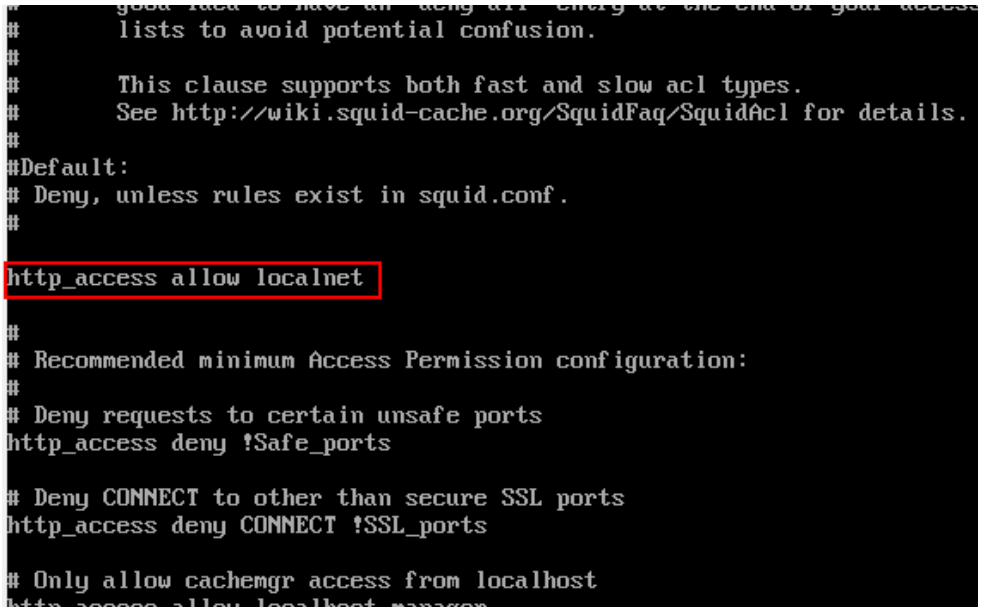
Για να λειτουργήσει ο διακομιστής διαμεσολάβησης πρέπει να κάνουμε μερικές ρυθμίσεις. Έτσι γράφουμε **sudo nano –c /etc/squid3/squid.conf** και μεταφέρουμε το δρομέα περίπου στη γραμμή 900 (Ο αριθμός της γραμμής προβάλλεται στο κάτω τμήμα του παραθύρου). Σ' αυτό το σημείο θα αλλάξουμε τα περιεχόμενα όπως στην επόμενη εικόνα.

```
#Default:
# ACLs all, manager, localhost, and to_localhost are predefined.
#
#
# Recommended minimum configuration:
#

# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
#acl localnet src 10.0.0.0/8     # RFC1918 possible internal network
#acl localnet src 172.16.0.0/12  # RFC1918 possible internal network
acl localnet src 192.168.1.0/24  # RFC1918 possible internal network
#acl localnet src fc00::/7       # RFC 4193 local private network range
#acl localnet src fe80::/10      # RFC 4291 link-local (directly plugge
```

Εικόνα 7.44: Πρώτη ρύθμιση διακομιστή διαμεσολάβησης

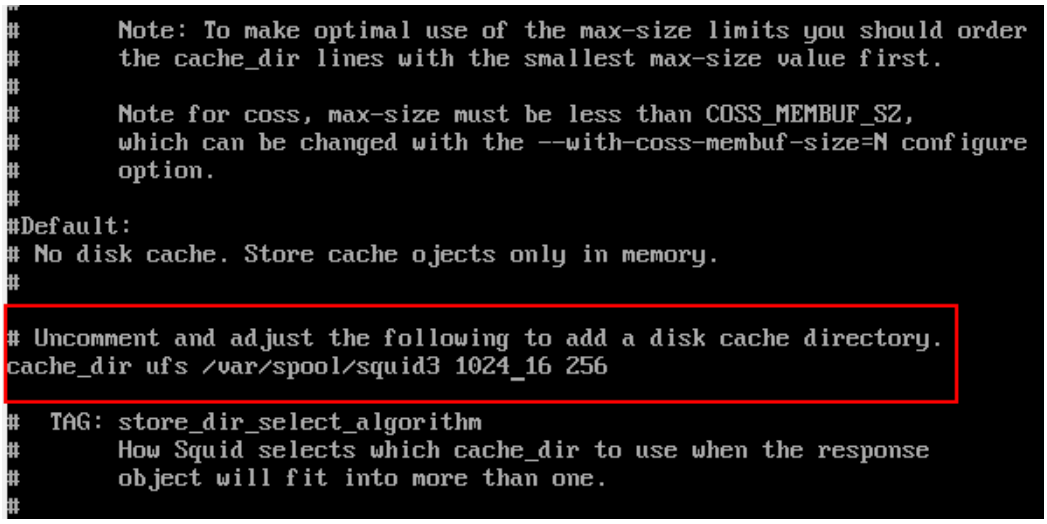
Η ρύθμιση που κάναμε καθορίζει το δίκτυο (στην περίπτωσή μας όλο το εσωτερικό δίκτυο) από το οποίο θα δέχεται ο διακομιστής διαμεσολάβησης αιτήσεις. Στη συνέχεια, θα

μεταφέρουμε το δρομέα στη γραμμή 1030 και θα προσθέσουμε την εντολή **http_access allow localnet**.



Εικόνα 7.45: Δεύτερη ρύθμιση διακομιστή διαμεσολάβησης

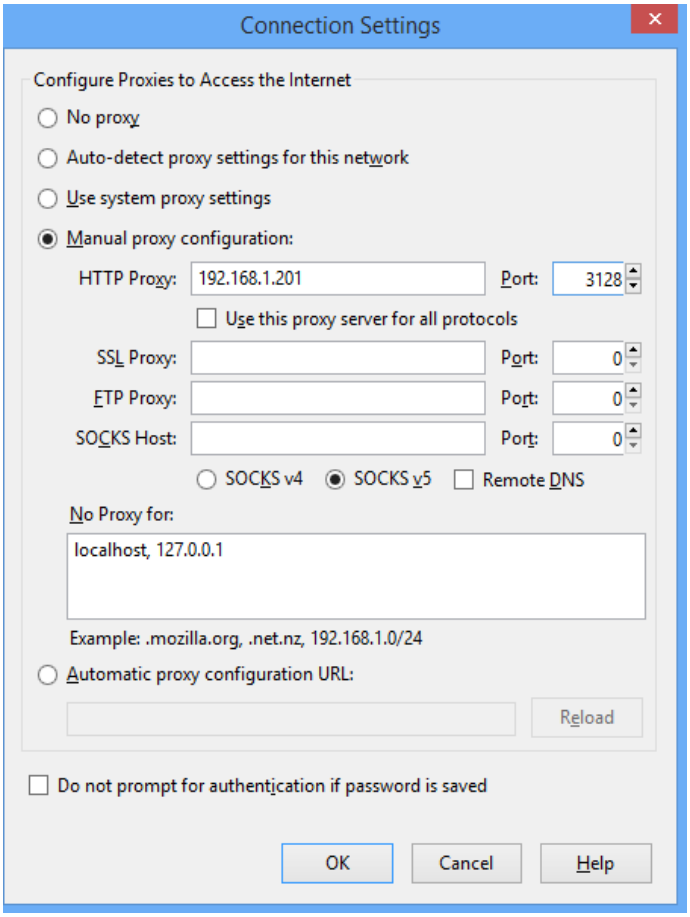
Με αυτήν τη ρύθμιση ανοίγουμε την πρόσβαση στους υπολογιστές που βρίσκονται στο δίκτυο που ορίσαμε πιο πάνω. Τέλος, θα πρέπει να ορίσουμε το μέγεθος και την τοποθεσία του φακέλου που θα χρησιμοποιείται για την προσωρινή αποθήκευση των ιστοσελίδων. Για αυτό το λόγο μεταφέρουμε το δρομέα στη γραμμή 3000 και αλλάζουμε τα περιεχόμενα σύμφωνα με την παρακάτω εικόνα.



Εικόνα 7.46: Καθορισμός θέσης και μεγέθους φακέλου προσωρινής αποθήκευσης

Αποθηκεύουμε το αρχείο ρυθμίσεων πατώντας **Ctrl+X** και **Y.** Για να εφαρμοστούν οι αλλαγές πρέπει να επανεκκινήσουμε το διακομιστή διαμεσολάβησης με την εντολή **sudo service squid3 restart**. Αυτή τη στιγμή ο διακομιστή διαμεσολάβησης είναι ενεργός και ρυθμισμένος έτσι ώστε να δέχεται αιτήσεις από όλους τους υπολογιστές του δικτύου 192.168.1.0/24.

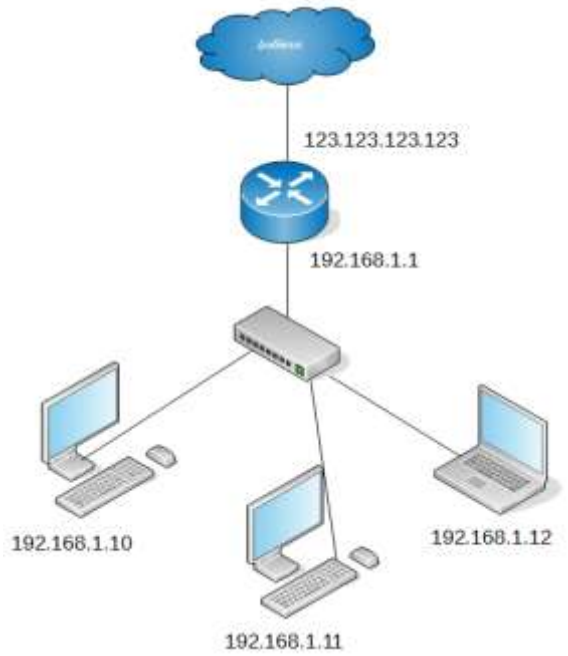
Για να χρησιμοποιήσουμε το διακομιστή διαμεσολάβησης σε ένα φυλλομετρητή, πρέπει να αλλάξουμε τις ρυθμίσεις του. Για το Firefox θα πρέπει να επιλέξουμε **Tools->Options** και από την πλευρική στήλη **Advanced.** Στη συνέχεια επιλέγουμε **Network** και αφού πατήσουμε **Settings** ρυθμίζουμε όπως στην παρακάτω εικόνα.



Εικόνα 7.47: Ρυθμίσεις διακομιστή διαμεσολάβησης

7.6.1 Προώθηση θύρας (Port Forward)

Κάθε ένας δρομολογητής έχει μια εξωτερική διεύθυνση IP την οποία παίρνει από τον πάροχο υπηρεσιών Διαδικτύου (ISP – Internet Service Provider) και μια εσωτερική την οποία αποδίδει ο κατασκευαστής του δρομολογητή. Η εξωτερική IP χρησιμοποιείται για την αλληλεπίδραση με άλλους υπολογιστές που βρίσκονται συνδεδεμένοι στο Διαδίκτυο, ενώ η εσωτερική διεύθυνση χρησιμοποιείται για την επικοινωνία με τους υπολογιστές του εσωτερικού δικτύου που ανήκει ο δρομολογητής.



Εικόνα 7.48: Δομή ενός απλού δικτύου

Ο δρομολογητής αναλαμβάνει να διεκπεραιώσει την αποστολή και λήψη δεδομένων από τους υπολογιστές του εσωτερικού δικτύου προς το Διαδίκτυο. Πρακτικά, όταν ένας υπολογιστής από το εσωτερικό δίκτυο ζητήσει μια ιστοσελίδα, τότε ο δρομολογητής αναλαμβάνει να στείλει το ανάλογο αίτημα στον απομακρυσμένο υπολογιστή και αφού λάβει την απάντησή του να την προωθήσει στον υπολογιστή του εσωτερικού δικτύου. Η αποστολή των δεδομένων στο σωστό υπολογιστή του εσωτερικού δικτύου πραγματοποιείται εύκολα από τη στιγμή που έχει μια μοναδική εσωτερική διεύθυνση IP.

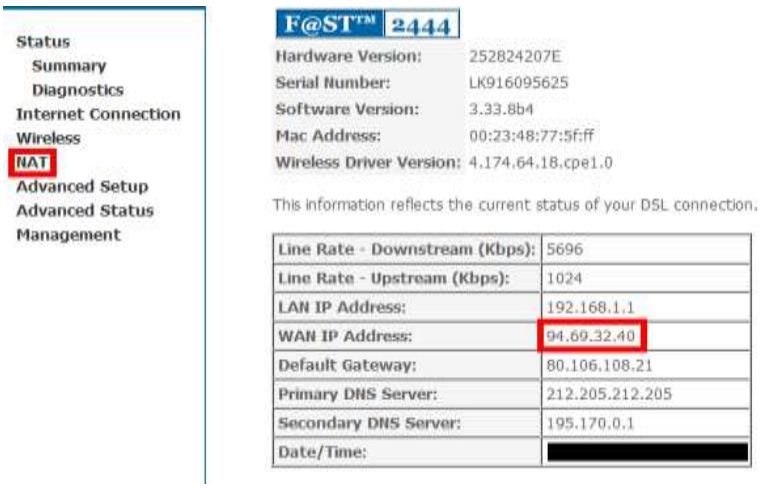
7.6.2 Θύρες

Η παραπάνω διαδικασία αποστολής και λήψης δεδομένων από το δρομολογητή υποβοηθείται από την έννοια της θύρας. Κάθε φορά που πραγματοποιείται ανάκτηση μια ιστοσελίδας τα δεδομένα μεταφέρονται μέσω της θύρας 80 ή στην περίπτωση της σύνδεσης με SSH τα δεδομένα μεταφέρονται μέσω της θύρας 22. Η θύρα δεν είναι υλικό, αλλά μια έννοια που προσδιορίζει μια υπηρεσία. Ο οργανισμός IANA (Internet Assigned Numbers Authority) έχει ορίσει μια λίστα, στην οποία καθορίζεται η υπηρεσία που παρέχει κάθε μια θύρα από το 0 μέχρι το 1024.

Αν ένας υπολογιστής που βρίσκεται στο Διαδίκτυο προσπαθήσει να προσπελάσει ένα στοιχείο που βρίσκεται σε υπολογιστή στο εσωτερικό δίκτυο, η αίτηση δεν θα ικανοποιηθεί γιατί ο δρομολογητής δεν ξέρει σε ποιον υπολογιστή απευθύνεται η αίτηση. Ευτυχώς, με την τεχνική προώθησης θύρας, έχουμε τη δυνατότητα να ορίσουμε από το διαχειριστικό περιβάλλον του δρομολογητή να προωθεί σε συγκεκριμένη διεύθυνση του εσωτερικού δικτύου όλα τα πακέτα μιας υπηρεσίας. Η υπηρεσία αναγνωρίζεται από τον αριθμό της θύρας. Έτσι για παράδειγμα, αν στο εσωτερικό μας δίκτυο έχουμε έναν διακομιστή ιστοσελίδων (θύρα 80) με διεύθυνση 192.168.1.201 αρκεί να δηλώσουμε στο δρομολογητή να προωθεί τα δεδομένα της θύρας 80 από το Διαδίκτυο στην εσωτερική διεύθυνση 192.168.1.201.

Επειδή ο κάθε ένας δρομολογητής έχει το δικό του περιβάλλον διαχείρισης, όταν θέλουμε να κάνουμε αυτήν τη διαδικασία καλό θα είναι να ανατρέχουμε στο εγχειρίδιο χρήσης του. Παρακάτω μπορούμε να δούμε σε εικόνες ένα παράδειγμα.

Ανοίγουμε έναν φυλλομετρητή και εισάγουμε στη γραμμή διευθύνσεων την εσωτερική διεύθυνση του δρομολογητή (πιθανόν 192.168.1.1). Φυσιολογικά θα μας ζητήσει να εισάγουμε το όνομα χρήστη και τον κωδικό πρόσβασης του διαχειριστή. Αφού τα εισάγουμε θα βρεθούμε σε μια οθόνη όπως η παρακάτω.

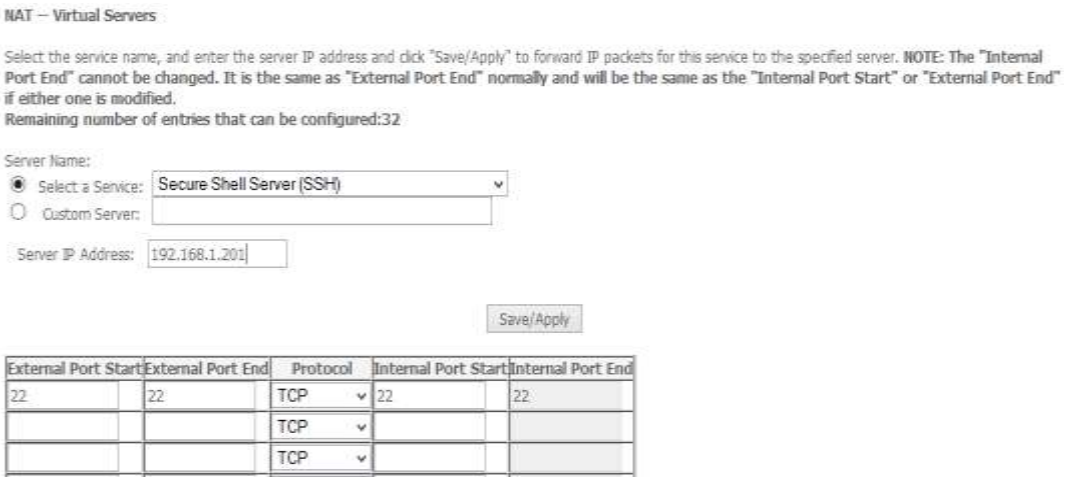


Εικόνα 7.49: Πρώτη οθόνη μετά τη σύνδεση στο περιβάλλον διαχείρισης του δρομολογητή

Εκτός των άλλων μπορούμε να δούμε την εξωτερική διεύθυνση IP του δρομολογητή. Από την αριστερή στήλη επιλέγουμε **NAT** και στη συνέχεια πατάμε το κουμπί Add.

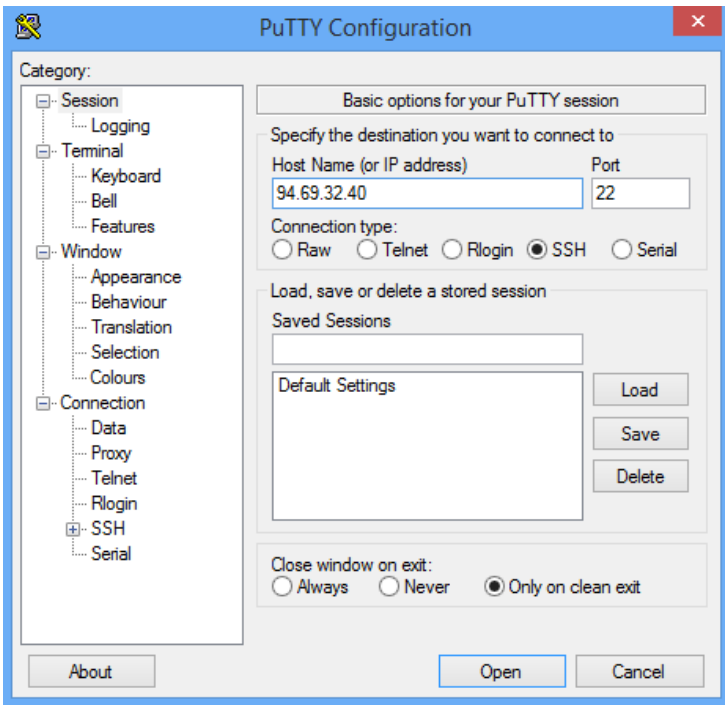
Εικόνα 7.50: Προώθηση θύρας

Ο στόχος μας είναι να αποκτήσουμε απομακρυσμένη πρόσβαση μέσω SSH στο διακομιστή μας. Άρα, θα πρέπει να προωθήσουμε τη θύρα 22 στη διεύθυνση 192.168.1.201 που είναι η διεύθυνση του διακομιστή.



Εικόνα 7.51: Προώθηση θύρας 22 στη διεύθυνση 192.168.1.201

Πατώντας **Save** γίνεται αποθήκευση της ρύθμισης. Πλέον, αν ανοίξουμε το putty από οποιονδήποτε υπολογιστή που βρίσκεται στο Διαδίκτυο και εισάγουμε σαν διεύθυνση την εξωτερική διεύθυνση του δρομολογητή, θα μπορούμε να συνδεθούμε στο διακομιστή.



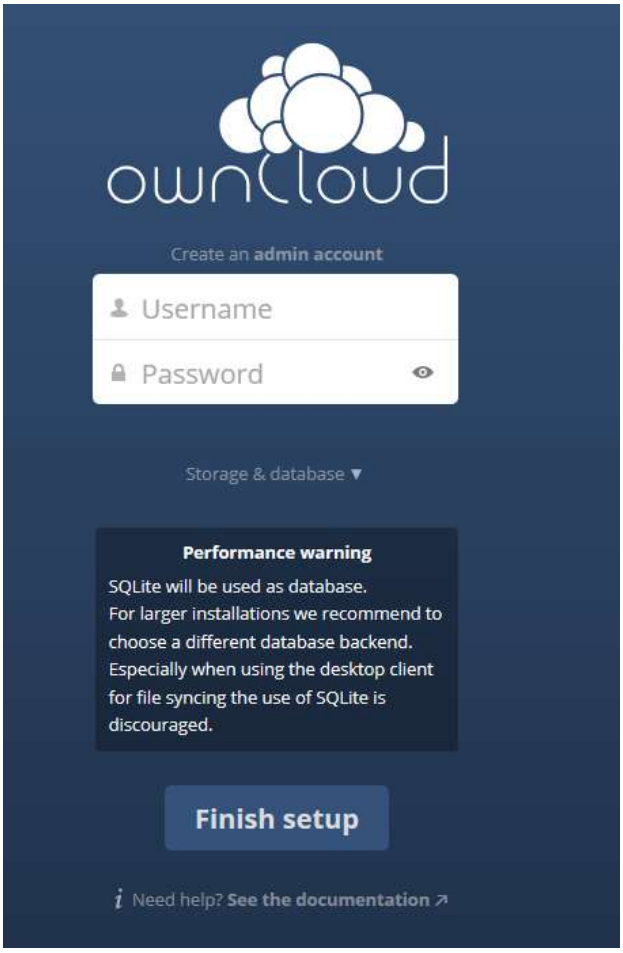
Εικόνα 7.52: Σύνδεση με SSH μετά από προώθηση θύρας

7.7 Εφαρμογές Δικτυακών Μέσων Αποθήκευσης (Cloud Computing)

Αν θέλουμε να δημιουργήσουμε το προσωπικό μας σύννεφο (cloud) έχουμε τη δυνατότητα εγκαθιστώντας το λογισμικό ownCloud (https://owncloud.org/). Επειδή το ownCloud δεν βρίσκεται σε κάποιο από τα ήδη υπάρχοντα αποθετήρια λογισμικού, θα χρειαστεί να το προσθέσουμε με την παρακάτω διαδικασία.

- sudo sh -c "echo 'deb http://download.opensuse.org/repositories/isv:/ownCloud:/community/xUbuntu_14.04/ /' >> /etc/apt/sources.list.d/owncloud.list"
- wget http://download.opensuse.org/repositories/isv:ownCloud:community/xUbuntu_14.04/Release.key
- sudo apt-key add - < Release.key
- sudo apt-get update
- sudo apt-get install owncloud

Το επόμενο βήμα είναι να ανοίξουμε έναν φυλλομετρητή και να εισάγουμε τη διεύθυνση http://192.168.1.201/owncloud. Θα δούμε την παρακάτω εικόνα, μέσω της οποίας θα δημιουργήσουμε το διαχειριστή του ownCloud εισάγοντας το όνομα χρήστη (admin) και τον κωδικό πρόσβασης (1234). Τέλος θα πρέπει να πατήσουμε του πλήκτρο **Finish Setup**.



Εικόνα 7.53: Αρχική οθόνη μετά την εγκατάσταση του ownCloud

Μετά την ολοκλήρωση της εγκατάστασης και σε συνδυασμό με την εφαρμογή συγχρονισμού (https://owncloud.org/install/#install-clients), έχουμε στη διάθεσή μας ένα λογισμικό που είναι αντίστοιχο σε λειτουργίες και ευκολία χρήσης με το Dropbox ή το Google Drive, έχοντας βέβαια ενεργοποιήσει και την προώθηση της θύρας 80.

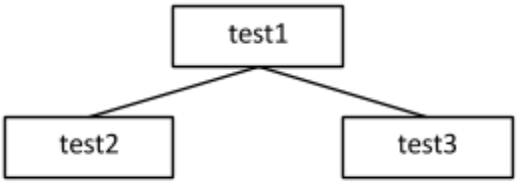
Ερωτήσεις Ανακεφαλαίωσης

1. Ποιοι λόγοι μας οδηγούν στην εγκατάσταση και ρύθμιση δικού μας διακομιστή;
2. Ποιος είναι ο λόγος δημιουργίας του δικού μας σύννεφου;
3. Τι είναι η προώθηση πόρτας και για ποιο λόγο την χρησιμοποιούμε;
4. Ποιος είναι ο ρόλος του διακομιστή διαμεσολάβησης;

Ασκήσεις

Άσκηση 1η

Αφού συνδεθείτε στο διακομιστή δημιουργήστε την παρακάτω ιεραρχική δομή φακέλων μέσα στον προσωπικό σας φάκελο.



Διαγράψτε το φάκελο test2.
Διαγράψτε το φάκελο test1.

Άσκηση 2η

Άσκηση στον FTP Server.

Αφού συνδεθείτε ανώνυμα στο διακομιστή αρχείων, να ανεβάσετε (upload) και να κατεβάσετε (download) μερικά αρχεία.

Άσκηση 3η

Άσκηση στον FTP Server.

Αφού συνδεθείτε με τη χρήση λογαριασμού στο διακομιστή αρχείων, να ανεβάσετε (upload) και να κατεβάσετε (download) μερικά αρχεία.

Να δημιουργήσετε στον προσωπικό σας υπολογιστή μια ιστοσελίδα και να την ανεβάσετε στο φάκελο public_html του προσωπικού σας φακέλου. Δείτε την ιστοσελίδα από τον προσωπικό σας υπολογιστή χρησιμοποιώντας έναν φυλλομετρητή.

adduser ονομα_χρήστη.

Βιβλιογραφία

Barnett, J. (2014, October 23). *How to Install and Configure VNC on Ubuntu 14.04.* Ανάκτηση από https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-vnc-on-ubuntu-14-04.

ownCloud. (2015). *ownCloud Documentation Overview.* Ανάκτηση από https://doc.owncloud.org/.

Shotts, W. (2013, July 6). *The Linux Command Line.* Ανάκτηση από http://sourceforge.net/projects/linuxcommand/files/TLCL/13.07/TLCL-13.07.pdf/download.

Timme, F. (2014). *The Perfect Server - Ubuntu 14.04.* Ανάκτηση από https://www.howtoforge.com/perfect-server-ubuntu-14.04-apache2-php-mysql-pureftpd-bind-dovecot-ispconfig-3.

Ubuntu. (2014). *Ubuntu Server Guide.* Ανάκτηση από https://help.ubuntu.com/lts/serverguide/serverguide.pdf.

Κεφάλαιο 8ο

Ασφάλεια Δεδομένων και Δικτύων

Εισαγωγή

Στο κεφάλαιο αυτό θα γίνει μια παρουσίαση των κυριότερων μεθόδων που χρησιμοποιούνται για την παραβίαση της ασφάλειας ενός υπολογιστικού συστήματος ή δικτύου, καθώς και των τρόπων με τους οποίους οι χρήστες και οι διαχειριστές δικτύων μπορούν να προστατεύσουν τα συστήματά τους, τα δεδομένα τους και τα προσωπικά τους στοιχεία.

Διδακτικοί Στόχοι

Με την ολοκλήρωση του 8ου κεφαλαίου οι μαθητές θα πρέπει να είναι σε θέση να:

- Εξηγούν τις πιο συνηθισμένες μεθόδους παραβίασης ενός υπολογιστικού συστήματος και τα αποτελέσματα που αυτές μπορεί να επιφέρουν.
- Χρησιμοποιούν έλεγχο ταυτότητας κωδικών ασφαλείας στα ΛΣ.
- Χρησιμοποιούν εφαρμογές των μεθόδων συμμετρικής κρυπτογράφησης.
- Διατυπώνουν τα πλεονεκτήματα και τα μειονεκτήματα των μεθόδων κρυπτογράφησης.
- Δημοσιεύουν δημόσια κλειδιά σε Εξυπηρετητές Δημόσιων Κλειδιών και να δημιουργούν Δίκτυο εμπιστοσύνης.
- Περιγράφουν τα βασικά χαρακτηριστικά των ψηφιακών υπογραφών, των ψηφιακών πιστοποιητικών, της Στεγανογραφίας και της Στεγανάλυσης.
- Ανταλλάσσουν μηνύματα με χρήση Ασυμμετρικής Κρυπτογράφησης.
- Αποκρύπτουν μηνύματα μέσα σε ένα αρχείο πολυμέσων.
- Χρησιμοποιούν το Κρυπτογραφημένο Σύστημα Αρχείων των Windows για να κρυπτογραφούν αρχεία.
- Διακρίνουν τις κατηγορίες Τείχους Προστασίας και να ρυθμίζουν τόσο το Τείχος Προστασίας ενός Η/Υ όσο και του δρομολογητή.
- Εγκαθιστούν και να ρυθμίζουν τις ειδικές διανομές Τείχους Προστασίας Linux.
- Να απαριθμούν τα βασικά χαρακτηριστικά των Εικονικών Ιδιωτικών Δικτύων.
- Επεξηγούν τη χρήση του Ανώνυμου Διακομιστή Μεσολάβησης και του Συστήματος Tor.
- Εφαρμόζουν στην πράξη μεθόδους και τεχνικές ασφαλείας ανάλογα με τις προδιαγραφές, τις ανάγκες και την εκάστοτε περίπτωση σχεδιασμένου δικτύου.

Διδακτικές Ενότητες

8.1 Μέθοδοι Επίθεσης σε Υπολογιστικά Συστήματα και Δίκτυα

Ακολουθεί μια συνοπτική περιγραφή των πιο συνηθισμένων τρόπων επίθεσης σε υπολογιστικά συστήματα και δίκτυα. Ο κατάλογος δεν είναι σε καμία περίπτωση πλήρης,

καθώς τόσο η πρόοδος της τεχνολογίας, όσο και η ανεξάντλητη ανθρώπινη εφευρετικότητα, εμπλουτίζουν καθημερινά το οπλοστάσιο των επιτιθέμενων με νέα εργαλεία.

8.1.1 Μεταμφίεση IP Διευθύνσεων (IP Spoofing)

Οι επιθέσεις αυτού του τύπου έχουν σαν στόχο την αλλαγή της IP διεύθυνσης των πακέτων που αποστέλλει κάποιος υπολογιστής, προκειμένου να δίνεται η εντύπωση ότι αυτά προέρχονται από έναν διαφορετικό υπολογιστή απ' ότι στην πραγματικότητα. Αυτό γίνεται με την αντικατάσταση της διεύθυνσης προέλευσης που αναγράφεται στην IP επικεφαλίδα των πακέτων που στέλνει ο επιτιθέμενος.

Το σύστημα που παραλαμβάνει τα πακέτα δεν γνωρίζει ότι η διεύθυνση αποστολέα που αναγράφεται στην κεφαλίδα είναι πλαστογραφημένη, οπότε απαντάει στέλνοντας πακέτα IP στην ψεύτικη διεύθυνση. Αυτό σημαίνει ότι ο επιτιθέμενος δεν λαμβάνει την απάντηση που στέλνει ο υπολογιστής στόχος, άρα η τεχνική αυτή εφαρμόζεται κυρίως σε επιθέσεις τύπου Άρνησης Υπηρεσίας, προσφέροντας και το επιπλέον πλεονέκτημα ότι αποκρύπτεται η πραγματική διεύθυνση του επιτιθέμενου.

8.1.2 Μεταμφίεση MAC Διευθύνσεων (MAC Address Spoofing)

Μία άλλη πολύ συνηθισμένη μέθοδος επίθεσης είναι η αλλαγή της φυσικής (MAC) διεύθυνσης της κάρτας δικτύου του επιτιθέμενου σε τιμή διαφορετική από αυτήν που στην πραγματικότητα έχει. Επειδή η φυσική διεύθυνση είναι καταχωρημένη στη μνήμη ROM της κάρτας δικτύου και δεν μπορεί να αλλάξει, αυτό που στην πραγματικότητα συμβαίνει είναι ότι αλλάζει η διεύθυνση που αναφέρει το λειτουργικό σύστημα και όχι η πραγματική διεύθυνση της κάρτας δικτύου.

Με την τεχνική αυτή γίνεται δυνατή η αποφυγή κανόνων περιορισμού των συσκευών που μπορούν να συνδεθούν σε π.χ. ένα ασύρματο δίκτυο, έχει όμως το μειονέκτημα ότι ο επιτιθέμενος θα πρέπει να έχει γνώση των επιτρεπόμενων διευθύνσεων ενός δικτύου. Σε αντίθεση με τη μεταμφίεση των IP διευθύνσεων ο επιτιθέμενος συνήθως ενδιαφέρεται να λάβει την απάντηση του στόχου, οπότε η τεχνική αυτή χρησιμοποιείται κυρίως για επιθέσεις τύπου Man-In-The-Middle.

[Ασκήσεις 1 και 2]

8.1.3 Κρυπταναλυτικές Επιθέσεις

Πρόκειται για επιθέσεις με τις οποίες γίνεται προσπάθεια να αποκρυπτογραφηθεί ένα κρυπτογραφημένο μήνυμα (κωδικός πρόσβασης, αρχείο κειμένου ή δεδομένων), χωρίς να είναι γνωστό το κλειδί με το οποίο κανονικά θα γίνονταν η αποκρυπτογράφηση. Ο τρόπος με τον οποίο γίνονται επιθέσεις αυτού του τύπου διαφέρει ανάλογα με το είδος της κρυπτογράφησης που έχει χρησιμοποιηθεί (συμμετρική, δημόσιου-ιδιωτικού κλειδιού, συνάρτηση κερματισμού κ.λ.π.)

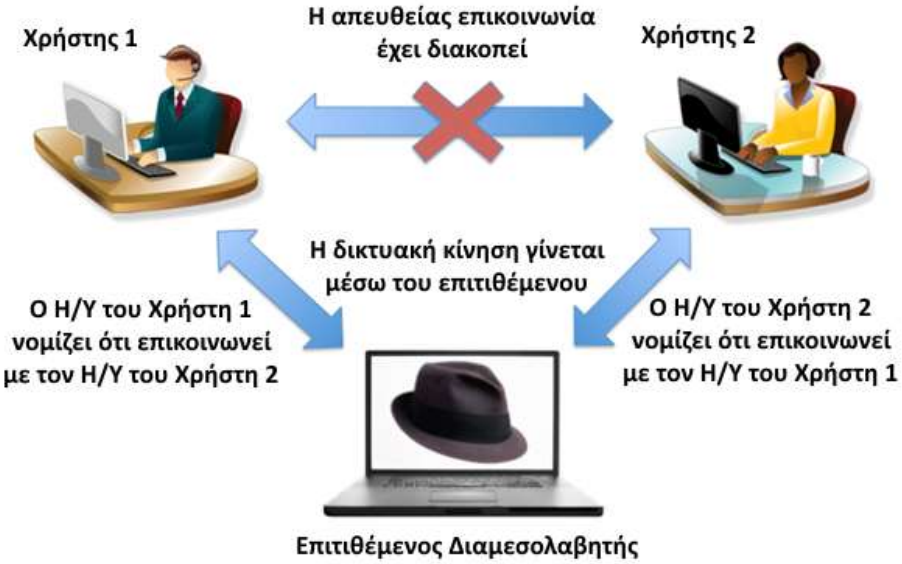
8.1.3.1 Επιθέσεις ωμής βίας ή εξαντλητική αναζήτηση κλειδιού (Brute-force attacks)

Χρησιμοποιούνται κατά κύριο λόγο όταν ο επιτιθέμενος χρειάζεται να δοκιμάσει όλους τους διαφορετικούς συνδυασμούς πιθανών κλειδιών μέχρι να ανακαλύψει τον κωδικό που ψάχνει. Είναι οι πιο χρονοβόρες μέθοδοι επίθεσης, αφού ακόμα και ένας υπερυπολογιστής ή μία συστοιχία υπολογιστών μπορεί να χρειαστεί δισεκατομμύρια χρόνια προκειμένου να εντοπίσει έναν κωδικό, αρκεί αυτός να είναι μεγάλος και σύνθετος. Οι επιθέσεις αυτού του τύπου φέρνουν συνήθως αποτέλεσμα όταν ένας κωδικός αποτελείται από λίγους χαρακτήρες, από ένα περιορισμένο σύνολο (π.χ. μόνο πεζά γράμματα ή μόνο αριθμοί). Όταν το πλήθος των χαρακτήρων είναι μεγάλο και η πολυπλοκότητά του αυξημένη, ο αριθμός των

πιθανών συνδυασμών γίνεται αστρονομικός και απαγορευτικός ακόμη και για τα πιο προηγμένα σύγχρονα συστήματα.

8.1.3.2 Διαμεσολαβητής (Man in the Middle-MitM)

Στην περίπτωση αυτή ο επιτιθέμενος παρεμβάλλεται στην επικοινωνία μεταξύ δύο κόμβων, παρακολουθώντας ή και αλλοιώνοντας τις πληροφορίες που ανταλλάσσονται. Ο επιτιθέμενος παραπλανεί τους κόμβους που επικοινωνούν και ενώ αυτοί πιστεύουν ότι επικοινωνούν άμεσα, στην πράξη όλη η κίνηση γίνεται μέσω του κόμβου του επιτιθέμενου, όπως φαίνεται στην επόμενη εικόνα.



Εικόνα 8.1: Επίθεση Διαμεσολαβητή

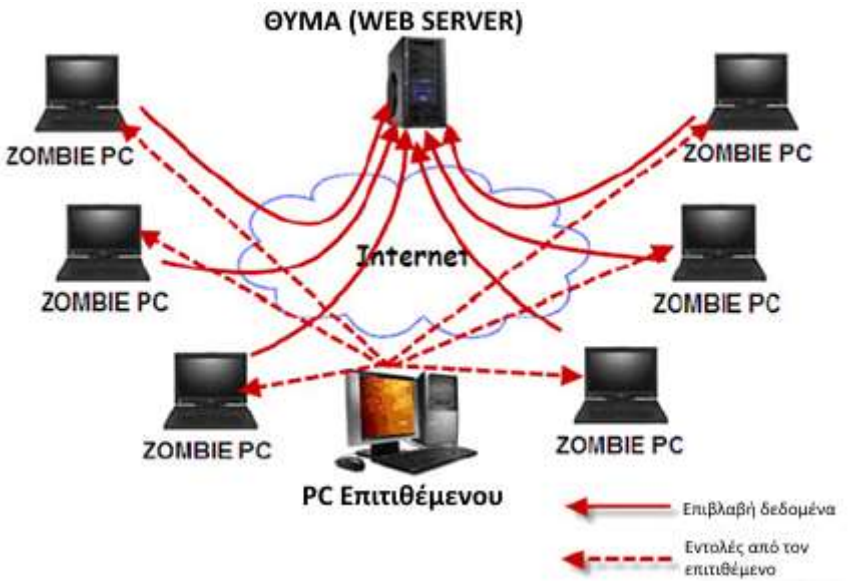
(Τροποποιημένη από: http://www.carmelowalsh.com/wp-content/uploads/2015/03/mitm.png)

Οι επιθέσεις αυτού του τύπου αποτελούν σοβαρή απειλή για την ασφάλεια της on-line επικοινωνίας, καθώς δίνουν στον επιτιθέμενο τη δυνατότητα να υποκλέπτει και να τροποποιεί ευαίσθητα δεδομένα σε πραγματικό χρόνο, ενώ ταυτόχρονα παρουσιάζεται σαν πιστοποιημένο μέλος μιας συνομιλίας, συναλλαγής ή μεταφοράς δεδομένων.

8.1.4. Άρνηση Εξυπηρέτησης (DoS) και Κατανεμημένη Άρνηση Εξυπηρέτησης (DDoS)

Οι επιθέσεις αυτού του τύπου δεν έχουν σαν σκοπό την υποκλοπή πληροφοριών, αλλά το να θέσουν εκτός λειτουργίας το σύστημα στόχο, έτσι ώστε να μην είναι σε θέση να προσφέρει υπηρεσίες στους εξουσιοδοτημένους χρήστες του, συνήθως αποστέλλοντας έναν μεγάλο αριθμό αιτημάτων εξυπηρέτησης που το σύστημα που υφίσταται την επίθεση δεν είναι σε θέση να διαχειριστεί, προκαλώντας την κατάρρευσή του.

Αν η επίθεση δεν γίνεται από μία μόνο τοποθεσία, αλλά από πολλές διαφορετικές τοποθεσίες ταυτόχρονα, τότε πρόκειται για μια Κατανεμημένη Άρνηση Εξυπηρέτησης (Distributed Denial of Service). Επιθέσεις αυτού του τύπου γίνονται συνήθως μέσω προγραμμάτων ιών που μεταδίδονται στους υπολογιστές ανυποψίαστων χρηστών (zombie pc) και είναι προγραμματισμένα να ξεκινήσουν την επίθεση σε κάποια συγκεκριμένη ημερομηνία και ώρα. Οι επιθέσεις αυτού του τύπου είναι πιο δύσκολο να αντιμετωπισθούν σε σχέση με τις απλές DoS.



Εικόνα 8.2: Επίθεση Κατανεμημένης Άρνησης Εξυπηρέτησης

(Τροποποιημένη από: https://eointernational.files.wordpress.com/2014/08/ddos-attack-mode.png?w=474&h=321)

8.1.5 Κοινωνική Μηχανική

Αν όλα τα προηγούμενα αποτύχουν (ή είναι δύσκολο να πραγματοποιηθούν) υπάρχει και η δυνατότητα κάποιος να πείσει ή να παραπλανήσει το χρήστη ενός συστήματος να του δώσει τις πληροφορίες που χρειάζεται. Ο όρος Κοινωνική Μηχανική (Social Engineering) χρησιμοποιήθηκε από τον πρώην εγκληματία υπολογιστών και αργότερα σύμβουλο ασφαλείας πληροφορικών συστημάτων Κέβιν Μίτνικ που επεσήμανε ότι είναι πολύ ευκολότερο να ξεγελάσεις κάποιον να δώσει έναν κωδικό πρόσβασης για ένα σύστημα από το να προσπαθήσεις να τον σπάσεις.

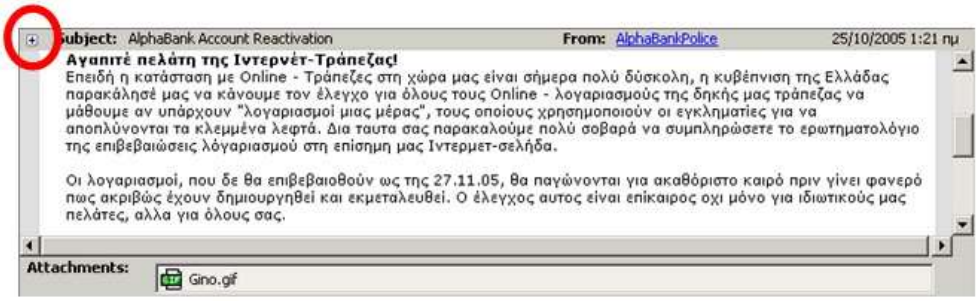
Δυσαρεστημένοι, άπληστοι ή αφελείς υπάλληλοι και χρήστες υπολογιστών μπορούν εν γνώσει ή άθελα τους να παρέχουν πολύτιμες πληροφορίες που θα οδηγήσουν στην παραβίαση της ασφάλειας ενός συστήματος ή δικτύου. Εκβιασμός, χειραγώγηση ή απλά παραπλάνηση είναι τα μέσα που θα χρησιμοποιηθούν για την εκμετάλλευση των αδυναμιών της ανθρώπινης φύσης και την επίτευξη του στόχου.

Κάποιες από τις κλασικές μεθόδους που χρησιμοποιούνται είναι και αυτές που περιγράφονται στα επόμενα:

- **Δημιουργία Σεναρίου (Pretexting)**: Η τεχνική της δημιουργίας και χρήσης ενός επινοημένου σεναρίου με στόχο να παραπλανήσει το θύμα με τέτοιο τρόπο ώστε να γίνει περισσότερο επιρρεπές στην εκχώρηση πληροφοριών. Ένα περίτεχνο ψέμα που πολλές φορές βασίζεται και σε πρότερη έρευνα και έχει σαν σκοπό να νομιμοποιήσει τον επιτιθέμενο στα μάτια του θύματος. Ο επιτιθέμενος μπορεί π.χ. να παριστάνει το δικηγόρο, τον αστυνομικό, τον εκπρόσωπο μιας τράπεζας ή κάποιον άλλο που σύμφωνα με το θύμα «δικαιούται να γνωρίζει». Πολλές φορές απλά μια σοβαρή και «επίσημη» φωνή, καθώς και μερικές προσχεδιασμένες απαντήσεις στις πιθανές ερωτήσεις του θύματος αρκούν για να ολοκληρωθεί η απάτη.

Εικόνα 8.3: Επίθεση κοινωνικής μηχανικής με δημιουργία σεναρίου

- **Ηλεκτρονικό Ψάρεμα (Phishing)**: Είναι ένας τρόπος εξαπάτησης των χρηστών υπολογιστών με στόχο να τους κάνει να αποκαλύψουν προσωπικές πληροφορίες ή οικονομικά στοιχεία, μέσω ενός παραπλανητικού μηνύματος ηλεκτρονικού ταχυδρομείου ή μιας παραπλανητικής τοποθεσίας Web. Μια συνηθισμένη απάτη ηλεκτρονικού "ψαρέματος" ξεκινά με ένα μήνυμα ηλεκτρονικού ταχυδρομείου, το οποίο μοιάζει με μια επίσημη ειδοποίηση από αξιόπιστη πηγή, όπως τράπεζα, εταιρεία πιστωτικής κάρτας ή ευυπόληπτη εταιρεία ηλεκτρονικού εμπορίου. Οι παραλήπτες του μηνύματος ηλεκτρονικού ταχυδρομείου κατευθύνονται στο να επισκεφθούν μια τοποθεσία Web, η οποία έχει δημιουργηθεί με στόχο την εξαπάτησή τους, όπου τους ζητείται να παράσχουν προσωπικές πληροφορίες, όπως ο αριθμός ή ο κωδικός πρόσβασης κάποιου λογαριασμού τους. Στη συνέχεια, οι πληροφορίες αυτές χρησιμοποιούνται συνήθως για υποκλοπή ταυτότητας.



Εικόνα 8.4: Παραπλανητικό e-mail

(Πηγή: http://oneiros.gr/blog/media/alphaphishing.jpg)

- **Δόλωμα (Bating)**: Το «δόλωμα» βασίζεται στην περιέργεια ή την απληστία του θύματος. Η τεχνική έχει πολλές ομοιότητες με αυτές του Δούρειου Ίππου. Ο επιτιθέμενος αφήνει ένα μολυσμένο CD ή ένα flash disk σε κάποια εμφανή τοποθεσία (ανελκυστήρα, διάδρομο, χώρο στάθμευσης) της εταιρίας που έχει σαν

στόχο. Κάποιος υπάλληλος μπορεί να το βρει και από περιέργεια να το βάλει στον υπολογιστή του για να δει τι περιέχει. Και μόνο η εισαγωγή του στον υπολογιστή αρκεί για να τον μολύνει με κακόβουλο λογισμικό που στη συνέχεια θα προσφέρει στον ιδιοκτήτη του πρόσβαση «εκ των έσω» στο δίκτυο της εταιρίας. Μερικές φορές μπορεί να χρησιμοποιηθούν και πιο ελκυστικές συσκευές, όπως π.χ. ένας media player που στέλνεται «μετά από κλήρωση» σε κάποιον «τυχερό».

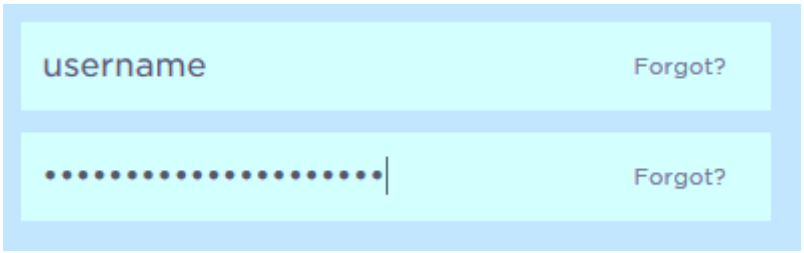
- **Quid pro quo (Κάτι για κάτι ή Δούναι και λαβείν)**: Ένας επιτιθέμενος καλεί τυχαίους αριθμούς (π.χ. σε μια εταιρία) παριστάνοντας υπάλληλο της Τεχνικής Υποστήριξης. Κάποια στιγμή θα βρει κάποιον που πραγματικά θα έχει πρόβλημα, και θα είναι ευγνώμων για τη βοήθεια. Ο επιτιθέμενος θα βοηθήσει τον υπάλληλο να λύσει το πρόβλημά του, ενώ κατά τη διάρκεια της διαδικασίας θα τον καθοδηγήσει να κάνει και τις ενέργειες που θα του δώσουν πρόσβαση στο δίκτυο.

8.2 Εφαρμογές Βασικών Μεθόδων και Τεχνικών Ασφάλειας

Στις επόμενες ενότητες περιγράφονται οι ενέργειες και τα μέσα που μπορεί να αξιοποιήσει ένας χρήστης ώστε να αυξήσει την ασφάλεια τόσο των προσωπικών δεδομένων του, όσο και του δικτύου του οργανισμού στον οποίο δραστηριοποιείται. Κάθε μία από τις ακόλουθες τεχνικές προστατεύει από συγκεκριμένους κινδύνους, και είναι για την εξασφάλιση όσο το δυνατόν μεγαλύτερης ασφάλειας είναι απαραίτητη μια ολιστική προσέγγιση που θα εφαρμόζει τις περισσότερες (αν όχι όλες) από αυτές τις τεχνικές.

8.2.1 Κωδικοί πρόσβασης

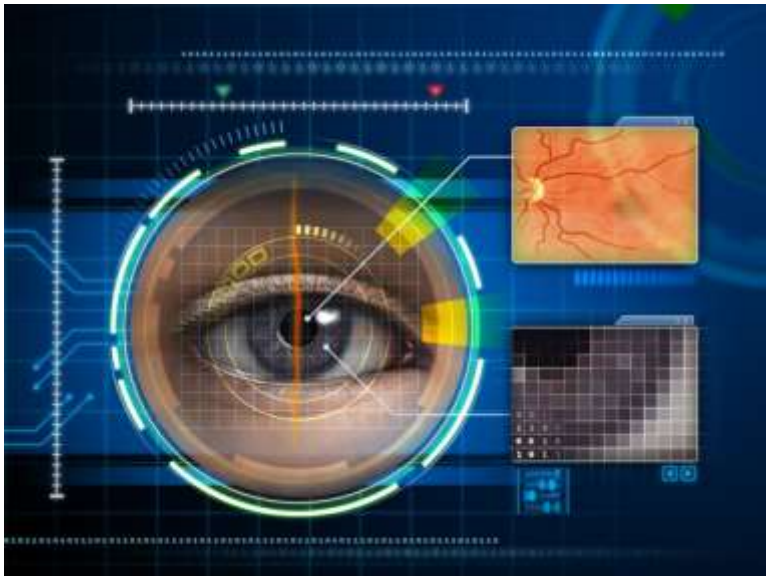
Ο πιο συνηθισμένος τρόπου ταυτοποίησης των χρηστών από ένα λειτουργικό σύστημα είναι η δημιουργία μιας συνθηματικής λέξης (password) για κάθε λογαριασμό χρήστη, η οποία θα ζητείται κάθε φορά που ο συγκεκριμένος χρήστης επιθυμεί να συνδεθεί με το σύστημα. Μία από τις πιο συνηθισμένες μεθόδους επίθεσης σε υπολογιστικά συστήματα στοχεύει στην ανεύρεση των κωδικών με τους οποίους συνδέονται σε αυτά οι χρήστες, με σκοπό την πρόσβαση στα δεδομένα του συγκεκριμένου υπολογιστικού συστήματος, αλλά και σε πιθανούς δικτυακούς πόρους στους οποίους οι συγκεκριμένοι λογαριασμοί έχουν πρόσβαση.



Εικόνα 8.5: Για να προστατευτούν οι κωδικοί πρόσβασης από «αδιάκριτα βλέμματα», δεν εμφανίζονται οι χαρακτήρες που πληκτρολογούμε. Στη θέση τους εμφανίζονται συνήθως τελείες ή αστεράκια, ή πολλές φορές και τίποτα, ώστε να μην αποκαλυφθεί ούτε το πλήθος των χαρακτήρων τους.

Για το λόγο αυτό σε περιπτώσεις που η ασφάλεια παίζει σημαντικό ρόλο λαμβάνονται επιπρόσθετα μέτρα ταυτοποίησης των χρηστών που έχουν να κάνουν είτε με τη χρήση π.χ. usb κλειδιών ή καρτών αναγνώρισης (μοιάζουν με τις γνωστές πιστωτικές κάρτες) ή ακόμα και με την αναγνώριση βιομετρικών στοιχείων του χρήστη (όπως π.χ. δακτυλικά αποτυπώματα, μοτίβο της ίριδας του ματιού, χροιά φωνής κ.α.). Σημαντικό ρόλο για την

επιτυχία των συστημάτων αυτών παίζει η ευκολία χρήσης τους και η αποδοχή τους από τους χρήστες.



Εικόνα 8.6: Αναγνώριση της ίριδας του ανθρώπινου ματιού.

(Πηγή: http://www.popsci.com/sites/popsci.com/files/styles/medium_1x_/public/images/2014/12/biometric-eyes.jpg?itok=WmuC7xw0)

8.2.2 Συναρτήσεις Κερματισμού (Hash functions)

Οι κωδικοί πρόσβασης στα λειτουργικά συστήματα δεν αποθηκεύονται σαν απλό κείμενο (plain text) οπότε θα ήταν απλό κάποιος να τους διαβάσει. Αντ' αυτού, το λειτουργικό σύστημα περνά το password από μία συνάρτηση κερματισμού η οποία δίνει σαν αποτέλεσμα μία συμβολοσειρά που ονομάζεται σύνοψη (digest). Π.χ. σύμφωνα με τη συνάρτηση κερματισμού NTLM που χρησιμοποιεί το Λ.Σ MS Windows ο κωδικός m@gn1fIc3nt μετατρέπεται σε A7CB237DABF384B97EF70B3B8DEFB1BD και αυτή η τιμή είναι που αποθηκεύεται στο σύστημα.

Οι συναρτήσεις που χρησιμοποιούνται για το σκοπό αυτό έχουν την εξής ιδιότητα. Κάθε φορά που δέχονται σαν είσοδο τον ίδιοι κωδικό, βγάζουν σαν αποτέλεσμα την ίδια σύνοψη, όμως αν κάποιος γνωρίζει μόνο τη σύνοψη είναι αδύνατον (ή πιο σωστά εξαιρετικά δύσκολο) να μπορέσει να βρει τον κωδικό, παρόλο που ο αλγόριθμος μετατροπής είναι γνωστός. Για το λόγο αυτό αναφέρονται πολλές φορές και σαν μονόδρομες (one-way) συναρτήσεις.

Εικόνα 8.7: Λειτουργία συνάρτησης κερματισμού

Η μέθοδος αυτή ωστόσο δεν μπορεί από μόνη της να εγγυηθεί την ασφάλεια του κωδικού πρόσβασης. Είναι γνωστό ότι πολλοί χρήστες χρησιμοποιούν για κωδικούς πολύ απλές λέξεις,

ή προσωπικά τους στοιχεία (π.χ. ημερομηνία γέννησης, τηλέφωνο, ΑΦΜ κ.λ.π.) ή λέξεις που υπάρχουν στην καθομιλούμενη γλώσσα). Τα στοιχεία αυτά είναι τα πρώτα που θα ελέγξει ένας επιτιθέμενος προκειμένου να ανακαλύψει κωδικούς.

Υπάρχουν μάλιστα έτοιμοι πίνακες με τη σύνοψη που παράγουν οι λέξεις αυτές (δεδομένου ότι η συνάρτηση κερματισμού είναι γνωστή) κι' έτσι το μόνο που χρειάζεται είναι να γίνει η σύγκριση με αυτούς που είναι αποθηκευμένοι στο σύστημα. Οι πίνακες αυτοί λέγονται πίνακες αντίστροφης αναζήτησης (reverse lookup tables ή rainbow tables). Αν η προσπάθεια αυτή αποτύχει, μπορεί να γίνει επίθεση με εξαντλητική δοκιμή κωδικών (brute force attack), όπου όμως ο χρόνος που χρειάζεται για να πραγματοποιηθεί αυξάνει δραματικά όσο αυξάνεται το μέγεθος του κωδικού, αλλά και το σύνολο χαρακτήρων από το οποίο αποτελείται (π.χ. πεζά, κεφαλαία, αριθμοί, σύμβολα).

Έτσι λοιπόν υποθέτοντας ένα σύστημα που μπορεί να πραγματοποιήσει 1000 δοκιμές το δευτερόλεπτο (π.χ. στα password ενός δικτυακού τόπου), ενώ για το αριθμητικό password των 8 χαρακτήρων (π.χ. το 98532548) θα χρειαστούν το πολύ 1,29 ημέρες για να γίνει δοκιμή όλων των συνδυασμών, για ένα αντίστοιχο password με χαρακτήρες από διαφορετικά σύνολα θα χρειαζόταν 2,13 χιλιάδες αιώνες.

[Ασκήσεις 4, και 5]

8.2.3 Πως δημιουργείται ένας ισχυρός κωδικός

Υπάρχουν μερικοί απλοί κανόνες που μπορούν να ενισχύσουν την ασφάλεια του ενός κωδικού πρόσβασης:

- **Να είναι ασυνήθιστος:** Αυτό σημαίνει ότι δεν θα πρέπει να είναι μια λέξη από αυτές που υπάρχουν στα λεξικά. Σε αυτό μπορεί να βοηθήσει και η αντικατάσταση κάποιων χαρακτήρων με σύμβολα που τους μοιάζουν (π.χ το 'a' με '@' ή το 'i' με '!' κ.ο.κ.
- **Να μην είναι προσωπικός:** Πρέπει να αποφεύγονται π.χ. τηλέφωνα, ημερομηνίες γέννησης, ονόματα συγγενικών προσώπων κ.α.
- **Να μην είναι προβλέψιμος:** Η ιστοσελίδα *http://www.whatsmypass.com/the-top-500-worst-passwords-of-all-time* όπως και άλλες ανάλογες περιέχει έναν κατάλογο με τα πιο συνηθισμένα password που χρησιμοποιούν χρήστες (και που θα πρέπει πάση θυσία να αποφεύγονται).
- **Να περιέχει πολλούς χαρακτήρες:** Όσο περισσότερους, τόσο το καλύτερο (σίγουρα όχι λιγότερους από 8), καθώς με τον τρόπο αυτόν γίνεται σχεδόν αδύνατη η ανεύρεσή του με επιθέσεις ωμής βίας.
- **Να περιέχει χαρακτήρες από πολλά διαφορετικά σύνολα:** Π.χ. πεζά, κεφαλαία, αριθμούς και ειδικούς χαρακτήρες. Όσο περισσότερα διαφορετικά σύνολα χαρακτήρων, τόσο περισσότεροι οι συνδυασμοί που θα πρέπει να δοκιμάσει ένας επίδοξος εισβολέας.
- **Να απομνημονεύεται εύκολα:** Είναι πολύ σημαντικό να θυμόμαστε το password που χρησιμοποιούμε. Αυτό θα επιτρέψει τη γρήγορη πληκτρολόγησή του στο σύστημα και θα δυσκολέψει κάποιον που παρακολουθεί αυτόν που το πληκτρολογεί. Αν τα password που χρησιμοποιούμε είναι πολλά και δεν μπορούμε να τα θυμόμαστε υπάρχουν εφαρμογές, όπως το Keepass (*http://sourceforge.net/ projects/keepass/*) ή η διαδικτυακή υπηρεσία LastPass (*https://lastpass.com/*) που επιτρέπουν την ασφαλή αποθήκευσή και διαχείρισή τους απαιτώντας την απομνημόνευση ενός μόνο κωδικού.

Ένα παράδειγμα χρήσης ισχυρού password είναι το ακόλουθο. Έστω ότι στο Γιώργο αρέσει πολύ η σοκολάτα. Θα μπορούσε λοιπόν να ξεκινήσει από τη φράση «*I love Chocolates*» και με την αντικατάσταση κάποιων χαρακτήρων με αριθμούς και σύμβολα να καταλήξει στο «!_L()v3_Ch0co/@t3$» που σύμφωνα με τη σελίδα αξιολόγησης κωδικών

http://www.passwordmeter.com/ είναι πολύ ασφαλές. Ακόμα ο Γιώργος θα μπορούσε να χρησιμοποιήσει και μια Greeklish εκδοχή, ξεκινώντας από τη φράση π.χ. «Λατρεύω τις Σοκολάτες» μετατρέποντας την σε «L@tR3vW_t1$_S0kO!@tE$», για το οποίο σύμφωνα με τη σελίδα https://howsecureismypassword.net/ ένας σύγχρονος υπολογιστής χρειάζεται (περίπου) 32.745.418.545.741.343.000.000 χρόνια για να το σπάσει.

Εικόνα 8.8: Ένας ισχυρός κωδικός χρειάζεται «μια αιωνιότητα» για να σπάσει

[Ασκήσεις 6, 7, 8, 9 και 10]

8.2.4 Εφαρμογές Κρυπτογράφησης και Κρυπτανάλυσης

Με την αποθήκευση κάθε είδους πληροφορίας σε ψηφιακή μορφή, αλλά και τη σχεδόν καθολική πραγματοποίηση συναλλαγών με ηλεκτρονικά μέσα, δημιουργείται η ανάγκη για ασφαλή φύλαξη και μετάδοση δεδομένων μέσω υπολογιστικών συστημάτων.

Οι εφαρμογές της κρυπτογραφίας έρχονται να καλύψουν την ανάγκη αυτή. Υπάρχουν δύο βασικά είδη αλγόριθμων κρυπτογράφησης. Οι συμμετρικοί και οι ασυμμετρικοί (ή δημόσιου-ιδιωτικού κλειδιού). Οι συμμετρικοί αλγόριθμοι χρησιμοποιούν το ίδιο κλειδί για κρυπτογράφηση και αποκρυπτογράφηση, ενώ οι ασσυμετρικοί ζευγάρια κλειδιών που με το ένα γίνεται κρυπτογράφηση και με το άλλο αποκρυπτογράφηση.

Από την εποχή που εφαρμόστηκαν οι πρώτες μέθοδοι κρυπτογράφησης ξεκίνησε και η προσπάθεια να διαβαστούν τα κρυπτογραφημένα μηνύματα. Η καλύτερη περίπτωση βέβαια θα ήταν να γίνει με κάποιο τρόπο γνωστό το κλειδί, όμως αυτό δεν ήταν πάντα εφικτό. Αναπτύχθηκαν λοιπόν κι' άλλες μέθοδοι, όπως π.χ. στατιστική ανάλυση με την οποία διαπιστώνεται η συχνότητα εμφάνισης του κάθε γράμματος στις λέξεις μιας γλώσσας. Η επιστήμη που ασχολείται με την αποκρυπτογράφηση μηνυμάτων χωρίς να είναι γνωστό το κλειδί ονομάζεται κρυπτανάλυση.

[Άσκηση 11, 12 και 13]

8.2.4.1 Κρυπτογράφηση Δεδομένων, Αρχείων και φακέλων

Τα περισσότερα λειτουργικά συστήματα προσφέρουν κάποιο είδος κρυπτογράφησης αρχείων και φακέλων, επιτρέποντας έτσι στο χρήστη να ασφαλίσει περισσότερο κάποια

ευαίσθητα δεδομένα που μπορεί να έχει αποθηκευμένα στον υπολογιστή του. Κάποια μάλιστα δίνουν τη δυνατότητα κρυπτογράφησης και ολόκληρου του δίσκου. Τα συστήματα αυτά χρησιμοποιούν συνήθως τεχνικές συμμετρικής κρυπτογράφησης, και κρυπτογραφούν τα δεδομένα χρησιμοποιώντας τον κωδικό εισόδου του χρήστη. Είναι αξιόπιστα στη χρήση τους, αλλά συνήθως περιορίζονται στη διαχείριση αρχείων στον υπολογιστή που είναι αποθηκευμένα.

Πολλές φορές πάντως παρουσιάζεται η ανάγκη κρυπτογραφημένες πληροφορίες να χρειάζεται να μεταφερθούν (και ενδεχομένως να αποκρυπτογραφηθούν σε άλλο σύστημα, ίδιας ή διαφορετικής αρχιτεκτονικής, από το αρχικό. Για την περίπτωση αυτή υπάρχουν εφαρμογές κρυπτογράφησης αρχείων και φακέλων που μπορούν να εκτελούνται σε διαφορετικούς υπολογιστές, σε πολλές δε περιπτώσεις χωρίς να χρειάζεται εγκατάσταση (portable), ενώ κάποιες άλλες, κυρίως αυτές που βασίζονται σε Java, μπορούν να εκτελεσθούν και σε συστήματα διαφορετικής αρχιτεκτονικής (cross-platform). Οι εφαρμογές αυτές συνήθως ζητούν από το χρήστη έναν κωδικό κατά τη διαδικασία της κρυπτογράφησης, που θα χρησιμοποιηθεί και για την αποκρυπτογράφηση.

[Ασκήσεις 15, 16, 17 και 18]

8.2.4.2 Κρυπτογράφηση Δημόσιου-Ιδιωτικού Κλειδιού

Η συμμετρική κρυπτογραφία, παρά το ότι έχει να παρουσιάσει εξαιρετικά εξελιγμένους αλγόριθμους που μπορούν να εξασφαλίσουν την εμπιστευτικότητα των δεδομένων, έχει μία βασική αδυναμία: Το ίδιο κλειδί που χρησιμοποιείται για την κρυπτογράφηση των δεδομένων, χρησιμοποιείται και για αποκρυπτογράφηση. Αυτό δεν δημιουργεί προβλήματα όταν το ίδιο άτομο που κάνει την κρυπτογράφηση, κάνει και την αποκρυπτογράφηση. Όταν όμως δημιουργείται η ανάγκη μεταφοράς του κλειδιού μέσα από ένα μη ασφαλές μέσο μετάδοσης, τότε μια πιθανή υποκλοπή του κλειδιού μπορεί να ακυρώσει και τον πιο σύγχρονο αλγόριθμο κρυπτογράφησης, και το πιο σύνθετο κλειδί. Στη σύγχρονη ψηφιακή εποχή, οι επικοινωνίες τέτοιου είδους είναι πολύ συνηθισμένες και τα δύο μέρη που ανταλλάσσουν πληροφορίες μπορεί να βρίσκονται πολλές χιλιάδες χιλιόμετρα μακριά το ένα από το άλλο και να μην είναι καν άνθρωποι, αλλά υπολογιστικές μηχανές.

Την απάντηση στο πρόβλημα αυτό έρχεται να δώσει η κρυπτογράφηση δημοσίου κλειδιού (Public Key Cryptography) ή ασύμμετρου κλειδιού (Asymmetric Cryptography), που χρησιμοποιεί διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση. Ο πρώτος τέτοιος αλγόριθμος παρουσιάστηκε το 1976 από τους Whitfield Diffie και Martin Hellman, ενώ αργότερα ακολούθησαν και άλλοι, με πιο γνωστούς τους RSA (από τα αρχικά των Ron Rivest, Adi Shamir και Leonard Adleman που τον ανέπτυξαν), τον ElGamal (πάλι από το όνομα του δημιουργού του Taher ElGamal) και τον NSA που αναπτύχθηκε από την Αμερικανική Εθνική Υπηρεσία Ασφαλείας (National Security Agency – NSA).

Η φιλοσοφία στην οποία στηρίζονται οι αλγόριθμοι αυτοί είναι ότι κάθε χρήστης (άνθρωπος ή μηχανή) εφοδιάζεται με δύο κλειδιά κρυπτογράφησης: το ένα από αυτά ονομάζεται ιδιωτικό κλειδί (private key) και όπως υποδεικνύει και το όνομά του πρέπει να μένει μυστικό και να μην ανακοινώνεται σε κανένα. Το άλλο κλειδί, που λέγεται δημόσιο κλειδί (public key) μπορεί (και επιβάλλεται) να ανακοινώνεται σε οποιονδήποτε θέλει να επικοινωνήσει με το συγκεκριμένο χρήστη με ασφάλεια. Έτσι το δημόσιο κλειδί μπορεί να σταλεί σε κάποιον μέσω ηλεκτρονικού ταχυδρομείου ή ακόμη και να αναρτηθεί στην ιστοσελίδα του ιδιοκτήτη του. Υπάρχουν δε και διαδικτυακοί διακομιστές δημοσίων κλειδιών (public key servers) στους οποίους μπορεί κάποιος να απευθυνθεί για να βρει το δημόσιο κλειδί του χρήστη που τον ενδιαφέρει, ή να ανεβάσει το δικό του δημόσιο κλειδί για να είναι διαθέσιμο σε κάθε ενδιαφερόμενο.

Το ιδιωτικό και το δημόσιο κλειδί χρησιμοποιούνται πάντα συνδυαστικά και τα συνδέει μια μαθηματική σχέση που έχει σαν αποτέλεσμα ό,τι κωδικοποιείται με το ένα κλειδί, να αποκωδικοποιείται με το άλλο. Ωστόσο, τα κλειδιά είναι τέτοια ώστε να μην είναι δυνατό γνωρίζοντας κάποιος το ένα από αυτά, και πιο συγκεκριμένα το δημόσιο, να μπορέσει να βρει το άλλο (το ιδιωτικό). Με τον τρόπο αυτό η αποτελεσματικότητα του αλγόριθμου εξαρτάται αποκλειστικά και μόνο από το πόσο καλά φυλάσσεται το ιδιωτικό κλειδί, αφού πλέον εξαλείφεται η ανάγκη μετάδοσής του, ενώ προσπάθειες αποκρυπτογράφησης μπορούν πια να γίνουν μόνο με εξαντλητική δοκιμή κλειδιών, που όμως, όπως έχει ήδη συζητηθεί, ο χρόνος που χρειάζεται είναι απαγορευτικά μεγάλος. Όπως συμβαίνει και με τους συμμετρικούς αλγόριθμους κρυπτογράφησης, έτσι και εδώ, όσο μεγαλύτερο το μέγεθος των κλειδιών τόσο πιο ανθεκτικά είναι σε τέτοιου είδους επιθέσεις, αλλά και τόσο περισσότερος χρόνος απαιτείται για τις διαδικασίες της κρυπτογράφησης και της αποκρυπτογράφησης.

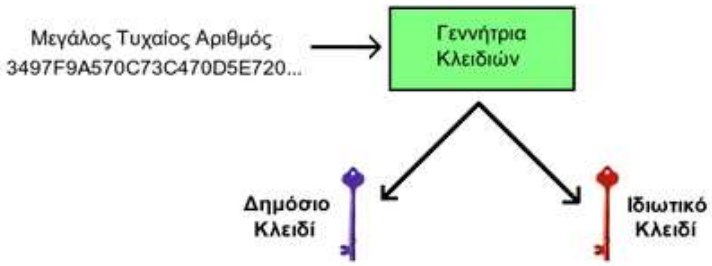
```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP Key Server 0.9.6

mQGiBDmXx8cRBADd0Dko7J7Gb5G/FINwO48AgrlYE87wCT5dlqSXl2uoDmR0/dKp
pJmvDeLQw+Z02yGx7TKf7PC5dfh61tIHyeI05fCZVA5DtRDk3keNXy2WLnLMg2yS
J44JG3I/o1QKXL8PKD2bkv/vUl7gtXe3qa57oC+2ZmxzptnLeBh08QrWXwCg/8A2
L7WHGKbhYKCApM+0FJStYrcD/1iTYhNsiZnW2tc86o/uHiX8rg7tD7VGm/Wg2E4V
Hadsb4wMLhlfi/vCSEZmlH3hFxvGk6YCWXkdFxzqhq2ZJRWQStqZqjSPWTI3HvOK
Nzjq5DbRMQY2O025g1FyWB62ZDrUWXqzyb14okoEdXT/lQA7Xe95T8uy1zfTUmBg
ieTtA/0RU3MYboVOyDgGvJ7fVyFNdk8+v6Hzcn6EZMWYJifE5hw/tSLnRAXb7ejh
wsLDDCGsjloUj4TnMHH0LUTZSWbgDZwCF6tig3mbhk7YH21zWrVQwPidSpS5O3Oh
85V3nJx5r0406nM4N1cp46yKUMekE6nhubCpVme6o+f9sUMXkLQhR2VydCBLYXNw
ZXJzZW4gPGdla2FzQHdtkGF0Y55jb20+iQ8LBBARAgALBQI5l8fHBAsDAgEACgkQ
Ls3rBj/p+6oQGwCgv5ML3xAatvJtY1mKnwzlSH2YbJ8AoPe8kUY73P+QDc5aFdHC
rCkobzlYuQQNBDmXx8cQEAD5GKB+WgZhekOQldwFbIeG7GHszUUfDtjgo3nGydx6
C6zkP+NGlLYwSlPXfAIWSIC1FeUpmamfB3TT/+OhxZYgTphluNgN7hBdq7YXHFHY
UMo1V0MpvpXoVis4eFwL2/hMTdXjqkbM+84X6CqlFGHjhKlP0YOEqHm274+nQ0YI
xswddlckOErixPDojhNnl06SE2H22+slDhf99pj3yHx5sHIdOHX79sFzxIMRJitD
YMPj6NYK/aEoJguuqa6zZQ+iAFMBoHzWq6MSHvoPKs4fdIRPyvMX86RA6dfSd7ZC
LQI2wSbLaF6dfJgkCo1+Le3kXXn11JJPmxiO/CqnS3wy9kJXtwh/CBdyorrWqULz
Bej5UxE5T7bxbrlLOCDaAadWoxTpj0BV89AHxstDqZSt90xkhkn4DIO9ZekX1KHT
UPj1WV/cdlJPPT2N286Z4VeSWc39uK50T8X8dryDxUcwYc58yWb/Ffm7/ZFexwGq
01uejaClcjrUGvC/RgBYK+X0iP1YTknbzSC0neSRBzZrM2w4DUUdD3yIsxx8Wy2O
9vPJI8BD8KVbGI2Du1WMuF040zT9fBdXQ6MdGGzeMyEstSr/P0GxKUAYEY18hKcK
ctaGxAMZyAcpesqVDNmWn6vQClCbAkbTCD1mpF1Bn5x8vYllIhkmuquiXsNV6z3W
FwACAhAAumPF6HT301BhkfuMTVI2jFXUJ7prdWy4pwZArvdDVYQ35M8sG/ISJjwg
B2GdpK9i02B25Cen309snOSj/aJkz7PQgD8CyB1V0KiDFX+KxR8S0le2k1tdbiP3
wNYxw7MDiz757IY9/hmv6YDwSeS2sWnyjgfQXR5z2RBs4r+UZ8YWk8h4YQsLSL2B
Z/PImaiopMScDJy1m4AzasXNdyr1SywU4tlwOXZhZh6ccZB/z6nlZJgMnwfVw1fZ
8wy1TKGoyOp5eh9edDFwtcAVNHVoI0hj9kDfa5sfA9zcKfeLH7TouYLuMcdws9Uc
fNeJI6AgzUvGwzvG9HVuVGf7n5b1j9Kp+jcSjvWqpQX1/iDEN8KG6/yk5mtok4lv
JBieGM2SahP1cTk1P4kcrlwJ419EhKtC6xZS96J0+TmyLBTSrJHazWR+n/lQsXvz
g7wNUycZx+/v1QDGO3HyekqZR76BSMVrpNEYEWcBclTeJ6nBJCPTGxqvP4IQhzhJ
3znANVOsViJZ7rG3DrygE+8vQ32GjbBZzouN/gHxmSKOuvw6yjFdkiSMNNdlIeKm
05Z5aV5XPuE7+TfkbFGHy+GCxjsH6FNhU/8QKtr712NO9laDARGCVaOiVvBVevVO
PXajFSW19F7Rswmh7kD5jUEy9E7ANAa0YD5i07ee0wvmaGSwfKKIRgQYEQIABgUC
0ZfHxwAKCRAuzesGP+n7qj2kAJ48xQqu8b8kzQHmmUvMFr8z+bfivQCgxXhBHUT1
LsvbbxbTJ/Da6n5YSYE=
=9v+B
-----END PGP PUBLIC KEY BLOCK-----
```

Εικόνα 8.9: Ένα δημόσιο κλειδί 1024 bit το οποίο αναπαρίσταται ως μία ακολουθία αλφαριθμητικών χαρακτήρων.

(Πηγή: https://upload.wikimedia.org/wikipedia/el/thumb/f/f8/Δημόσιο_Κλειδί.png/300px-Δημόσιο_Κλειδί.png)

Δημιουργία κλειδιών: Τη δημιουργία του δημόσιου και του ιδιωτικού κλειδιού του χρήστη αναλαμβάνουν ειδικές μαθηματικές συναρτήσεις οι οποίες δέχονται ως είσοδο έναν μεγάλο τυχαίο αριθμό και στην έξοδο παράγουν το ζεύγος των κλειδιών. Είναι προφανές ότι όσο πιο τυχαίος είναι ο αριθμός που δίνεται σαν είσοδος στη γεννήτρια κλειδιών τόσο πιο ασφαλή είναι τα κλειδιά που παράγονται. Ο τυχαίος αυτός αριθμός που απαιτεί σαν είσοδο ο αλγόριθμος παραγωγής κλειδιών δεν μπορεί και δεν είναι πρακτικό να δοθεί από έναν άνθρωπο, γι' αυτό και στα σύγχρονα προγράμματα κρυπτογράφησης παράγεται λαμβάνοντας υπόψη δεδομένα από τον υπολογιστή όπως π.χ. το χρονικό διάστημα για το οποίο είναι ανοιχτός, τον ελεύθερο χώρο στο δίσκο, την ημερομηνία και την ώρα, το πλήθος των αρχείων στο δίσκο, κ.α. Με βάση αυτά τα πραγματικά τυχαία (με την έννοια ότι σχεδόν

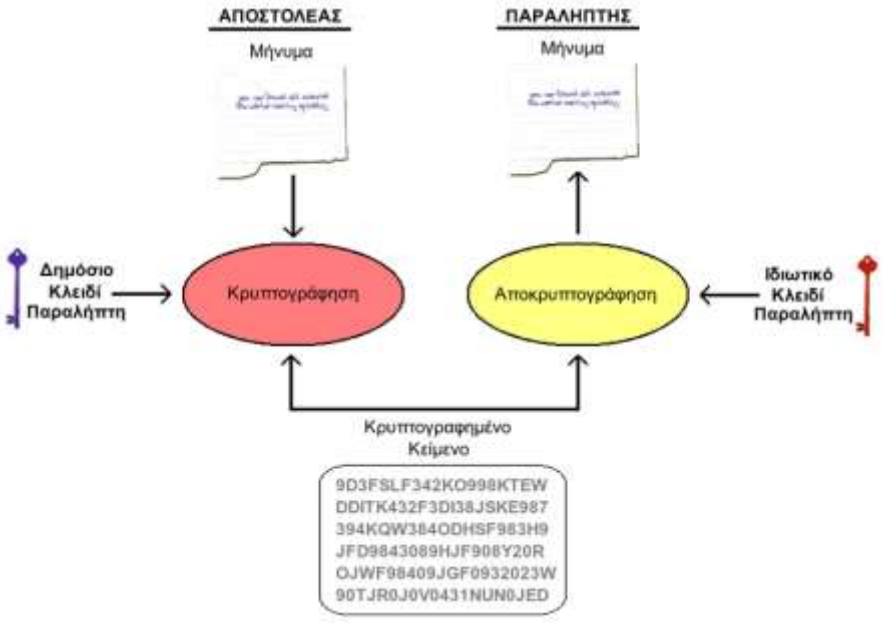
αποκλείεται να βρεθούν δύο διαφορετικά συστήματα στα οποία να συμπίπτουν) δεδομένα υπολογίζεται ο τυχαίος αριθμός και εισάγεται στη γεννήτρια κλειδιών για να δημιουργηθεί το δημόσιο και το ιδιωτικό κλειδί του χρήστη.



Εικόνα 8.10: Δημιουργία δημόσιου-ιδιωτικού κλειδιού.

(Πηγή: https://upload.wikimedia.org/wikipedia/el/thumb/f/f9/Γεννήτρια_Κλειδιών.png/400px-Γεννήτρια_Κλειδιών.png)

Εμπιστευτικότητα – Κρυπτογράφηση – Πιστοποίηση: Για να στείλει ένας αποστολέας ένα μυστικό μήνυμα σε έναν παραλήπτη, θα πρέπει πρώτα να το κρυπτογραφήσει με το δημόσιο κλειδί του παραλήπτη. Στη συνέχεια ο παραλήπτης θα χρησιμοποιήσει το ιδιωτικό του κλειδί προκειμένου να αποκρυπτογραφήσει το μήνυμα. Το σχήμα αυτό εγγυάται την εμπιστευτικότητα (confidentiality), το γεγονός δηλαδή ότι ο παραλήπτης του μηνύματος θα είναι και ο μόνος που θα μπορεί να το αποκρυπτογραφήσει. Κάποιος τρίτος θα μπορούσε να υποκλέψει το κρυπτογραφημένο μήνυμα, όμως χωρίς γνώση του ιδιωτικού κλειδιού θα του ήταν άχρηστο. Ακόμα και ο ίδιος ο αποστολέας του μηνύματος δεν θα μπορούσε να το αποκρυπτογραφήσει, αν π.χ. κατά λάθος διαγράψει το αρχικό μήνυμα.



Εικόνα 8.11: Εξασφάλιση εμπιστευτικότητας.

(*Πηγή: https://upload.wikimedia.org/wikipedia/el/thumb/f/f4/Κρυπτογράφηση_Δημόσιου_Κλειδιού_-_Εμπιστευτικότητα.png/800px-Κρυπτογράφηση_Δημόσιου_Κλειδιού_-_Εμπιστευτικότητα.png*

Με τη μέθοδο αυτή ο αποστολέας διασφαλίζει ότι ο παραλήπτης θα είναι ο μόνος που θα μπορεί να διαβάσει το μήνυμα, όμως από την πλευρά του παραλήπτη δεν πιστοποιείται η ταυτότητα του αποστολέα. Εφόσον το δημόσιο κλειδί του παραλήπτη είναι γενικά γνωστό,

οποιοσδήποτε θα μπορούσε να στείλει ένα παραπλανητικό μήνυμα, παριστάνοντας ότι είναι κάποιος άλλος. Στην ασφαλή επικοινωνία (ειδικά όταν γίνεται αυτόματα μεταξύ μηχανών) σημασία δεν έχει μόνο η διασφάλιση του απόρρητου των πληροφοριών που μεταδίδονται, αλλά και η εξακρίβωση της ταυτότητας των «συνομιλητών».

Το πρόβλημα αυτό αντιμετωπίζεται αν ο αποστολέας κρυπτογραφήσει ένα μήνυμα με το ιδιωτικό του κλειδί, το στείλει στον παραλήπτη και αυτός το αποκρυπτογραφήσει με το δημόσιο κλειδί του αποστολέα (θυμηθείτε πως ότι κρυπτογραφείται με το ένα κλειδί, αποκρυπτογραφείται με το άλλο). Στην περίπτωση αυτή βέβαια το μήνυμα κάθε άλλο παρά μυστικό είναι, αφού το δημόσιο κλειδί του αποστολέα είναι γενικά γνωστό, άρα η αποκρυπτογράφηση μπορεί να γίνει από οποιονδήποτε. Ωστόσο πετυχαίνει να πιστοποιήσει την ταυτότητα του αποστολέα.

Οι δύο αυτές μέθοδοι μπορούν να συνδυαστούν, όπως θα δούμε παρακάτω, επιτρέποντας σε έναν χρήστη να στείλει ένα κρυπτογραφημένο μήνυμα το οποίο να έχει «υπογράψει» ψηφιακά με το ιδιωτικό του κλειδί, έτσι ώστε να μην αμφισβητείται η προέλευσή του.

Μία ταχυδρομική αναλογία (παράδειγμα από https://skytal.es/wiki/Κρυπτογράφηση_δημόσιου_κλειδιού): **«***Για να γίνουν καλύτερα κατανοητές οι διαφορές μεταξύ συμμετρικής και ασύμμετρης κρυπτογράφησης, μπορεί κάποιος να φανταστεί δύο ανθρώπους, την Αντιγόνη και τον Βασίλη (Alice και Bob στην Αγγλική) που θέλουν να ανταλλάξουν κρυφά μηνύματα μέσω του ταχυδρομείου.*

Με ένα σύστημα συμμετρικού κλειδιού, η Αντιγόνη πρώτα βάζει το μυστικό μήνυμα που θέλει να στείλει σε ένα κουτί, το οποίο κλειδώνει με μία κλειδαριά για την οποία έχει το κλειδί. Στη συνέχεια το στέλνει στον Βασίλη μέσω ταχυδρομείου. Όταν ο Βασίλης λάβει το μήνυμα, χρησιμοποιεί ένα κλειδί πανομοιότυπο με αυτό της Αντιγόνης (το οποίο έχει αποκτήσει προηγουμένως, ίσως σε πρόσωπο με πρόσωπο συνάντηση με την Αντιγόνη) για να ξεκλειδώσει και να διαβάσει το μήνυμα. Στη συνέχεια ο Βασίλης μπορεί να χρησιμοποιήσει το ίδιο λουκέτο για να στείλει την κρυφή του απάντηση στην Αντιγόνη.

Σε ένα σύστημα ασυμμετρικού κλειδιού, η Αντιγόνη και ο Βασίλης έχουν ξεχωριστές κλειδαριές. Πρώτα, η Αντιγόνη ζητάει από τον Βασίλη να της στείλει το ξεκλείδωτο λουκέτο του μέσω απλού ταχυδρομείου, ενώ το κλειδί για το λουκέτο αυτό το κρατάει για τον εαυτό του. Όταν η Αντιγόνη το λάβει, το χρησιμοποιεί για να κλειδώσει ένα κουτί το οποίο περιέχει το μήνυμά της και στέλνει το κλειδωμένο κουτί στον Βασίλη. Όταν αυτός το λάβει, είναι ο μόνος που έχει το κλειδί για το λουκέτο, και άρα ο μόνος που μπορεί να το διαβάσει. Για να απαντήσει στην Αντιγόνη, θα πρέπει αντίστοιχα και αυτός να πάρει ένα ανοιχτό λουκέτο από την Αντιγόνη.

Το κρίσιμο πλεονέκτημα που μας προσφέρει η ασυμμετρική κρυπτογραφία είναι ότι η Αντιγόνη και ο Βασίλης δεν χρειάζεται να ανταλλάξουν κλειδιά. Αυτό αποτρέπει κάποιον τρίτο (ίσως, στο παράδειγμά μας, κάποιον ταχυδρομικό υπάλληλο) από το να υποκλέψει το κλειδί καθώς αυτό μεταφέρεται, κάτι το οποίο θα επέτρεπε σε αυτόν τον τρίτο να κατασκοπεύει όλα τα μελλοντικά μηνύματα μεταξύ του Βασίλη και της Αντιγόνης. Οπότε, στο σύστημα δημοσίου κλειδιού, η Αντιγόνη και ο Βασίλης δε χρειάζεται να εμπιστεύονται ιδιαίτερα το ταχυδρομείο (και γενικά τον οποιοδήποτε δίαυλο επικοινωνίας).

Φυσικά, υπάρχει πάντα το ενδεχόμενο κάποιος να παραβιάσει την κλειδαριά της Αντιγόνης ή του Βασίλη. Μεταξύ των αλγορίθμων κρυπτογράφησης συμμετρικού κλειδιού, μόνο ο One-time pad είναι απόλυτα ασφαλής απέναντι σε οποιονδήποτε αντίπαλο, ανεξαρτήτως της υπολογιστικής ισχύος που αυτός μπορεί να διαθέτει. Δυστυχώς, δεν υπάρχει αλγόριθμος κρυπτογράφησης δημόσιου κλειδιού με αυτή την ιδιότητα, και έτσι όλοι αυτοί οι αλγόριθμοι είναι ευάλωτοι σε Brute-force attack (επίθεση ωμής βίας).

Στην πράξη, η παραπάνω ανασφάλεια αντιμετωπίζεται με την επιλογή κλειδιών αρκετά μεγάλων, ώστε η καλύτερη γνωστή επίθεση να έπαιρνε τόσο χρόνο που να μην άξιζε το χρόνο και τα χρήματα για τον αντίπαλο. Για παράδειγμα, κανένας δε θα έμπαινε στον κόπο να προσπαθήσει με brute force επίθεση να σπάσει την κρυπτογράφηση των μηνυμάτων σου, όσο σημαντικές πληροφορίες κι αν περιείχαν, αν η επίθεση θα έπαιρνε κατά μέσο όρο 1000 χρόνια.»

[Ασκήσεις 18, 19, 20, 21, 22 και 23]

8.2.5 Δημοσίευση σε Εξυπηρετητές Δημόσιων Κλειδιών (Public Key Servers)

Το δημόσιο κλειδί, όπως λέει και η λέξη, προορίζεται στο να είναι διαθέσιμο σε οποιονδήποτε θέλει να μας στείλει ένα κρυπτογραφημένο μήνυμα. Υπάρχουν πολλοί τρόποι με τους οποίους μπορεί να δημοσιοποιηθεί το δημόσιο κλειδί μας π.χ. με μεταφορά σε ένα usb-stick, ή μέσω ηλεκτρονικού ταχυδρομείου ή μέσω της προσωπικής μας web σελίδας (αν υπάρχει).

Παρόλα αυτά, υπάρχει η περίπτωση να θέλει να επικοινωνήσει μαζί μας κάποιος που δεν μας γνωρίζει δεν μπορεί να πληροφορηθεί το δημόσιο κλειδί μας με κάποιον από τους παραπάνω τρόπους. Για το σκοπό αυτό έχουν δημιουργηθεί ειδικοί εξυπηρετητές δημόσιων κλειδιών (public key servers) στους οποίους μπορεί κάποιος να μεταφορτώσει το δημόσιο κλειδί του. Οι εξυπηρετητές αυτοί διαθέτουν έναν μηχανισμό αναζήτησης με τον οποίο μπορεί κάποιος να εντοπίσει το δημόσιο κλειδί ενός χρήστη, χρησιμοποιώντας το όνομα ή την e-mail διεύθυνσή του. Μάλιστα πολλοί από αυτούς τους server επικοινωνούν και με άλλους, ενημερώνοντάς τους την εισαγωγή νέων κλειδιών, απαλλάσσοντας το χρήστη από αυτή την εργασία. Ένα ωστόσο μειονέκτημα αυτών των εξυπηρετητών είναι ότι συνήθως δεν περιλαμβάνουν άλλα στοιχεία για τα άτομα που έχουν μεταφορτώσει τα δημόσια κλειδιά τους, δημιουργώντας έτσι δυσκολίες σε περίπτωση συνωνυμίας.

[Άσκηση 24]

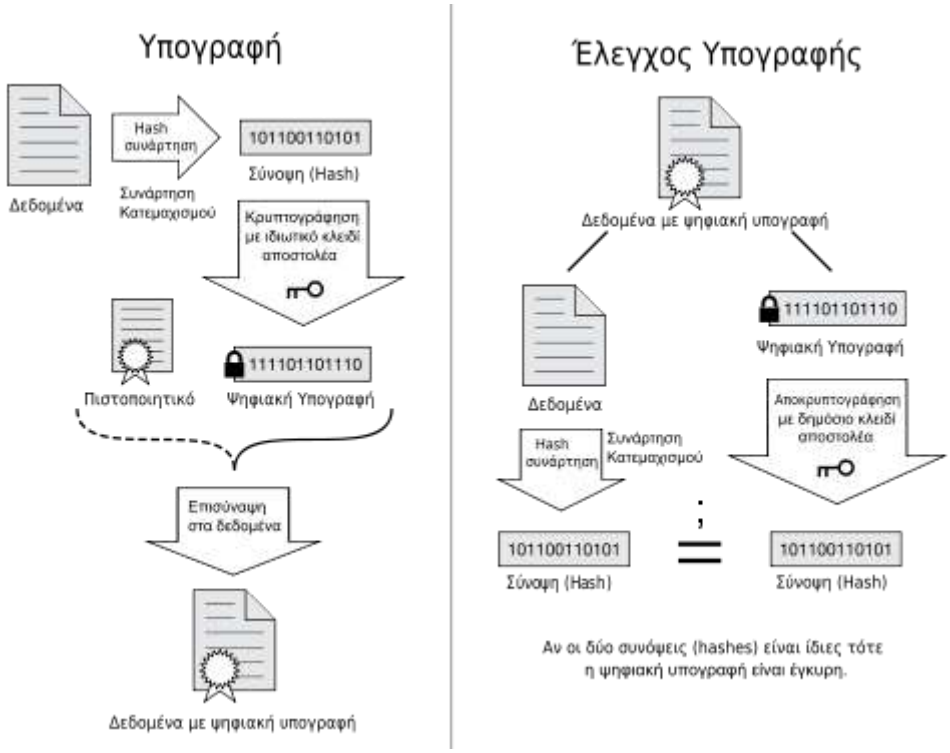
8.2.6 Δημιουργία Δικτύου Εμπιστοσύνης (Web of Trust - WoT)

Οι key server μπορούν να πληροφορήσουν το κοινό για το δημόσιο κλειδί μας, δεν μπορούν όμως να μας εξασφαλίσουν ότι οι άλλοι χρήστες είναι αυτοί που ισχυρίζονται. Το εμπόδιο αυτό μπορεί να ξεπεραστεί ως εξής: Με τον ίδιο τρόπο που ένας χρήστης μπορεί με χρήση του ιδιωτικού του κλειδιού να υπογράψει ψηφιακά ένα μήνυμα που θα στείλει σε κάποιον άλλο, έτσι μπορεί να υπογράψει ψηφιακά και το δημόσιο κλειδί κάποιου άλλου, υποδηλώνοντας έτσι ότι τον γνωρίζει και τον εμπιστεύεται. Έτσι π.χ. ο Βασίλης μπορεί να υπογράψει το δημόσιο κλειδί της Αντιγόνης με το δικό του και να στείλει το υπογεγραμμένο κλειδί στην Αντιγόνη. Εάν η Αντιγόνη το επιθυμεί θα ανεβάσει ξανά το κλειδί της στον key server, προσθέτοντας στην ουσία την υπογραφή του Βασίλη. Πλέον στην αναζήτηση του δημόσιου κλειδιού της Αντιγόνης, θα έχει προστεθεί η υπογραφή του Βασίλη. Με τον τρόπο αυτό οι ψηφιακές υπογραφές κλειδιών μεταξύ ατόμων γνωστοποιούνται σε τρίτους, δίνοντας τη δυνατότητα να δημιουργηθεί ένας ιστός εμπιστοσύνης μεταξύ χρηστών (Web of Trust). Για παράδειγμα ο Κώστας γνωρίζει τον Βασίλη και αναζητώντας το δημόσιο κλειδί της Αντιγόνης βλέπει την υπογραφή του Βασίλη. Αν ο Κώστας εμπιστεύεται τον Βασίλη, μπορεί να εμπιστευθεί (σε όποιο βαθμό επιθυμεί) και την Αντιγόνη. Το μειονέκτημα εδώ είναι ότι κάθε αλυσίδα είναι τόσο δυνατή όσο ο πιο αδύναμος κρίκος της. Αν ένας χρήστης δηλώσει την εμπιστοσύνη του προς κάποιον άλλο, χωρίς πραγματικά να τον γνωρίζει, μπορεί να παραπλανήσει και άλλους χρήστες στο να τον εμπιστευθούν.

8.2.7 Ψηφιακές Υπογραφές

Όπως αναφέρθηκε προηγουμένως υπάρχει η δυνατότητα ένας χρήστης χρησιμοποιώντας το ιδιωτικό του κλειδί να «σημαδέψει» (υπογράψει) ψηφιακά ένα μήνυμα, έτσι ώστε να επιβεβαιώνεται η ταυτότητά του από τον παραλήπτη. Η διαδικασία αυτή λέγεται «ψηφιακή υπογραφή» και γίνεται με τον ακόλουθο τρόπο:

- Αρχικά το μήνυμα εισάγεται σε μια συνάρτηση κερματισμού από την οποία προκύπτει η σύνοψή του. Όπως έχει αναφερθεί στα προηγούμενα οι συναρτήσεις κατατεμαχισμού είναι τέτοιες που είναι εξαιρετικά απίθανο (όχι όμως και αδύνατο) δύο διαφορετικά μηνύματα να παράγουν την ίδια σύνοψη.
- Στη συνέχεια η σύνοψη του μηνύματος κρυπτογραφείται με το ιδιωτικό κλειδί του αποστολέα. Η κρυπτογραφημένη αυτή σύνοψη είναι η «ψηφιακή υπογραφή».
- Η «ψηφιακή υπογραφή» συνενώνεται με το αρχικό μήνυμα και όλα μαζί αποστέλλονται στον παραλήπτη. Αν ο αποστολέας το επιθυμεί μπορεί πριν στείλει το μήνυμα με τη σύνοψη να τα κρυπτογραφήσει με το δημόσιο κλειδί του αποστολέα, έτσι ώστε κανείς άλλος να μην μπορεί να τα διαβάσει.



Εικόνα 8.12: Ψηφιακές Υπογραφές.

(Πηγή: https://upload.wikimedia.org/wikipedia/commons/thumb/6/6f/Digital_Signature_diagram_el.svg/500px-Digital_Signature_diagram_el.svg.png)

- Ο παραλήπτης του μηνύματος το αποκρυπτογραφεί (αν χρειάζεται) με το ιδιωτικό του κλειδί και στη συνέχεια εξάγει την κρυπτογραφημένη σύνοψη.
- Η κρυπτογραφημένη σύνοψη αποκρυπτογραφείται με το δημόσιο κλειδί του αποστολέα (θυμηθείτε ότι είχε κρυπτογραφηθεί με το ιδιωτικό του κλειδί) και αν η διαδικασία ολοκληρωθεί με επιτυχία πιστοποιείται η ταυτότητα του αποστολέα.
- Στη συνέχεια από τα δεδομένα του μηνύματος υπολογίζεται εκ' νέου η σύνοψή του. Η νέα αυτή σύνοψη συγκρίνεται με την ενσωματωμένη και εφόσον είναι ίδιες είμαστε επιπλέον σίγουροι ότι το αρχείο δεν έχει αλλοιωθεί ή παραποιηθεί κατά τη μεταφορά του.

8.2.8 Ψηφιακά Πιστοποιητικά

Η ψηφιακή υπογραφή επιβεβαιώνει ότι ένα μήνυμα έχει σταλεί από τον κάτοχο του συγκεκριμένου ιδιωτικού κλειδιού, και ότι το μήνυμα δεν έχει υποστεί τροποποιήσεις, όμως δεν μας εξασφαλίζει ότι αυτός είναι πράγματι το πρόσωπο που ισχυρίζεται. Μια τέτοια προσπάθεια γίνεται με τους εξυπηρετητές δημόσιων κλειδιών και τη δημιουργία δικτύων εμπιστοσύνης, που περιγράφηκε προηγουμένως, όμως σε πολλές περιπτώσεις, ειδικά σε θέματα εμπορικών συναλλαγών, αυτό δεν είναι αρκετό. Φανταστείτε για παράδειγμα έναν απατεώνα που θέλει να παραστήσει ότι είναι ένα ευυπόληπτο διαδικτυακό κατάστημα ή έναν χάκερ που προσπαθεί να πείσει ότι πρόκειται για εταιρία ανάπτυξης προγραμμάτων προστασίας από ιούς. Στις περιπτώσεις αυτές, η εμπιστοσύνη κάποιων τρίτων προσώπων απλά δεν είναι επαρκής. Η λύση μπορεί να δοθεί με τη χρήση ψηφιακών πιστοποιητικών που εκδίδουν οι Αρχές Πιστοποίησης (Certification Authorities – CA).

Ψηφιακό πιστοποιητικό (ή πιστοποιητικό δημοσίου κλειδιού) είναι ένα ηλεκτρονικό έγγραφο, το οποίο κάνει χρήση της λειτουργίας των ψηφιακών υπογραφών, για να αντιστοιχίσει δεσμευτικά ένα δημόσιο κλειδί με μια ταυτότητα προσώπου, οργανισμού ή εταιρείας. Στην ουσία πρόκειται για το δημόσιο κλειδί του χρήστη, υπογεγραμμένο ψηφιακά από την Αρχή Πιστοποίησης.

Μια αρχή πιστοποίησης είναι μια γνωστή και αναγνωρισμένη εταιρία που αναλαμβάνει να δημιουργήσει το ψηφιακό πιστοποιητικό ενός χρήστη αφού επαληθεύσει, συνήθως έναντι αμοιβής, την ταυτότητα και την ιδιότητά του. Πολύ γνωστές εταιρίες στο χώρο είναι η Symantec (πρώην Verisign), η Commodo, η Global Sign κ.α. Άλλες, λιγότερο γνωστές εταιρίες δραστηριοποιούνται στο εσωτερικό διαφόρων κρατών ή οργανισμών. Το Πανελλήνιο Σχολικό Δίκτυο για παράδειγμα είναι σε θέση να εκδίδει, δωρεάν, ψηφιακά πιστοποιητικά για τα εγγεγραμμένα μέλη του (Σχολικές μονάδες και μεμονωμένους χρήστες), αφού μπορεί να γνωρίζει την πραγματική τους ταυτότητα (δείτε: http://ca.sch.gr/cert_authority.php).

8.2.9 Στεγανογραφία - Στεγανάλυση

Με τον όρο στεγανογραφία αναφερόμαστε στο σύνολο των τεχνικών που μας επιτρέπει την απόκρυψη της πληροφορίας που πρόκειται να μεταδοθεί σε κάποιον παραλήπτη, μέσα σε κάποιο άλλο, φαινομενικά «αθώο» μέσο. Προκύπτει από τις λέξεις στεγανός = καλυμμένος, σκεπασμένος και γραφή. Σημαίνει δηλαδή γραφή που καλύπτεται ή μυστική γραφή.

Η στεγανογραφία δεν εντάσσεται στην κρυπτογραφία, αλλά αποτελεί μία ξεχωριστή τεχνική ασφαλείας. Αυτό που προσπαθεί να κάνει είναι όχι να κρύψει το περιεχόμενο ενός μηνύματος, το γεγονός ότι μεταδίδεται κάποια Πληροφορία, με την προσδοκία ότι ο «αντίπαλος» δεν θα ανακαλύψει ποτέ τη μετάδοσή της. Φυσικά, μπορεί να συνδυαστεί και με κρυπτογράφηση, έτσι ώστε ακόμη κι' αν ανακαλυφθεί η ύπαρξη του μηνύματος, αυτό να μην είναι δυνατό (ή να είναι πολύ δύσκολο) να διαβαστεί.

Όπως και η κρυπτογραφία, έτσι και η στεγανογραφία βρίσκει εφαρμογή σε όλη την ιστορική διαδρομή του ανθρώπου. Σε ένα από τα γραπτά του ο Ηρόδοτος αναφέρει πως όταν Δημάρατος θέλησε να ειδοποιήσει τη Σπάρτη ότι ο Ξέρξης σκόπευε να εισβάλει στην Ελλάδα έγραψε το μήνυμά του σε ξύλινη πινακίδα, αφού έξυσε το κερί που αυτή είχε και την οποία μετά κάλυψε πάλι με κερί. Οι πινακίδες φαίνονταν λευκές και αχρησιμοποίητες και με αυτό το τρόπο πέρασαν κάθε έλεγχο. Μια άλλη μέθοδος ήταν το ξύρισμα του κεφαλιού ενός αγγελιοφόρου, η σχεδίαση στο δέρμα ενός μηνύματος ή σχεδίου και η αποστολή του αγγελιοφόρου στον προορισμό του, όταν τα μαλλιά του θα είχαν ξαναμακρύνει. Κατά τη διάρκεια του Β' Παγκοσμίου Πολέμου χρησιμοποιήθηκαν «αόρατα μελάνια» που εμφανίζονταν όταν θερμαίνονταν ή επεξεργάζονταν με συγκεκριμένες χημικές ουσίες.

Με την εξέλιξη της μικρο-φωτογραφίας οι Γερμανοί ανέπτυξαν τα Microdots, μικροσκοπικές φωτογραφίες σε μέγεθος κουκκίδας (dot) που μετά από μεγέθυνση αποκάλυπταν κείμενα, σχέδια και φωτογραφίες.

Πολλές φορές το μυστικό μήνυμα μεταδίδονταν σε κοινή θέα μέσα σε ένα φαινομενικά αθώο κείμενο. Π.χ αν από το ακόλουθο κείμενο (*Παραδείγματα από Γεωργακόπουλος Ν., 2006*):

«**Χ**ωρίς **τ**α **υ**πόλοιπα, **π**ου **ή**ταν **σ**ε **τ**ελικό **έ**λεγχο, **τ**έσσερις **ώ**ρες **ρ**ύθμισης **α**ρκούσαν.»

απομονωθεί το πρώτο γράμμα κάθε λέξης, σχηματίζεται το μήνυμα:

«Χτυπήστε τώρα»

Το ίδιο μπορούσε να γίνει και απομονώνοντας συγκεκριμένες λέξεις από π.χ. ένα άρθρο εφημερίδας ή μια ραδιοφωνική εκπομπή. Ακόμη και η μορφοποίηση του κειμένου μπορεί να χρησιμοποιηθεί για την απόκρυψη ενός μηνύματος. Έστω π.χ. το ακόλουθο κείμενο:

We explore new steganographic and cryptographic

algorithms and techniques throughout the world to

produce wide variety and security in the electronic web

called the Internet.

Αν στο κείμενο αυτό επισημανθούν τα κενά πριν από κάθε λέξη

We␣␣explore␣new␣steganographic␣and␣cryptographic

algorithms␣and␣techniques␣throughout␣␣the␣␣world␣to

produce␣␣wide␣variety␣and␣security␣in␣the␣electronic␣␣web

called␣the␣Internet.

και καταγραφούν οι λέξεις που έχουν μπροστά τους δύο κενά, προκύπτει το μήνυμα:

explore the world wide web

Σε αντιστοιχία με την κρυπτανάλυση, η στεγανάλυση είναι το σύνολο των τεχνικών που χρησιμοποιούνται για να ανακαλύψουν την ύπαρξη και να εξάγουν το περιεχόμενο μιας στεγανογραφικά κρυμμένης πληροφορίας. Οι τεχνικές αυτές εξαρτώνται κυρίως από το μέσο το οποίο έχει χρησιμοποιηθεί για την απόκρυψη του αρχικού μηνύματος.

8.2.10 Απόκρυψη μηνύματος μέσα σε αρχεία πολυμέσων

Στη σύγχρονη ψηφιακή εποχή η στεγανογραφία στηρίζεται στο γεγονός ότι αρχεία που περιέχουν εικόνες, ήχο και κατά συνέπεια βίντεο, μπορούν να αλλάξουν έως ένα βαθμό χωρίς αλλοίωση της λειτουργικότητάς τους, σε αντίθεση π.χ. με αρχεία εφαρμογών που η αλλοίωση έστω και ενός bit μπορεί να καταστήσει ένα πρόγραμμα μη λειτουργικό.

Εκτός αυτού, οι ανθρώπινη όραση και ακοή δεν είναι τόσο ευαίσθητη ώστε να διακρίνει μικρές αλλοιώσεις στα χρώματα μιας εικόνας ή στην ποιότητα του ήχου. Σε αυτό το γεγονός εξάλλου στηρίζονται και οι αλγόριθμοι απωλεστικής συμπίεσης εικόνας και ήχου (όπως ο JPEG ή ο MP3) που πετυχαίνουν εξαιρετικά μεγάλη μείωση του αρχικού μεγέθους των αρχείων πολυμέσων.

Έτσι λοιπόν τα αρχεία αυτά είναι ιδανικά για την απόκρυψη μυστικών μηνυμάτων εντός τους. Ωστόσο και αυτά τα αρχεία ακόμη πρέπει να επιλέγονται με προσοχή. Π.χ. η αλλοίωση ενός αρχείου εικόνας θα είναι πολύ περισσότερο εμφανής αν αυτή περιλαμβάνει μεγάλες επιφάνειες ίδιου χρώματος, όπως π.χ. συμβαίνει στα σχέδια. Επίσης είναι πολύ πιθανότερο η ύπαρξη ενός μυστικού μηνύματος να αποκαλυφθεί σε μία φωτογραφία που έχει μεταφορτωθεί από το Διαδίκτυο και υπάρχει η αρχική εικόνα για σύγκριση, απ' ότι σε μια

φωτογραφία που τραβήχτηκε με μια ψηφιακή φωτογραφική μηχανή ή ένα κινητό τηλέφωνο. Για ακόμη δε μεγαλύτερη ασφάλεια καλό είναι να διαγράφεται το πρωτότυπο αρχείο.

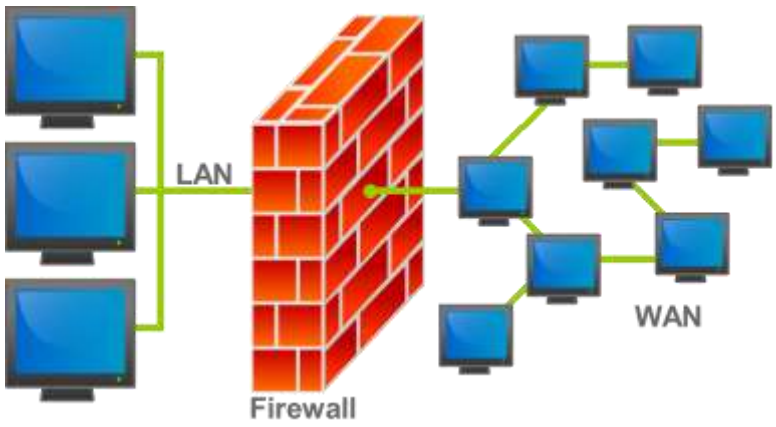
Κάθε αρχείο πολυμέσων έχει τη δυνατότητα να δεχθεί μέχρι ένα συγκεκριμένο όγκο νέων πληροφοριών πριν η αλλοίωσή του αρχίσει να γίνεται αισθητή. Για το λόγο αυτό έχει αναπτυχθεί λογισμικό που μπορεί να χρησιμοποιήσει συνδυασμό αρχείων πολυμέσων, αυξάνοντας έτσι το μέγεθος των δεδομένων που μπορούν να φιλοξενήσουν. Πολλές δε από αυτές τις εφαρμογές μπορούν επιπλέον και να κρυπτογραφήσουν τα μυστικά δεδομένα, με σκοπό να μην μπορέσουν να αξιοποιηθούν ακόμη κι' αν αποκαλυφθεί η ύπαρξή τους.

Παρά το γεγονός ότι τα αρχεία πολυμέσων είναι τα υπ' αριθμόν ένα υποψήφια για χρήση στεγανογραφικών μεθόδων, δεν αποκλείεται η απόκρυψη πληροφοριών και σε αρχεία άλλου είδους, όπως π.χ. αρχεία pdf (αντικαθιστώντας τα κενά του κειμένου με άλλους επίσης μη ορατούς χαρακτήρες https://www.os3.nl/media/2012-2013/courses/ssn/using_steganography_to_hide_messages_inside_pdf_files.pdf), ή ακόμη και σε απλά αρχεία κειμένου, προσθέτοντας tab και κενά στο τέλος κάθε γραμμής.

[Άσκηση 25]

8.2.11 Τείχος Προστασίας (Firewall)

Ένα τείχος προστασίας είναι ένα σύστημα ασφάλειας που παρακολουθεί και ελέγχει την εισερχόμενη και εξερχόμενη δικτυακή κίνηση σε ένα δίκτυο ή έναν υπολογιστή, βασιζόμενο σε προκαθορισμένους κανόνες. Η τυπική λειτουργία ενός firewall είναι να εγκαθιστά ένα φράγμα ανάμεσα σε έναν υπολογιστή ή ένα έμπιστο εσωτερικό δίκτυο και σε ένα εξωτερικό δίκτυο, όπως π.χ. το Internet που δεν θεωρείται ασφαλές ή έμπιστο. Είναι ένα από τα πιο σημαντικά συστατικά στην οικοδόμηση της ασφάλειας ενός δικτύου.



Εικόνα 8.13: Τείχος Προστασίας.

(Πηγή: https://upload.wikimedia.org/wikipedia/commons/thumb/5/5b/Firewall.png/400px-Firewall.png)

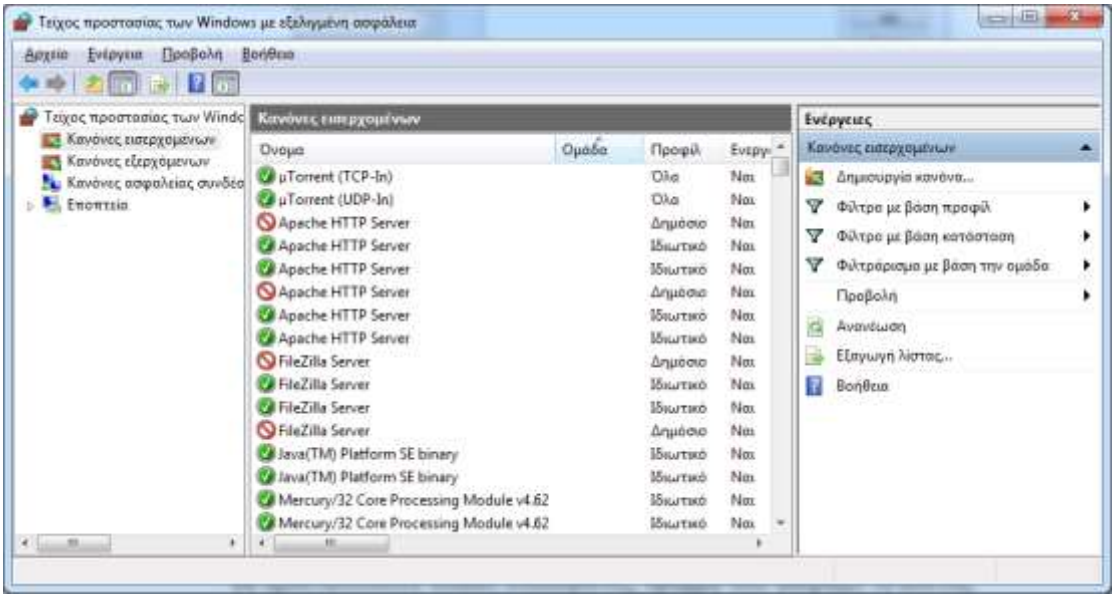
Ένα firewall μπορεί να επιτρέψει ή να απαγορεύσει την επικοινωνία υπολογιστών για συγκεκριμένες IP διευθύνσεις, MAC διευθύνσεις, Υπηρεσίες (π.χ. HTTP, FTP, TELNET κ.α.), συγκεκριμένες θύρες (TCP/UDP ports) ή ακόμη και συγκεκριμένες εφαρμογές. Εμποδίζει επίσης επιθέσεις που έχουν σαν σκοπό να εντοπίσουν αδυναμίες (vulnerabilities) των λειτουργικών συστημάτων που χρησιμοποιούνται σε ένα δίκτυο, με σκοπό την εκμετάλλευσή τους.

[Άσκηση 26]

8.2.11.1 Κατηγορίες

Υπάρχουν δύο βασικά είδη Firewall. Τα firewall λογισμικού (software firewalls) και τα firewall υλικού (hardware firewalls).

Τα firewall λογισμικού είναι ουσιαστικά εφαρμογές οι οποίες εγκαθίστανται στο λειτουργικό σύστημα του υπολογιστή με τον ίδιο τρόπο που εγκαθίστανται και οι περισσότερες εφαρμογές. Μάλιστα τα περισσότερα σύγχρονα λειτουργικά συστήματα περιλαμβάνουν από μόνα τους κάποια τέτοιου είδους εφαρμογή με λιγότερες ή περισσότερες δυνατότητες.



Εικόνα 8.14: Ρύθμιση πρόσβασης εφαρμογών σε software firewall

Πλεονεκτήματα των software firewall:

- Είναι πιο οικονομικά από τα firewall υλικού, σε αρκετές δε περιπτώσεις είναι και εντελώς δωρεάν.
- Είναι πιο εύκολα στη ρύθμιση και τη χρήση.
- Μπορούν να αποκλείσουν την επικοινωνία συγκεκριμένων εφαρμογών με το Διαδίκτυο, ανεξάρτητα από τις θύρες που αυτές χρησιμοποιούν.

Μειονεκτήματα των software firewall:

- Προστατεύουν μόνο τον υπολογιστή στον οποίο είναι εγκατεστημένα.
- Στην περίπτωση που δεν είναι δωρεάν, χρειάζεται η αγορά πολλαπλών αδειών για να προστατευθούν πολλοί υπολογιστές, πράγμα που ανεβάζει το κόστος.
- Καταναλώνουν πόρους (επεξεργαστική ισχύ, μνήμη) από το σύστημα στο οποίο εγκαθίστανται.
- Έχουν λιγότερες επιλογές στις ρυθμίσεις τους.
- Κάποιο κακόβουλο πρόγραμμα μπορεί να επηρεάσει τη λειτουργία τους.

Τα firewall υλικού είναι ανεξάρτητες συσκευές που συνήθως τοποθετούνται στο σημείο σύνδεσης του εσωτερικού έμπιστου δικτύου με τον εξωτερικό κόσμο, έτσι ώστε όλη η κίνηση από και προς το εσωτερικό δίκτυο να περνάει μέσα από το firewall.

Εικόνα 8.15: Τείχος προστασίας υλικού.

(*Πηγή: https://pixabay.com/static/uploads/photo/2013/07/13/09/47/firewall-156010_640.png*)

Στην κατηγορία αυτή μπορεί να ενταχθεί και η χρήση παλαιότερης τεχνολογίας υπολογιστών, που με κατάλληλο λογισμικό (συνήθως ειδικές δωρεάν διανομές Linux) μπορούν να αναλάβουν το ρόλο firewall.

Πλεονεκτήματα των hardware firewall:

- Ένα firewall μπορεί να προστατεύσει ένα ολόκληρο τοπικό δίκτυο.
- Δεν επιβαρύνουν τη λειτουργία των υπολογιστών που προστατεύουν.
- Δεν επηρεάζονται από κακόβουλα προγράμματα.
- Προστατεύουν υπολογιστές με οποιοδήποτε λειτουργικό σύστημα

Μειονεκτήματα των hardware firewall:

- Κοστίζουν περισσότερο από τα software firewall
- Η ρύθμισή τους είναι σαφώς πιο πολύπλοκη και απευθύνεται σε πιο προχωρημένους χρήστες
- Απαιτούν εγκατάσταση στο σωστό σημείο του δικτύου.
- Δεν ειδοποιούν όταν εμποδίζουν την επικοινωνία κάποιας εφαρμογής
- Αν δεν είναι σωστά ρυθμισμένα ή για κάποιο λόγο δεν λειτουργούν σωστά, ολόκληρο το δίκτυο μένει εκτεθειμένο.

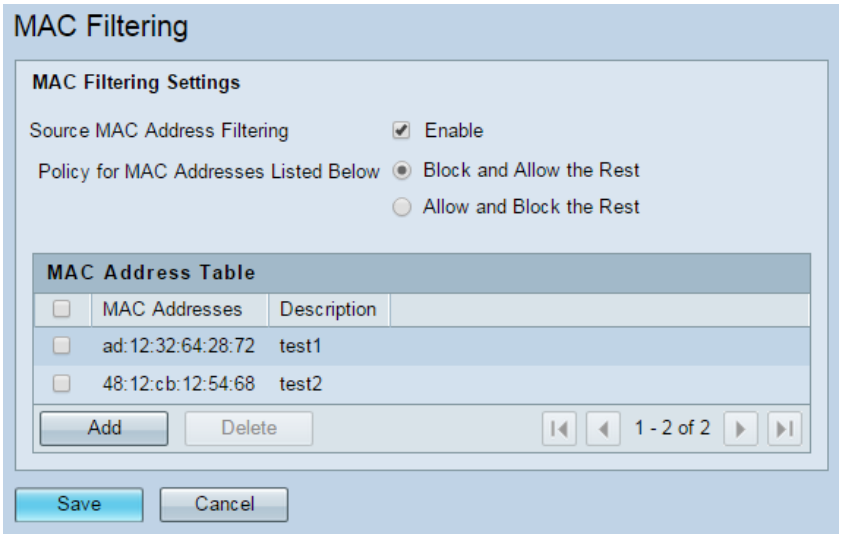
8.2.11.2 Ρύθμιση πρόσβασης σε υπηρεσίες

Τα περισσότερα firewall ρυθμίζονται βάσει μιας σειράς κανόνων που καθορίζουν τη ροή δεδομένων από και προς τον υπολογιστή/δίκτυο που προστατεύουν. Οι κανόνες αυτοί χωρίζονται σε δύο βασικές κατηγορίες:

- Κανόνες που αφορούν την εισερχόμενη κίνηση (inbound)
- Κανόνες που αφορούν την εξερχόμενη κίνηση (outbound)

Ένας κανόνας μπορεί να επιτρέπει ή να απαγορεύει τη ροή δεδομένων ανάλογα με το εξής κριτήρια:

- Το πρωτόκολλο επιπέδου μεταφοράς (TCP ή UDP)
- Την υπηρεσία ή το πρωτόκολλο επιπέδου εφαρμογής όπως καθορίζεται από τις θύρες που χρησιμοποιούνται (π.χ. 80 για το HTTP)
- Τις IP διευθύνσεις των δικτυακών συσκευών που επικοινωνούν
- Τις MAC διευθύνσεις των δικτυακών συσκευών



Εικόνα 8.16: Φιλτράρισμα MAC διευθύνσεων

- Σε ποιο προχωρημένες περιπτώσεις ακόμη και τα περιεχόμενα των πακέτων (deep packet inspection)

Επιπλέον τα περισσότερα software firewall έχουν τη δυνατότητα να επιτρέπουν ή να απαγορεύουν την επικοινωνία σε συγκεκριμένες εφαρμογές. Έτσι είναι δυνατό να επιτρέπεται π.χ. σε έναν browser να έχει πρόσβαση στο Διαδίκτυο, ενώ σε έναν άλλο όχι, παρόλο που και οι δύο χρησιμοποιούν τα ίδια πρωτόκολλα.

[Άσκηση 27, 28, 29, 30, 31, 32 και 33]

8.3. Αυξάνοντας την ασφάλεια των Εξυπηρετητών

Με την πληθώρα των κινδύνων και των τύπων επιθέσεων που μπορούν να χρησιμοποιηθούν για την παραβίαση ενός υπολογιστή ή δικτύου, γεννάται εύλογα το ερώτημα αν και κατά πόσο μπορεί κάποιος να προφυλάξει την ακεραιότητα και εμπιστευτικότητα των δεδομένων του.

Παρά το γεγονός ότι το επίπεδο ασφαλείας που είναι δυνατό να επιτευχθεί εξαρτάται άμεσα από τα χρήματα και το χρόνο που επενδύονται για την υλοποίησή του, υπάρχουν ορισμένες απλές συμβουλές που μπορούν να εφαρμοσθούν χωρίς ιδιαίτερο κόστος και μπορούν να δυσκολέψουν σημαντικά έναν επίδοξο εισβολέα.

- Κρυπτογράφηση της επικοινωνίας: Τα δεδομένα που μεταδίδονται θα πρέπει να κρυπτογραφούνται όπου αυτό είναι δυνατόν χρησιμοποιώντας κωδικούς πρόσβασης ή κατάλληλα ψηφιακά πιστοποιητικά. Στο πλαίσιο αυτό πρέπει να αποφεύγεται και η χρήση των υπηρεσιών FTP και Telnet. Οι υπηρεσίες αυτές μεταδίδουν δεδομένα και κωδικούς σύνδεσης χωρίς κρυπτογράφηση. Μπορούν να αντικατασταθούν από τις SSH, SFTP ή FTPS.
- Απεγκατάσταση των εφαρμογών που δεν χρειάζονται: Με τον τρόπο αυτόν μειώνονται τα κενά ασφαλείας και οι ευπάθειες που προέρχονται από το λογισμικό.
- Εκτέλεση μόνο μίας υπηρεσίας ανά υπολογιστή ή εικονική μηχανή: Αν ένα σύστημα παραβιαστεί θα επηρεαστεί μόνο η συγκεκριμένη υπηρεσία.
- Τακτική εγκατάσταση ενημερώσεων: Οι ενημερώσεις διορθώνουν τυχόν κενά ασφαλείας και αδυναμίες που ανακαλύπτονται κατά τη διάρκεια του κύκλου ζωής του λογισμικού
- Χρήση ισχυρών κωδικών και πολιτικών για πρόσβαση σε λογαριασμούς: Αλλαγή των κωδικών ανά τακτά χρονικά διαστήματα, απαγόρευση της επαναχρησιμοποίησης

προηγούμενων κωδικών, κλείδωμα των λογαριασμών μετά από διαδοχικές αποτυχίες σύνδεσης, κλείδωμα των ανενεργών λογαριασμών

- Φυσική Ασφάλεια των Server: Τοποθέτηση κωδικού στο BIOS, απενεργοποίηση της εκκίνησης από εξωτερικές μονάδες (CD, DVD, USB), τοποθέτηση των server σε κλειδωμένες ντουλάπες εξοπλισμού, περιορισμός των ατόμων που έχουν φυσική πρόσβαση σε αυτούς.
- Χρήση και σωστή ρύθμιση Firewall: Ο καλύτερος συνδυασμός είναι να υπάρχει software firewall σε κάθε υπολογιστή και hardware firewall στο δίκτυο.
- Αποθήκευση των δεδομένων σε διαφορετικά διαμερίσματα (partitions) από το λειτουργικό σύστημα.
- Διατήρηση αρχείων καταγραφής: Τα λειτουργικά συστήματα, αλλά και οι δικτυακές συσκευές έχουν τη δυνατότητα να κρατούν αρχεία καταγραφής με τις απόπειρες σύνδεσης, τις επιτυχημένες συνδέσεις κ.α. Αυτά μπορούν να χρησιμοποιηθούν για την αντιμετώπιση προβλημάτων, αλλά και μιας ενδεχόμενης απόπειρας παραβίασης.
- Σωστή ρύθμιση των δικαιωμάτων πρόσβασης σε αρχεία και φακέλους.
- Εκπαίδευση του προσωπικού: Πολλές φορές η ασφάλεια ενός συστήματος υποβαθμίζεται λόγω της άγνοιας ή της απροθυμίας του προσωπικού να εφαρμόσουν αυστηρά τις ισχύουσες πολιτικές ασφαλείας

8.4. Εικονικά Ιδιωτικά Δίκτυα (Virtual Private Networks-VPN)

Ένα Εικονικό Ιδιωτικό Δίκτυο, όπως υποδεικνύει και το όνομά του, μία τεχνολογία που επιτρέπει σε υπολογιστές που βρίσκονται σε απόσταση μεταξύ τους να μπορούν να συνδεθούν για να ανταλλάξουν πληροφορίες, να μοιραστούν αρχεία και να χρησιμοποιήσουν υπηρεσίες, σαν να ήταν συνδεδεμένοι στο ίδιο ασφαλές τοπικό δίκτυο.

Η σύνδεση των υπολογιστών γίνεται φυσικά μέσω του Διαδικτύου και για τη μετάδοση των δεδομένων χρησιμοποιούνται τεχνολογίες κρυπτογράφησης ώστε να εμποδιστεί η διάδοση των ιδιωτικών πληροφοριών σε μη εξουσιοδοτημένους χρήστες.

Υπάρχουν αρκετοί λόγοι για τους οποίους μπορεί να είναι επιθυμητή η χρήση ενός VPN:

- ***Ασφαλής σύνδεση σε απομακρυσμένο δίκτυο*:** Πολλές εταιρίες υλοποιούν VPN έτσι ώστε οι υπάλληλοί τους να έχουν απομακρυσμένη πρόσβαση σε αρχεία, εφαρμογές, εκτυπωτές ή άλλους πόρους του δικτύου εργασίας, χωρίς να κινδυνεύει η ασφάλεια του δικτύου.
- ***Σύνδεση πολλών ανεξάρτητων δικτύων μεταξύ τους*:** Πολλές μικρές ή μεγάλες επιχειρήσεις χρησιμοποιούν VPN για να συνδέουν μεταξύ τους υπολογιστές, εξυπηρετητές ή άλλες συσκευές που βρίσκονται σε γραφεία και καταστήματα που μπορεί να βρίσκονται οπουδήποτε στον κόσμο.
- ***Εξασφάλιση της Ιδιωτικότητας*:** Η χρήση ενός VPN κατά τη διάρκεια μιας σύνδεσης από ένα δημόσιο ή μη ασφαλές δίκτυο (π.χ. το wifi μιας καφετέριας ή ενός ξενοδοχείου) εμποδίζει άλλους χρήστες από το να υποκλέψουν κωδικούς και δεδομένα που μεταφέρονται μέσα από αυτήν.
- ***Άρση γεωγραφικού αποκλεισμού (geoblocking)*:** Πολλές διαδικτυακές υπηρεσίες επιβάλλουν περιορίζουν στη χρήση τους από συγκεκριμένες τοποθεσίες. Με τη χρήση ενός VPN ένας υπολογιστής μπορεί να εμφανίζεται σε διαφορετική τοποθεσία από αυτήν που βρίσκεται στην πραγματικότητα.

Οι τεχνολογίες VPN κάνουν χρήση πολλών διαφορετικών πρωτοκόλλων, που το καθένα έχει τα δικά του χαρακτηριστικά.

- **Point-to-Point Tunneling Protocol (PPTP):** Είναι το λιγότερο ασφαλές, όμως υποστηρίζεται από πολλά λειτουργικά συστήματα όπως τα Λ.Σ MS Windows, Linux και MAC OS.
- ***Layer 2 Tunneling Protocol (L2TP) και Internet Protocol Security (IPsec)*:** Περισσότερο ασφαλή από το PPTP, αλλά και περισσότερο πολύπλοκα και στην εγκατάσταση και τη διαμόρφωσή τους.
- ***Secure Sockets Layer (SSL)*:** Προσφέρει τον ίδιο βαθμό ασφάλειας όπως και οι συνδέσεις σε συστήματα τραπεζών ή άλλες ασφαλείς δικτυακές τοποθεσίες. Η σύνδεση σε αυτά συνήθως γίνεται μέσω ενός browser χωρίς να χρειάζεται ειδικό λογισμικό από την πλευρά του πελάτη.

Εικόνα 8.17: SSL VPN

8.5. Ανωνυμία στο Διαδίκτυο

«Στο Internet κανείς δεν ξέρει ότι είσαι σκύλος» έγραφε η λεζάντα στο σκίτσο του Πίτερ Στάινερ που δημοσιεύτηκε στο περιοδικό «The New Yorker» στις 5 Ιουλίου του 1993 και περιγράφει με χαρακτηριστικό τρόπο την ευρέως διαδεδομένη άποψη στη Διαδικτυακή επικοινωνία ότι οποιοσδήποτε μπορεί να παριστάνει τον οποιονδήποτε, αφού τα πρωτόκολλα επικοινωνίας δεν απαιτούν την ταυτοποίηση του χρήστη.

Εικόνα 8.18: Το διάσημο σκίτσο του Πίτερ Στάινερ.

(Πηγή: https://upload.wikimedia.org/wikipedia/en/f/f8/Internet_dog.jpg)

Από τις αρχές της διάδοσης της χρήσης του Διαδικτύου από το ευρύ κοινό, η χαοτική και αποκεντρωμένη φύση του το κατέστησαν ένα από τα σημαντικότερα μέσα έκφρασης των ανθρώπων σε όλον τον κόσμο. Στο γεγονός αυτό συνέβαλε και το ότι ο οποιοσδήποτε μπορούσε να δημοσιεύσει τις απόψεις του, χωρίς να χρειαστεί να αποκαλύψει την πραγματική του ταυτότητα ή καλυπτόμενος πίσω από ένα ψευδώνυμο, αποφεύγοντας έτσι τις πιθανές αρνητικές συνέπειες της έκφρασης μιας αντισυμβατικής θέσης.

Στον αντίποδα, αυτή η αίσθηση της διευρυμένης ελευθερίας είχε και τις αρνητικές της επιπτώσεις αφού επέτρεπε σε κάποιους να υβρίζουν, να συκοφαντούν, να εκφοβίζουν, να παρενοχλούν, να διαδίδουν σεξιστικές ή ρατσιστικές απόψεις, ακόμη και να οργανώνουν εγκληματικές ενέργειες θεωρώντας ότι δεν πρόκειται να εντοπισθούν.

Στην πραγματικότητα η ανωνυμία στο Διαδίκτυο είναι πολύ πιο σύνθετο θέμα απ' ότι εκ' πρώτης όψεως φαίνεται. Κάθε διακομιστής στο Διαδίκτυο κρατά λεπτομερή αρχεία με τις IP διευθύνσεις των υπολογιστών που συνδέονται σε αυτόν. Αντίστοιχα οι εταιρίες που παρέχουν πρόσβαση στο Διαδίκτυο (Internet Service Providers – ISP) γνωρίζουν και καταγράφουν το ποια IP διεύθυνση αντιστοιχεί σε κάθε χρήστη ανά πάσα χρονική στιγμή. Είναι λοιπόν απλό ζήτημα για τις διωκτικές αρχές κάποιας χώρας να εντοπίσουν κάποιον χρήστη που χρησιμοποιεί το Διαδίκτυο για την τέλεση παράνομων πράξεων.

Σήμερα, ειδικά με τη ραγδαία εξάπλωση των μέσων κοινωνικής δικτύωσης και των ιστολογιών, η αντιπαράθεση για τα οφέλη και τους κινδύνους από την ανωνυμία στο Διαδίκτυο είναι πιο έντονη από ποτέ. Και οι δύο πλευρές προβάλουν ισχυρά επιχειρήματα, ενώ δεν διαφαίνεται η ύπαρξη κάποιας λύσης που να μπορεί να συνδυάσει τα πλεονεκτήματα και των δύο πλευρών.

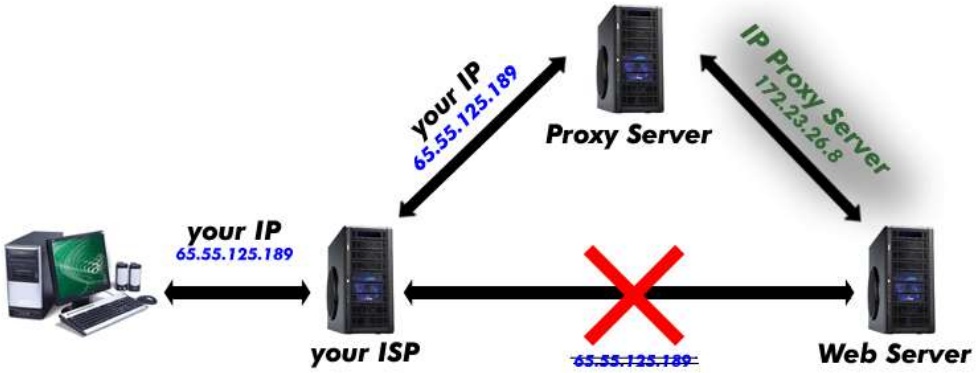
[Άσκηση 34 και 35]

8.5.1 Ανώνυμος Διακομιστής Μεσολάβησης (Anonymous Proxy)

Ένας διακομιστής μεσολάβησης (proxy server) είναι ένας εξυπηρετητής που παρεμβάλλεται ανάμεσα στη σύνδεση με το Internet ενός υπολογιστή ή ενός δικτύου, έτσι ώστε όλη η κίνηση από και προς το Διαδίκτυο να περνά μέσα από αυτόν.

Η πιο συνηθισμένη χρήση του είναι να αποθηκεύει τοπικά τις σελίδες του Διαδικτύου που ζητούνται πιο συχνά έτσι ώστε να μην υπάρχει ανάγκη μεταφοράς τους κάθε φορά από το Διαδίκτυο και με τον τρόπο αυτό να δίνεται η εντύπωση μιας ταχύτερης σύνδεσης. Επιπλέον μπορεί να χρησιμοποιηθεί για περιορισμό της πρόσβασης χρηστών σε σελίδες με ακατάλληλο γι' αυτούς περιεχόμενο, καταγραφή και περιορισμό του όγκου δεδομένων που διακινούνται ή ακόμη και του συνολικού χρόνου που διαρκεί μια σύνδεση ή της ώρα της ημέρας που αυτή πραγματοποιείται.

Ένας ανώνυμος διακομιστής μεσολάβησης είναι ένας ειδικού τύπου διακομιστής μεσολάβησης που αφαιρεί την IP διεύθυνση του υπολογιστή που ζήτησε μια σελίδα και την αντικαθιστά με τη δική του. Όταν τα δεδομένα της σελίδας φτάσουν στο διακομιστή μεσολάβησης αυτός τα στέλνει στον υπολογιστή που τα ζήτησε. Με τον τρόπο αυτό γίνεται δυνατή η απόκρυψη της IP διεύθυνσης (άρα και της τοποθεσίας) του χρήστη που περιηγείται στο Διαδίκτυο.



Εικόνα 8.19: Λειτουργία ανώνυμου διακομιστή μεσολάβησης

(Πηγή: https://proxysiteslists21.files.wordpress.com/2015/01/unblock-youtube.gif?w=534&h=219)

Οι πιο συνηθισμένοι ανώνυμοι διακομιστές μεσολάβησης είναι αυτοί που στηρίζονται στο Web. Το μόνο που έχει να κάνει ένας χρήστης είναι να επισκεφθεί την Web σελίδα του διακομιστή και να γράψει εκεί, σε ένα ειδικό πλαίσιο κειμένου, τη διεύθυνση της σελίδας που θέλει να δει. Η υπηρεσία θα μεταδώσει τα δεδομένα ανώνυμα.

Θα πρέπει να τονισθεί ότι η χρήση ενός ανώνυμου διακομιστή μεσολάβησης δεν εξασφαλίζει απόλυτα την ανωνυμία, διότι μπορεί ο τελικός αποδέκτης να μην γνωρίζει τη διεύθυνση του υπολογιστή του χρήστη, τη γνωρίζει όμως ο proxy server και συνήθως την καταχωρεί στα αρχεία καταγραφής της χρήσης της υπηρεσίας. Έτσι στην περίπτωση τέλεσης μιας αξιόποινης πράξης, τα αρχεία αυτά μπορούν να χρησιμοποιηθούν για να αποκαλυφθεί η πραγματική ταυτότητα του χρήστη. Ένα άλλο μειονέκτημα είναι ότι με τη χρήση αυτών των διακομιστών μειώνεται, λιγότερο ή περισσότερο, η ταχύτητα με την οποία κατεβαίνουν οι σελίδες, αφού αυτές έχουν πια μεγαλύτερη διαδρομή να ακολουθήσουν.

[Άσκηση 35 και 36]

8.5.2 Δίκτυο Tor (The onion router-Tor)

Το Tor είναι ένα αξιόπιστο και δυνατό εργαλείο κρυπτογράφησης που παρέχει ανωνυμία κατά την πλοήγηση στο Διαδίκτυο και προστατεύει το ηλεκτρονικό απόρρητο του χρήστη. Η πλήρης ονομασία του είναι The Onion Router (Tor), υποδηλώνοντας τα πολλά «στρώματα» (onion=κρεμμύδι) κρυπτογράφησης και το πλήθος διαμεσολαβητών υπολογιστών που χρησιμοποιούνται για την αποτελεσματική λειτουργία του εργαλείου. Οι διαμεσολαβητές υπολογιστές διαχειρίζονται από εθελοντές, οι οποίοι είναι συνδεδεμένοι στο δίκτυο Tor και χρησιμοποιούν το λογισμικό ανοικτού κώδικα στο οποίο βασίζεται η εφαρμογή. Τα δεδομένα που ανταλλάσσονται κινούνται κρυπτογραφημένα σε τυχαίες διαδρομές, τις οποίες κανένας συνδεδεμένος υπολογιστής δε γνωρίζει ολόκληρες εξασφαλίζοντας, έτσι, τη μεγίστη δυνατή ανωνυμία και προστασία.

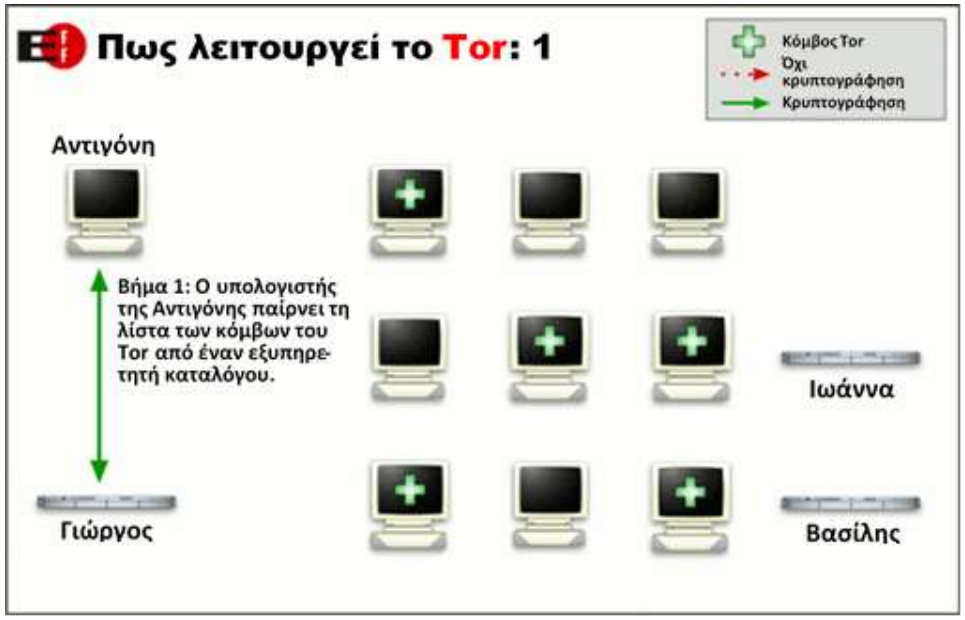
Η χρήση του Tor προστατεύει από μια κοινή μορφή επιτήρησης του Διαδικτύου που είναι γνωστή ως «ανάλυση κυκλοφορίας». Η ανάλυση κυκλοφορίας μπορεί να χρησιμοποιηθεί για να εξαχθούν συμπεράσματα για το ποιος μιλάει σε ποιον μέσω ενός δημόσιου δικτύου. Η γνώση της προέλευσης και του προορισμού της κίνησης στο Διαδίκτυο επιτρέπει σε άλλους να παρακολουθούν την παρακολούθηση της συμπεριφοράς και των ενδιαφερόντων των χρηστών.

Πώς δουλεύει η ανάλυση κυκλοφορίας; Όπως είναι γνωστό ένα πακέτων δεδομένων IP αποτελείται από δύο μέρη: το τμήμα δεδομένων και την επικεφαλίδα που χρησιμοποιείται (μεταξύ άλλων) για τη δρομολόγηση. Ακόμα κι το τμήμα δεδομένων είναι κρυπτογραφημένο,

η ανάλυση της κυκλοφορίας επικεντρώνεται στην κεφαλίδα, που αποκαλύπτει την προέλευση, τον προορισμό, το μέγεθος, τη χρονική στιγμή, και ούτω καθεξής.

Υπάρχουν πολλά και ισχυρά είδη ανάλυσης της κίνησης. Μερικοί επιτιθέμενοι παρακολουθούν πολλά μέρη του Διαδικτύου και χρησιμοποιούν εξελιγμένες στατιστικές τεχνικές για να παρακολουθούν τις επικοινωνίες πολλών διαφορετικών οργανισμών και ιδιωτών. Η Κρυπτογράφηση δεν βοηθά στην αντιμετώπιση αυτών των επιτιθεμένων, αφού κρύβει μόνο το περιεχόμενο της κίνησης στο Διαδίκτυο, όχι τις επικεφαλίδες.

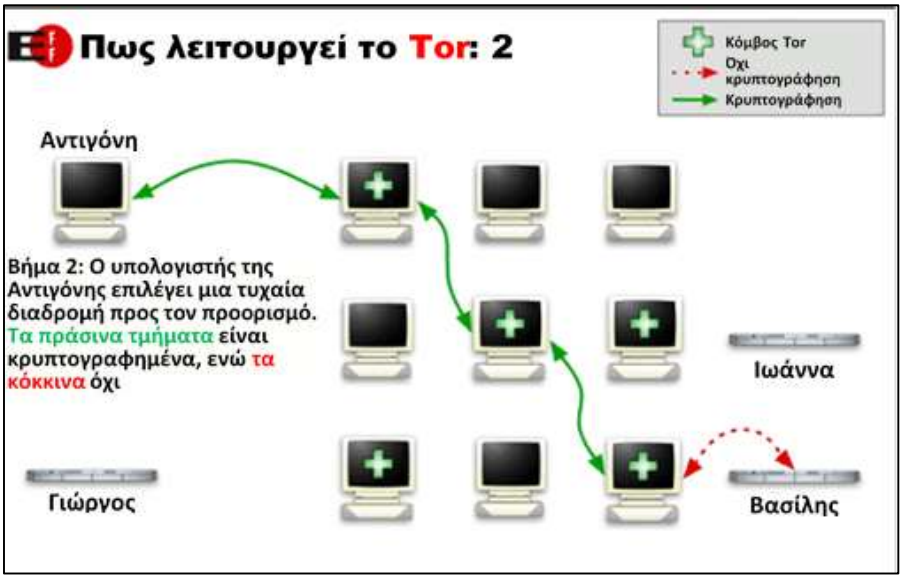
Το Tor βοηθά να μειωθούν οι κίνδυνοι τόσο από την απλή όσο και από την εξελιγμένη ανάλυση της κυκλοφορίας, με τη κατανομή της δικτυακής κίνησης πάνω σε διάφορα σημεία στο Διαδίκτυο, έτσι ώστε κανένα σημείο να μην μπορεί να παραπέμψει στην αρχική τοποθεσία. Η ιδέα είναι παρόμοια με τη χρήση ενός γεμάτου στροφές δρόμους, στον οποίο είναι δύσκολο να γίνει παρακολούθηση, ενώ επιπρόσθετα διαγράφεται ανά τακτά χρονικά διαστήματα κάθε ίχνος δραστηριότητας. Αντί τα πακέτα δεδομένων να ακολουθήσουν μια άμεση διαδρομή από την πηγή στον προορισμό, το δίκτυο Tor επιλέγει μια τυχαία διαδρομή μέσα από πολλούς ενδιάμεσους κόμβους, έτσι ώστε κανένας παρατηρητής να μην μπορεί να πει από πού προήλθαν τα δεδομένα, ή πού πηγαίνουν.



Εικόνα 8.20: Λειτουργία του Tor (βήμα 1).

(Τροποποιήθηκε από: https://www.torproject.org/images/htw1.png)

Για να δημιουργήσει ένα ιδιωτικό δίκτυο μονοπάτι με το Tor, το λογισμικό του χρήστη χτίζει σταδιακά ένα κύκλωμα κρυπτογραφημένων συνδέσεων μέσω των κόμβων του δικτύου. Το κύκλωμα επεκτείνεται κατά ένα βήμα τη φορά, και κάθε κόμβος κατά μήκος της διαδρομής ξέρει μόνο τον κόμβο που του έδωσε στοιχεία και τον κόμβο στον οποίο θα τα προωθήσει. Κανένας μεμονωμένος κόμβος δεν ξέρει την πλήρη διαδρομή που ακολουθεί ένα πακέτο δεδομένων που έχει λάβει. Ο πελάτης χρησιμοποιεί ένα ξεχωριστό σύνολο κλειδιών κρυπτογράφησης για κάθε βήμα κατά μήκος της διαδρομής, ώστε να εξασφαλίσει ότι κάθε σε κάθε βήμα δεν θα μπορεί να εντοπιστεί η προέλευση των συνδέσεων που εξυπηρετούνται.

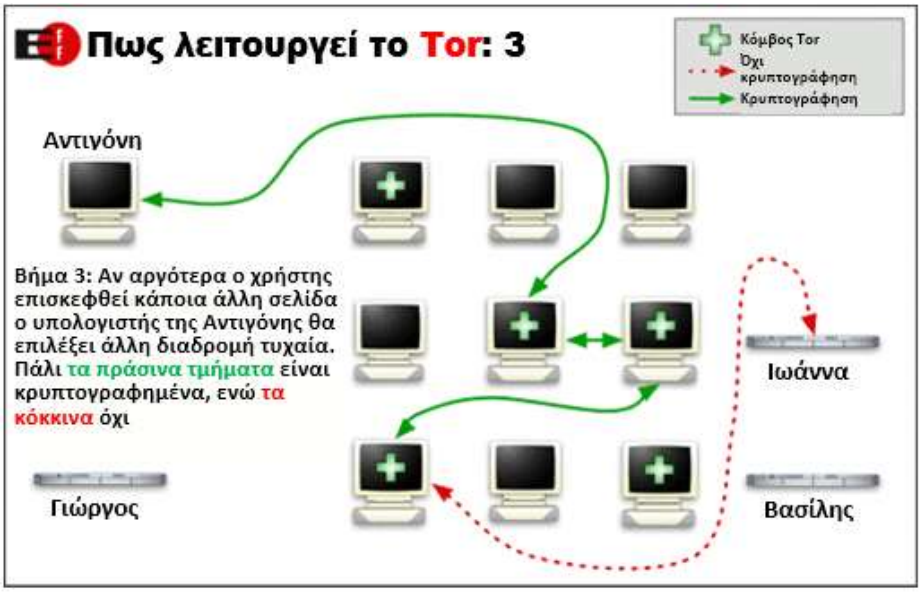


Εικόνα 8.21: Λειτουργία του Tor (βήμα 2).

(Τροποποιήθηκε από: https://www.torproject.org/images/htw2.png)

Μόλις ένα κύκλωμα εγκατασταθεί, μπορούν να το χρησιμοποιήσουν πολλές εφαρμογές ανταλλάσσοντας διάφορα είδη δεδομένων μέσα από το δίκτυο Tor. Επειδή κάθε κόμβος δεν βλέπει πέρα από ένα βήμα στο κύκλωμα, ένας εισβολέας σε κάποιον ενδιάμεσο κόμβου δεν μπορεί να χρησιμοποιήσει την ανάλυση της κυκλοφορίας για να συνδέσει την προέλευση με τον προορισμό της σύνδεσης. Το Tor λειτουργεί μόνο για TCP συνδέσεις και μπορεί να χρησιμοποιηθεί από οποιαδήποτε εφαρμογή που υποστηρίζει το πρωτόκολλο SOCKS.

Για αποτελεσματικότητα, το λογισμικό Tor χρησιμοποιεί το ίδιο κύκλωμα για συνδέσεις που δημιουργούνται εντός των δέκα λεπτών. Σε μεταγενέστερα αιτήματα δίνεται ένα νέο κύκλωμα, για να εμποδίσει τη συσχέτιση των προηγούμενων ενεργειών με τις επόμενες.



Εικόνα 8.22: Λειτουργία του Tor (βήμα 3).

(Τροποποιήθηκε από: https://www.torproject.org/images/htw3.png)

Το Tor δεν μπορεί να λύσει όλα τα προβλήματα της ανωνυμίας. Επικεντρώνεται μόνο στην προστασία της μεταφοράς των δεδομένων. Θα πρέπει να χρησιμοποιηθεί ειδικό λογισμικό υποστήριξης, από κάποιον που δεν θέλει οι ιστοσελίδες που επισκέπτεται να βλέπουν πληροφορίες με τις οποίες θα μπορούν να τον αναγνωρίσουν. Για παράδειγμα, μπορεί να γίνει χρήση του Tor Browser κατά την περιήγηση στο Διαδίκτυο ώστε να μην εμφανίζονται πληροφορίες σχετικά με τη διαμόρφωση του υπολογιστή.

Επίσης, η προστασία της ανωνυμίας επιβάλει την επαγρύπνηση του χρήστη που δεν θα πρέπει να δίνει το όνομά του ή άλλες πληροφορίες σε φόρμες. Θα πρέπει να γνωρίζετε ότι, όπως και όλα τα ανώνυμα δίκτυα που προσφέρουν ικανοποιητικές ταχύτητες για περιήγηση στο Web, το Tor δεν παρέχει προστασία απέναντι σε επιθέσεις «απ' άκρη σ' άκρη» (end-to-end). Αν ο επιτιθέμενος μπορεί να παρακολουθήσει την κίνηση που βγαίνει από ένα υπολογιστή, καθώς και την κίνηση που φθάνει στον επιλεγμένο προορισμό, μπορεί να χρησιμοποιήσει στατιστική ανάλυση για να ανακαλύψει ότι είναι μέρος του ίδιου κυκλώματος. Γενικά οι ενέργειες που πρέπει να κάνει ένας χρήστης για να αξιοποιήσει την ανωνυμία του Tor συνοψίζονται στα ακόλουθα:

- Να χρησιμοποιεί τον Tor Browser
- Να μην χρησιμοποιεί το Tor για κατέβασμα torrent.
- Να επισκέπτεται sites με ασφάλεια (https)
- Να μην ανοίγει αρχεία που κατέβασε με το Tor, αν πριν δεν αποσυνδεθεί από το Internet.

[Άσκηση 37 και 38]

Ερωτήσεις Ανακεφαλαίωσης

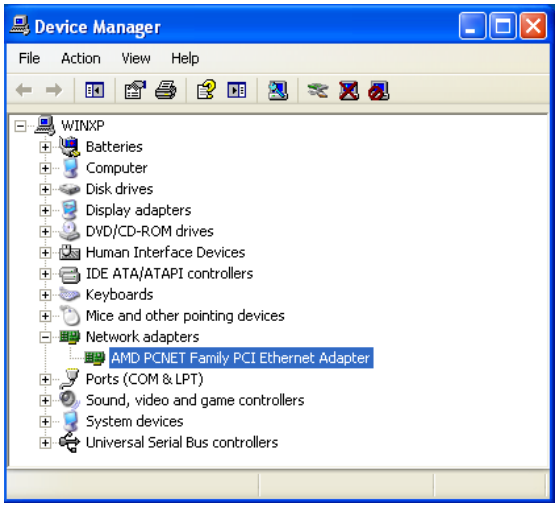
1. Τι γνωρίζετε για τη Μεταμφίεση MAC διευθύνσεων;
2. Σε τι αποσκοπεί μια επίθεση Κατανεμημένης Άρνησης Υπηρεσίας;
3. Τι είναι το ηλεκτρονικό ψάρεμα (phising);
4. Αναφέρετε δύο από τα χαρακτηριστικά που πρέπει να έχει ένας ισχυρός κωδικός πρόσβασης (password).
5. Ποιο το σημαντικότερο χαρακτηριστικό μιας συνάρτησης κερματισμού;
6. Ποια η βασική διαφορά της συμμετρικής από την ασυμμετρική κρυπτογράφηση;
7. Πως εξασφαλίζεται η εμπιστευτικότητα στην κρυπτογράφηση Δημόσιου-Ιδιωτικού κλειδιού;
8. Με ποιους τρόπους μπορεί κάποιος να γνωστοποιήσει το Δημόσιο κλειδί του;
9. Τι είναι ένα ψηφιακό πιστοποιητικό;
10. Ποιος ο σκοπός της Στεγανογραφίας;
11. Αναφέρετε δύο είδη αρχείων στα οποία μπορούν να ενσωματωθούν πληροφορίες με τη μέθοδο της Στεγανογραφίας, και δύο στα οποία δεν μπορούν.
12. Με ποια κριτήρια μπορεί ένα Τείχος Προστασίας να επιτρέψει ή να απαγορεύσει την επικοινωνία μεταξύ υπολογιστών;
13. Αναφέρετε δύο μειονεκτήματα των software firewall.
14. Αναφέρετε δύο από τις ενέργειες που ένας διαχειριστής μπορεί να κάνει για να αυξήσει την ασφάλεια ενός εξυπηρετητή (server).
15. Τι είναι ένα Εικονικό Ιδιωτικό Δίκτυο (VPN);
16. Πως λειτουργούν οι ανώνυμοι διακομιστές μεσολάβησης (Anonymous Proxy Servers);

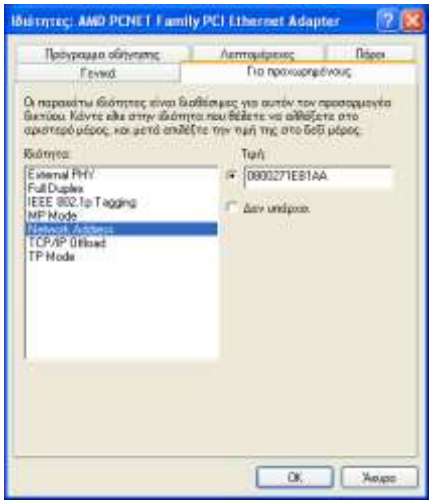
Ασκήσεις σε Εργαστηριακό Περιβάλλον

1η Άσκηση (Σε εργαστηριακό περιβάλλον Windows).

Στην άσκηση αυτή θα αλλάξετε τη MAC διεύθυνση μιας κάρτας δικτύου στο Λ.Σ MS Windows.

1. Ανοίξτε μια εικονική μηχανή με το Λ.Σ MS Windows XP και συνδεθείτε σε αυτήν με λογαριασμό διαχειριστή.
2. Βρείτε και καταγράψτε την MAC διεύθυνση της κάρτας δικτύου του υπολογιστή. Αυτό μπορεί να γίνει με την εντολή **ipconfig /all** από τη γραμμή εντολών ή από τις ιδιότητες της σύνδεσης δικτύου;
3. Από πόσες ομάδες χαρακτήρων αποτελείται η MAC διεύθυνση;
4. Σε ποιο αριθμητικό σύστημα είναι γραμμένη η MAC διεύθυνση;
5. Ποιοι είναι οι έγκυροι χαρακτήρες που μπορούν να χρησιμοποιηθούν σε κάθε ψηφίο μίας MAC διεύθυνσης;
6. Ξαναγράψτε τη MAC διεύθυνση του ερωτήματος 2, αλλάζοντας τους δύο τελευταίους χαρακτήρες της σε κάποιους άλλους (έγκυρους χαρακτήρες) της επιλογής σας.
7. Ανοίξτε τη διαχείριση συσκευών και μεταβείτε στην ενότητα «Προσαρμογείς Δικτύου» (Network Adapters), και κάντε διπλό-click πάνω στον προσαρμογέα δικτύου που εμφανίζεται.



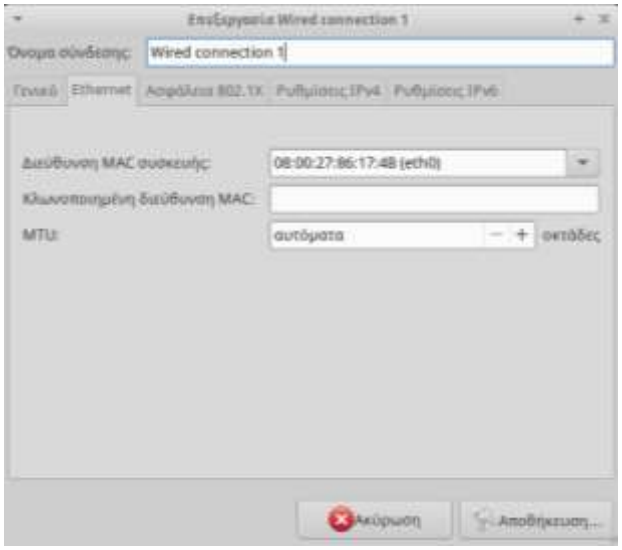


8. Στο παράθυρο των ιδιοτήτων πατήστε στην καρτέλα «Για προχωρημένους» και μετά στην ιδιότητα «Network Address». Εκεί βάλτε τη διεύθυνση που γράψατε στο βήμα 6, χωρίς όμως τους διαχωριστικούς χαρακτήρες (: ή -) και πατήστε [OK].
9. Με τη μέθοδο που χρησιμοποιήσατε στο βήμα 2 επιβεβαιώστε την αλλαγή της MAC διεύθυνσης.
10. Κάντε επανεκκίνηση των Windows και ελέγξτε αν η MAC διεύθυνση επανήλθε στην αρχική τιμή της. Αν όχι, κάντε τις απαραίτητες ενέργειες για να αναιρέσετε τις αλλαγές. Επιβεβαιώστε την επαναφορά της αρχικής τιμής.
11. Αφού η MAC διεύθυνση μιας κάρτας δικτύου είναι γραμμένη σε μνήμη ROM, την αλλάξατε στην πραγματικότητα; Τι ακριβώς συνέβη;

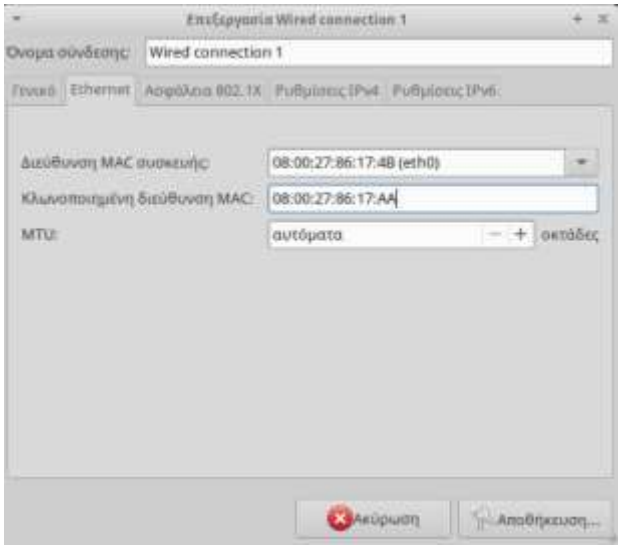
2η Άσκηση (Σε εργαστηριακό περιβάλλον Linux). Στην άσκηση αυτή θα αλλάξετε τη MAC διεύθυνση μιας κάρτας δικτύου στο Linux.

1. Ανοίξτε μια εικονική μηχανή με Linux και συνδεθείτε σε αυτήν με λογαριασμό διαχειριστή.

Βρείτε και καταγράψτε την MAC διεύθυνση της κάρτας δικτύου του υπολογιστή. Αυτό μπορεί να γίνει με την εντολή **ifconfig** στη γραμμή εντολών και κοιτώντας την τιμή του πεδίου HWaddr στη σύνδεση eth0 (για την 1η ενσύρματη κάρτα δικτύου), ή από το μενού Έναρξη → Ρυθμίσεις → Συνδέσεις Δικτύου, επιλέγοντας τη σύνδεση (συνήθως η «Wired connection 1») και πατώντας [Επεξεργασία…].



2. Από πόσες ομάδες χαρακτήρων αποτελείται η MAC διεύθυνση;
3. Σε ποιο αριθμητικό σύστημα είναι γραμμένη η MAC διεύθυνση;
4. Ποιοι είναι οι έγκυροι χαρακτήρες που μπορούν να χρησιμοποιηθούν σε κάθε ψηφίο μίας MAC διεύθυνσης;
5. Ξαναγράψτε τη MAC διεύθυνση του ερωτήματος 2, αλλάζοντας τους δύο τελευταίους χαρακτήρες της σε κάποιους άλλους (έγκυρους χαρακτήρες) της επιλογής σας.
6. Πατήστε Έναρξη → Ρυθμίσεις → Συνδέσεις Δικτύου, επιλέξτε τη σύνδεση δικτύου και πατήστε [Επεξεργασία…].
7. Στο πλαίσιο «Κλωνοποιημένη Διεύθυνση MAC» γράψτε την τροποποιημένη MAC διεύθυνση και πατήστε [Αποθήκευση…].



8. Για να ενεργοποιηθεί η αλλαγή θα πρέπει να γίνει αποσύνδεση και επανασύνδεση. Πατήστε στο εικονίδιο στη γραμμή εργασιών και επιλέξτε «Αποσύνδεση». Στη συνέχεια πατήστε ξανά στο εικονίδιο και επιλέξτε τη δικτυακή σύνδεση.
9. Επιβεβαιώστε δίνοντας την εντολή **ifconfig** ότι έγινε η αλλαγή.
10. Κάντε επανεκκίνηση του συστήματος και ελέγξτε αν η MAC διεύθυνση επανήλθε στην αρχική τιμή της. Αν όχι, κάντε τις απαραίτητες ενέργειες για να αναιρέσετε τις αλλαγές. Επιβεβαιώστε την επαναφορά της αρχικής τιμής.
11. Αφού η MAC διεύθυνση μιας κάρτας δικτύου είναι γραμμένη σε μνήμη ROM, την αλλάξατε στην πραγματικότητα; Τι ακριβώς συνέβη;

3η Άσκηση (Σε εργαστηριακό περιβάλλον).

Μία μέθοδος για να γίνει ένας κωδικός πρόσβασης πιο ασφαλής, αλλά ταυτόχρονα εύκολος στην απομνημόνευση είναι η αντικατάσταση γραμμάτων που περιέχει με αριθμούς ή σύμβολα που τους μοιάζουν.

1. Συμπληρώστε τον παρακάτω πίνακα με τα ψηφία ή τα σύμβολα που θεωρείτε ότι μπορούν να αντικαταστήσουν τα γράμματα που δίνονται. Μην περιοριστείτε απαραίτητα σε ένα σύμβολο (π.χ. D → I>).
2. Στις δύο τελευταίες κενές γραμμές γράψτε κάποιους άλλους χαρακτήρες μαζί με την πρότασή σας για σύμβολα αντικατάστασης.

a	b	c	E	B	i	L	q
Z	D	M	H	T	t	O	G

4η Άσκηση (Σε εργαστηριακό περιβάλλον).

Στην άσκηση αυτή θα δούμε ένα παράδειγμα του πως λειτουργούν οι μονόδρομες (one-way) συναρτήσεις που χρησιμοποιούνται για την αποθήκευση των κωδικών εισόδου των λειτουργικών συστημάτων.

Η Αντιγόνη και ο Βασίλης έχουν πάθος με τα σταυρόλεξα. Κάθε εβδομάδα ανταγωνίζονται στο σταυρόλεξο της Κυριακάτικης εφημερίδας. Την Κυριακή το βράδι μιλούν στο τηλέφωνο και συγκρίνουν τις λέξεις που έχει ο καθένας βρει. Ωστόσο, επειδή κανένας από τους δύο δεν θέλει να αποκαλύψει τις λέξεις που βρήκε, έχουν συμφωνήσει στον εξής κανόνα:

Έστω ότι η Αντιγόνη γνωρίζει ότι η σωστή απάντηση στο 1 κάθετα Β είναι η λέξη "**Περιφρονώ"**. Αντί να πει απευθείας της λέξη, χρησιμοποιεί το "Ερμηνευτικό Λεξικό της Νέας Ελληνικής" και κάνει τις ακόλουθες ενέργειες:

- Βρίσκει τον ορισμό της λέξης **"Περιφρονώ"** (ενδεχομένως μαζί με παράδειγμα): αισθάνομαι[1] ή εκδηλώνω πλήρη αδιαφορία και έλλειψη εκτίμησης για κπ ή κτ ≠ σέβομαι. Βρίσκει στον παραπάνω ορισμό την **πρώτη** λέξη που είναι ουσιαστικό, επίθετο ή ρήμα, στην περίπτωση αυτή τη λέξη **"Αισθάνομαι"**.
- Βρίσκει τον ορισμό της λέξης **"Αισθάνομαι":** νιώθω[1] (μτβ.) αντιλαμβάνομαι[2] μέσω των αισθήσεων. Βρίσκει στον παραπάνω ορισμό τη **δεύτερη** λέξη που είναι η **"Αντιλαμβάνομαι"**.
- Βρίσκει τον ορισμό της λέξης **"Αντιλαμβάνομαι":** καταλαβαίνω[1] κτ μέσω των αισθήσεών[2] μου: Ο κλέφτης[3] μπήκε στο διαμέρισμα χωρίς να τον αντιληφθούμε. Βρίσκει στον παραπάνω ορισμό την **τρίτη** λέξη που είναι η λέξη **"Κλέφτης"**.
- Βρίσκει τον ορισμό της λέξης **"Κλέφτης"** (κάτω από το βασικό λήμμα Κλέβω): άτομο[1] που κλέβει[2] κτ από κπ: ~ μπήκαν[3] στο διπλανό μαγαζί[4] και το άδειασαν. Βρίσκει στον παραπάνω ορισμό την **τέταρτη** λέξη που είναι η λέξη **"Μαγαζί"** (η λέξη διπλανό παραλείπεται γιατί είναι επίρρημα).
- Βρίσκει τον ορισμό της λέξης **"Μαγαζί"**: κτίριο[1] ή τμήμα[2] κτιρίου[3] όπου πουλιούνται[4] διάφορα[5] αγαθά = κατάστημα. Βρίσκει στον παραπάνω ορισμό την **πέμπτη** λέξη που είναι η λέξη **"Διάφορα"**.
- Λέει στον Βασίλη τη λέξη **"Διάφορα"**. Αν ο Βασίλης έχει βρει και αυτός τη σωστή λέξη, μπορεί εύκολα ακολουθώντας το λεξικό να επιβεβαιώσει ότι η Αντιγόνη έχει βρει τη σωστή απάντηση.

1. Δοκιμάστε να κάνετε κι' εσείς το ίδιο με μια λέξη και το λεξικό που θα σας δώσει ο καθηγητής σας και που θα αποτελεί τη σωστή απάντηση σε κάποιον από τους υπόλοιπους ορισμούς του σταυρόλεξου.
2. Στο παραπάνω παράδειγμα, συζητήστε με τα μέλη της ομάδας σας πως ο Βασίλης, στην περίπτωση που δεν γνωρίζει ο ίδιος τη σωστή λέξη, θα μπορούσε να βρει τη σωστή λέξη βασισμένος στην τελική λέξη ("Διάφορα") που του έδωσε η Αντιγόνη. Θα είναι μια διαδικασία εξίσου εύκολη με την εύρεση της τελικής λέξης από την αρχική;
3. Υπάρχει κάτι που θα μπορούσε να κάνει ο Βασίλης ώστε να "επιταχύνει" τη διαδικασία αυτή, γνωρίζοντας ότι το πλήθος των λέξεων του λεξικού είναι συγκεκριμένο;
4. Ανοίξτε τη σελίδα *http://www.fileformat.info/tool/hash.htm* για να δείτε μερικές από τις πραγματικές μονόδρομες συναρτήσεις κατατεμαχισμού (hash functions). Στη σελίδα αυτή μπορείτε να καταχωρήσετε μια λέξη ή φράση και να δείτε τη σύνοψη που προκύπτει.
5. Καταχωρήστε στο πρώτο πεδίο τη λέξη **AADVARK**, πατήστε στο κουμπί [Hash] και δείτε στο τέλος της σελίδας τα αποτελέσματα.
6. Δείτε στη σελίδα *http://www.rapidtables.com/code/text/ascii-table.htm* τον ASCII κώδικα για το γράμμα **A**. Από πόσα δυαδικά ψηφία αποτελείται;

7. Στην ίδια σελίδα δείτε και τον κώδικα για το γράμμα **B**. Κατά πόσα bit διαφέρει από αυτόν του A;
8. Αλλάξτε το πρώτο A της λέξης σε B και υπολογίστε ξανά τις συνόψεις.
9. Κατά πόσα δυαδικά ψηφία αλλάξατε την αρχική λέξη;
10. Τι αποτέλεσμα επέφερε στις συνόψεις η αλλαγή που πραγματοποιήσατε;
11. Εισάγετε μερικά ακόμη πιθανά password διαφόρων μεγεθών (όχι κάποιο που χρησιμοποιείτε) και υπολογίστε για το καθένα τη σύνοψη
12. Επηρεάζεται το πλήθος των χαρακτήρων της σύνοψης κάθε αλγορίθμου από το μέγεθος της φράσης που εισάγατε;
13. Συμπληρώστε το ακόλουθο πίνακα:

Αλγόριθμος	**Πλήθος Χαρακτήρων Σύνοψης**	**Πλήθος bit Σύνοψης**
Adler32		
CRC32		
Haval		
MD2		
MD4		
MD5		
RipeMD128		
RipeMD160		
SHA-1		
SHA-256		
SHA-384		
SHA-512		
Tiger		
Whirlpool		
* Ένας εύκολος τρόπος για να μετρήσετε το πλήθος των χαρακτήρων της σύνοψης είναι να τους επικολλήσετε σε έναν διορθωτή κειμένου τύπου Notepad και να δείτε από εκεί το πλήθος τους από τη γραμμή κατάστασης.		

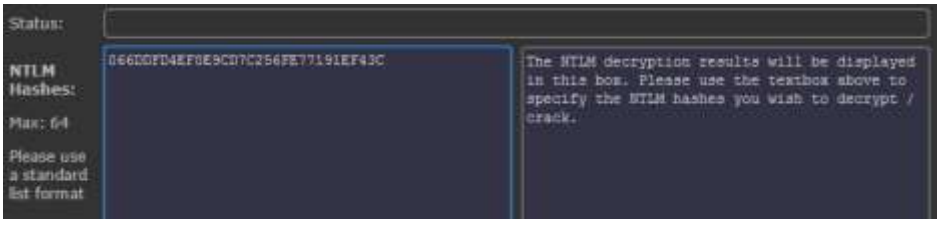
14. Ένα πρόβλημα με τις συναρτήσεις κατατεμαχισμού είναι η περίπτωση δύο διαφορετικές φράσεις να δώσουν το ίδιο αποτέλεσμα (αναζητήστε στο Internet "**hash collision**"). Γράψτε τα ονόματα των δύο αλγορίθμων που θεωρείτε ότι υπάρχει η μεγαλύτερη πιθανότητα να συμβεί κάτι τέτοιο και των δύο αλγορίθμων που έχουν τις μικρότερες πιθανότητες να συμβεί κάτι τέτοιο. Σε ποιο γεγονός στηρίζετε την απάντησή σας;

5η Άσκηση (Σε εργαστηριακό περιβάλλον).

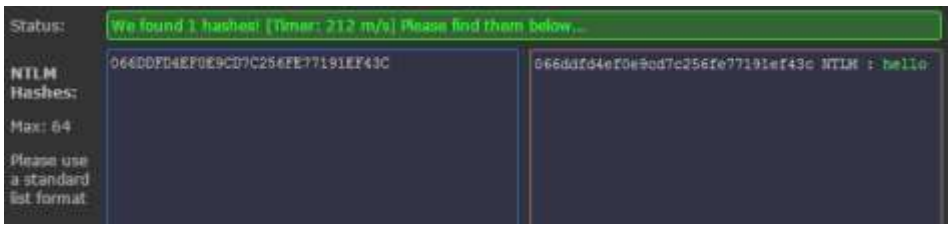
Η συνάρτηση κερματισμού που χρησιμοποιεί το Λ.Σ MS Windows (από την έκδοση 7 και μετά) για την εύρεση της σύνοψης ενός συνθηματικού λέγεται NTLM.

1. Ανοίξτε τη σελίδα *http://www.tobtu.com/lmntlm.php* (εφεξής σελίδα Α). Στη σελίδα αυτή μπορείτε να δώσετε μια συνθηματική λέξη και να πάρετε τη σύνοψή της όπως την υπολογίζει το Λ.Σ MS Windows. Για να το κάνετε αυτό γράψτε τη λέξη ή φράση που θέλετε στο πεδίο **κάτω** από τη λέξη [Passwords] και πατήστε [Generate Passwords]. Η σύνοψη εμφανίζεται κάτω από το [NTLM Hashes]. Δοκιμάστε π.χ. με τη λέξη "hello".

2. Από έρευνες έχει διαπιστωθεί ότι οι περισσότεροι χρήστες χρησιμοποιούν λέξεις της καθομιλουμένης σαν κωδικούς πρόσβασης. Έτσι οι λέξεις αυτές είναι από τις πρώτες για τις οποίες δημιουργήθηκαν πίνακες αντίστροφης αναζήτησης. Η σελίδα *http://www.hashkiller.co.uk/ntlm-decrypter.aspx* (σελίδα Β) περιέχει τέτοιους πίνακες (για 43,745 δις κωδικούς) και σας επιτρέπει να αναζητήσετε τον κωδικό, δίνοντας τη σύνοψη. Από τη σελ. Α αντιγράψτε το NTLM Hash και επικολλήστε το στη σελ. Β στα αριστερά.



3. Κατεβείτε στο κάτω μέρος της σελίδας, συμπληρώστε το CAPTCHA και πατήστε [Submit]. Αν η σύνοψη που δώσατε υπάρχει στον αντίστροφο πίνακα, θα σας εμφανιστεί το password που της αντιστοιχεί.



4. Μπορείτε να χρησιμοποιήσετε τις δύο αυτές σελίδες για να ελέγξετε κατά πόσο έχει ήδη σπάσει ένας νέος κωδικός που θέλετε να χρησιμοποιήσετε. Δοκιμάστε π.χ. τις ακόλουθες λέξεις (από τη Σελ. Α θα πάρετε τη σύνοψη που θα επικολλήσετε στη σελ. Β) και σημειώστε για ποιες από αυτές υπάρχουν ήδη στον αντίστροφο πίνακα.

Κωδικός	Αποτέλεσμα (✓ ή Χ)	Κωδικός	Αποτέλεσμα (✓ ή Χ)
letmein		password!	
password		p@ssw0rd!	
independent		BadBoy	
corresponding		thisisatest	
discovery		!nd3p3nI)ent	
discoveries		123456789	

6η Άσκηση (Σε εργαστηριακό περιβάλλον Windows, Linux)

Στην άσκηση αυτή θα χρησιμοποιήσετε την εφαρμογή ophcrack σε μια προσπάθεια να βρείτε έναν κωδικό windows που πιθανόν να έχετε ξεχάσει. Η εφαρμογή ξεκινά από live-cd και χρησιμοποιεί έναν συνδυασμό πινάκων αναζήτησης και εξαντλητικής δοκιμής κωδικών (brute force) προκειμένου να ανακαλύψει τον κωδικό κάθε λογαριασμού χρήστη.

1. Ξεκινήστε μια εικονική μηχανή με Windows 7 και συνδεθείτε με λογαριασμό διαχειριστή.
2. Δημιουργήστε τους ακόλουθους λογαριασμούς με τους αντίστοιχους κωδικούς:

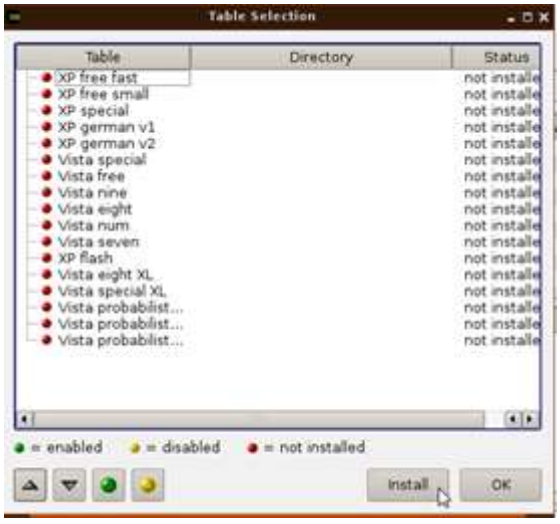
Όνομα Χρήστη	**Κωδικός**
dictionary	history
weak	ntfs17
medium	f@c3b0ok
strong	I.L0v3.Ch0k0L@t3$

3. Κάντε τερματισμό των Windows.
4. Στις ιδιότητες της εικονικής μηχανής τοποθετείστε στο εικονικό DVD το αρχείο “ophcrack-vista-livecd-3.6.0.iso”, από την τοποθεσία που θα σας πει ο καθηγητής σας.

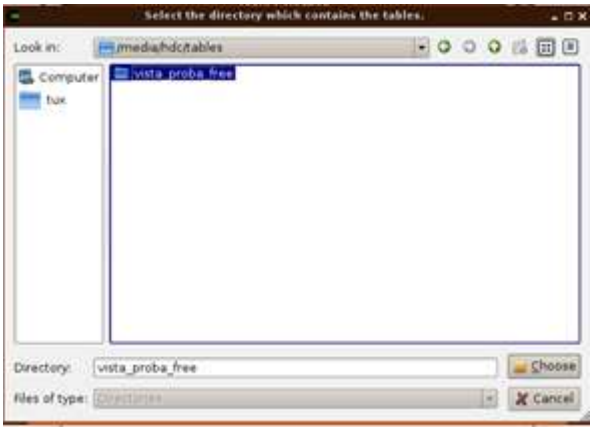
5. Ξεκινήστε πάλι την εικονική μηχανή που τώρα θα πρέπει να φορτώσει το λειτουργικό που υπάρχει στο CD.
6. Στην αρχικό μενού που θα εμφανιστεί αφήστε επιλεγμένη την πρώτη καταχώρηση (Αυτόματο) και πατήστε [Enter].

7. Όταν φορτώσει το λειτουργικό (μια έκδοση του Linux) θα εμφανιστεί το παράθυρο του ophcrack. Πατήστε στο κουμπί [Stop].
8.

9. Στη συνέχεια πατήστε στο κουμπί [Tables] ώστε να φορτώσουμε τον πίνακα αντίστροφης αναζήτησης (lookup ή rainbow table). Στο παράθυρο που θα εμφανιστεί πατήστε στο κουμπί [Install].

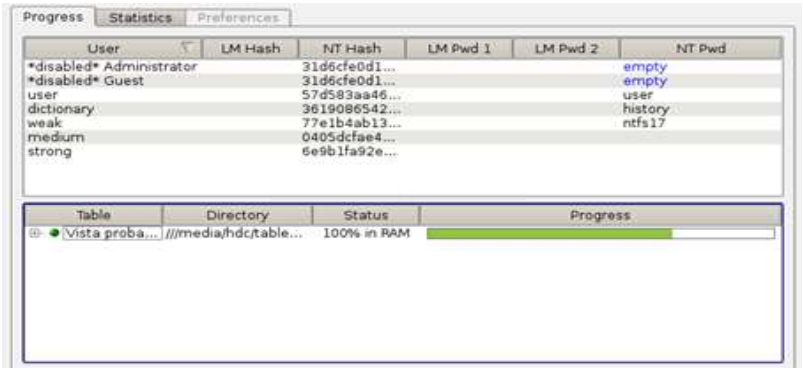


10. Από τον κατάλογο Look In επιλέξτε / και μετά media/hdc/tables/vista_ proba_free και πατήστε [Choose] και [OK].



11. Θα επιστρέψετε στο αρχικό παράθυρο. Πατήστε στο [Crack] για να ξεκινήσει η διαδικασία ανεύρεσης των κωδικών.

12. Παρατηρείστε ότι ενώ οι κωδικοί που είναι λέξεις από λεξικό ή μικροί σε μέγεθος και πολυπλοκότητα εμφανίζονται γρήγορα, οι υπόλοιποι μπορεί και να μην βρεθούν καθόλου.



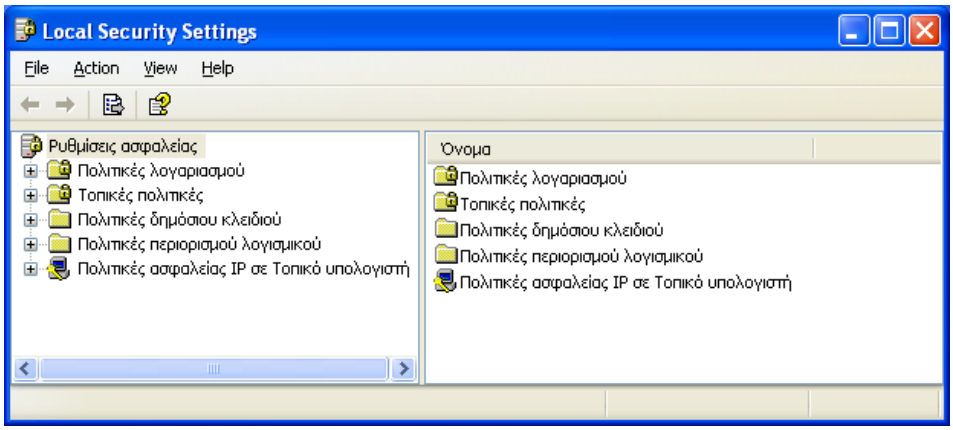
13. Θεωρείτε ότι αν το ophcrack δεν μπορεί να βρει έναν κωδικό, αυτό σημαίνει ότι αυτός είναι ασφαλής; Ανοίξτε τη σελίδα https://www.objectif-securite.ch/en/ophcrack.php που περιέχει επιπλέον πίνακες αναζήτησης (Free NTHASH tables) για το ophcrack.
14. Με δεδομένο ότι το πρόγραμμα και οι πίνακες χώρεσαν σε ένα cd, ποιους πίνακες πιστεύετε ότι χρησιμοποιεί το live-cd και ποιο το μέγεθός τους;
15. Ποιο είναι το μεγαλύτερο μέγεθος δωρεάν πινάκων NTHASH;
16. Εκτός από τους δωρεάν πίνακες υπάρχουν και άλλοι (Professional) που χρεώνονται. Ποιο το μεγαλύτερο μέγεθός τους;
17. Τελικά τι απαντάτε στην ερώτηση 12;

7η Άσκηση (Σε εργαστηριακό περιβάλλον Windows).

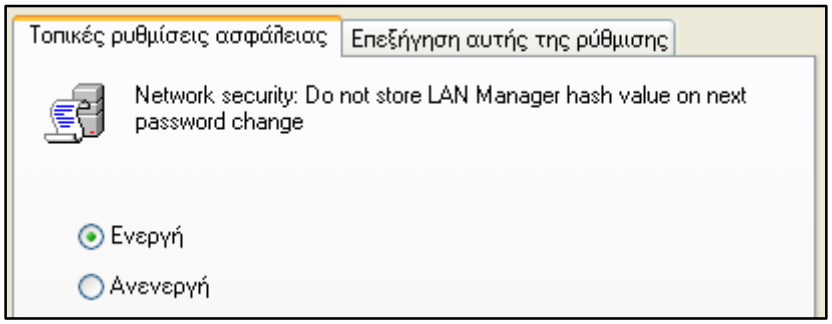
Το Λ.Σ MS Windows XP χρησιμοποιεί μία λιγότερο ασφαλή μέθοδο διαχείρισης των κωδικών (LM Hashes αντί NTLM Hashes), χωρίζοντας τους κωδικούς με πλήθος έως και 14 χαρακτήρες σε δύο κομμάτια και υπολογίζοντας ξεχωριστή σύνοψη για τον καθένα. Στην άσκηση αυτή θα δούμε πως μπορούμε να αλλάξουμε αυτή τη συμπεριφορά και να τα

υποχρεώσουμε να χρησιμοποιούν την πιο ασφαλή μέθοδο που εφαρμόζεται εξ' ορισμού από τα Vista και μετά.

1. Ανοίξτε μια εικονική μηχανή με Windows XP Professional και συνδεθείτε με λογαριασμό διαχειριστή.
2. Πατήστε Έναρξη/Εκτέλεση, γράψτε "secpol.msc" και πατήστε [Enter]. Θα ανοίξει το παράθυρο ρυθμίσεων των Πολιτικών Ασφαλείας.



3. Από τον κατάλογο στα αριστερά επιλέξτε Τοπικές πολιτικές → Επιλογές ασφαλείας. Στα δεξιά βρείτε την επιλογή «Ασφάλεια δικτύου: Να μην γίνει αποθήκευση της τιμής κατακερματισμού της Διαχείρισης τοπικού δικτύου στην επόμενη αλλαγή κωδικού πρόσβασης» (Network security: Do not store LAN Manager hash value on next password change) και ανοίξτε την.



4. Αλλάξτε τη ρύθμιση από «Ανενεργή» σε «Ενεργή» και πατήστε [OK]. Η νέα ρύθμιση θα ενεργοποιηθεί για κάθε λογαριασμό χρήστη στην επόμενη αλλαγή του κωδικού πρόσβασης.
5. Η ρύθμιση αυτή μπορεί να επηρεάσει την επικοινωνία στο δίκτυο μεταξύ υπολογιστών με Windows XP και παλαιότερων λειτουργικών όπως τα Windows 95 και τα Windows 98 (αν υπάρχουν).

8η Άσκηση (Σε εργαστηριακό περιβάλλον Linux)

Στην άσκηση αυτή θα χρησιμοποιήσετε το Live-CD Kali Linux σε μια προσπάθεια να βρείτε έναν κωδικό windows που πιθανόν να έχετε ξεχάσει. Η εφαρμογή ξεκινά από live-cd και χρησιμοποιεί έναν συνδυασμό πινάκων αναζήτησης και εξαντλητικής δοκιμής κωδικών (brute force) προκειμένου να ανακαλύψει τον κωδικό κάθε λογαριασμού χρήστη.

1. Ξεκινήστε μια εικονική μηχανή με Linux και συνδεθείτε με λογαριασμό διαχειριστή.
2. Δημιουργήστε τους ακόλουθους λογαριασμούς με τους αντίστοιχους κωδικούς:

Όνομα Χρήστη	Κωδικός
dictionary	history
weak	ntfs17
medium	f@c3b0ok
strong	I.L0v3.Ch0k0L@t3$

3. Κάντε τερματισμό του Linux.
4. Στις ιδιότητες της εικονικής μηχανής τοποθετείστε στο εικονικό DVD το αρχείο “kali-linux-1.1.0a-i386.iso”, από την τοποθεσία που θα σας πει ο καθηγητής σας.
5. Ξεκινήστε πάλι την εικονική μηχανή που τώρα θα πρέπει να φορτώσει το λειτουργικό που υπάρχει στο CD.
6. Στο αρχικό μενού που θα εμφανιστεί αφήστε επιλεγμένη την πρώτη καταχώρηση και πατήστε [Enter].
7. Όταν φορτώσει το λειτουργικό ανοίξτε ένα νέο παράθυρο τερματικού πατώντας στο εικονίδιο ή επιλέγοντας Applications → Accessories → Terminal.
8. Δώστε την εντολή **fdisk -l** για να δείτε τους δίσκους που είναι συνδεδεμένοι στο σύστημα.

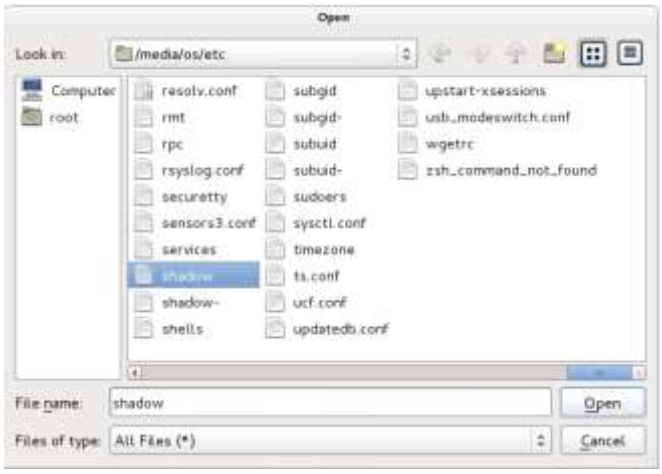
```
root@kali:~# fdisk -l

Disk /dev/sda: 42.9 GB, 42949672960 bytes
255 heads, 63 sectors/track, 5221 cylinders, total 83886080 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x0006ff09

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *        2048    82315263    41156608   83  Linux
/dev/sda2        82317310    83884031      783361    5  Extended
/dev/sda5        82317312    83884031      783360   82  Linux swap / Solaris
```

9. Ο δίσκος του λειτουργικού της εικονικής μηχανής είναι ο /dev/sda1. Για να μπορέσετε να τον προσπελάσετε θα πρέπει να τον προσαρτήσετε (mount) σε έναν φάκελο του Live-CD. Δώστε την εντολή **mkdir /media/os** για να φτιάξετε ένα φάκελο με όνομα os μέσα στο φάκελο media.
10. Δώστε την εντολή **mount /dev/sda1 /media/os** για να γίνει η προσάρτηση του δίσκου στο φάκελο os. Τα περιεχόμενα του δίσκου αυτού θα φαίνονται πλέον σαν αρχεία και φάκελοι μέσα στο φάκελο os. Για να δείτε αν όντως συμβαίνει αυτό δώστε την εντολή **ls /media/os** ώστε να δείτε τα περιεχόμενα του φακέλου.

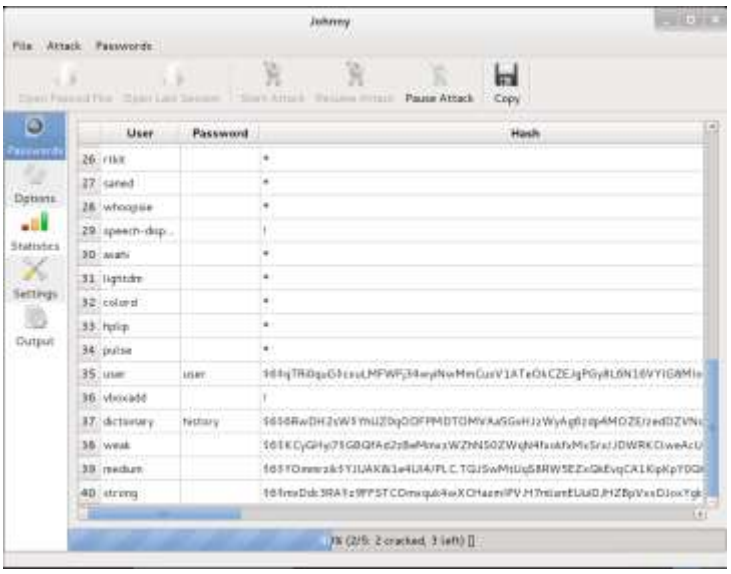
```
root@kali:~# ls /media/os
bin   dev   initrd.img      lost+found  opt   run   sys  var
boot  etc   initrd.img.old  media       proc  sbin  tmp  vmlinuz
cdrom home  lib             mnt         root  srv   usr  vmlinuz.old
```

11. Επιλέξτε Applications → Kai Linux → Password Attacks → Offline Attakcs → johnny. Αυτό είναι ένα γραφικό περιβάλλον για το πρόγραμμα John the Ripper (Τζων ο «Αντεροβγάλτης») !!!.
12. Το αρχείο στο οποίο το Linux κρατά τη σύνοψη των κωδικών είναι το /etc/shadow. Εδώ, επειδή ο δίσκος του Linux έχει προσαρτηθεί στην τοποθεσία /media/os, το αρχείο με τους κωδικούς είναι τελικά στη θέση /media/os/etc/shadow. Πατήστε στο

κουμπί [Open Passwd File], βρείτε το παραπάνω αρχείο και πατήστε [Open] και μετά [Start Attack].



13. Θα εμφανιστούν οι λογαριασμοί χρηστών που υπάρχουν στο σύστημα και θα ξεκινήσει η διαδικασία ανεύρεσης των κωδικών. Εντοπίστε τους λογαριασμούς που φτιάξατε στην αρχή της άσκησης.
14. Αφήστε τη διαδικασία να εκτελεστεί για μερικά λεπτά. Ποιων λογαριασμών οι κωδικοί θα εμφανιστούν πρώτοι;



15. Ανάλογα με την πολυπλοκότητα κάποιων κωδικών μπορεί να χρειαστεί πολύς χρόνος για την ανεύρεσή τους. Διακόψτε τη διαδικασία και κλείστε την εικονική μηχανή.

9η Άσκηση (Σε εργαστηριακό περιβάλλον Windows).

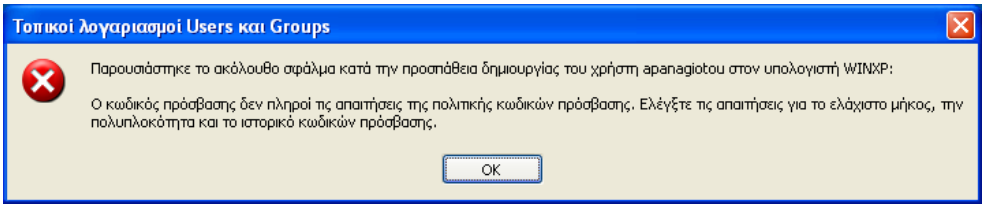
Στην άσκηση αυτή θα ρυθμίσετε το λειτουργικό σύστημα ώστε να δέχεται κωδικούς πρόσβασης που να πληρούν συγκεκριμένα χαρακτηριστικά (κανόνες πολυπλοκότητας).

1. Ανοίξτε μια εικονική μηχανή με το Λ.Σ MS Windows XP ή μεταγενέστερα και συνδεθείτε σε αυτήν με λογαριασμό διαχειριστή.
2. Από το μενού έναρξη επιλέξτε Εκτέλεση και δώστε την εντολή **secpol.msc**
3. Στο παράθυρο που θα εμφανιστεί πατήστε στα αριστερά στις «*Πολιτικές Λογαριασμού*» και μετά στο «*Πολιτική Κωδικού Πρόσβασης*».

4. Εξετάστε την πολιτική *«Οι κωδικοί πρόσβασης πρέπει να πληρούν τις προϋποθέσεις πολυπλοκότητας»*. Πατήστε στην καρτέλα Επεξήγηση για να πάρετε περισσότερες πληροφορίες. Συμπληρώστε τον ακόλουθο πίνακα ανάλογα με το ποιες προϋποθέσεις πληρούν οι κωδικοί της 1ης στήλης, αν το όνομα του χρήστη είναι apanag. Δίνονται οι απαντήσεις για τον πρώτο κωδικό:

Κωδικός	**Πληροί το Ελάχιστο Μήκος;**	**Περιέχει το όνομα χρήστη;**	**Πλήθος κατηγοριών χαρακτήρων**	**Πληροί όλους τους κανόνες;**
letmein	ΝΑΙ (7≥6)	ΟΧΙ	1	ΟΧΙ
Chargers1				
Panthers1				
#apanag12!				
!QaZ2				
Prototype1				
@WSX2wsx				

5. Ενεργοποιήστε την πολιτική ασφάλειας.
6. Δημιουργήστε έναν λογαριασμό απλού χρήστη (όχι διαχειριστή) με όνομα **apanag** και δοκιμάστε να του δώσετε τους παραπάνω κωδικούς πρόσβασης. Συμφωνούν τα Windows με τις εκτιμήσεις που εσείς κάνατε; Αν όχι, ψάξτε να βρείτε που κάνατε λάθος. Π.χ. για τον πρώτο κωδικό θα πάρουμε:



7. Έστω ότι θέλουμε επιπλέον να επιβάλουμε και τους ακόλουθους περιορισμούς στους κωδικούς των λογαριασμών των χρηστών:
   - Οι κωδικοί να αποτελούνται από οκτώ τουλάχιστον χαρακτήρες.
   - Όταν ένας χρήστης χρησιμοποιεί τον ίδιο κωδικό για 30 ημέρες να υποχρεώνεται να τον αλλάξει.
   - Όταν ένας χρήστης αλλάξει κωδικό να μην μπορεί να τον αλλάξει ξανά πριν περάσουν 5 ημέρες.
   - Κατά την αλλαγή κωδικού ο χρήστης να μην μπορεί να ξαναδώσει τον κωδικό που χρησιμοποιούσε μέχρι εκείνη τη στιγμή.

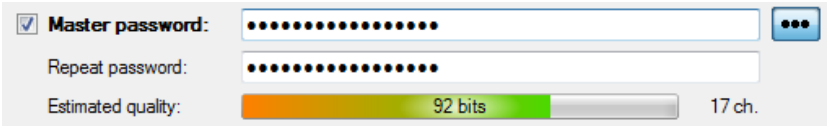
   Συμπληρώστε τον πίνακα με τις τιμές που θα πρέπει να πάρουν οι ακόλουθες πολιτικές έτσι ώστε να υλοποιηθούν αυτοί οι περιορισμοί:

Πολιτική	Παλιά Τιμή	Νέα Τιμή
Ελάχιστη διάρκεια κωδικού πρόσβασης		
Ελάχιστο μήκος κωδικού πρόσβασης		
Επιβολή ιστορικού κωδικών πρόσβασης		
Μέγιστη διάρκεια κωδικού πρόσβασης		

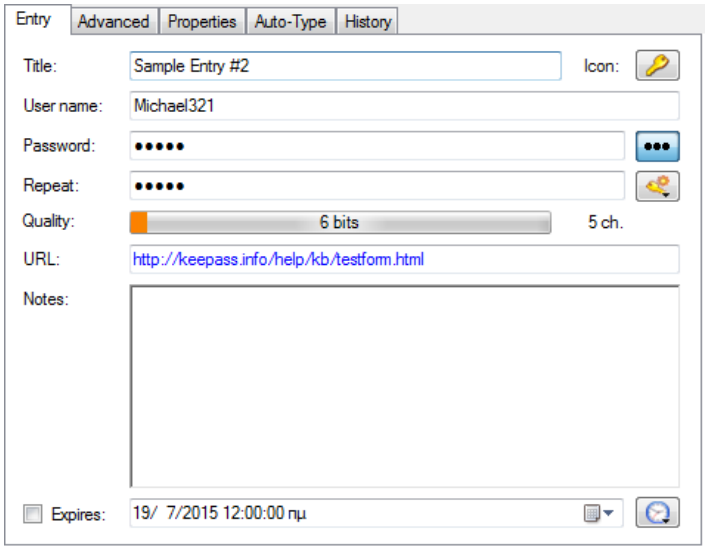
8. Συνδεθείτε σαν χρήστης apanag (με τον τελευταίο σωστό κωδικό του ερωτήματος 4) και δοκιμάστε να αλλάξετε τη συνθηματική σας λέξη. Ποια πολιτική θεωρείτε ότι παραβιάζετε;
9. Συνδεθείτε με τον αρχικό λογαριασμό διαχειριστή, επαναφέρετε τις πολιτικές λογαριασμών στις αρχικές τους τιμές και διαγράψτε το χρήστη apanag.

10η Άσκηση (Σε εργαστηριακό περιβάλλον Linux ή Windows). Η ανάγκη για χρήση διαφορετικών, ισχυρών κωδικών σε κάθε λειτουργικό σύστημα ή δικτυακό τόπο δημιουργεί το πρόβλημα της απομνημόνευσής τους. Τη λύση έρχονται να δώσουν εφαρμογές στις οποίες μπορούν να αποθηκευτούν οι κωδικοί και να ανακαλούνται όταν υπάρχει ανάγκη. Με τον τρόπο αυτόν ο χρήστης χρειάζεται να θυμάται μόνο έναν κωδικό, αυτόν για την πρόσβαση στην εφαρμογή. Μια τέτοια δωρεάν εφαρμογή είναι το KeePass2 που είναι διαθέσιμη για Windows, Linux, MacOS, σαν φορητή (portable) εφαρμογή, αλλά και για φορητές συσκευές με Android και iOS.

1. Ανοίξτε την εφαρμογή KeePass.
2. Για να ξεκινήσετε τη χρήση της εφαρμογής θα πρέπει να δημιουργήσετε μια νέα βάση δεδομένων. Νέα βάση δεδομένων μπορεί επίσης να δημιουργείται και κάθε φορά που ένας νέος χρήστης θέλει να αποθηκεύει κωδικούς. Πατήστε File → New…
3. Δώστε σαν όνομα της βάσης το **testdb.kdbx** και πατήστε [Αποθήκευση]
4. Στο παράθυρο που θα εμφανιστεί έχετε τρεις επιλογές (δύο αν χρησιμοποιείτε Linux) για το password με το οποίο θα ξεκλειδώνετε τη βάση:
    i. *Master Password:* Δίνεται έναν κωδικό τον οποίο θα πρέπει να θυμάστε και να εισάγετε κάθε φορά που θέλετε να χρησιμοποιήσετε το KeePass. Υπάρχει μάλιστα και μετρητής της ισχύος του κωδικού. Ποια πλεονεκτήματα και ποια μειονεκτήματα θεωρείτε ότι έχει η χρήση κωδικού;
    ii. *Key file / provider:* Μπορείτε να δώσετε σαν κλειδί ένα αρχείο που ήδη έχετε ή που θα κατασκευάσει για εσάς το KeePass. Πως αξιολογείτε τη δυνατότητα αυτή σε σχέση με την προηγούμενη; Είναι περισσότερο ή λιγότερο ασφαλής; Σας εξυπηρετεί καλύτερα ή όχι; Δικαιολογείστε την απάντησή σας.
    iii. *Windows user account:* Με αυτή την επιλογή (που είναι διαθέσιμη μόνο σε Windows) η βάση μπορεί να ξεκλειδώσει μόνο από το συγκεκριμένο λογαριασμό χρήστη των Windows. Τι περιορισμούς εισάγει αυτή η επιλογή;
    iv. Οι επιλογές αυτές μπορούν να εφαρμοστούν συνδυαστικά. Εσείς ποια επιλογή ή συνδυασμός επιλογών θεωρείτε ότι σας ταιριάζει καλύτερα;
5. Αφήστε ενεργή την πρώτη επιλογή μόνο και δώστε ένα ισχυρό password που να περιέχει ποικιλία χαρακτήρων, αλλά ταυτόχρονα να είναι εύκολο στην απομνημόνευση. Γράψτε το password που χρησιμοποιήσατε (να μην είναι κάποιο από αυτά που χρησιμοποιείτε ήδη). Καλό θα είναι ο δείκτης της ισχύος του password να πρασινίσει.

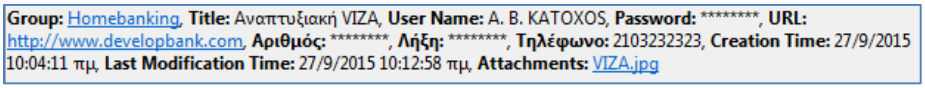


6. Στο επόμενο παράθυρο μπορείτε να ορίσετε κάποια χαρακτηριστικά της βάσης και της εφαρμογής όπως π.χ. να αυξήσετε την ασφάλεια σε επιθέσεις λεξικογραφικές ή ωμής βίας, να ορίσετε να συμπιέζεται η βάση (για εξοικονόμηση χώρου) κ.α. Πατήστε [OK].
7. Στη βάση δεδομένων του KeePass υπάρχουν διάφορες κατηγορίες δύο δοκιμαστικές εγγραφές. Πατήστε στη δεύτερη από αυτές (Sample Entry #2) και απαντήστε στις ακόλουθες ερωτήσεις:



   i. Τι κάνει το κουμπί icon;
   ii. Τι αποθηκεύεται στο User Name;
   iii. Τι κάνει το κουμπί με τις τρεις τελείες;
   iv. Τι γίνεται αν πατήσετε στη διεύθυνση στο πεδίο URL;
8. Ο Α. Β. ΚΑΤΟΧΟΣ χρησιμοποιεί την κάρτα VIZA που διαθέτει για αγορές από διαδικτυακά καταστήματα. Επειδή δεν θέλει να κρατά την κάρτα μαζί του αποφασίζει να καταχωρήσει τα στοιχεία της στο KeePass.

i. Στα αριστερά πατήστε στην κατηγορία HomeBanking. Στη συνέχεια επιλέξτε Edit → Add Entry (ή στο εικονίδιο με το κλειδί) για να προσθέσετε μια νέα εγγραφή.
ii. Αλλάξτε το εικονίδιο σε κάποιο που να μοιάζει με πιστωτική κάρτα
iii. Σαν τίτλο καταχωρήστε το όνομα της τράπεζας και το είδος της κάρτας
iv. Σαν user name βάλτε το όνομα του ιδιοκτήτη της κάρτας
v. Στο password σβήστε ό,τι ενδεχομένως υπάρχει και τοποθετείστε το PIN της κάρτας (έστω ότι είναι το **4859**).
vi. Στο πεδίο URL καταχωρήστε τη διεύθυνση του ιστότοπου της τράπεζας. (http://www.developbank.com).
vii. Υπάρχουν ακόμα στοιχεία της κάρτας που δεν έχουν καταχωρηθεί. Μεταβείτε στην καρτέλα Advanced.
viii. Πατήστε στο κουμπί [Add] (δεξιά από το πεδίο String Fields) για να δημιουργήσετε ένα νέο πεδίο κειμένου. Δώστε του το όνομα **Αριθμός** και σαν τιμή γράψτε τον 16ψήφιο αριθμό της κάρτας μαζί με τα κενά.
ix. Επιλέξτε το κουτάκι «Enable in-memory protection» ώστε το KeePass να διατηρεί τον αριθμό της κάρτας κρυπτογραφημένο ακόμη και κατά τη διάρκεια της εκτέλεσης της εφαρμογής, και πατήστε [OK].
x. Με τον ίδιο τρόπο δημιουργήστε ένα νέο πεδίο για την ημερομηνία λήξης της κάρτας και αποθηκεύστε εκεί τη σχετική πληροφορία.
xi. Δημιουργήστε ένα ακόμα πεδίο για το τηλέφωνο επικοινωνίας με την Τράπεζα (2103232323). Στο πεδίο αυτό δεν χρειάζεται να επιλέξετε το «Enable in-memory protection».
xii. Τι διαφορά παρατηρείτε στον τρόπο εμφάνισης των πεδίων που είχαν επιλεγμένο το «Enable in-memory protection» και σε αυτό που δεν το είχε;
xiii. Ο χρήστης της κάρτας επιθυμεί να αποθηκεύσει και την εικόνα της. Πατήστε στο κουμπί [Attach] και επιλέξτε [Attach File(s)…]. Εντοπίστε στον υπολογιστή σας το αρχείο «VIZA.jpg» και επιλέξτε το. Στη συνέχεια πατήστε [OK].
xiv. Παρατηρείστε ότι όταν η εγγραφή που φτιάξατε είναι επιλεγμένη στο κάτω μέρος του παραθύρου φαίνονται οι λεπτομέρειές της.



xv. Τι θα συμβεί αν πατήσετε στο URL και τι αν πατήσετε στο Attachments;

9. Η Μαρία έχει πολλούς λογαριασμούς σε σελίδες κοινωνικής δικτύωσης και θέλει να καταχωρήσει στο KeePass τους κωδικούς που χρησιμοποιεί, σε μία ομάδα με όνομα «Social Media» **μέσα** στην ομάδα Internet. Επιλέξτε την ομάδα Internet. Από το μενού Edit επιλέξτε Add New Group. Στο παράθυρο που θα εμφανισθεί συμπληρώστε το όνομα της ομάδας και αλλάξτε το εικονίδιό της. Πατήστε [OK] για να δημιουργηθεί η ομάδα.
10. Μέσα στην ομάδα που φτιάξατε δημιουργείστε μία καταχώρηση για ένα λογαριασμό του Facebook (όχι τον δικό σας) και καταχωρήστε όλες τις απαραίτητες πληροφορίες.
11. Αποθηκεύστε τα περιεχόμενα της βάσης και βγείτε από την εφαρμογή. Στη συνέχεια ξεκινήστε ξανά την εφαρμογή, δώστε το password για τη βάση και εντοπίστε τις πληροφορίες που καταχωρήσατε.

11η Άσκηση (Σε εργαστηριακό περιβάλλον).

Στην άσκηση αυτή θα κρυπτογραφήσετε μία φράση χρησιμοποιώντας τον αλγόριθμο συμμετρικής κρυπτογράφησης του Καίσαρα. Ο Αλγόριθμος του Καίσαρα κρυπτογραφεί ένα κείμενο, αλλάζοντας κάθε γράμμα με αυτό που βρίσκεται κάποιες θέσεις πιο κάτω στο αλφάβητο. Αν Ο αριθμός που δείχνει πόσες θέσεις πιο κάτω είναι το κλειδί της κρυπτογράφησης.

1. Θεωρείστε την Αγγλική αλφάβητο. Για ευκολία έστω ότι χρησιμοποιούμε μόνο πεζούς χαρακτήρες. Αν σαν κλειδί θεωρήσουμε τον αριθμό 5, συμπληρώστε τον πίνακα έτσι ώστε κάτω από κάθε χαρακτήρα να φαίνεται αυτός που τον αντικαθιστά κατά την κρυπτογράφηση. Όταν στην κάτω γραμμή φτάσετε στο τελευταίο γράμμα της αλφαβήτου, ξεκινήστε πάλι από την αρχή.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

2. Με δεδομένο ότι η Αγγλική αλφάβητος έχει 26 γράμματα, πόσα διαφορετικά κλειδιά μπορούμε να χρησιμοποιήσουμε με αυτόν τον αλγόριθμο και να πάρουμε διαφορετικά αποτελέσματα κωδικοποίησης;
3. Σύμφωνα με τον παραπάνω πίνακα, πως κρυπτογραφείται η φράση **happy birthday to you** (θεωρείστε ότι αφήνουμε τα κενά ως έχουν):
4. Αποκρυπτογραφήστε τη φράση: **mfaj f snhj ifd** και γράψτε αυτό που βρήκατε:
5. Ανοίξτε τη σελίδα *http://crypo.in.ua/tools/eng_caesar.php* και επιβεβαιώστε ότι απαντήσατε σωστά στα ερωτήματα Γράψτε το κείμενο στο πλαίσιο, εισάγετε την τιμή του κλειδιού και πατήστε [encrypt] για κρυπτογράφηση και [decrypt] για αποκρυπτογράφηση.

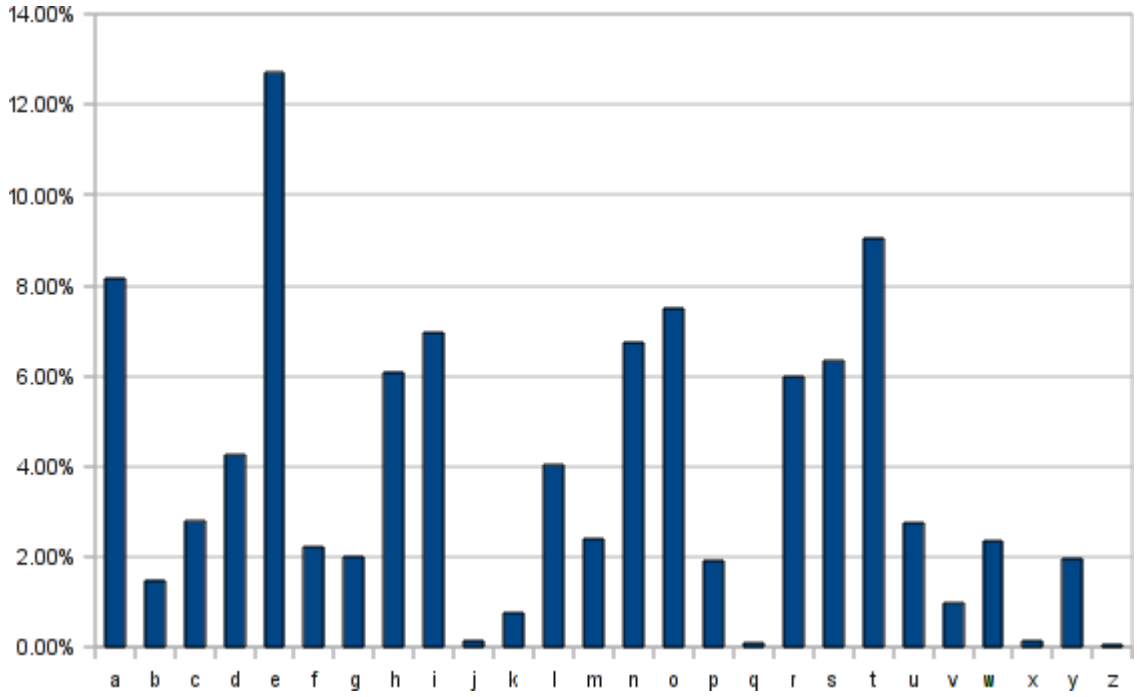
12η Άσκηση (Σε εργαστηριακό περιβάλλον).

Δύο συμμαθητές σας ανταλλάσσουν μεταξύ τους μηνύματα κρυπτογραφημένα με τον αλγόριθμο του Καίσαρα. Ένα από τα μηνύματα αυτά έπεσε στα χέρια σας, δεν ξέρετε όμως το κλειδί για να κάνετε την αποκρυπτογράφηση. Στην άσκηση αυτή θα αποκρυπτογραφήσετε το μήνυμα δοκιμάζοντας όλα τα πιθανά κλειδιά, πραγματοποιώντας δηλ. μια επίθεση «ωμής βίας».

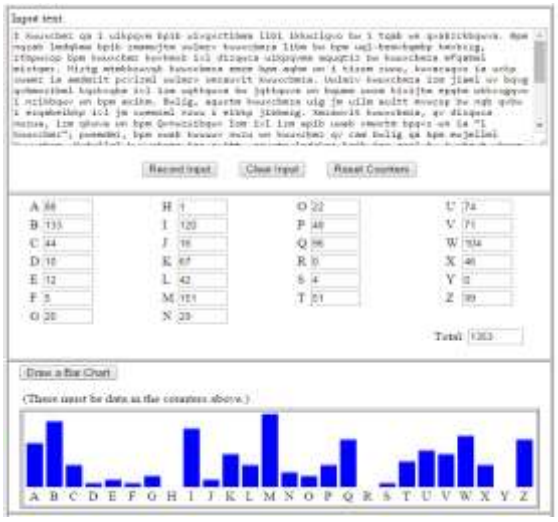
1. Ανοίξτε τη σελίδα *http://crypo.in.ua/tools/eng_caesar.php* και στο πλαίσιο κειμένου γράψτε τη φράση **dp tfdglkvi zj mvip wrjk** που είναι το κρυπτογραφημένο μήνυμα.
2. Δοκιμάστε όλες τις δυνατές τιμές για το κλειδί ώστε να αποκρυπτογραφήσετε τη φράση.
3. Σε ποια τιμή πέτυχε η αποκρυπτογράφηση;
4. Τι λέει η φράση;
5. Πόσο χρόνο πιστεύετε θα χρειαζόσασταν αν κάνατε την αποκρυπτογράφηση χωρίς υπολογιστή;

13η Άσκηση (Σε εργαστηριακό περιβάλλον).

Από μελέτες που έχουν γίνει έχει βρεθεί ότι οι συχνότητα εμφάνισης των γραμμάτων της Αγγλικής γλώσσας δίνεται από το ακόλουθο διάγραμμα:



1. Ποιο είναι το γράμμα που εμφανίζεται πιο συχνά;
2. Ποιο είναι το αμέσως επόμενο συχνότερο γράμμα;
3. Και ποιο το τρίτο κατά σειρά;
4. Πως μπορεί η πληροφορία αυτή να μας βοηθήσει να αποκρυπτογραφήσουμε πιο γρήγορα ένα κείμενο που έχει κρυπτογραφηθεί με τον αλγόριθμο του Καίσαρα;
5. Ανοίξτε το αρχείο κειμένου **encrypted.txt** από την τοποθεσία που θα σας πει ο καθηγητής σας.
6. Ανοίξτε την ακόλουθη ιστοσελίδα *https://www.mtholyoke.edu/courses/quenell/s2003/ma139/js/count.html* και αντιγράψτε το κείμενο του αρχείου στο πλαίσιο Input Text. Πατήστε στο κουμπί [Record Input] για να γίνει η μέτρηση των εμφανίσεων του κάθε γράμματος. Μπορείτε να πατήσετε και στο πλήκτρο [Draw a Bar Chart] για να δείτε και ένα γράφημα.



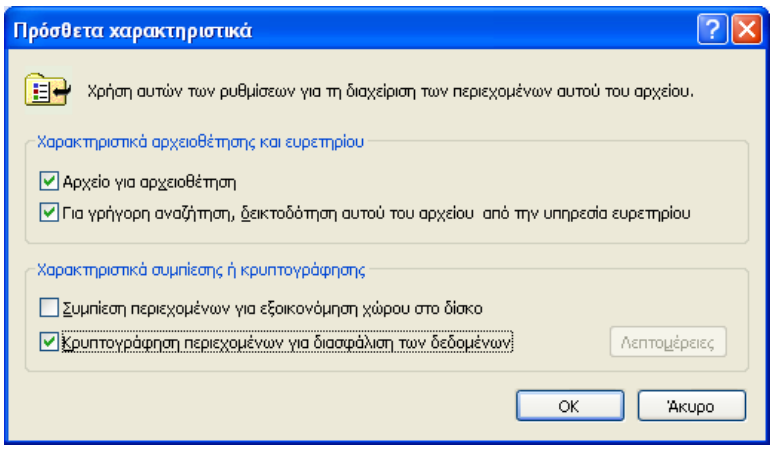
7. Ποιο είναι εδώ το γράμμα με την πιο συχνή εμφάνιση;
8. Πόσες θέσεις απέχει αυτό το γράμμα από το ‘e’ που είναι το πιο συχνό γράμμα της Αγγλικής αλφαβήτου;

9. Ανοίξτε τη σελίδα http://crypo.in.ua/tools/eng_caesar.php και στο πλαίσιο κειμένου αντιγράψτε το κείμενο που μόλις αναλύσατε.
10. Δώστε σαν κλειδί την τιμή που δώσατε στην ερώτηση 8.
11. Γράψτε τις πέντε πρώτες λέξεις από το αποκρυπτογραφημένο κείμενο.

14η Άσκηση (Σε εργαστηριακό περιβάλλον Windows).

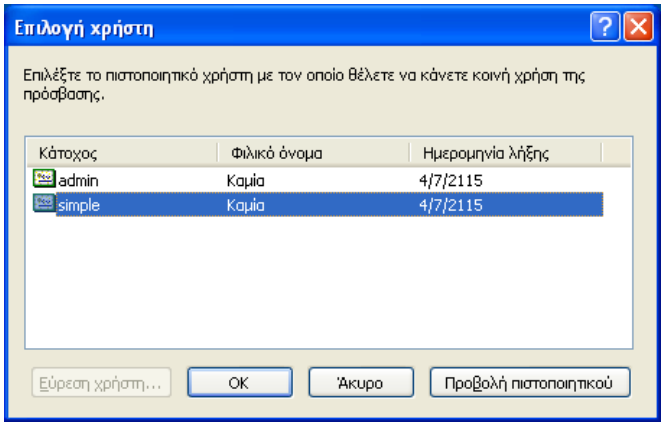
Τα Windows σας δίνουν τη δυνατότητα να κρυπτογραφήσετε αρχεία και φακέλους μέσω του συστήματος EFS (Encrypted File System), έτσι ώστε αυτά να μπορεί να τα διαβάσει μόνο ο χρήστης που τα κρυπτογράφησε. Η διαδικασία είναι διαφανής στο χρήστη και για κλειδί χρησιμοποιείται το password του λογαριασμού σύνδεσης. Για να μπορέσει να γίνει κρυπτογράφηση θα πρέπει τα αρχεία να βρίσκονται σε δίσκο μορφοποιημένο με NTFS.

1. Ξεκινήστε μια εικονική μηχανή με Windows XP Pro ή νεότερη και συνδεθείτε με λογαριασμό διαχειριστή.
2. Δημιουργήστε έναν λογαριασμό **διαχειριστή** με όνομα «simple» και ίδιο (για ευκολία) κωδικό πρόσβασης.
3. Δημιουργήστε έναν λογαριασμό **διαχειριστή** με όνομα «admin» και ίδιο (για ευκολία) κωδικό πρόσβασης.
4. Κάντε αποσύνδεση και συνδεθείτε με το λογαριασμό «simple».
5. Μέσα στο δίσκο C:\ φτιάξτε έναν φάκελο με όνομα «secret».
6. Βρείτε από το Διαδίκτυο μια εικόνα ενός λουκέτου (αναζητήστε «Lock» και αποθηκεύστε την στο φάκελο «secret».
7. Κάντε δεξί-click στην εικόνα και πατήστε [Ιδιότητες]. Στη συνέχεια πατήστε [Για προχωρημένους].
8. Επιλέξτε το πλαίσιο [Κρυπτογράφηση περιεχομένων για διασφάλιση των δεδομένων] και πατήστε δύο φορές [OK].



9. Στο παράθυρο που θα εμφανισθεί δίνεται η δυνατότητα να κρυπτογραφήσουμε ολόκληρο το φάκελο. Προς το παρόν πατήστε [Κρυπτογράφηση μόνο του αρχείου] και [OK].
10. Βλέπετε κάποια αλλαγή στην εμφάνιση του αρχείου;
11. Μπορείτε να δείτε την εικόνα που περιέχει;
12. Αποσυνδεθείτε, συνδεθείτε με το λογαριασμό «admin» και ανοίξτε το φάκελο «secret».
13. Μπορείτε να δείτε την εικόνα;
14. Μπορείτε να αφαιρέσετε την κρυπτογράφηση;
15. Μπορείτε να διαγράψετε το αρχείο;
16. Ανοίξτε τον κάδο ανακύκλωσης και επαναφέρετε το αρχείο. Μήπως τώρα μπορείτε να το διαβάσετε;

17. Μπορείτε να αντιγράψετε το αρχείο στον ίδιο ή σε άλλο φάκελο;
18. Μετονομάστε το αρχείο σε **Lock1**. Μπορείτε να δείτε τώρα τα περιεχόμενά του;
19. Δημιουργείστε στο φάκελο «secret» ένα νέο αρχείο κειμένου με όνομα «shared». Γράψτε μέσα σε αυτό τη φράση «**Για κοινή χρήση με τον simple**» και αποθηκεύστε το.
20. Κρυπτογραφήστε το αρχείο όπως και προηγουμένως. Μην κρυπτογραφήσετε όλο το φάκελο.
21. Ανοίξτε πάλι τις ιδιότητες του αρχείου, πατήστε [Για προχωρημένους] και μετά στο κουμπί [Λεπτομέρειες].
22. Προσθέστε το χρήστη «simple» να έχει πρόσβαση στα δεδομένα του αρχείου. Για να προσθέσετε έναν χρήστη θα πρέπει αυτός να έχει κρυπτογραφήσει ένα τουλάχιστον αρχείο ώστε να έχουν δημιουργηθεί τα κατάλληλα πιστοποιητικά.

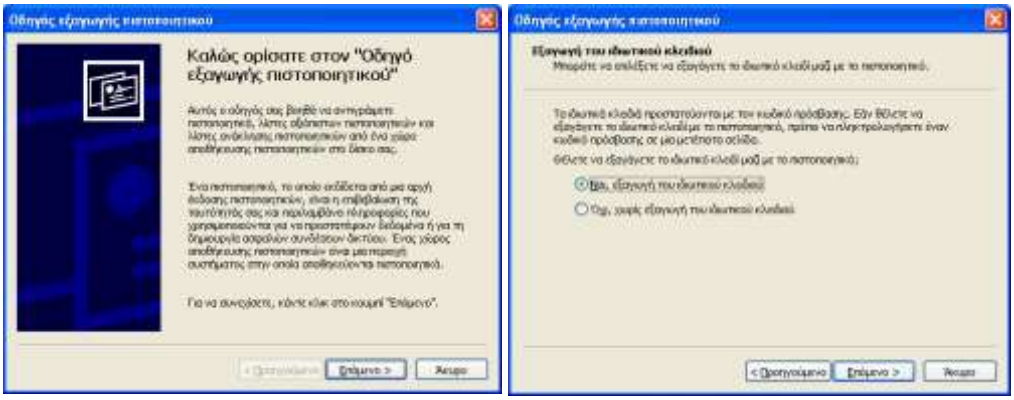


23. Αποσυνδεθείτε και συνδεθείτε ξανά σαν «simple».
24. Έχετε πρόσβαση στα περιεχόμενα του αρχείου;
25. Μπορείτε να το τροποποιήσετε; Δοκιμάστε π.χ. να προσθέσετε τη φράση «**και τον admin**» στα ήδη υπάρχοντα περιεχόμενα. Μπορείτε;
26. Μπορείτε να αφαιρέσετε την κρυπτογράφηση;
27. Διαγράψτε μόνιμα το αρχείο. Αφήστε μόνο το αρχείο «Lock1».
28. Αποσυνδεθείτε από το λογαριασμό.

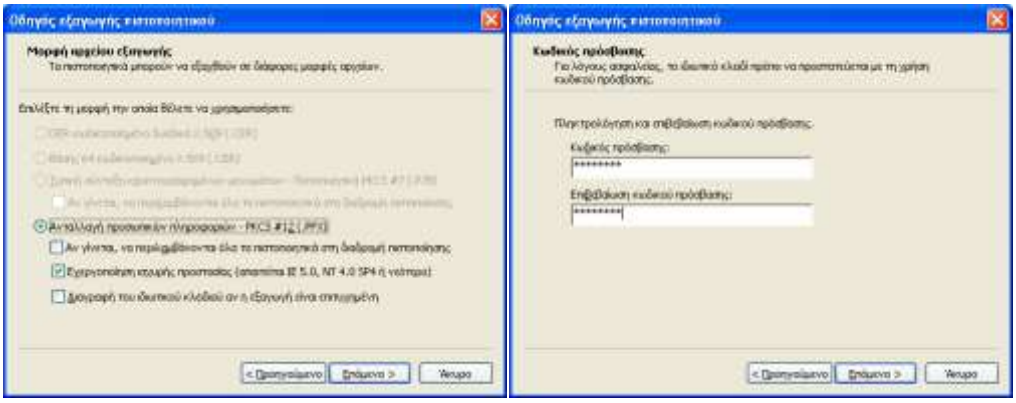
15η Άσκηση (Σε εργαστηριακό περιβάλλον Windows).

Το σύστημα EFS κρυπτογραφεί τα αρχεία στον υπολογιστή που βρίσκονται, τι συμβαίνει όμως αν χρειαστεί να χρησιμοποιηθούν σε διαφορετικό υπολογιστή; Ή αν υπάρξει ανάγκη επανεγκατάστασης των Windows; Ή αν για κάποιο λόγο αλλοιωθεί το πιστοποιητικό της κρυπτογράφησης; Στην άσκηση αυτή θα αποθηκεύσετε το πιστοποιητικό κρυπτογράφησης σε μία άλλη θέση, ώστε να μπορέσετε να το χρησιμοποιήσετε σε τέτοιες περιπτώσεις.

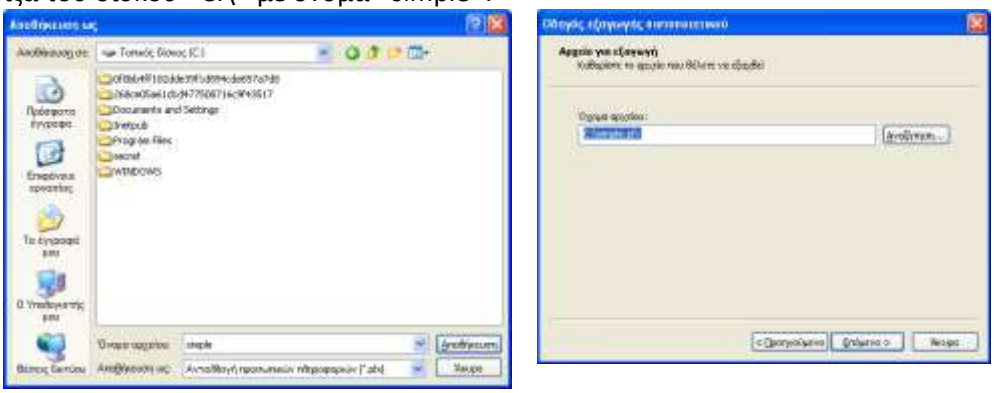
1. Στην εικονική μηχανή που χρησιμοποιήσατε και στην προηγούμενη άσκηση συνδεθείτε σαν χρήστης «simple».
2. Πατήστε Έναρξη → Πίνακας Ελέγχου → Επιλογές Internet.
3. Μεταβείτε στην καρτέλα *Περιεχόμενο* και πατήστε στο κουμπί [Πιστοποιητικά].
4. Στο νέο παράθυρο που εμφανίζεται βεβαιωθείτε ότι βρίσκεστε στην καρτέλα «Προσωπικά Στοιχεία».
5. Επιλέξτε το πιστοποιητικό σας και πατήστε [Εξαγωγή...].
6. Στο πρώτο βήμα του οδηγού πατήστε [Επόμενο]. Στη συνέχεια επιλέξτε «Ναι, εξαγωγή του ιδιωτικού κλειδιού» και πατήστε [Επόμενο]



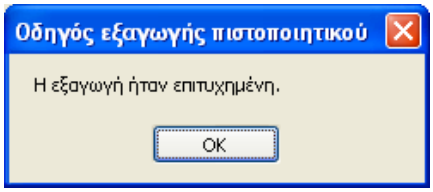
7. Στο επόμενο βήμα πατήστε [Επόμενο] και μετά γράψτε έναν κωδικό πρόσβασης. Αυτός δεν χρειάζεται να είναι ίδιος με αυτόν που έχει ο λογαριασμός σας και θα σας ζητηθεί όταν θα εισάγετε το πιστοποιητικό σε ένα άλλο σύστημα. Για ευκολία εδώ δώστε τη λέξη **password**. Πατήστε [Επόμενο].



8. Στην επόμενη οθόνη θα σας ζητηθεί η θέση που θα αποθηκευτεί το πιστοποιητικό. Για ευκολία στην άσκηση πατήστε στο κουμπί [Αναζήτηση] και αποθηκεύστε το στη ρίζα του δίσκου «C:\» με όνομα «simple».



9. Πατήστε [Τέλος] στην τελευταία οθόνη του οδηγού. Ένα μήνυμα θα σας ενημερώσει αν η διαδικασία ολοκληρώθηκε σωστά.

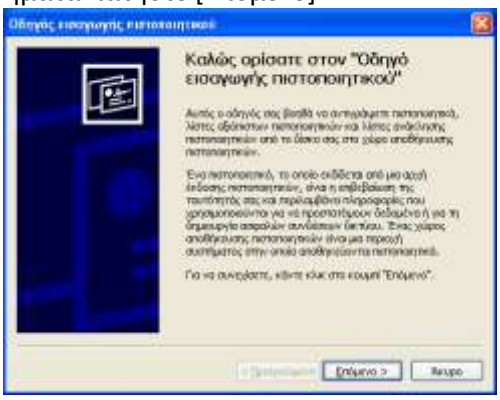


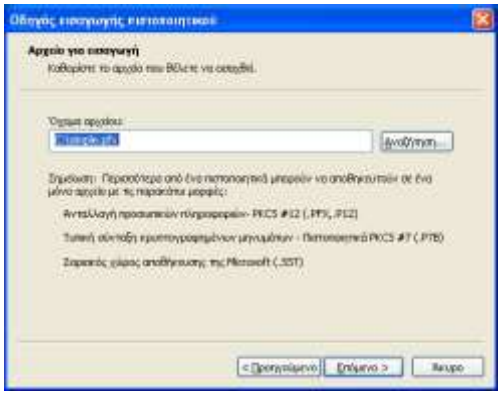
10. Στην πραγματικότητα, που θα αποθηκεύατε το πιστοποιητικό ώστε να βρίσκεται σε ασφαλή τοποθεσία;
11. Αποσυνδεθείτε από το λογαριασμό.

16η Άσκηση (Σε εργαστηριακό περιβάλλον Windows).

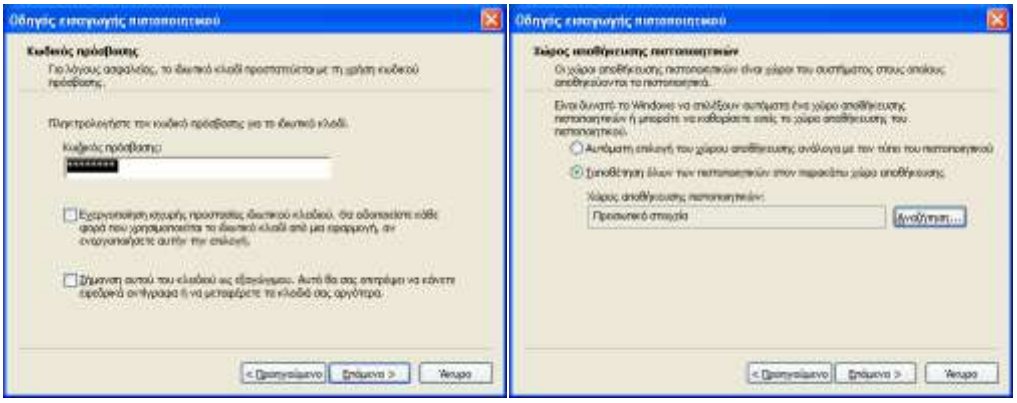
Στην άσκηση αυτή θα δείτε πως μπορείτε να ανακτήσετε την πρόσβαση σε κρυπτογραφημένα αρχεία μετά από ένα ενδεχόμενο πρόβλημα του υπολογιστή, ή τυχόν διαγραφή του λογαριασμού που πραγματοποίησε την κρυπτογράφηση.

1. Στην εικονική μηχανή που χρησιμοποιήσατε και στην προηγούμενη άσκηση συνδεθείτε σαν χρήστης «admin».
2. Από τον Πίνακα Ελέγχου διαγράψτε το χρήστη «simple». Κατά τη διαγραφή του λογαριασμού ζητήστε να διαγραφούν και τα αρχεία του χρήστη. Ποιας τοποθεσίας τα αρχεία θα διαγραφούν;
3. Δημιουργήστε ένα νέο λογαριασμό διαχειριστή, πάλι με όνομα «simple» και κωδικό «simple». Μετά τη δημιουργία του λογαριασμού συνδεθείτε σε αυτόν.
4. Δοκιμάστε να ανοίξετε το αρχείο «Lock1» από το φάκελο «secret». Μπορείτε να δείτε τα περιεχόμενά του;
5. Αρκεί η ύπαρξη ενός λογαριασμού με το ίδιο όνομα και κωδικό πρόσβασης για να αποκτήσουμε πρόσβαση σε κρυπτογραφημένα αρχεία σε ένα άλλο μηχάνημα;
6. Αποσυνδεθείτε από το λογαριασμό, συνδεθείτε σαν χρήστης «admin» και διαγράψτε και πάλι το χρήστη «simple».
7. Δημιουργήστε έναν νέο λογαριασμό διαχειριστή με όνομα «recovery» και κωδικό την ίδια λέξη. Στη συνέχεια συνδεθείτε με το λογαριασμό αυτό.
8. Ανοίξτε τα περιεχόμενα του δίσκου C:\ και κάντε διπλό-click στο πιστοποιητικό «simple.pfx». Θα ξεκινήσει ο οδηγός εισαγωγής πιστοποιητικού. Στα δύο πρώτα βήματα πατήστε [Επόμενο].

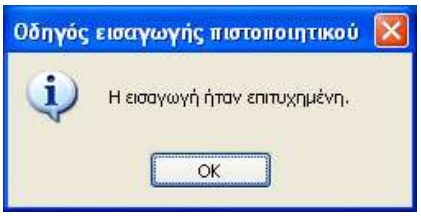




9. Πληκτρολογήστε τον κωδικό πρόσβασης που είχατε δώσει κατά την εξαγωγή του πιστοποιητικού (εδώ «password») και πατήστε [Επόμενο]. Κατόπιν επιλέξτε «Τοποθέτηση όλων των πιστοποιητικών στον παρακάτω χώρο αποθήκευσης», πατήστε το κουμπί [Αναζήτηση] και επιλέξτε «Προσωπικά Στοιχεία».



10. Πατήστε [Επόμενο] και [Τέλος]. Ένα μήνυμα θα σας πει αν το πιστοποιητικό εισήχθη με επιτυχία.



11. Μεταβείτε στο φάκελο «secret». Έχετε τώρα πρόσβαση στο κρυπτογραφημένο αρχείο;
12. Αποσυνδεθείτε από το λογαριασμό «recovery», συνδεθείτε με ένα λογαριασμό διαχειριστή και διαγράψτε τους λογαριασμούς «admin» και «recovery», μαζί με τα αρχεία τους. Ακόμη διαγράψτε από το C:\ το αρχείο «simple.pfx» καθώς και το φάκελο «secret».

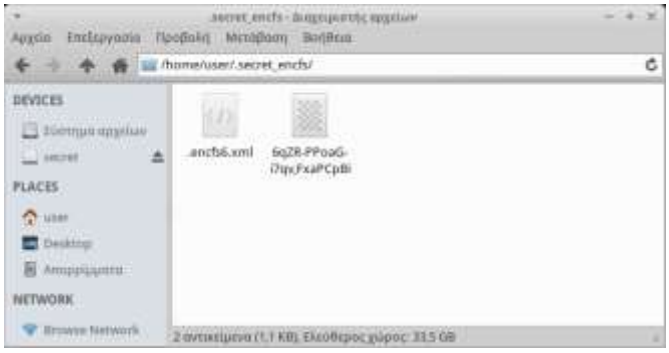
17η Άσκηση (Σε εργαστηριακό περιβάλλον Linux).

Στην άσκηση αυτή θα δείτε πως μπορείτε να δημιουργήσετε έναν φάκελο με κρυπτογραφημένα αρχεία σε περιβάλλον Linux. Για να εκτελέσετε τα βήματα της άσκησης θα πρέπει να έχετε εγκαταστήσει, χρησιμοποιώντας τον Software Manager της διανομής Linux που χρησιμοποιείτε, το σύστημα encfs (Encrypted virtual File System) και το CryptKeeper που είναι ένα γραφικό περιβάλλον για τη διαχείριση των εντολών του encfs.

1. Σε εικονική ή φυσική μηχανή με λειτουργικό σύστημα Linux συνδεθείτε με λογαριασμό διαχειριστή.
2. Από το κουμπί [Έναρξη] επιλέξτε Σύστημα → **CryptKeeper**. Αυτό θα έχει σαν αποτέλεσμα να εμφανιστεί το εικονίδιο ενός κλειδιού στη γραμμή έναρξης.
3. Πατήστε πάνω στο κλειδί και επιλέξτε «New Encrypted Folder».
4. Στο παράθυρο που θα εμφανισθεί δώστε στο πλαίσιο «Name:» τη λέξη «secret» και μετά επιλέξτε στα αριστερά από το κατάλογο «Places» το εικονίδιο με το σπιτάκι που αντιπροσωπεύει τον προσωπικό κατάλογο του χρήστη. Πατήστε [Forward] για να μεταφερθείτε στο επόμενο βήμα του οδηγού.

5. Στο βήμα αυτό θα σας ζητηθεί να δώσετε έναν κωδικό για την κρυπτογράφηση και την αποκρυπτογράφηση των αρχείων που θα βάλετε στο φάκελο. Μόνο οι χρήστες που θα γνωρίζουν αυτόν τον κωδικό θα έχουν πρόσβαση στα αρχεία του φακέλου. Για ευκολία δώστε τη λέξη **password** (δύο φορές). Πατήστε [Forward].
6. Τέλος ο οδηγός θα σας ενημερώσει ότι η δημιουργία του κρυπτογραφημένου φακέλου ολοκληρώθηκε. Πατήστε [OK].
7. Δείτε τα περιεχόμενα του προσωπικού σας φακέλου. Θα διαπιστώσετε ότι υπάρχουν δύο επιπλέον φάκελοι. Ο φάκελος secret και ο φάκελος .secret_encfs. Στον πρώτο αποθηκεύονται τα αρχεία αποκρυπτογραφημένα, έτοιμα για επεξεργασία, ενώ στο δεύτερο βρίσκονται στην κρυπτογραφημένη τους μορφή.

8. Μπείτε στο φάκελο secret και δημιουργήστε ένα νέο αρχείο με όνομα «message». Ανοίξτε το αρχείο και γράψτε μέσα τη φράση **secret message** και αποθηκεύστε το.
9. Ανοίξτε το φάκελο .secret_encfs και δείτε τα περιεχόμενά του. Δείτε το αρχείο που φτιάξατε με κρυπτογραφημένο ακόμα και το όνομα.



10. Όταν τελειώσετε την εργασία σας με τα κρυπτογραφημένα αρχεία πατήστε πάλι στο εικονίδιο του κλειδιού. Οι κρυπτογραφημένοι φάκελοι που φτιάξατε εμφανίζονται στη λίστα. Από-επιλέξτε το φάκελο secret. Σε περίπτωση που δεν εμφανίζονται κλείστε το CryptKeeper και ξανανοίξτε το.
11. Θα διαπιστώσετε ότι ο φάκελος *secret* δεν υπάρχει πια, έχει μείνει μόνο ο .secret_encfs. Τι θα συμβεί αν ξανα-επιλέξετε το φάκελο secret;
12. Αν πατήσετε πάνω στο κλειδί και επιλέξετε [Edit], τι ενέργειες μπορείτε να κάνετε;
13. Αν κάνετε επανεκκίνηση του συστήματος, ποια ενέργεια θα πρέπει να κάνετε πρώτα ώστε να έχετε πάλι πρόσβαση στα κρυπτογραφημένα αρχεία σας;
14. Μέσα από την επιλογή [Edit] του CryptKeeper διαγράψτε το φάκελο secret.
15. Ποιες οι βασικές διαφορές του συστήματος αυτού από το EFS των Windows;

18η Άσκηση (Σε εργαστηριακό περιβάλλον Linux ή Windows).

Οι λύσεις κρυπτογράφησης που προτείνουν τα λειτουργικά συστήματα λειτουργούν καλά όταν τα αρχεία προορίζονται για χρήση στο συγκεκριμένο υπολογιστή. Στην περίπτωση όμως που χρειάζεται η μεταφορά κρυπτογραφημένων αρχείων και η επεξεργασία τους σε διαφορετικά συστήματα τότε πρέπει να χρησιμοποιηθεί κάποια εφαρμογή που

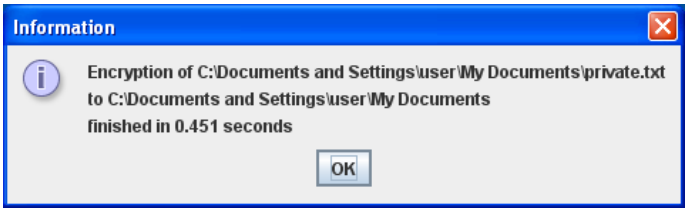
1. Να είναι φορητή (δηλ. να μην χρειάζεται εγκατάσταση) και
2. Να μπορεί να χρησιμοποιηθεί με διαφορετικά λειτουργικά συστήματα

Μια τέτοια εφαρμογή είναι το FreeSecurity (*http://www.softpedia.com/get/Security/Encrypting/FreeSecurity.shtml*) που μπορεί να μεταφερθεί ακόμη και σε ένα usb flash disk και για να τρέξει χρειάζεται μόνο να υπάρχει εγκατεστημένη Java. Κρυπτογραφεί αρχεία με τον αλγόριθμο AES 128-bit.

1. Σε εικονική ή φυσική μηχανή με λειτουργικό σύστημα Windows ή Linux και εγκατεστημένο Java Run-Time συνδεθείτε με λογαριασμό διαχειριστή.
2. Αν χρησιμοποιείτε Windows μεταβείτε στο φάκελο του προγράμματος και κάντε διπλό-click στο αρχείο FreeSecurity.jar (το όνομα μπορεί να είναι διαφορετικό αν χρησιμοποιείτε άλλη έκδοση).
3. Αν χρησιμοποιείτε Linux ανοίξτε ένα παράθυρο γραμμής εντολών στο φάκελο του προγράμματος και πληκτρολογήστε *java ./FreeSecurity.sh*


(προσοχή στα πεζά και τα κεφαλαία).

4. Δημιουργείστε ένα αρχείο κειμένου με όνομα π.χ. «private.txt». Στα περιεχόμενά του βάλτε κείμενο από κάποια σελίδα του Internet ή αν αυτό δεν είναι δυνατό γράψτε ένα δικό σας μικρό κείμενο. Αποθηκεύστε το αρχείο.
5. Στο παράθυρο του FreeSecurity επιλέξτε [Encrypt] και [Use file compression] στην περίπτωση που θέλετε εκτός να γίνει και συμπίεση του κρυπτογραφημένου αρχείου.
6. Στο πρώτο πλαίσιο κειμένου βρείτε το αρχείο «private.txt». Στο δεύτερο πλαίσιο κειμένου δώστε την τοποθεσία στην οποία θα δημιουργηθεί το κρυπτογραφημένο αρχείο. Η τοποθεσία αυτή μπορεί να είναι και η ίδια με αυτήν που βρίσκεται το αρχικό αρχείο.
7. Δώστε δύο φορές τον κωδικό με τον οποίο θα γίνει η κρυπτογράφηση και αργότερα η αποκρυπτογράφηση. Για ευκολία στο παράδειγμα χρησιμοποιήστε τη λέξη **password** και πατήστε [Encrypt the file]. Ένα μήνυμα θα σας ενημερώσει για το αποτέλεσμα και το χρόνο που χρειάστηκε.



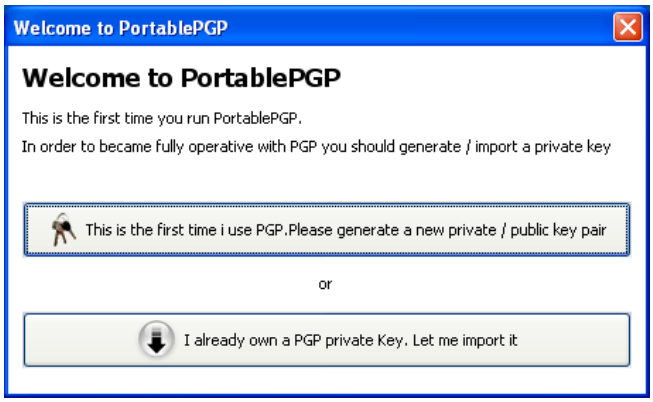
8. Το κρυπτογραφημένο αρχείο δημιουργείται στην τοποθεσία που προσδιορίσατε με το ίδιο όνομα με το αρχικό και την κατάληξη *.enc* στο τέλος. Τι όνομα έχει το αρχείο που προέκυψε;
9. Στείλτε το κρυπτογραφημένο αρχείο στη διπλανή σας ομάδα (π.χ. με e-mail). Αντίστοιχα ζητήστε και εσείς το δικό τους κρυπτογραφημένο αρχείο.
10. Αποκρυπτογραφήστε το αρχείο που σας έστειλε η διπλανή ομάδα χρησιμοποιώντας την επιλογή decrypt και επιβεβαιώστε ότι εμφανίζεται το κείμενο που είχε τοποθετηθεί μέσα.

19η Άσκηση (Σε εργαστηριακό περιβάλλον Linux ή Windows).

Στην άσκηση αυτή θα δείτε πως μπορείτε να χρησιμοποιήσετε την εφαρμογή PortablePGP για να δημιουργήσετε ένα συνδυασμό δημόσιου και ιδιωτικού κλειδιού ώστε να μπορείτε να επικοινωνείτε με ασυμμετρική κρυπτογράφηση. Η εφαρμογή είναι φορητή, που

σημαίνει ότι μπορεί να εκτελεστεί χωρίς εγκατάσταση και cross-platform, δηλ. εκτελείται και σε Windows και σε Linux.

1. Συνδεθείτε σε εικονική ή φυσική μηχανή με λειτουργικό σύστημα Linux ή Windows.
2. Μεταβείτε στο φάκελο που είναι αποθηκευμένη η εφαρμογή. Αν χρησιμοποιείτε Windows τρέξτε το αρχείο «PortablePGP.exe». Σε Linux το αντίστοιχο αρχείο είναι το «PortablePGP.sh»
3. Την πρώτη φορά που τα τρέξετε το πρόγραμμα θα εμφανίσει την ακόλουθη οθόνη. Πατήστε στην πρώτη επιλογή για να κατασκευάσετε ένα ζευγάρι δημόσιου-ιδιωτικού κλειδιού. Η δεύτερη επιλογή είναι για την περίπτωση που έχετε ήδη κάποιο κλειδί και θέλετε να το εισάγετε στην εφαρμογή.



4. Στο παράθυρο που θα εμφανισθεί εισάγετε το Επώνυμο και το Όνομά σας, αφήστε το μέγεθος του κλειδιού σε 1024 bit (όσο πιο μεγάλο, τόσο πιο ασφαλές, αλλά και τόσο πιο αργή η κρυπτογράφηση-αποκρυπτογράφηση). Θα πρέπει επίσης να δώσετε (δύο φορές) και έναν κωδικό που θα σας ζητείται κάθε φορά που θα χρησιμοποιείτε το ιδιωτικό σας κλειδί. Ο κωδικός αυτός θα πρέπει να πληροί τις ιδιότητες ενός ισχυρού κωδικού, στα πλαίσια όμως της άσκησης μπορείτε να δώσετε και κάτι απλό που δεν θα το ξεχάσετε. Στο τέλος πατήστε το πλήκτρο [Generate].

5. Μετά από λίγο θα εμφανιστεί η βασική οθόνη του προγράμματος (καρτέλα Keyring) στην οποία φαίνονται στο πάνω μέρος τα αποθηκευμένα Ιδιωτικά και στο κάτω τα Δημόσια κλειδιά.

6. Πατήστε στο κουμπί με την κλειδοθήκη έτσι ώστε να δημιουργήσουν και τα υπόλοιπα μέλη της ομάδας σας τα δικά τους ζευγάρια κλειδιών.
7. Στην περιοχή των Δημόσιων κλειδιών πατήστε πάνω στο όνομά σας και στη συνέχεια στο κουμπί με τη δισκέτα ώστε να εξάγετε το Δημόσιο κλειδί σας.
8. Αποθηκεύστε το κλειδί δίνοντας σαν όνομα αρχείου το Ονοματεπώνυμό σας και σαν επέκταση το .key π.χ. «ΑγγέλουΓεώργιος.pubKey». Η επέκταση δεν χρειάζεται, αλλά βοηθά στο να θυμάστε τι είναι το αρχείο.
9. Προσοχή στο ότι πρέπει να εξάγετε το Δημόσιο κλειδί σας. Το portablePGP (όπως και όλα τα αντίστοιχα προγράμματα) έχει τη δυνατότητα να εξάγετε και το Ιδιωτικό κλειδί. Για ποιο λόγο να θέλετε να κάνετε κάτι τέτοιο;
10. Ανοίξτε το αρχείο με έναν διορθωτή κειμένου (π.χ. το Notepad) και δείτε τα περιεχόμενά του. Αυτό είναι το Δημόσιο κλειδί σας.
11. Ποιοι χρειάζεται να γνωρίζουν το Δημόσιο κλειδί σας και για ποιο λόγο;
12. Στείλτε (π.χ. με e-mail ή μέσω του τοπικού δικτύου) τα Δημόσια κλειδιά των μελών της ομάδας σας στις υπόλοιπες ομάδες συμμαθητών σας. Αποθηκεύστε τα Δημόσια κλειδιά που θα σας στείλουν οι συμμαθητές σας στο φάκελο εργασίας σας.

20η Άσκηση (Σε εργαστηριακό περιβάλλον Linux ή Windows).

Στην άσκηση αυτή θα δείτε πως μπορείτε να εισάγετε στην εφαρμογή PortablePGP Δημόσια κλειδιά άλλων χρηστών προκειμένου να μπορείτε να τους στέλνετε κρυπτογραφημένα μηνύματα.

1. Συνδεθείτε σε εικονική ή φυσική μηχανή με λειτουργικό σύστημα Linux ή Windows.
2. Μεταβείτε στο φάκελο που είναι αποθηκευμένη η εφαρμογή. Αν χρησιμοποιείτε Windows τρέξτε το αρχείο «PortablePGP.exe». Σε Linux το αντίστοιχο αρχείο είναι το «PortablePGP.sh»
3. Στην περιοχή των Δημόσιων κλειδιών πατήστε στο εικονίδιο με το βέλος για να εισάγετε ένα από τα Δημόσια κλειδιά που σας έχουν στείλει οι συμμαθητές σας. Σε περίπτωση που το κλειδί δεν σας το έστειλαν σαν μεμονωμένο αρχείο, αλλά σαν κείμενο π.χ. σε e-mail θα πρέπει να το επιλέξετε ξεκινώντας από το -----BEGIN PGP PUBLIC KEY BLOCK----- μέχρι και το -----END PGP PUBLIC KEY BLOCK----- και να το αποθηκεύσετε σε ένα αρχείο σαν απλό κείμενο χωρίς μορφοποίηση.
4. Βρείτε το αρχείο που θέλετε να εισάγετε και κάντε πάνω του διπλό-click.
5. Θα εμφανιστεί ένα παράθυρο που θα σας ενημερώνει για τη σωστή εισαγωγή και θα δείτε ότι το όνομα προστέθηκε στη λίστα με τα Δημόσια κλειδιά.

6. Κάντε τη ίδια διαδικασία για όλα τα Δημόσια κλειδιά που σας έχουν στείλει οι συμμαθητές σας.

21η Άσκηση (Σε εργαστηριακό περιβάλλον Linux ή Windows).

Στην άσκηση αυτή θα δείτε πως μπορείτε να κρυπτογραφήσετε ένα μήνυμα με το Δημόσιο κλειδί ενός χρήστη, έτσι ώστε να μην μπορεί να το διαβάσει κανένας άλλος, παρά μόνο ο ίδιο, αφού πρώτα το αποκρυπτογραφήσει με το Ιδιωτικό κλειδί του.

1. Συνδεθείτε σε εικονική ή φυσική μηχανή με λειτουργικό σύστημα Linux ή Windows.

2. Μεταβείτε στο φάκελο που είναι αποθηκευμένη η εφαρμογή PortablePGP. Αν χρησιμοποιείτε Windows τρέξτε το αρχείο «PortablePGP.exe». Σε Linux το αντίστοιχο αρχείο είναι το «PortablePGP.sh»
3. Συνδεθείτε στο Διαδίκτυο και κατεβάστε την αφίσα μιας ταινίας που είδατε πρόσφατα και σας άρεσε. Φροντίστε η εικόνα που θα κατεβάσετε να περιλαμβάνει και τον τίτλο της ταινίας.
4. Μετονομάστε το αρχείο βάζοντας στη θέση του ονόματος το ονοματεπώνυμο ενός από τους συμμαθητές σας της διπλανής ομάδας στον οποίο θα στείλετε τελικά το κρυπτογραφημένο αρχείο.
5. Στο PortablePGP πατήστε στην επιλογή «Encrypt». Ποια από τις δύο επιλογές είναι κατάλληλη για την κρυπτογράφηση ενός αρχείου;
6. Εντοπίστε την εικόνα που κατεβάσατε και στο κάτω μέρος επιλέξτε το Δημόσιο κλειδί του συμμαθητή σας στον οποίο θα στείλετε την εικόνα. Πατήστε το κουμπί [Encrypt] και αποθηκεύστε το αρχείο με το ίδιο όνομα προσθέτοντας στο τέλος την κατάληξη *.enc*
7. Στείλτε (π.χ. με e-mail ή μέσω του τοπικού δικτύου) το αρχείο στο συμμαθητή σας. Θα πρέπει κι εσείς αντίστοιχα να λάβετε κρυπτογραφημένα αρχεία από άλλους συμμαθητές σας.
8. Σε περίπτωση που μετά την κρυπτογράφηση είχατε διαγράψει το αρχικό αρχείο, θα μπορούσατε να το ανακτήσετε αποκρυπτογραφώντας το μήνυμα που μόλις κρυπτογραφήσατε; Δικαιολογήστε την απάντησή σας.

22η Άσκηση (Σε εργαστηριακό περιβάλλον Linux ή Windows).

Στο σημείο αυτό θα δείτε πως μπορείτε να αποκρυπτογραφήσετε ένα αρχείο που σας έχουν στείλει κρυπτογραφημένο με το Δημόσιο κλειδί σας

1. Συνδεθείτε σε εικονική ή φυσική μηχανή με λειτουργικό σύστημα Linux ή Windows.
2. Μεταβείτε στο φάκελο που είναι αποθηκευμένη η εφαρμογή PortablePGP. Αν χρησιμοποιείτε Windows τρέξτε το αρχείο «PortablePGP.exe». Σε Linux το αντίστοιχο αρχείο είναι το «PortablePGP.sh»
3. Πατήστε στην επιλογή «Decrypt» και εντοπίστε ένα από τα κρυπτογραφημένα αρχεία που σας έστειλαν οι συμμαθητές σας. Στη συνέχεια πατήστε στο κουμπί [Decrypt]. Θα σας ζητηθεί ο κωδικός που είχατε δηλώσει όταν δημιουργήσατε τα κλειδιά σας.

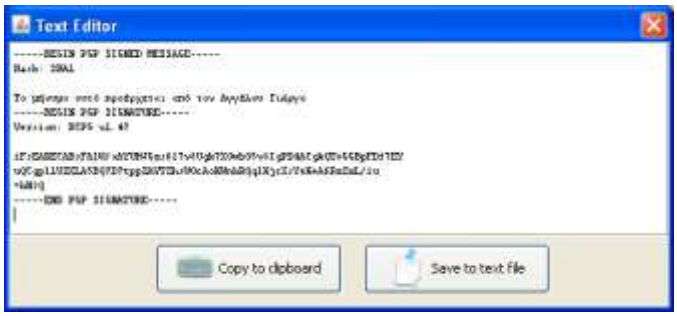
4. Δώστε τον κωδικό και αποθηκεύστε το αποκρυπτογραφημένο αρχείο. Ανοίξτε την εικόνα και δείτε ποια ταινία άρεσε στο συμμαθητή σας. Επιβεβαιώστε ότι όντως πρόκειται για το αρχείο που σας έστειλε.

23η Άσκηση (Σε εργαστηριακό περιβάλλον Linux ή Windows).

Στις εφαρμογές κρυπτογράφησης είναι πολύ σημαντική και η δυνατότητα να μπορούμε να επαληθεύσουμε την ταυτότητα του αποστολέα ενός μηνύματος, ώστε να αποκλείσουμε την πιθανότητα κάποιος να παριστάνει ένα διαφορετικό πρόσωπο. Στην άσκηση αυτή θα χρησιμοποιήσετε το PortablePGP για να στείλετε και να λάβετε ψηφιακά υπογεγραμμένα μηνύματα κειμένου.

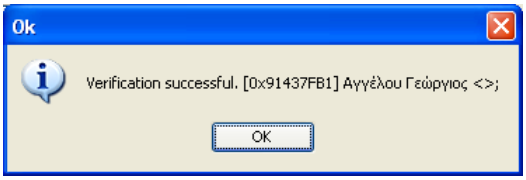
1. Συνδεθείτε σε εικονική ή φυσική μηχανή με λειτουργικό σύστημα Linux ή Windows.
2. Μεταβείτε στο φάκελο που είναι αποθηκευμένη η εφαρμογή PortablePGP. Αν χρησιμοποιείτε Windows τρέξτε το αρχείο «PortablePGP.exe». Σε Linux το αντίστοιχο αρχείο είναι το «PortablePGP.sh»
3. Πατήστε στην επιλογή Sign → Sign a Text Message. Στο πλαίσιο κειμένου γράψτε το μήνυμα «Καλημέρα, το μήνυμα αυτό προέρχεται από » και προσθέστε το ονοματεπώνυμό σας.
4. Στο κάτω μέρος επιλέξτε το δικό σας κλειδί και πατήστε [Sign]. Θα σας ζητηθεί να δώσετε τον κωδικό που αντιστοιχεί στο κλειδί σας.

5. Θα εμφανιστεί ένα παράθυρο με το ακολουθούμενο από την ψηφιακή υπογραφή.



6. Αντιγράψτε το κείμενο και στείλτε το στους υπόλοιπους συμμαθητές σας. Αν χρειαστεί μπορείτε και να το σώσετε σαν αρχείο κειμένου.
7. Ανοίξτε ένα από τα αντίστοιχα μηνύματα που πήρατε από τους συμμαθητές σας και αντιγράψτε το κείμενο από το «-----BEGIN PGP SIGNED MESSAGE-----» μέχρι και το «-----END PGP SIGNATURE-----».
8. Πατήστε στην επιλογή Verify → Verify an ASCII Armored Text Message, επικολλήστε εκεί το κείμενο και πατήστε το κουμπί [Verify].

9. Εφόσον το Δημόσιο κλειδί του αποστολέα περιλαμβάνεται στην εφαρμογή θα εμφανιστεί ένα παράθυρο που θα σας λέει ποιος είναι αυτός.



24η Άσκηση (Σε εργαστηριακό περιβάλλον Linux ή Windows).

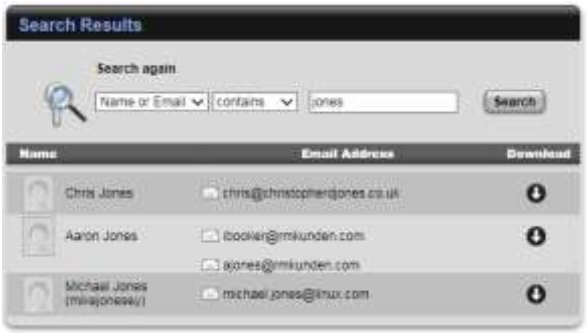
Μία μέθοδος για να γίνει γνωστό το Δημόσιο κλειδί σας και να μπορούν να το χρησιμοποιούν αυτοί που θέλουν να σας στείλουν κρυπτογραφημένα μηνύματα είναι να το δημοσιεύσετε σε ένα Key Server. Αντίστοιχα από εκεί μπορείτε να βρείτε και τα Δημόσια κλειδιά άλλων προσώπων με τα οποία επιθυμείτε να επικοινωνήσετε με ασφάλεια.

1. Χρησιμοποιώντας έναν browser ανοίξτε τη σελίδα *https://keyserver2.pgp.com*
2. Στην αρχική σελίδα αναζήτησης κλειδιών πατήστε στο «advanced».

3. Στη δεύτερη λίστα αλλάξτε το «is» σε «contains» και στο πλαίσιο κειμένου γράψτε τη λέξη «jones» και πατήστε [Search].

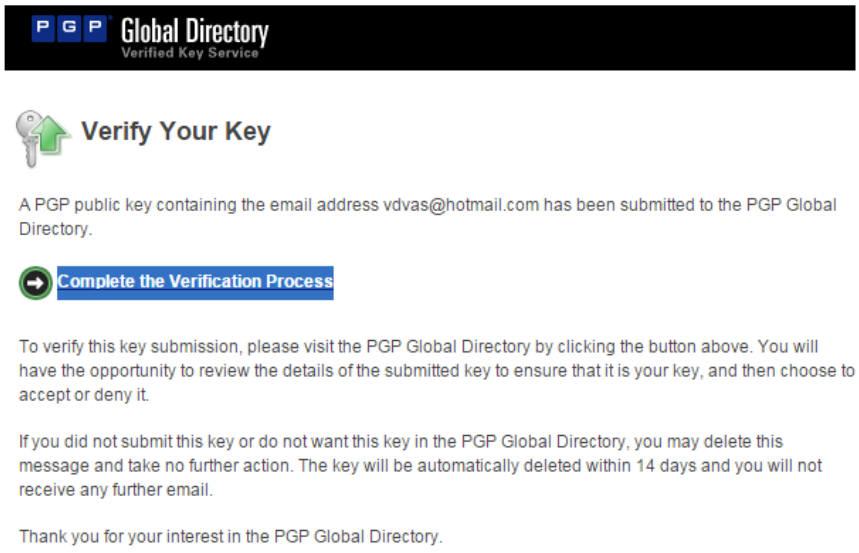
4. Για να δείτε τα αποτελέσματα της αναζήτησης θα πρέπει πρώτα να δώσετε το CAPTCHA.

5. Διαλέξτε ένα από τα κλειδιά που εμφανίστηκαν και πατήστε στο για να το κατεβάσετε.



6. Εισάγετε το κλειδί αυτό στην εφαρμογή PortablePGP.
7. Για να δημοσιεύσετε το δικό σας Δημόσιο κλειδί πατήστε στο «Publish Your Key» από την αρχική σελίδα. Στη σελίδα που θα εμφανιστεί μπορείτε να πατήστε [Αναζήτηση], για να βρείτε το αρχείο του Δημόσιου κλειδιού σας και μετά [Upload] για να το ανεβάσετε. Θα πρέπει κατά τη δημιουργία του κλειδιού να έχετε δηλώσει μία έγκυρη e-mail διεύθυνση, διότι ο συγκεκριμένος Server θα ζητήσει επιβεβαίωση πριν τη δημοσίευση του κλειδιού.

8. Για να δημοσιευτεί το κλειδί θα πρέπει να πατήσετε στο σύνδεσμο «Complete the Verification Process» στο μήνυμα που θα σας σταλεί.



9. Για να αφαιρέσετε ένα κλειδί από το Server επιλέγετε «Remove Your Key» από την αρχική οθόνη και γράφετε την e-mail διεύθυνση που περιλαμβάνεται στο κλειδί. Θα σας σταλεί πάλι μήνυμα που θα ζητά επιβεβαίωση.

25η Άσκηση (Σε εργαστηριακό περιβάλλον Linux ή Windows).

Η στεγανογραφία αποσκοπεί στο να συγκαλύψει την προσπάθεια μετάδοσης ενός μηνύματος, κρύβοντάς το μέσα σε άλλα, φαινομενικά «αθώα» δεδομένα. Η εφαρμογή steg μπορεί να κρύψει αρχεία δεδομένων μέσα σε αρχεία εικόνων. Δεν χρειάζεται εγκατάσταση και μπορεί να τρέξει και από ένα usb flash disk.

1. Συνδεθείτε σε εικονική ή φυσική μηχανή με λειτουργικό σύστημα Linux ή Windows.
2. Στο φάκελο που αποθηκεύετε τα προσωπικά σας αρχεία δημιουργήστε έναν φάκελο με όνομα «Στεγανογραφία».
3. Χρησιμοποιώντας έναν browser κατεβάστε από το Διαδίκτυο την εικόνα ενός τοπίου (σε μορφή jpeg) και αποθηκεύστε την στο φάκελο που φτιάξατε με το όνομα «**carrier.jpg**». Βρείτε μια φωτογραφία διαστάσεων τουλάχιστον 1920x1080 που να μην έχει μεγάλες περιοχές με ίδιο χρώμα. Τα σχέδια είναι επίσης ακατάλληλα. Ένα καλό παράδειγμα είναι η επόμενη εικόνα. Σημειώστε το αρχικό μέγεθος της εικόνας που βρήκατε:

4. Ανοίξτε ακόμη τη σελίδα της Ελληνικής Wikipedia (https://el.wikipedia.org) και στο πλαίσιο της αναζήτησης γράψτε «Στεγανογραφία» και πατήστε το εικονίδιο με το μεγεθυντικό φακό.

5. Επιλέξτε το κείμενο που θα εμφανιστεί, επικολλήστε το σε έναν διορθωτή κειμένου και αποθηκεύστε το στο φάκελο που φτιάξατε με το όνομα «**message.txt**». Σημειώστε το μέγεθος που έχει το αρχείο που φτιάξατε:
6. Μεταβείτε στο φάκελο που είναι αποθηκευμένη η εφαρμογή Steg. Αν χρησιμοποιείτε Windows τρέξτε το αρχείο «steg-v1.0.0.2-win32». Σε Linux το αντίστοιχο αρχείο είναι το «steg.sh».
7. Από τη γραμμή μενού του Steg πατήστε File → Open JPEG Image. Βρείτε και επιλέξτε την εικόνα «cover.jpg». Το Steg θα εμφανίσει την εικόνα σε δύο πλαίσια. Στο αριστερό είναι η αρχική εικόνα, ενώ στο δεξί η εικόνα μετά την ενσωμάτωση του κρυφού μηνύματος. Έτσι θα μπορείτε να δείτε πόσο αλλοιώνει την εικόνα η ενσωμάτωση των δεδομένων.

8. Για να κρύψετε το μήνυμα πατήστε Hide → Hide Data… Εντοπίστε και επιλέξτε το αρχείο «message.txt». Αν όλα πάνε καλά θα δείτε την ακόλουθη ειδοποίηση:

9. Βλέπετε διαφορές στη δεξιά εικόνα μετά την ενσωμάτωση του κρυφού μηνύματος; Μπορείτε να κάνετε και zoom για να δείτε περισσότερες λεπτομέρειες.
10. Πατήστε Hide → Save… για να σώσετε την εικόνα με το κρυφό μήνυμα. Αποθηκεύστε την στον ίδιο φάκελο με όνομα «hidden.jpg».
11. Βρείτε το μέγεθος της νέας εικόνας. Πόσο διαφέρει από αυτό της αρχικής;
12. Πατήστε File → Close
13. Με το πρόγραμμα προβολής εικόνων του υπολογιστή σας δείτε την αρχική και την τελική εικόνα. Μπορείτε να εντοπίσετε εύκολα διαφορές;
14. Με το πρόγραμμα προβολής εικόνων του υπολογιστή σας δείτε την αρχική και την τελική εικόνα. Μπορείτε να εντοπίσετε εύκολα διαφορές;
15. Μέσα στο φάκελο «Στεγανογραφία» φτιάξτε έναν ακόμη με όνομα «Μήνυμα».
16. Ανοίξτε πάλι την εφαρμογή Stego.
17. Από τη γραμμή μενού του Steg πατήστε File → Open JPEG Image. Βρείτε και επιλέξτε την εικόνα «hidden.jpg».
18. Πατήστε Extract → Extract Data…

19. Βρείτε και επιλέξτε το φάκελο «Δεδομένα». Πατήστε [Choose].
20. Αν όλα πάνε καλά θα εμφανιστεί η ακόλουθη ειδοποίηση:

21. Μέσα στο φάκελο «Δεδομένα» θα βρείτε το αρχείο «message.txt» που είχατε κρύψει στην αρχική εικόνα. Ποιο το μέγεθός του;
22. Είναι τα περιεχόμενά του ίδια με του αρχικού;
23. Δοκιμάστε να επαναλάβετε τη διαδικασία κρύβοντας αρχεία μεγαλύτερου μεγέθους που θα βρείτε στον υπολογιστή σας. Από ποιο σημείο και μετά παρατηρείτε αλλοιώσεις στη νέα εικόνα;
24. Τι συμβαίνει όταν το μέγεθος του αρχείου που θέλετε να κρύψετε είναι πολύ μεγάλο;

26η Άσκηση (Σε εργαστηριακό περιβάλλον Linux ή Windows).

Όταν στη γραμμή διευθύνσεων ενός browser γράφετε μια web διεύθυνση, το σύστημα DNS αναλαμβάνει τη μετατροπή της διεύθυνσης αυτής σε διεύθυνση IP. Πριν όμως ο υπολογιστής σας απευθυνθεί σε έναν DNS Server, κοιτάζει πρώτα στο δικό του πίνακα αντιστοίχισης.

Ο πίνακας αυτός είναι αποθηκευμένος σε ένα αρχείο κειμένου που λέγεται hosts. Στα Windows το αρχείο αυτό βρίσκεται στη θέση C:\Windows\System32\drivers\etc, ενώ στο Linux στη θέση /etc.

1. Συνδεθείτε σε εικονική ή φυσική μηχανή με λειτουργικό σύστημα Linux ή Windows.
2. Βρείτε και καταγράψτε την IP διεύθυνση του Web Server του Πανελλήνιου Σχολικού Δικτύου (*http://www.sch.gr*). Χρησιμοποιείστε την εντολή **nslookup** για το σκοπό αυτό.
3. Βρείτε και καταγράψτε την IP διεύθυνση του Web Server του Εθνικού και Καποδιστριακού Πανεπιστήμιου Αθηνών (*http://www.uoa.gr*).
4. Ανοίξτε το αρχείο hosts. Θα χρειαστείτε δικαιώματα διαχειριστή, διότι αργότερα θα το τροποποιήσετε. Στα Windows αυτό γίνεται ως εξής: Πατήστε Έναρξη → Όλα τα Προγράμματα → Βοηθήματα, κάντε δεξί-click στο Σημειωματάριο και επιλέξτε «Εκτέλεση ως διαχειριστής». Στη συνέχεια ανοίξτε το αρχείο από μέσα από την εφαρμογή. Στο Linux ανοίξτε ένα παράθυρο τερματικού και δώστε τις εντολές:

   cd /etc
   sudo mousepad hosts

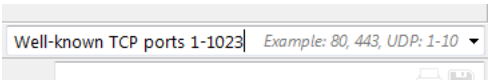
   Αν δεν υπάρχει ο editor mousepad στο σύστημά σας αντικαταστήστε το όνομά του με ό,ποιον υπάρχει.

5. Το αρχείο hosts αποτελείται από δύο στήλες (οι γραμμές που ξεκινούν από # είναι σχόλια). Τι πιστεύετε ότι γράφεται στην πρώτη και τι στη δεύτερη στήλη;
6. Προσθέστε μία νέα γραμμή όπου αρχικά θα γράφει την IP διεύθυνση του ΠΣΔ που βρήκατε στο ερώτημα 2 και στη συνέχεια το *www.uoa.gr* . Αποθηκεύστε το αρχείο.
7. Ανοίξτε έναν browser και δώστε τη διεύθυνση *www.uoa.gr*. Ποια σελίδα τελικά άνοιξε;
8. Πως θα μπορούσε κάποιο κακόβουλο λογισμικό να αλλάζει τα περιεχόμενα του αρχείου hosts έτσι ώστε να υποκλέψει κωδικούς σύνδεσης π.χ. σε ένα site;
9. Σβήστε τη γραμμή που προσθέσατε, αποθηκεύστε και κλείστε το αρχείο hosts.

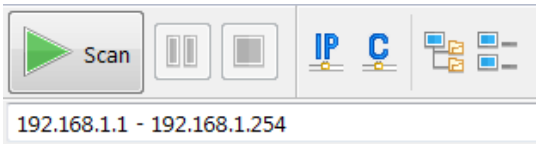
27η Άσκηση (Σε εργαστηριακό περιβάλλον Windows).

Μία ανοιχτή θύρα (open port) είναι μία θύρα TCP ή UDP που έχει ρυθμιστεί ώστε να δέχεται δεδομένα. Μια ειδική κατηγορία εφαρμογών που ονομάζονται port scanner, χρησιμοποιείται για να ελέγξει τα μηχανήματα ενός τοπικού δικτύου και τις θύρες που έχει ανοιχτές το καθένα.

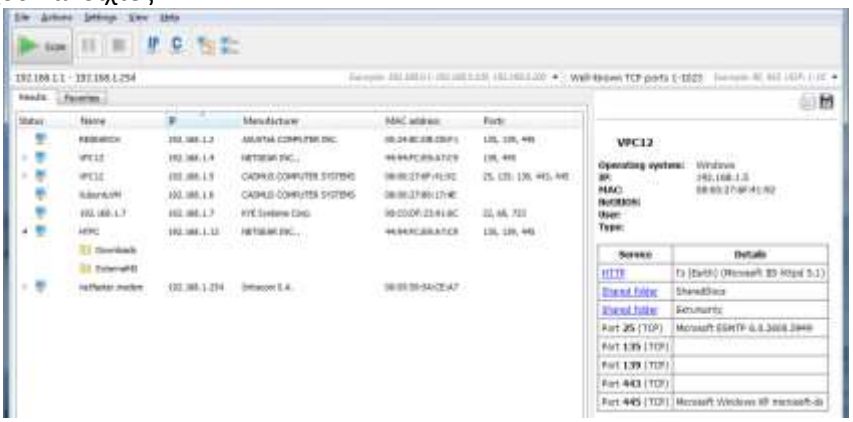
1. Συνδεθείτε σε εικονική ή φυσική μηχανή με λειτουργικό σύστημα Windows με λογαριασμό διαχειριστή.
2. Τρέξετε την εφαρμογή «advanced port scanner». Η εφαρμογή είναι διαθέσιμη από τη διεύθυνση http://www.advanced-port-scanner.com/ και μπορεί είτε να εγκατασταθεί είτε να τρέξει σαν φορητή εφαρμογή.
3. Η εφαρμογή εξ' ορισμού ανιχνεύει τα port 1-1023, τα λεγόμενα Well Known Ports. Αν θέλετε μπορείτε να το αλλάξετε αυτό από το πλαίσιο κειμένου στα δεξιά.



4. Στην πάνω αριστερή μεριά του παραθύρου δώστε το εύρος των διευθύνσεων του τοπικού σας δικτύου, αν δεν έχει ήδη βρεθεί, και πατήστε το κουμπί [Scan].



5. Μετά από κάποια ώρα θα εμφανιστούν οι υπολογιστές και οι συσκευές που βρίσκονται στο δίκτυό σας με τις IP και MAC διευθύνσεις τους καθώς και τις θύρες που έχουν ανοιχτές.



6. Στη δεξιά πλευρά του παραθύρου εμφανίζονται λεπτομέρειες για την επιλεγμένη συσκευή. Επιλέξτε μία από τις θύρες που είναι ανοικτές σε κάποιον από τους υπολογιστές του δικτύου σας και αναζητήστε στο Internet ποια υπηρεσία αντιστοιχεί σε αυτήν.

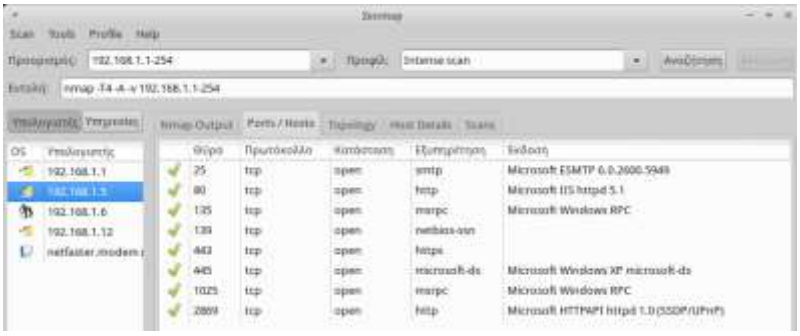
28η Άσκηση (Σε εργαστηριακό περιβάλλον Linux).

Μία ανοιχτή θύρα (open port) είναι μία θύρα TCP ή UDP που έχει ρυθμιστεί ώστε να δέχεται δεδομένα. Μια ειδική κατηγορία εφαρμογών που ονομάζονται port scanner, χρησιμοποιείται για να ελέγξει τα μηχανήματα ενός τοπικού δικτύου και τις θύρες που έχει ανοιχτές το καθένα.

1. Συνδεθείτε σε εικονική ή φυσική μηχανή με λειτουργικό σύστημα Linux.

2. Η κλασική εφαρμογή για port scan στο Linux είναι η «nmap». Η εφαρμογή λειτουργεί από τη γραμμή εντολών, όμως υπάρχει και ένα γραφικό περιβάλλον για το χειρισμό της, το «Zenmap». Και τα δύο μπορούν να εγκατασταθούν από το Software Center. Πατήστε Έναρξη → Διαδίκτυο → Zenmap (as root) την εφαρμογή «Zenmap ».
3. Στην πάνω αριστερή μεριά του παραθύρου δώστε το εύρος των διευθύνσεων του τοπικού σας δικτύου και πατήστε το κουμπί [Αναζήτηση].

4. Μετά από κάποια (αρκετή) ώρα θα εμφανιστούν οι υπολογιστές και οι συσκευές που βρίσκονται στο δίκτυό σας στην αριστερή πλευρά, καθώς και έξοδος που θα παίρνατε αν εκτελούσατε το πρόγραμμα από τη γραμμή εντολών στα αριστερά. Πατήστε στην καρτέλα Ports/Hosts και θα εμφανιστούν οι πληροφορίες για την επιλεγμένη συσκευή.



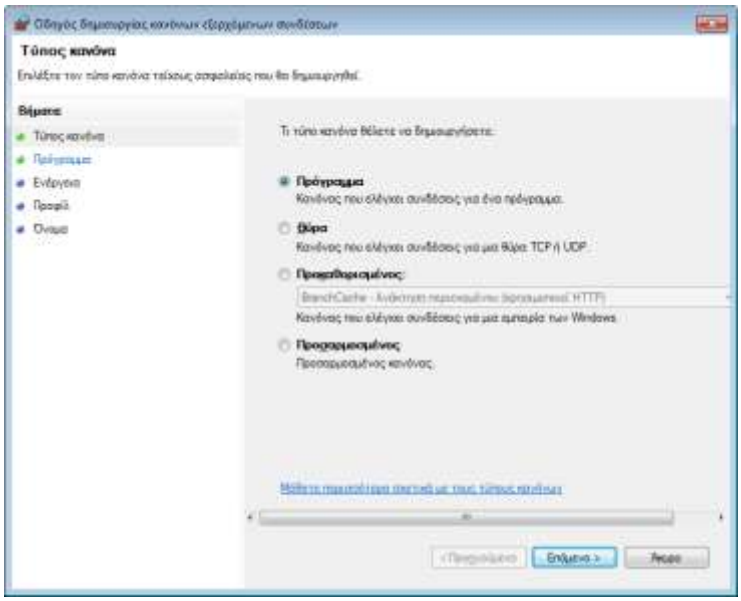
5. Επιλέξτε μία από τις θύρες που είναι ανοικτές σε κάποιον από τους υπολογιστές του δικτύου σας και αναζητήστε στο Διαδίκτυο την υπηρεσία που αντιστοιχεί σε αυτήν.

29η Άσκηση (Σε εργαστηριακό περιβάλλον Windows).

Στην άσκηση αυτή θα δημιουργήσετε ένα κανόνα για το firewall των Windows που θα αποκλείει την πρόσβαση μιας εφαρμογής στο Internet.

1. Συνδεθείτε με λογαριασμό διαχειριστή σε εικονική ή φυσική μηχανή με λειτουργικό σύστημα Windows 7 ή μεταγενέστερο.
2. Εγκαταστήστε την εφαρμογή SlimBrowser που θα βρείτε στη διεύθυνση *http://www.slimbrowser.net/*. Πρόκειται για έναν μικρό σε μέγεθος browser.
3. Μετά την εγκατάσταση ξεκινήστε το πρόγραμμα και ανοίξτε π.χ. τη σελίδα του Πανελλήνιου Σχολικού Δικτύου (http://www.sch.gr) για να βεβαιωθείτε ότι έχει πρόσβαση στο Internet.

4. Κλείστε τον browser.
5. Πατήστε Έναρξη → Πίνακας Ελέγχου → Σύστημα και Ασφάλεια → Τείχος Προστασίας των Windows → Ρυθμίσεις για Προχωρημένους.
6. Από την αριστερή πλευρά πατήστε «Κανόνες Εξερχόμενων».
7. Πατήστε Ενέργεια → Δημιουργία κανόνα



8. Στο βήμα «Τύπος Κανόνα» βεβαιωθείτε ότι είναι επιλεγμένο το «Πρόγραμμα» και πατήστε [Επόμενο].
9. Στο βήμα «Πρόγραμμα» πατήστε [Αναζήτηση] και εντοπίστε το εκτελέσιμο αρχείο του SlimBrowser (η διαδρομή είναι «C:\Αρχεία Εφαρμογών\SlimBrowser\ SBRender.exe». Πατήστε [Επόμενο].
10. Στο βήμα «Ενέργεια» επιλέξτε «Αποκλεισμός της σύνδεσης». Πατήστε [Επόμενο].
11. Στο βήμα «Προφίλ» όλα τα διαθέσιμα πεδία. Θέλετε ο κανόνας να ισχύει για όλους τους τύπους δικτύων. Πατήστε [Επόμενο].
12. Στο όνομα δώστε «Πολιτική για Slim Browser». Πατήστε [Τέλος].
13. Η πολιτική εμφανίστηκε στον κατάλογο.

14. Ανοίξτε πάλι τον Slim Browser και προσπαθήστε να ανοίξτε κάποια σελίδα. Τι παρατηρείτε;
15. Αν ξεκινήσετε τον Explorer, μπορεί αυτός να ανοίξει σελίδες;
16. Βρείτε τον κανόνα που φτιάξατε, πατήστε με δεξί-click πάνω του και απενεργοποιήστε τον.

30η Άσκηση (Σε εργαστηριακό περιβάλλον Windows).

Στην άσκηση αυτή θα δημιουργήσετε ένα κανόνα για το firewall των Windows που θα αποκλείει την πρόσβαση στον Παγκόσμιο Ιστό.

1. Συνδεθείτε με λογαριασμό διαχειριστή σε εικονική ή φυσική μηχανή με λειτουργικό σύστημα Windows 7 ή μεταγενέστερο.
2. Πατήστε Έναρξη → Πίνακας Ελέγχου → Σύστημα και Ασφάλεια → Τείχος Προστασίας των Windows → Ρυθμίσεις για Προχωρημένους.
3. Από την αριστερή πλευρά πατήστε «Κανόνες Εξερχόμενων».
4. Πατήστε Ενέργεια → Δημιουργία κανόνα
5. Στο βήμα «Τύπος Κανόνα» βεβαιωθείτε ότι είναι επιλεγμένο το «Θύρα» και πατήστε [Επόμενο].
6. Ποιο πρωτόκολλο (TCP ή UDP) και ποια θύρα χρησιμοποιείται για πρόσβαση στον Παγκόσμιο Ιστό; Αν δεν θυμάστε κάντε μια αναζήτηση για HHTP Port.
7. Στο βήμα «Πρωτόκολλο και Θύρες» επιλέξτε το πρωτόκολλο και συμπληρώστε το σωστό αριθμό θύρας. Πατήστε [Επόμενο].
8. Στο βήμα «Ενέργεια» επιλέξτε «Αποκλεισμός της σύνδεσης». Πατήστε [Επόμενο].
9. Στο βήμα «Προφίλ» όλα τα διαθέσιμα πεδία. Θέλετε ο κανόνας να ισχύει για όλους τους τύπους δικτύων. Πατήστε [Επόμενο].
10. Στο όνομα δώστε «Αποκλεισμός WEB». Πατήστε [Τέλος].
11. Ανοίξτε έναν οποιονδήποτε browser και προσπαθήστε να συνδεθείτε με το Πανελλήνιο Σχολικό Δίκτυο στη διεύθυνση http://www.sch.gr. Μπορείτε; Τι διαφορά έχει αυτός ο κανόνας σε σχέση με αυτόν της προηγούμενης άσκησης;
12. Προσπαθήστε να ανοίξτε τη σελίδα https://www.gmail.com. Τι παρατηρείτε; Τι διαφορά έχει αυτή από τις υπόλοιπες σελίδες; Ποια θύρα χρησιμοποιεί το πρωτόκολλο ασφαλούς σύνδεσης https;
13. Απενεργοποιείστε τον κανόνα που φτιάξατε.

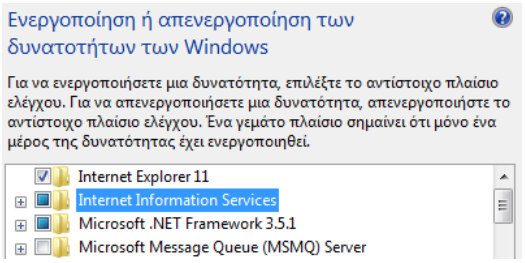
31η Άσκηση (Σε εργαστηριακό περιβάλλον Windows).

Στην άσκηση αυτή θα δημιουργήσετε ένα κανόνα για το firewall των Windows που θα επιτρέπει την πρόσβαση μόνο ενός συγκεκριμένου υπολογιστή στο δικό σας.

1. Συνδεθείτε με λογαριασμό διαχειριστή σε εικονική ή φυσική μηχανή με λειτουργικό σύστημα Windows 7 ή μεταγενέστερο.
2. Βρείτε την IP διεύθυνσή σας και δώστε την στους συμμαθητές σας της διπλανής ομάδας (συνεργάτες). Αντίστοιχα ζητήστε τους την IP διεύθυνση του δικού τους υπολογιστή. Συμπληρώστε τον παρακάτω πίνακα:

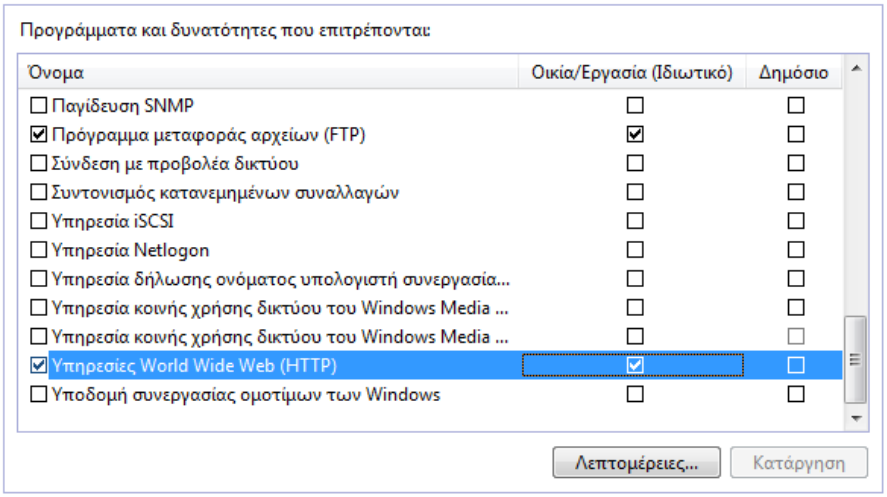
Η δική σας IP	
Η IP των συνεργατών σας	

3. Αν δεν υπάρχει ήδη ενεργός Web Server στον υπολογιστή σας, ενεργοποιείστε τον IIS (Internet Information Services) πατώντας Έναρξη → Πίνακας Ελέγχου → Προγράμματα → Ενεργοποίηση και απενεργοποίηση δυνατοτήτων των Windows → Internet Information Services.



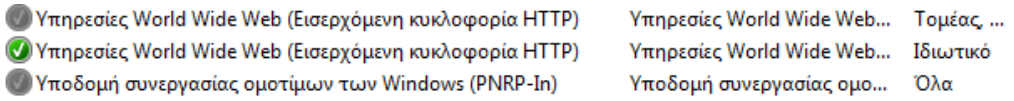
4. Όταν ολοκληρωθεί η εγκατάσταση επιβεβαιώστε ότι ο Web Server λειτουργεί, ανοίγοντας έναν Browser και δίνοντας στη γραμμή διεύθυνσης την IP του δικού σας μηχανήματος. Θα πρέπει να δείτε την ακόλουθη οθόνη (εκτός αν έχετε αλλάξει την αρχική σελίδα):

5. Δώστε τη δυνατότητα στους υπόλοιπους χρήστες του τοπικού δικτύου σας να βλέπουν τη σελίδα σας, ρυθμίζοντας κατάλληλα το Τείχος Προστασίας.
6. Πατήστε Έναρξη → Πίνακας Ελέγχου → Σύστημα και Ασφάλεια → Τείχος Προστασίας των Windows.
7. Από την αριστερή πλευρά πατήστε «Να επιτρέπεται ένα πρόγραμμα ή δυνατότητα μέσω του τείχους προστασίας των Windows».
8. Στον κατάλογο που θα εμφανισθεί πατήστε πρώτα το κουμπί [Αλλαγή Ρυθμίσεων] και στη συνέχεια βρείτε στον κατάλογο (προς το τέλος) το «☐ Υπηρεσίες World Wide Web», και τσεκάρετε το κουτάκι στη στήλη «Οικία/Εργασία (Ιδιωτικό)». Αυτό θα επιτρέψει την επικοινωνία με τον Web Server από οποιοδήποτε δίκτυο έχει χαρακτηριστεί σαν Οικιακό ή Εργασίας. Πατήστε [OK]. Μην κλείσετε το παράθυρο του Τείχους Προστασίας.

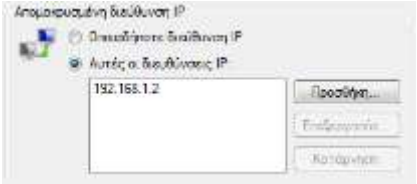


9. Ζητείστε από τους συνεργάτες σας να σας επιβεβαιώσουν ότι βλέπουν τη σελίδα σας όταν βάζουν την IP του μηχανήματός σας σε έναν Browser. Ζητείστε και από μία ακόμη ομάδα να κάνει το ίδιο.

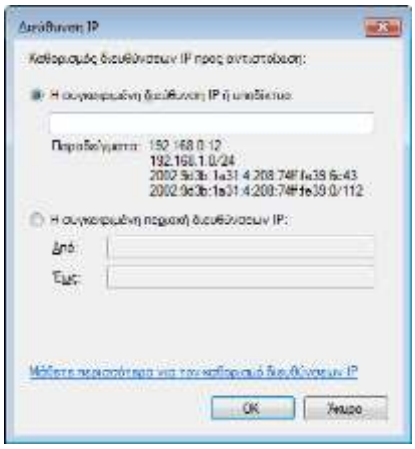
10. Επιτρέψτε την πρόσβαση στον Web Server σας μόνο στους συνεργάτες σας. Στο παράθυρο του τείχους προστασίας πατήστε «Ρυθμίσεις για προχωρημένους». Επιλέξτε τους «Κανόνες Εισερχομένων».
11. Μετακινηθείτε προς το τέλος της λίστας, βρείτε τον κανόνα «Υπηρεσίες World Wide Web (Εισερχόμενη κυκλοφορία HTTP)» και κάντε πάνω του διπλό-click.



12. Ανοίξτε την καρτέλα «Εύρος». Στο πλαίσιο «Απομακρυσμένη διεύθυνση IP επιλέξτε «Αυτές οι διευθύνσεις IP» και προσθέστε τη διεύθυνση των συνεργατών σας. Πατήστε [OK].



13. Πατήστε Ενέργεια → Δημιουργία κανόνα
14. Στο βήμα «Τύπος Κανόνα» βεβαιωθείτε ότι είναι επιλεγμένο το «Προσαρμοσμένος» και πατήστε [Επόμενο].
15. Στο βήμα «Πρόγραμμα» αφήστε επιλεγμένο το «Όλα τα προγράμματα». Πατήστε [Επόμενο].
16. Στο βήμα «Πρωτόκολλο και Θύρες» αφήστε τις επιλογές ως έχουν. Πατήστε [Επόμενο].
17. Στο βήμα «Εύρος» επιλέξτε «Αυτές οι διευθύνσεις IP» κάτω από την ενότητα «Για ποιες τοπικές διευθύνσεις ισχύει αυτός ο κανόνας» και μετά πατήστε στο κουμπί [Προσθήκη].
18. Στο παράθυρο που θα εμφανιστεί συμπληρώστε την IP διεύθυνση που σας έδωσε η διπλανή ομάδα. Πατήστε [OK]. Πατήστε [Επόμενο].



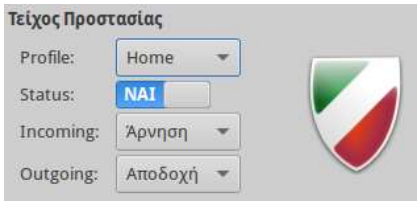
19. Στο βήμα «Ενέργεια» επιλέξτε «Αποκλεισμός της σύνδεσης». Πατήστε [Επόμενο].
20. Στο βήμα «Προφίλ» όλα τα διαθέσιμα πεδία. Θέλετε ο κανόνας να ισχύει για όλους τους τύπους δικτύων. Πατήστε [Επόμενο].
21. Στο όνομα δώστε «Αποκλεισμός IP διεύθυνσης». Πατήστε [Τέλος].

22. Ζητείστε από τους συνεργάτες σας να σας επιβεβαιώσουν ότι βλέπουν τη σελίδα σας όταν βάζουν την IP του μηχανήματός σας σε έναν Browser.
23. Επιβεβαιώστε ότι άλλοι υπολογιστές δεν έχουν πρόσβαση στη σελίδα σας.

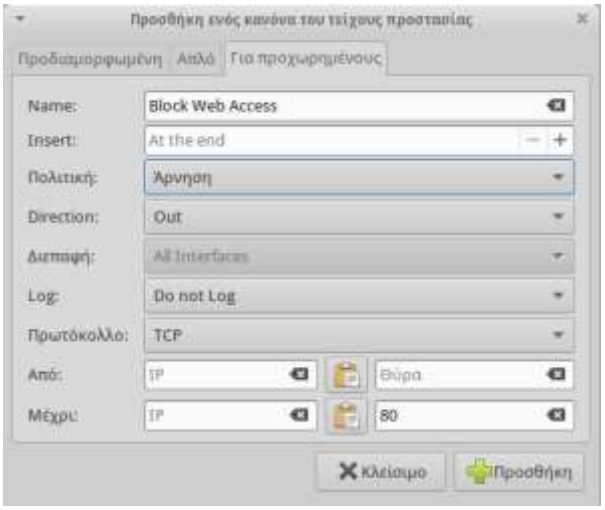
32η Άσκηση (Σε εργαστηριακό περιβάλλον Linux).

Στην άσκηση αυτή θα δημιουργήσετε ένα κανόνα για το firewall του Linux που θα αποκλείει την πρόσβαση στον Παγκόσμιο Ιστό. Το firewall του Linux είναι το iptables, που ρυθμίζεται με κανόνες που δίνονται από τη γραμμή εντολών. Υπάρχει ωστόσο και το γραφικό περιβάλλον gufw που διευκολύνει αρκετά τα πράγματα

1. Συνδεθείτε με λογαριασμό διαχειριστή σε εικονική ή φυσική μηχανή με λειτουργικό σύστημα Linux.
2. Από το Software Center βεβαιωθείτε ότι είναι εγκατεστημένες οι εφαρμογές ufw και gufw. Αν δεν είναι εγκαταστήστε τις.
3. Πατήστε Έναρξη → Ρυθμίσεις → Ρύθμιση Τείχους Προστασίας. Θα σας ζητηθεί το password του διαχειριστή.
4. Σε περίπτωση που το firewall είναι ανενεργό θα φαίνεται η ένδειξη ΟΧΙ. Πατήστε στο αριστερά κουμπί για να το ενεργοποιήσετε. Αυτό μπορεί να χρειαστεί λίγο χρόνο.



5. Για να προσθέσετε ένα κανόνα πατήστε στο + στην ενότητα Κανόνες. Στο παράθυρο που θα εμφανισθεί πατήστε στην καρτέλα Για προχωρημένους.
6. Δώστε στον κανόνα το όνομα «Block Web Access».
7. Στο πεδίο Πολιτική δώστε «Άρνηση».
8. Στο πεδίο Direction (κατεύθυνση) δώστε «Out».
9. Ποιο πρωτόκολλο (TCP ή UDP) και ποια θύρα χρησιμοποιείται για πρόσβαση στον Παγκόσμιο Ιστό; Αν δεν θυμάστε κάντε μια αναζήτηση για HHTP Port.
10. Στο πεδίο Πρωτόκολλο δώστε το σωστό πρωτόκολλο.
11. Στο πεδίο Μέχρι στα δεξιά συμπληρώστε τον αριθμό της θύρας που θέλετε να αποκλείσετε.
12. Πατήστε στο [Προσθήκη] και [Κλείσιμο]. Θα παρατηρήσετε ότι θα δημιουργηθούν δύο κανόνες, ένας για το πρωτόκολλο IP v4 και ένας για το IP v6.



13. Ανοίξτε έναν οποιονδήποτε browser και προσπαθήστε να συνδεθείτε με το Πανελλήνιο Σχολικό Δίκτυο στη διεύθυνση http://www.sch.gr. Μπορείτε;
14. Προσπαθήστε να ανοίξτε τη σελίδα https://www.gmail.com. Τι παρατηρείτε; Τι διαφορά έχει αυτή από τις υπόλοιπες σελίδες; Ποια θύρα χρησιμοποιεί το πρωτόκολλο ασφαλούς σύνδεσης https;
15. Διαγράψτε τους κανόνες που φτιάξατε επιλέγοντάς τους και πατώντας -.

33η Άσκηση (Σε εργαστηριακό περιβάλλον Linux).

Στην άσκηση αυτή θα δημιουργήσετε ένα κανόνα για το firewall του Linux που θα επιτρέπει την πρόσβαση μόνο ενός συγκεκριμένου υπολογιστή στο δικό σας.

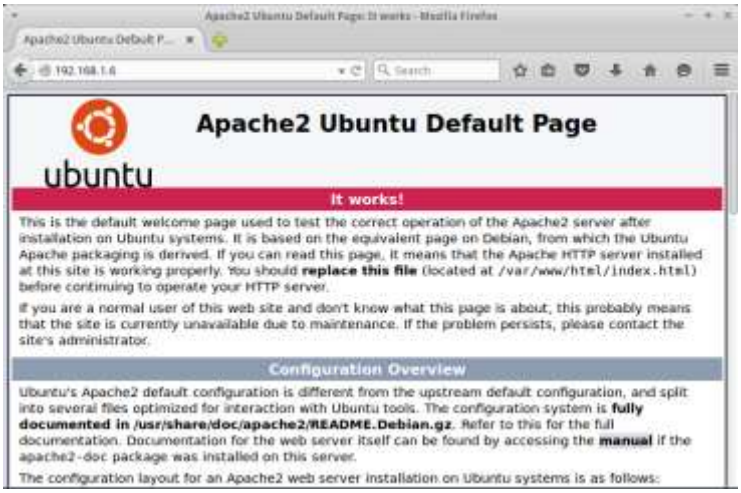
1. Συνδεθείτε με λογαριασμό διαχειριστή σε εικονική ή φυσική μηχανή με λειτουργικό σύστημα Linux.
2. Βρείτε την IP διεύθυνσή σας και δώστε την στους συμμαθητές σας της διπλανής ομάδας (συνεργάτες). Αντίστοιχα ζητήστε τους την IP διεύθυνση του δικού τους υπολογιστή. Συμπληρώστε τον παρακάτω πίνακα:

Η δική σας IP	
Η IP των συνεργατών σας	

3. Αν δεν υπάρχει ήδη ενεργός Web Server στον υπολογιστή σας, ενεργοποιείστε τον Apache Web Server ανοίγοντας ένα παράθυρο τερματικού και δίνοντας την εντολή:

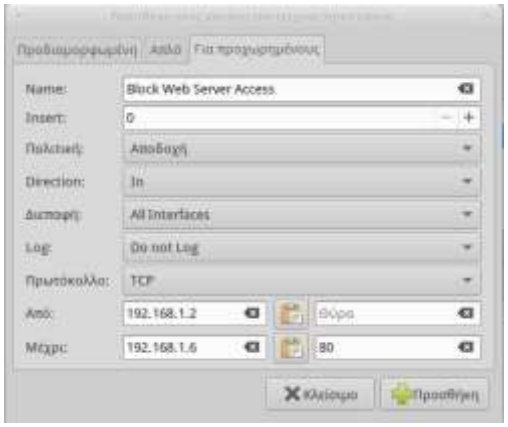
sudo apt-get install apache2

4. Όταν ολοκληρωθεί η εγκατάσταση επιβεβαιώστε ότι ο Web Server λειτουργεί, ανοίγοντας έναν Browser και δίνοντας στη γραμμή διεύθυνσης την IP του δικού σας μηχανήματος. Θα πρέπει να δείτε την ακόλουθη οθόνη (εκτός αν έχετε αλλάξει την αρχική σελίδα):



5. Επιτρέψτε την πρόσβαση στον Web Server σας μόνο στους συνεργάτες σας. Πατήστε Έναρξη → Ρυθμίσεις → Ρύθμιση Τείχους Προστασίας. Θα σας ζητηθεί το password του διαχειριστή.
6. Σε περίπτωση που το firewall είναι ανενεργό θα φαίνεται η ένδειξη ΟΧΙ. Πατήστε στο αριστερά κουμπί για να το ενεργοποιήσετε. Αυτό μπορεί να χρειαστεί λίγο χρόνο.
7. Για να προσθέσετε ένα κανόνα πατήστε στο + στην ενότητα Κανόνες. Στο παράθυρο που θα εμφανισθεί πατήστε στην καρτέλα Για Προχωρημένους.
8. Δώστε στον κανόνα το όνομα «Block Web Server Access».
9. Στο πεδίο Πολιτική δώστε «Αποδοχή».
10. Στο πεδίο Direction (κατεύθυνση) δώστε «In».
11. Στο πεδίο Πρωτόκολο δώστε το «TCP».
12. Συμπληρώστε τα πεδία Από και Μέχρι, όπως στον ακόλουθο πίνακα (αντικαταστήστε τις περιγραφές με τις πραγματικές διευθύνσεις):

Από:	IP συνεργατών	αφήστε το κενό
Μέχρι:	IP δική σας	80



Αυτό σημαίνει ότι θα επιτρέπονται εισερχόμενες συνδέσεις από τον υπολογιστή των συνεργατών σας προς το δικό σας υπολογιστή στη θύρα 80 (HTTP).

13. Πατήστε στο [Προσθήκη] και [Κλείσιμο].
14. Ζητείστε από τους συνεργάτες σας να σας επιβεβαιώσουν ότι βλέπουν τη σελίδα σας όταν βάζουν την IP του μηχανήματός σας σε έναν Browser.
15. Επιβεβαιώστε ότι άλλοι υπολογιστές δεν έχουν πρόσβαση στη σελίδα σας.

16. Διαγράψτε τον κανόνα που φτιάξατε επιλέγοντάς τον και πατώντας -.

34η Άσκηση (Σε εργαστηριακό περιβάλλον).

Για την ανωνυμία στο Διαδίκτυο υπάρχουν πλήθος άρθρων που πραγματεύονται τις θετικές και τις αρνητικές της συνέπειες. Ενδεικτικά αναφέρονται τα:

- Περί ανωνυμίας στο Διαδίκτυο: http://osarena.net/opinions/peri-anonimias-sto-diadiktio.html
- Δίωξη Ηλεκτρονικού Εγκλήματος: «Δεν υπάρχει ανωνυμία στο ίντερνετ - το πάρτι τελείωσε» http://www.newsit.gr/default.php?pname=Article&art_id=248808&catid =4
- Ποιους βολεύει η ανωνυμία στο Διαδίκτυο; http://www.aixmi.gr/index.php/poious-voleuei-anwnymia-internet-2/
- Διαδικτυακή ελευθερία και παραβατικότητα http://e-keimena.gr/index.php?option=com_content&view=article&id=94:q-q&catid=85:internet&Itemid =27

1. Αφού μελετήσετε το υλικό των παραπάνω (ή και άλλων αν θέλετε) σελίδων καταγράψτε δύο πλεονεκτήματα και δύο μειονεκτήματα της ανωνυμίας στο Διαδίκτυο και συζητήστε τα στην ολομέλεια.
2. Μετά τη συζήτηση στην ολομέλεια προσθέστε ένα ακόμη πλεονέκτημα και μειονέκτημα που δεν περιλαμβάνονταν στην αρχική σας λίστα.

35η Άσκηση (Σε εργαστηριακό περιβάλλον).

«Στο Internet κανείς δεν ξέρει ότι είσαι σκύλος» έγραφε η λεζάντα στο σκίτσο του Πίτερ Στάινερ που δημοσιεύτηκε στο περιοδικό «The New Yorker» στις 5 Ιουλίου του 1993, εννοώντας ότι δεν μπορούμε να είμαστε σίγουροι για την ταυτότητα του χρήστη με τον οποίο επικοινωνούμε. Από την προσωπική σας πείρα, αλλά αν χρειαστεί και με αναζήτηση στο Internet, απαντήστε τις ακόλουθες ερωτήσεις και συζητήστε τις απόψεις σας στην ολομέλεια.

1. Τι γνωρίζετε για τα ψεύτικα (fake) προφίλ του Facebook;
2. Ποιος μπορεί να φτιάξει ένα ψεύτικο προφίλ;
3. Από πού μπορεί κάποιος να βρει υλικό για ένα ψεύτικο προφίλ;
4. Πως καταλαβαίνετε αν ένα προφίλ είναι ψεύτικο;
5. Πόσους φίλους έχετε στο Facebook;
6. Για πόσους από αυτούς γνωρίζετε με βεβαιότητα ότι τα προφίλ τους είναι γνήσια;
7. Τι κακόβουλες ενέργειες μπορεί να κάνει ένας χρήστης χρησιμοποιώντας ένα ψεύτικο προφίλ;

36η Άσκηση (Σε εργαστηριακό περιβάλλον).

Κατά την περιήγησή σας στο Διαδίκτυο αφήνετε «ίχνη» σε όποια τοποθεσία επισκέπτεστε. Στην άσκηση αυτή θα δείτε τι πληροφορίες μπορεί να συλλέξει για εσάς ένας δικτυακός τόπος με μια απλή επίσκεψη σε αυτόν, αλλά και πως μπορείτε να «κρύψετε» κάποια από τα ίχνη σας.

Η εκτέλεση της άσκησης αυτής μετά το βήμα 5 μπορεί να επιτρέψει την πρόσβαση σε δικτυακούς τόπους με ακατάλληλο περιεχόμενο, ξεπερνώντας τους περιορισμούς που επιβάλει το Πανελλήνιο Σχολικό Δίκτυο. Προτείνεται στα βήματα αυτά να γίνει μόνο επίδειξη με βιντεοπροβολέα από τον εκπαιδευτικό.

1. Συνδεθείτε σε εικονική ή φυσική μηχανή με λειτουργικό σύστημα Linux ή Windows.
2. Χρησιμοποιώντας ένα browser ανοίξτε τη σελίδα *http://mybrowserinfo.com/*

3. Πατήστε στο σύνδεσμο «See Detailed Location and Browser Information» για να δείτε όλες τις πληροφορίες που ο browser αναφέρει στον Web Server.

4. Ποιες από αυτές τις πληροφορίες πιστεύετε ότι είναι οι πιο σημαντικές και μπορούν να «προδώσουν» την ταυτότητά σας;
5. Άνοιγμα της σελίδα *http://kproxy.com/*, ή κάποια άλλης αντίστοιχης.
6. Στο πλαίσιο κειμένου αναγραφή της διεύθυνσης «mybrowserinfo.com» και πάτημα του πλήκτρου [Surf].

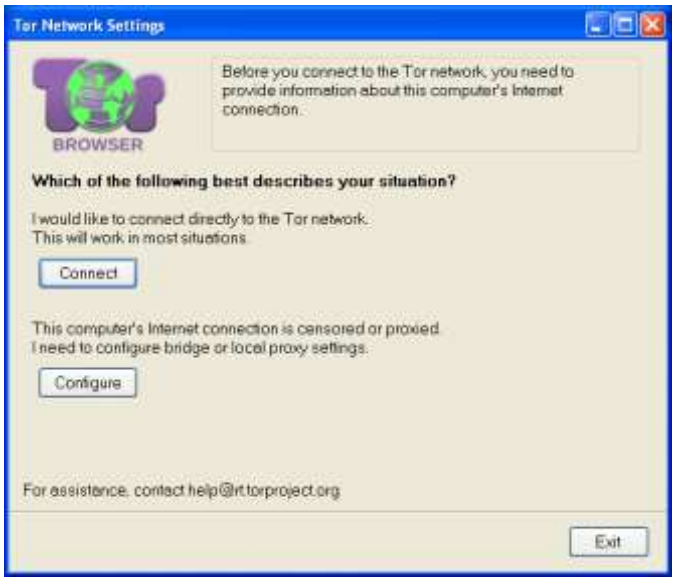
7. Υπάρχει αλλαγή στην IP διεύθυνση; Ποια χώρα αναγράφεται τώρα;
8. Άλλαξε κάτι σε σχέση με προηγουμένως στις αναλυτικές πληροφορίες;

37η Άσκηση (Σε εργαστηριακό περιβάλλον Windows ή Linux).

Ο πιο απλός τρόπος για να χρησιμοποιήσει κάποιος το δίκτυο TOR είναι να κατεβάσει τον Tor Browser που είναι μία έκδοση του Mozilla Firefox, χωρίς επεκτάσεις ή άλλα πρόσθετα, ειδικά διαμορφωμένη ώστε να χρησιμοποιεί το Tor.

Η εκτέλεση της άσκησης αυτής μπορεί να επιτρέψει την πρόσβαση σε δικτυακούς τόπους με ακατάλληλο περιεχόμενο, ξεπερνώντας τους περιορισμούς που επιβάλει το Πανελλήνιο Σχολικό Δίκτυο. Προτείνεται να γίνει μόνο επίδειξη με βιντεοπροβολέα από τον εκπαιδευτικό.

1. Σύνδεση σαν διαχειριστής σε εικονική ή φυσική μηχανή με λειτουργικό σύστημα Windows.
2. Άνοιγμα της σελίδα https://www.torproject.org/projects/torbrowser.html.en και μεταφόρτωση της σταθερής (stable) έκδοση του Tor Browser για το λειτουργικό σύστημα Windows. Στην ίδια σελίδα υπάρχουν και οδηγίες εγκατάστασης.
3. Διπλό click στο αρχείο εγκατάστασης (.exe).
4. Εγκατάσταση όπως σε οποιαδήποτε άλλη εφαρμογή.
5. Άνοιγμα της εφαρμογής από Έναρξη → Όλα τα προγράμματα → Start Tor Browser.



6. Πάτημα το κουμπί [Connect] για να γίνει η σύνδεση στο δίκτυο Tor και να ξεκινήσει ο Browser. Στην αρχική σελίδα που θα εμφανισθεί πάτημα στο σύνδεσμο «Test Tor Network Settings». Η παρακάτω σελίδα επιβεβαιώνει την έναρξη της ανώνυμης πλοήγησης.

7. Άνοιγμα τη σελίδα *http://mybrowserinfo.com/*
8. Από ποια χώρα φαίνεται να προέρχεται η IP διεύθυνση;
9. Άνοιγμα της αρχικής σελίδας της Google στη διεύθυνση *http://www.google.com* Εμφανίζεται η σελίδα της ίδιας χώρας;

10. Άνοιγμα μερικών άλλων σελίδων. Υπάρχει διαφορά στην ταχύτητα με την οποία εμφανίζονται;

Βιβλιογραφία

Ελληνική

Βασιλάκης, Β., Τζανάκης, Δ. (2013). *Αξιοποίηση της Τεχνολογίας των Εικονικών Μηχανών στην Επαγγελματική Εκπαίδευση και την Κατάρτιση Πληροφορικής*, Πρακτικά Εργασιών 3ου Πανελλήνιου Συνεδρίου «Ένταξη των ΤΠΕ στην Εκπαιδευτική Διαδικασία», Πειραιάς.

Βασιλάκης, Β., Φίλου, Σ. (2014). *Διδακτικό Σενάριο για τη Διδασκαλία Λειτουργικών Συστημάτων με χρήση Εικονικών Μηχανών στην Επαγγελματική Εκπαίδευση και Κατάρτιση* Πληροφορικής, Πρακτικά Εργασιών Πανελλήνιου Συνεδρίου «Η Εκπαίδευση στην εποχή των Τ.Π.Ε.», Αθήνα.

Γιαλούρης Π. (2011). *Μέθοδοι και εργαλεία ανάλυσης ευπαθειών δικτύων και εφαρμογών*. Διπλωματική Εργασία. Πειραιάς, Πανεπιστήμιο Πειραιά

Κάτσικας Σ. (2001). *Ασφάλεια Δικτύων.* Πάτρα. ΕΑΠ

Μάγκος Κ., Νιξαρλίδης Α. (1999). *Ασφάλεια στο Διαδίκτυο.* Πτυχιακή Εργασία, ανακτήθηκε στις 25/7/2015 από http://www.islab.demokritos.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/index.htm

Ν. Γεωργακόπουλος. (2006). *Στεγανογραφία*, Πτυχιακή στον Τομέα της Ασφάλειας, Α.Τ.Ε.Ι. Κρήτης, ανακτήθηκε 20/7/2015 από http://nefeli.lib.teicrete.gr/browse/stef/epp/2006/GeorgapopoulosNikolaos/attached-document/2006Georgapopoulos.pdf

Φούσκας Γ. (2002). *Δίκτυα Υπολογιστών Ι*. Πάτρα. ΕΑΠ

Ξενόγλωσση

Simpson A. (2001). *Windows XP Bible*. New York. Hungry Minds, Inc

Bott E., Siechert C., Stinson C. (2011). *Windows 7 Inside Out Deluxe Edition*. Redmond, Washinghton, Microsoft Press

Stanek W. (2010). *Windows 7: The Definitive Guide*. Sebastopol, O'Reilly Media Inc.

Sobell M. (2014). *A Practical Guide to Ubuntu Linux,* Pearson Education

Jang M. (2009). *Ubuntu Server Administration*. Mc Graw Hill

Tanebaum A. (2011). *Computer Networks (fifth edition)*. Prentice Hall

Naugle M. (1998). *Illustrated TCP/IP*. Wiley Computer Publishing, John Wiley & Sons, Inc.

Kizza J. Bott E., Siechert C., Stinson C. (2014). *Computer Network Security and Cyber Ethics*. Jefferson, North Carolina. McFarland & Company, Inc.

Cole E. (2002). *Hackers Beware*. United States of America. New Riders Publishing

Δικτυογραφία

Τι είναι το ηλεκτρονικό "ψάρεμα"; http://windows.microsoft.com/el-gr/windows-vista/what-is-phishing

:Ισχυρό Password - Τα Μεγαλύτερα Λάθη και οι Κίνδυνοι, http://www.pcsteps.gr/1245-ισχυρό-password-λάθη-κίνδυνοι-ασφάλεια

Wikipedia (Social Engineering), https://en.wikipedia.org/wiki/Social_engineering_(security)

Βικιπαιδεία (Κρυπτογράφηση Δημόσιου Κλειδιού), https://el.wikipedia.org/wiki/Κρυπτογράφηση_Δημόσιου_Κλειδιού

20 Linux Server Hardening Security Tips, http://www.cyberciti.biz/tips/linux-security.html

How (and why) to set up a VPN today, http://www.pcworld.com/article/2030763/how-and-why-to-set-up-a-vpn-today.html

Tor: Overview, https://www.torproject.org/about/overview.html.en

Κεφάλαιο 9ο

Τεχνολογίες Ασύρματης Δικτύωσης

Εισαγωγή

Τα ασύρματα δίκτυα είναι πλέον μέρος του σύγχρονου τρόπου ζωής του ανθρώπου και όλο και περισσότερες καθημερινές λειτουργίες του ολοκληρώνονται με τη χρήση εφαρμογών που συνεργάζονται με έξυπνες συσκευές με ασύρματη δικτυακή κάλυψη. Τα πολλά πλεονεκτήματα της τεχνολογίας ασύρματης δικτύωσης, σε συνδυασμό με τα παγκόσμια υιοθετημένα πρότυπα και τη πληθώρα συνεργαζόμενων συσκευών, την καθιστούν μια διαρκώς εξελισσόμενη τεχνολογία. Τα ασύρματα συνδυάζονται μαζί με τα ενσύρματα για να δημιουργήσουν πιο ευέλικτες τοπολογίες και να καλύψουν όλο και μεγαλύτερες περιοχές με τις υπηρεσίες που προσφέρουν. Ωστόσο ιδιαίτερη προσοχή απαιτούν τα θέματα ασφαλείας που τα καθιστούν ευαίσθητα σε επιθέσεις.

Διδακτικοί Στόχοι

Με την ολοκλήρωση του 9ου κεφαλαίου οι μαθητές θα πρέπει να είναι σε θέση να:

- Απαριθμούν τα πλεονεκτήματα και τις αδυναμίες της ασύρματης δικτύωσης.
- Επεξηγούν τα διάφορα πρωτόκολλα ασύρματης δικτύωσης και να διακρίνουν τις μεταξύ τους διαφορές.
- Αντιπαραβάλλουν τις δύο βασικές κατηγορίες ασύρματων δικτύων και να εξηγούν τις μεταξύ τους διαφορές.
- Αντιστοιχίζουν τα εξαρτήματα υλικού που χρησιμοποιούνται στην ασύρματη δικτύωση, με το έργο που το κάθε ένα επιτελεί.
- Επιλέγουν το κατάλληλο υλικό για τη δημιουργία ενός ασύρματου δικτύου, ανάλογα με τις υφιστάμενες απαιτήσεις.
- Εξηγούν τους τρόπους με τους οποίους η λειτουργία άλλων συσκευών επηρεάζει το ασύρματο δίκτυο.
- Επιλέγουν την καταλληλότερη τοποθεσία για την εγκατάσταση του υλικού ενός ασύρματου δικτύου, έτσι ώστε να μεγιστοποιούν την εμβέλειά του και την ισχύ του σήματός του.
- Ανιχνεύουν τα γειτονικά ασύρματα και να επιλέγουν το κανάλι επικοινωνίας με τις λιγότερες παρεμβολές.
- Συνδέουν έναν σταθμό εργασίας σε ένα ελεύθερο (χωρίς ασφάλεια) ασύρματο δίκτυο.
- Απαριθμούν και να εξηγούν τους κινδύνους για την ασφάλεια των δεδομένων και του δικτύου από τα δίκτυα με ελεύθερη πρόσβαση.
- Διατυπώνουν τις προφυλάξεις που πρέπει να λαμβάνονται κατά τη σύνδεση σε ελεύθερα Σημεία Πρόσβασης (Hotspots).
- Χρησιμοποιούν τον αλγόριθμο WEP προκειμένου να προσδώσουν ασφάλεια σε ένα ασύρματο δίκτυο.
- Αναγνωρίζουν τις αδυναμίες που προσφέρει η ασφάλεια WEP και να προτείνουν εναλλακτικές για την αύξηση της ασφάλειας.
- Να χρησιμοποιούν τους αλγόριθμους WPA και WPA2 για την αύξηση της ασφάλεια του δικτύου.
- Αξιοποιούν την τεχνική MAC φιλτραρίσματος (MAC Filtering) για τον επιπλέον περιορισμό της πρόσβασης στο ασύρματο δίκτυο.

- Διακρίνουν τις διαφορετικές ανάγκες ασφάλειας στο Οικιακό και στο επιχειρησιακό περιβάλλον και να υλοποιούν ασφάλεια με χρήση Εξυπηρετητή Radius.
- Δημιουργούν σημεία πρόσβασης από κινητές συσκευές για το διαμοιρασμό της σύνδεσης Διαδικτύου μέσω κινητής τηλεφωνίας.

Διδακτικές Ενότητες

9.1 Τεχνολογία Ασύρματης Δικτύωσης.
9.2 Πρότυπα ασύρματης δικτύωσης.
9.3 Εξοπλισμός για τη δημιουργία Ασύρματων Δικτύων.
9.4 Εγκατάσταση και Σύνδεση σε Ασύρματο Δίκτυο.
9.5 Κάλυψη χώρου με Ασύρματο Δίκτυο.
9.6 Ασφάλεια στα Ασύρματα Δίκτυα.

9.1 Τεχνολογία Ασύρματης Δικτύωσης

9.1.1 Η ανάγκη για ασύρματη δικτύωση

Ένα **ασύρματο δίκτυο** είναι ένα δίκτυο το οποίο δεν χρησιμοποιεί καλώδια για τις συνδέσεις των διαφόρων συσκευών που δικτυώνονται σε αυτό. Αντί του καλωδίου χρησιμοποιείται η μετάδοση μέσω ειδικά διαμορφωμένων οπτικών, υπέρυθρων ή ακόμα και ραδιοκυματικών σημάτων. Προϋπόθεση για τη σύνδεση των μεταξύ τους συσκευών είναι και το να είναι εξοπλισμένες με το κατάλληλο υλικό διεπαφής που επιτρέπει τη σύνδεσή τους μέσω ασύρματης τεχνολογίας.

Εικόνα 9.1: Συσκευές και πιθανές χρήσεις με εφαρμογές ενσύρματου και ασύρματου δικτύου.

(Τροποποιημένη από πηγή: http://www.conceptdraw.com/How-To-Guide/home-area-network)

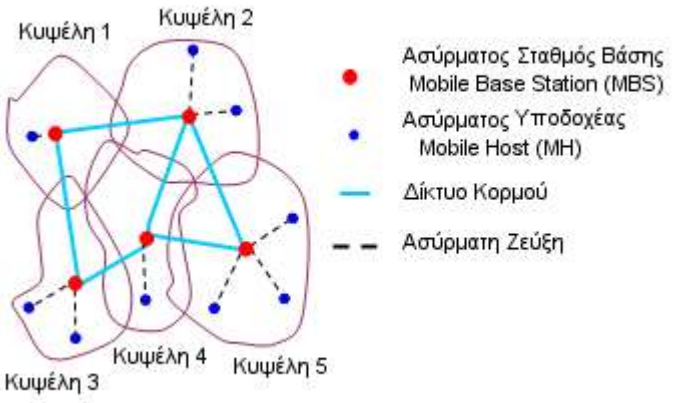
Η ασύρματη δικτύωση σήμερα έχει επαναστατικά αλλάξει τον τρόπο ζωής μας, όπως συνέβη με τους προσωπικούς υπολογιστές τη δεκαετία 1980 και το Διαδίκτυο, τα οποία άλλαξαν τον τρόπο που επικοινωνούμε και προσλαμβάνουμε πληροφορίες. Η χρήση ασύρματων φορητών συσκευών, όπως έξυπνα τηλέφωνα (smartphones), Η/Υ ταμπλέτες (tablets) και οι φορητοί υπολογιστές (laptops), για την αποστολή και λήψη μηνυμάτων, την πλοήγηση στο Διαδίκτυο, την πρόσβαση σε εταιρικές εφαρμογές και βάσεις δεδομένων, είναι πλέον μέρος της καθημερινής ρουτίνας του σύγχρονου ανθρώπου. Επίσης πλήθος άλλων συσκευών προστίθενται συνεχώς στη λίστα αυτών που μπορούν να επικοινωνήσουν χωρίς τη χρήση καλωδίων, όπως βιντεοκάμερες, φορητές συσκευές αναπαραγωγής ήχου, ακόμα και ψυγεία.

Σήμερα οι άνθρωποι χρησιμοποιούν τις ασύρματες συσκευές τους όχι μόνο για να επικοινωνήσουν μέσω ηχητικού σήματος, αλλά και για να έχουν πρόσβαση σε πληροφορίες, να προμηθεύονται εισιτήρια για τα μέσα μεταφοράς, για αγορές σε ηλεκτρονικά καταστήματα και πολλές άλλες χρήσεις. Αρκεί ο χρήστης της συσκευής να βρει ένα σημείο ασύρματης πρόσβασης στο Internet (hotspot).

9.1.2 Ιστορικά στοιχεία

Η ασύρματη επικοινωνία είναι ένας χώρος που αναπτύσσεται εδώ και 100 χρόνια, ξεκινώντας γύρω στο 1897 με την επιτυχή επίδειξη της ασύρματης τηλεγραφίας του Marconi, ενώ το 1901, εγκαταστάθηκε η ραδιο-επικοινωνία διαμέσου του Ατλαντικού Ωκεανού. Μέσα σε αυτά τα χρόνια πολλοί τύποι ασύρματης δικτύωσης εμφανίστηκαν, άλλοι άκμασαν και άλλοι εγκαταλείφθηκαν.

Σήμερα τα ασύρματα δίκτυα με τη μεγαλύτερη εξάπλωση και εφαρμογή είναι τα κυψελοειδή, καθώς πολλά από τα ασύρματα συστήματα μπορούν να καταταχθούν ως ιδιαίτερες εφαρμογές ή απλές γενικεύσεις των κυψελοειδών δικτύων. Κάθε δίκτυο καλύπτει μια περιοχή που ονομάζεται κυψέλη χρησιμοποιώντας ένα σταθμό βάσης και πολλούς ασύρματους χρήστες-δέκτες. Αντίστοιχα, κάθε κυψέλη καλύπτει με ασύρματο σήμα μια περίπου εξαγωνική ή κυκλική περιοχή που όμως στην πράξη δεν είναι τέλεια γεωμετρικά σχηματισμένη, καθώς η κάλυψη του σήματος εξαρτάται από τη μορφολογία του εδάφους της περιοχής και τα φυσικά ή τεχνητά εμπόδια που υπάρχουν σε αυτή. Όπως φαίνεται και στο παράδειγμα του σχήματος 9.1, η κάλυψη της περιοχής του παραδείγματος γίνεται με τη χρήση Ασύρματων Σταθμών Βάσης (Mobile Base Hosts - MBS) συνδεόμενων μεταξύ του με ένα ενσύρματο Δίκτυο Κορμού και οι Ασύρματοι Υποδοχείς (Mobile Hosts -MH) συνδέονται στο δίκτυο μέσω του σταθμού βάσης, που έχει το ισχυρότερο σήμα στην περιοχή που βρίσκονται.



Σχήμα 9.1: Κάλυψη περιοχής με ασύρματο δίκτυο με χρήση τεχνολογίας κυψελών.

Το 1997, μετά από επτά χρόνια μελέτης, η IEEE δημοσίευσε το πρότυπο IEEE 802.11, το πρώτο πρότυπο για ασύρματη δικτύωση, το οποίο προβλέπει ρυθμούς μετάδοσης 1 και 2 Mbps. Το IEEE 802.11 χρησιμοποιούταν στα πρώτα ασύρματα δίκτυα αισθητήρων (wireless sensor networks, WSN) και μπορούν ακόμα να βρεθούν σε δίκτυα με υψηλές απαιτήσεις σε εύρος ζώνης, όπως είναι οι αισθητήρες πολυμέσων (multimedia sensors). Σήμερα το πρότυπο διαιρείται σε μια οικογένεια προτύπων ασύρματης δικτύωσης, τα οποία αποτελούν τα επικρατέστερα πρότυπα αυτής παγκοσμίως.

9.1.3 Πλεονεκτήματα και Μειονεκτήματα

Τα βασικά πλεονεκτήματα της ασύρματης δικτύωσης είναι:

- **Ευκολία και ευελιξία στην εγκατάσταση** - Δεν χρειάζεται να εγκαταστήσουμε καλωδιώσεις μέσα από τοίχους και ταβάνια. Μπορεί να γίνει η δικτύωση σε μέρη όπου η καλωδίωση θα ήταν αδύνατη, όπως η δικτύωση γραφείων τα οποία βρίσκονται σε απόσταση μεταξύ τους. Η εγκατάσταση στις περισσότερες περιπτώσεις μπορεί να γίνει εύκολα, αν ακολουθηθούν κάποιοι βασικοί κανόνες εγκατάστασης.
- **Κινητικότητα** - Οι χρήστες των ασύρματων συσκευών μπορούν να μετακινούνται εντός της εμβέλειας του ασύρματου δικτύου, δηλαδή σε χώρο που θα έχουν επαρκές σήμα, διατηρώντας τη συνδεσιμότητα τους με αυτό.
- **Δυνατότητα επέκτασης** - Τα ασύρματα δίκτυα μπορούν να οργανωθούν σε ένα πλήθος από τοπολογίες, οι οποίες αλλάζουν εύκολα και επεκτείνονται από απλά δίκτυα με μικρό αριθμό χρηστών, ως μεγάλες δομές δικτύων με εκατοντάδες χρήστες και δυνατότητα περιαγωγής (roaming).
- **Χαμηλό κόστος συντήρησης** – Αν και το αρχικό κόστος εγκατάστασης είναι υψηλότερο σε σχέση με λύσεις ενσύρματης δικτύωσης, το κόστος διαχείρισης του δικτύου είναι πολύ μικρό. Η ευελιξία επέκτασης του δικτύου, ιδιαίτερα σε δυναμικό περιβάλλον που απαιτεί συχνές αλλαγές, καθιστά το συνολικό κόστος μικρότερο, για όλη τη διάρκεια ζωής της επένδυσης. Επίσης ο έντονος ανταγωνισμός των κατασκευαστών υλικού έχει συμβάλει στη μείωση του κόστους των συσκευών και στην άνοδο των ποιοτικών χαρακτηριστικών τους.
- **Συνεχή αύξηση των ταχυτήτων μετάδοσης -** Ήδη ο μέγιστος ρυθμός μετάδοσης δεδομένων έχει σήμερα σε ταχύτητες πάνω από 100Mbps, ενώ ήδη έχουν εξαγγελθεί ακόμα μεγαλύτερες ταχύτητες.
- **Εμβέλεια -** Η εμβέλεια ενός ασύρματου δικτύου μπορεί να είναι μερικές δεκάδες μέτρα. Τα ραδιοκύματα που έχουν να διαπεράσουν τοίχους και οροφές υφίστανται σημαντική εξασθένηση, όμως σε ανοικτό χώρο με οπτική επαφή ανάμεσα στις ασύρματες συσκευές, οι αποστάσεις που μπορεί να καλυφθούν είναι μεγαλύτερες.
- **Συμβατότητα με υπάρχοντα δίκτυα -** Τα περισσότερα ασύρματα δίκτυα έχουν προτυποποιημένο τρόπο σύνδεσης με τα προϋπάρχοντα ενσύρματα δίκτυα. Έτσι, η προσθήκη ασύρματης δικτύωσης σε υπάρχουσες δομές δικτύων είναι εύκολη, αποτελώντας επέκταση ενός ενσύρματου δικτύου.

Αντίστοιχα βασικά μειονεκτήματα είναι:

- **Ασφάλεια –** Η ασύρματη μετάδοση είναι πιο ευάλωτη σε επιθέσεις από μη εξουσιοδοτημένους χρήστες, σε σχέση με τα ενσύρματα δίκτυα. Επειδή τα ασύρματα δίκτυα είναι έτσι κατασκευασμένα ώστε επεξεργάζονται όλες τις ραδιομεταδόσεις εντός εμβέλειας, ακόμα και τις μη εξουσιοδοτημένες από το διαχειριστή του δικτύου. Επομένως απαιτείται ιδιαίτερη προσοχή στη θωράκιση της ασφάλειάς τους.

- **Παρεμβολές –** Η χρήση και άλλων ασύρματων ραδιο-συνδέσεων μέσα σε ένα κτίριο μπορεί προκαλέσει παρεμβολές, οδηγώντας σε προβληματική επικοινωνία ή ακόμα και απώλεια της σύνδεσης.
- **Κάλυψη σήματος** – Σε ορισμένα κτίρια, η ολοκληρωμένη και συνεχής κάλυψη είναι δύσκολη, οδηγώντας στην ύπαρξη μαύρων σημείων (black spots) με απουσία σήματος.
- **Χαμηλές ταχύτητες** – Μπορεί οι ταχύτητες μετάδοσης των δεδομένων στην ασύρματη δικτύωση να αυξάνονται συνεχώς, όμως ακόμα υπολείπονται των ενσύρματων. Για αυτό το λόγο τα δίκτυα κορμού, τα οποία απαιτούν υψηλότατες ταχύτητες, εξακολουθούν να είναι ενσύρματα.

9.1.4 Τοπολογίες Ασύρματων Δικτύων

9.1.4.1 Ασύρματα Δίκτυα Αυτοοργανωμένα (Ad Hoc)

Ένα **ασύρματο ad hoc δίκτυο (αυτοοργανωμένο ή κατ' απαίτηση),** γνωστό και ως Peer-to-peer, είναι ένας αποκεντρωμένος τύπος ασύρματου δικτύου. Το δίκτυο είναι ad hoc επειδή δε βασίζεται σε κάποια προϋπάρχουσα υποδομή, όπως δρομολογητές στα ενσύρματα δίκτυα ή ασύρματα σημεία πρόσβασης (AP, access points) στα διαχειριζόμενα ασύρματα δίκτυα. Αντίθετα, κάθε κόμβος λαμβάνει μέρος στη δρομολόγηση προωθώντας τα δεδομένα προς τους άλλους κόμβους, κι έτσι ο καθορισμός του ποιοι κόμβοι προωθούν δεδομένα γίνεται δυναμικά με βάση τη συνδεσιμότητα του δικτύου.

Τα ασύρματα ad hoc δίκτυα μπορούν να ταξινομηθούν περαιτέρω με βάση την εφαρμογή τους σε:

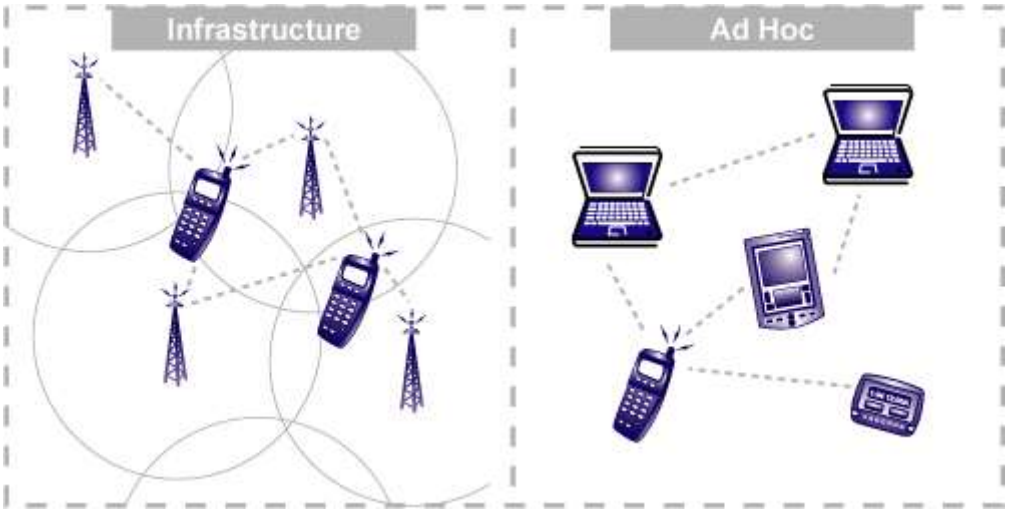
- Κινητά ad hoc δίκτυα (MANET - Mobile Ad hoc NETworks)
- Ασύρματα δίκτυα πλέγματος (WMN - Wireless Mesh Networks)
- Ασύρματα δίκτυα αισθητήρων (WSN - Wireless Sensor Networks)

Πλεονεκτήματα

Ο αποκεντρωμένος χαρακτήρας των ασύρματων ad hoc δικτύων τα καθιστά κατάλληλα για ποικίλες εφαρμογές, οι οποίες δε μπορούν να βασίζονται σε κεντρικούς κόμβους και μπορούν να **βελτιώσουν την ευελιξία τους** σε σχέση με τα διαχειριζόμενα ασύρματα δίκτυα. Η **γρήγορη εγκατάσταση** και η **ελάχιστη απαιτούμενη διαμόρφωση** καθιστούν τα ασύρματα ad hoc δίκτυα **κατάλληλα για καταστάσεις έκτακτης ανάγκης**, όπως φυσικές καταστροφές ή πολεμικές συρράξεις. Επίσης τα ad hoc δίκτυα είναι ευέλικτα και κατάλληλα για την **απευθείας σύνδεση δύο συσκευών**, χωρίς τη χρήση ενός κεντρικού σημείου πρόσβασης. Γενικότερα η παρουσία δυναμικών και προσαρμοστικών πρωτοκόλλων επιτρέπει στα ad hoc δίκτυα να σχηματίζονται γρήγορα.

Μειονεκτήματα

Ωστόσο, απαιτεί **περισσότερους πόρους από τις συσκευές για τη διατήρηση της σύνδεσης**, αν αυτές μετακινούνται και παράλληλα η **εμβέλεια των συστημάτων σύνδεσής του είναι μικρότερη** σε σχέση με ένα σταθερό σημείο πρόσβασης. Τέλος βασικό μειονέκτημα τους είναι **αδυναμία πρόβλεψης της ποικιλίας των πιθανών καταστάσεων** που μπορεί να προκύψουν, λόγω του δυναμικού τους χαρακτήρα.



Εικόνα 9.2: Τρόπος σύνδεσης δικτύων Infrastructure και Ad hoc

(Πηγή: http://www.e-cartouche.ch/content_reg/cartouche/LBStech/en/html/LBStechU2_wlantopo.html)

9.1.4.2 Ασύρματα Δίκτυα Υποδομής (Infrastructure)

Αντίθετα τα **ασύρματα δίκτυα υποδομής (Infrastructure Wireless Networks)** είναι μια πιο σύνθετη τοπολογία ασύρματης δικτύωσης. Σε αυτή το ασύρματο δίκτυο έχει μια κυψελοειδή μορφή, αποτελούμενο από έναν αριθμό από κυψέλες. Σε κάθε κυψέλη υπάρχει ένας σημείο πρόσβασης (AP, Access Point) και ένας αριθμός από ασύρματους σταθμούς, οι οποίοι εξυπηρετούνται από το σημείο πρόσβασης. Η κυψέλη είναι το βασικό δομικό στοιχείο ενός ασύρματου δικτύου. Κάθε σταθμός που θέλει να συνδεθεί στο ασύρματο δίκτυο πρέπει να κάνει αίτημα σύνδεσης σε ένα σημείο πρόσβασης και ξεκινά τη διαδικασία συσχετισμού (Association Process), όπου στο τέλος της το σημείο πρόσβασης κάνει δεκτό το αίτημα ή το απορρίπτει.

Η τρόπος αυτός ασύρματης σύνδεσης είναι **ιδανικός για την εγκατάσταση ενός μόνιμου δικτύου**. Οι ασύρματοι δρομολογητές που χρησιμοποιούνται ως σημεία πρόσβασης έχουν συνήθως **μεγαλύτερη εμβέλεια κάλυψης** και **διευκολύνουν την κινητικότητα** των ασυρμάτων συσκευών εντός της κυψελοειδούς περιοχής.

Τέλος υπάρχουν και υβριδικές τοπολογίες, οι οποίες συνδυάζουν και τις δύο προαναφερόμενες τοπολογίες, αυτοοργανωμένες και υποδομής, για καλύτερη κάλυψη περιοχών με ασύρματο σήμα.

9.2 Πρότυπα ασύρματης δικτύωσης

9.2.1 IEEE 802.11

Η IEEE 802.11 είναι μια οικογένεια πρωτοκόλλων που περιγράφουν τη λειτουργία ασύρματων τοπικών δικτύων (WLAN, Wireless Local Access Network) καλύπτουν όλα τα απαραίτητα στοιχεία για τη συνεργασία συσκευών και λογισμικού σε ένα ασύρματο δίκτυο. Στο πρωτόκολλο αυτό περιγράφονται τα δύο κατώτερα επίπεδα του OSI, δηλαδή το φυσικό επίπεδο και το επίπεδο σύνδεσης δεδομένων, επιτρέποντας τη συνεργασία των συσκευών που το ακολουθούν και οποιαδήποτε εφαρμογή συνεργάζεται με μια συσκευή που ακολουθεί το πρότυπο αυτό 802.11. Οι συσκευές 802.11 δηλαδή μεταφέρουν την πληροφορία από τα πιο πάνω επίπεδα του OSI. Υποστηρίζει δυνατότητες όπως είναι η προτεραιοποίηση της κίνησης και η υποστήριξη εφαρμογών πραγματικού χρόνου.

Ωστόσο το πρότυπο σχεδιάστηκε και για υψηλούς ρυθμούς μετάδοσης, με αποτέλεσμα η κατανάλωση ενέργειας και το εύρος ζώνης του πρότυπου είναι πολύ υψηλότερα από τις

συνήθεις απαιτήσεις μετάδοσης δεδομένων. Το γεγονός αυτό οδήγησε στη δημιουργία μιας πληθώρας προτύπων που καλύπτουν καλύτερα τις ανάγκες χαμηλής κατανάλωσης ενέργειας και χαμηλών ρυθμών μετάδοσης δεδομένων.

9.2.2 IEEE 802.11a

Το 1999 δημιουργήθηκε η επέκταση IEEE 802.11a στο αρχικό πρότυπο, που αποσκοπούσε να καλύψει την ανάγκη για μεγαλύτερους ρυθμούς μετάδοσης. Η επέκταση αυτή προβλέπει μετάδοση 5GHz με ρυθμούς μετάδοσης 1, 2, 5.5, 11, 6, 12, 24 Mbps και προαιρετικά 36, 48, 54 Mbps χρησιμοποιώντας OFDM (Orthogonal Frequency Division Multiplexing) διαμόρφωση. Επιλέχθηκε η λειτουργία του σε μια υψηλότερη ζώνη συχνοτήτων, αφενός για να μπορούν να υποστηριχθούν οι μεγαλύτεροι ρυθμοί, αφετέρου ώστε να μην υπάρχει παρεμβολή από τις άλλες συσκευές. Επομένως οι συσκευές του 802.11a είναι ασύμβατες με αυτές που εργάζονται με άλλα μέλη της οικογένειας του προτύπου, όπως το πιο γνωστό 802.11b, αφού ο τρόπος μετάδοσης αλλά και οι ραδιοσυχνότητες που χρησιμοποιούνται είναι διαφορετικές.

9.2.3 IEEE 802.11b

Το IEEE 802.11b αναπτύχθηκε το 1999 και αποτελεί μια επέκταση στο αρχικό πρότυπο. Συγκεκριμένα υποστηρίζει μετάδοση σε ρυθμούς 5.5 και 11Mbps και στη ζώνη συχνοτήτων των 2.4GHz. Είναι το πιο δημοφιλές από όλα τα πρότυπα και το πρότυπο με τη μεγαλύτερη διαλειτουργικότητα, καθώς είναι ένα δοκιμασμένο και αποτελεσματικό πρότυπο. Οι προσθήκες του 802.11b σε σχέση με το αρχικό 802.11 αφορούν μόνο τον τρόπο μετάδοσης, ενώ ο τρόπος πρόσβασης των συσκευών και οι τρόποι λειτουργίας παραμένουν οι ίδιοι.

9.2.4 IEEE 802.11g

Το 802.11g αποτελεί επέκταση του 802.11b, ώστε να υποστηρίζει ακόμα μεγαλύτερους ρυθμούς. Έτσι εκτός από τους ρυθμούς μετάδοσης του 802.11b , υποστηρίζει και ρυθμούς μέχρι 54Mbps. Οι αντίστοιχες συσκευές εργάζονται στη ζώνη συχνοτήτων των 2.4GHz, διατηρώντας συμβατότητα με το 802.11b.

9.2.5 IEEE 802.11n

Η IEEE ξεκίνησε να εργάζεται πάνω στο πρότυπο 802.11n το 2004, ως μια βελτίωση της τεχνολογίας των ασύρματων τοπικών δικτύων, καθώς ήταν ξεκάθαρο ότι τα 54 Mbps δεν ήταν πλέον αρκετά για την κάλυψη των συνεχώς αυξανόμενων αναγκών σε εύρος ζώνης των ασυρμάτων δικτύων. Βασικό χαρακτηριστικό του προτύπου είναι η υποστήριξη της τεχνολογίας MIMO (Multiple-input and multiple-output), η οποία βασίζεται στη χρήση προδιαγραφών πολλαπλών συχνοτήτων και κεραιών, αποστέλλοντας δεδομένα ταυτόχρονα σε πολλές κεραίες και πορείες σημάτων. Με μέγιστο αριθμό τεσσάρων πομπών και τεσσάρων δεκτών και υποστηρίζοντας παράλληλα συχνότητες 2,4 GHz and 5 GHz, σχεδόν διπλασιάζει το εύρος κάλυψης των ασύρματων τοπικών δικτύων, φτάνοντας την ταχύτητα μετάδοσης στα 600 Mbps. Οι υψηλές του ταχύτητες μπορούν θεωρητικά να υποστηρίξουν ακόμα και κανάλια πολλαπλών καναλιών ψηφιακής τηλεόρασης HDTV (high definition TV), τα οποία τα σημερινά δίκτυα δεν μπορούν να τα υποστηρίξουν.

Πολλοί κατασκευαστές υλικού έχουν ήδη ξεκινήσει να παράγουν συσκευές που υποστηρίζουν το πρότυπο αυτό, οι οποίες πρέπει επίσης να υποστηρίζουν τα πρότυπα πολυμέσων του Wi-Fi (Wi-Fi multimedia, WMM), την ποιότητα υπηρεσιών QoS (quality-of-service) και μηχανισμούς ασφαλείας WPA και WPA2. Ωστόσο το πρότυπο 802.11n είναι ακόμα στα πρώτα βήματα του και δεν είναι ακόμα πλήρως δοκιμασμένο στην πράξη.

Πρότυπο IEEE	Μέγιστος ρυθμός μετάδοσης	Συχνότητες
802.11	1 Mbps / 2 Mbps	2.4 GHz
802.11a	11 Mbps	5 GHz
802.11b	5.5 Mbps / 11 Mbps	2.4 GHz
802.11g	54 Mbps	2.4 GHz
802.11n	600 Mbps	2.4 GHz & 5 GHz

Πίνακας 9.1: Συγκριτικός πίνακας προτύπων του IEEE 802.11

9.2.5 Wi-Fi

Το πρότυπο Wi-Fi (Wireless Fidelity) δημιουργήθηκε από την ένωση WECA (Wireless Ethernet Compatibility Alliance) ύστερα από μία ακολουθία δοκιμασιών προκειμένου να πιστοποιηθεί η συμβατότητα των προϊόντων με το πρωτόκολλο IEEE 802.b. Οι συσκευές οι οποίες περνούν με επιτυχία τις δοκιμασίες αυτές, αποκτούν το λογότυπο Wi-Fi, το οποίο πιστοποιεί τη συμβατότητα του με οποιαδήποτε άλλη συσκευή με αυτό το λογότυπο. Η πιστοποίηση αφορά λειτουργία των συσκευών στα πρότυπα 802.11a, 802.11b, 802.11g και υποστήριξη δυνατότητας βελτιωμένου πρότυπου ασφάλειας WPA/WPA2 στα ασύρματα δίκτυα.

9.3 Εξοπλισμός για τη δημιουργία Ασύρματων Δικτύων

9.3.1 Ασύρματες Κάρτες Δικτύου

Η ασύρματη κάρτα δικτύου (Wi-Fi NIC, Network Interface Controller) είναι μια μονάδα και παρέχει σε μια συσκευή δυνατότητα σύνδεσης της με ένα ασύρματο δίκτυο. Είναι συνήθως συμβατή με τα πρότυπα 802.11b/g/n και συνήθως υποστηρίζει τα πιο γνωστά πρωτόκολλα ασφαλείας, όπως WEP, WPA, WPA2. Η ασύρματη κάρτα δικτύου μπορεί να έχει τη μορφή ενός USB Stick, να είναι μια κάρτα επέκτασης PCI ή να είναι ενσωματωμένη στα κυκλώματα της συσκευής.

Εικόνα 9.3: Δύο μορφές καρτών Δικτύων: Κάρτα επέκτασης PCI (αριστερά) και USB Stick (δεξιά)

9.3.2 Σημεία Πρόσβασης

Ένα **Ασύρματο Σημείο Πρόσβασης (Access Point, AP)** είναι μια **συσκευή** που αναλαμβάνει τη λειτουργία της ραδιοεπικοινωνίας με τους ασύρματους σταθμούς σε μια κυψέλη. Λειτουργεί σαν σταθμός βάσης συγκεντρώνοντας την κίνηση από τους ασύρματους σταθμούς και κατευθύνοντας την προς το υπόλοιπο δίκτυο. Άλλες λειτουργίες που αναλαμβάνει, είναι η αυθεντικοποίηση ενός καινούργιου σταθμού που ζητά πρόσβαση στο ασύρματο δίκτυο και η συσχέτιση μαζί του.

Συνήθως ένα σημείο πρόσβασης είναι εξωτερική συσκευή συνδεόμενή ενσύρματα με ένα δρομολογητή, εσωτερική μονάδα σε ένα δρομολογητή ή υλοποιείται με χρήση λογισμικού και μιας κάρτας PCI σε ένα Η/Υ.

Ένα **hotspot ή ελεύθερο σημείο ασύρματης πρόσβασης** είναι μια **φυσική τοποθεσία** που προσφέρει μια ασύρματη σύνδεση με ένα ασύρματο τοπικό δίκτυο (WLAN) και η οποία παρέχει υπηρεσίες Διαδικτύου ευρείας σύνδεσης (broadband). Η σύνδεση πραγματοποιείται μέσω ενός ασύρματου δρομολογητή που συνδέεται με έναν Παροχέα Υπηρεσιών Διαδικτύου και τυπικά χρησιμοποιεί τεχνολογία προτύπου Wi-Fi. Όλο και περισσότερα μέρη διαθέτουν πλέον hotspots και ένας χρήστης μπορεί να τα βρει σε αρκετά δημόσια μέρη, όπως αεροδρόμια, ξενοδοχεία ή καταστήματα εστίασης, τα οποία προσφέρουν τις υπηρεσίες τους είτε δωρεάν, είτε με χρέωση χρήσης.

Βασικό **μειονέκτημα των hotspot** είναι ότι σε πολλά από αυτά είναι απενεργοποιημένα τα συστήματα ασφαλείας, που συνήθως διαθέτουν τα ασύρματα δίκτυα, ώστε να επιτυγχάνουν ταχύτερο συσχετισμό με στις ασύρματες φορητές συσκευές, καθιστώντας τα πιο ευάλωτα σε επιθέσεις υποκλοπής πληροφοριών.

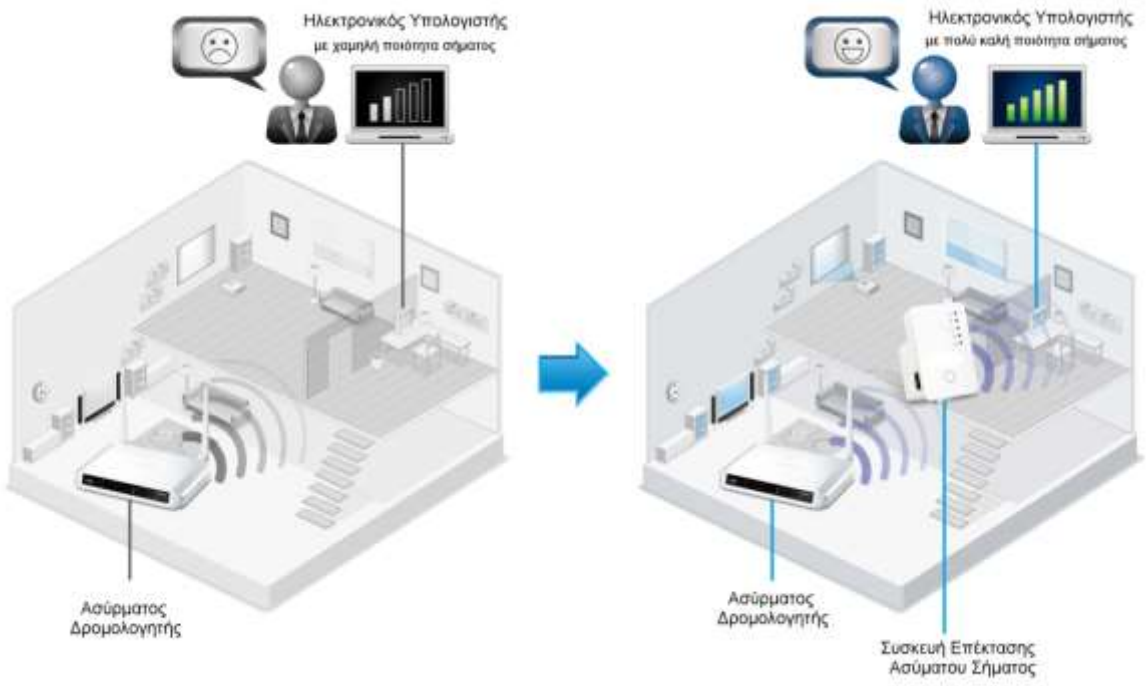
Η **βασική διαφορά ενός AP με ένα hotspot** είναι ότι το πρώτο είναι συσκευή ενώ το δεύτερο είναι μια φυσική τοποθεσία ή περιοχή.

9.3.3 Επεκτάσεις (Extenders)

Μια επέκταση ασύρματου σήματος (range extender ή range expander) είναι ένας τύπος ασύρματου επαναλήπτη που χρησιμοποιείται για την επέκταση ενός ασύρματου τοπικού δικτύου. Η συσκευή τοποθετείται ανάμεσα στο δρομολογητή βάσης ή στο σημείο πρόσβασης (AP) και τη συσκευή/ες που απαιτούν σύνδεση με το ασύρματο τοπικό δίκτυο και αδυνατούν λόγω ύπαρξης φυσικών εμποδίων ή έχουν μεγάλη απόσταση από το εύρος κάλυψης της αρχικής βάσης. Η επέκταση ασύρματου σήματος συνδέεται ασύρματα με το δρομολογητή ή το AP, λαμβάνει το αρχικό σήμα και το αναμεταδίδει. Η ταχύτητα του σήματος που λαμβάνει μια συσκευή από την επέκταση δεν είναι ίδια με τη ταχύτητα που θα είχε σε μια απευθείας σύνδεση με το βασικό σημείο εκπομπής, λόγω της καθυστέρησης που απαιτείται για την αναμετάδοση.

Τα βασικά χαρακτηριστικά μιας επέκτασης ασύρματου σήματος είναι ότι:

- Πρέπει να είναι τοποθετημένη σε ακτίνα κάλυψης σήματος τόσο από την πηγή εκπομπής, όσο και από τη συσκευή λήψης (client).
- Απαιτεί τα κρυπτογραφημένα κλειδιά συσχέτισης αν το σήμα είναι κρυπτογραφημένο.
- Έχει σταθερή IP διεύθυνση και δεν αναγνωρίζεται ως συσκευή λήψης (client).
- Το σήμα που αναμεταδίδει είναι το ίδιο με αυτό της πηγής εκπομπής.
- Η διεργασία της λειτουργεί καλύτερα όταν χρησιμοποιεί τα ίδια σύνολα ολοκληρωμένων κυκλωμάτων (chipsets) και λογισμικό με το δρομολογητή βάσης ή σημείο εκπομπής.



Εικόνα 9.4: Παράδειγμα χρήσης συσκευής επέκτασης για καλύτερη κάλυψη του χώρου

(Τροποποιημένη από πηγή: http://www.edimax.com/au/produce_detail.php?pd_id=513&pl1_id=1&pl2_id=99)

9.3.4 Κεραίες

Μια κεραία είναι μια αγώγιμη συσκευή που χρησιμοποιείται για τη μετάδοση ή/και για τη λήψη ραδιοκυματικών σημάτων. Είναι κατά βάση παθητική συσκευή και ίσως η πιο απλή μονάδα-εξάρτημα σε ένα ασύρματο δίκτυο. Ωστόσο για τη λειτουργία τους υπάρχει σημαντικός μηχανικός σχεδιασμός και πολύπλοκα μαθηματικά χάρη στα οποία οι κεραίες πληρώνουν τις απαιτούμενες ανάγκες λειτουργίας τους. Η κεραία είναι απαραίτητος εξοπλισμός μια για τις συσκευές που θέλουν να συνδεθούν σε ένα ασύρματο δίκτυο.

Υπάρχουν δύο βασικοί τύποι κεραιών που χρησιμοποιούνται στα ασύρματα δίκτυο:

- Οι κατευθυντικές κεραίες (directional antennas), που είναι σχεδιασμένες να εκπέμπουν το σήμα σε μια συγκεκριμένη κατεύθυνση σε μορφή δέσμης (beam).
- Οι πανκατευθυντικές κεραίες (omnidirectional antennas), που μεταδίδουν/δέχονται σήμα από/προς όλες τις κατευθύνσεις.

9.3.5 Φορητές Συσκευές

Τα σύρματα δίκτυα είναι σχεδιασμένα να μεταφέρουν δεδομένα μεταξύ φορητών συσκευών. Μια φορητή συσκευή είναι μια υπολογιστική μηχανή με διεπαφή ασύρματου δικτύου, η οποία λειτουργεί με χρήση μπαταρίας, όπως ένας φορητός υπολογιστής (laptop), ένας υπολογιστής ταμπλέτα (tablet) ή ένα έξυπνο τηλέφωνο (smartphone). Βασικό χαρακτηριστικό τους είναι η συνεχής ή περιοδική μετακίνησή τους εντός της ακτίνας εμβέλειας ενός δικτύου.

9.4 Εγκατάσταση και Σύνδεση σε Ασύρματο Δίκτυο

Για τη δημιουργία ενός ασύρματου δικτύου απαιτείται η εγκατάσταση ενός ή περισσότερων σημείων πρόσβασης (Access Points) ή επέκτασης, ανάλογα με την ανάγκη κάλυψης μια μεγαλύτερης ή με εμπόδια περιοχή. Τα σημεία πρόσβασης μπορεί να συνδέονται αντίστοιχα

με ένα ενσύρματο δίκτυο κορμού, ώστε να προσφέρουν υπηρεσίες Διαδικτύου ή διαμοιρασμού πληροφοριών.

Το ασύρματο δίκτυο είναι εξοπλισμένο με ένα σύστημα διανομής σήματος, το οποίο εξασφαλίζει την κινητικότητα των συσκευών που συνδέονται με μέσω των σημείων εκπομπής. Αρκεί όλες οι συνεργαζόμενες συσκευές εκπομπής και λήψης σήματος να είναι πιστοποιημένες με τα ίδια πρότυπα ασύρματης δικτύωσης, όπως το 802.11 ή Wi-Fi και να υποστηρίζουν τα ίδια πρότυπα ασφάλειας (WEP/WPA).

Μετά την εγκατάσταση του ασύρματης βάσης, όποια συσκευή με ενσωματωμένη κάρτα ασύρματου δικτύου βρίσκεται μέσα στην ακτίνα εκπομπής του σήματος, μπορεί να κάνει διαδικασία συσχέτισης και να συνδεθεί με το δίκτυο.

9.5 Κάλυψη χώρου με Ασύρματο Δίκτυο

Καθώς το ασύρματο δίκτυο είναι εξοπλισμένο με ένα σύστημα διανομής, εξασφαλίζει την κινητικότητα των συνδεόμενων συσκευών και φροντίζει να παραδίδει τα πλαίσια πληροφοριών (frames) στο σωστό σημείο πρόσβασης (AP) και στη συνέχεια στην επιθυμητή συσκευή προορισμού.

9.5.1 Κινητικότητα (Mobility)

Κινητικότητα είναι η δυνατότητα ελευθερίας κίνησης που έχει ένα υπολογιστικό σύστημα χωρίς την εξάρτηση του από καλώδια, ενώ ταυτόχρονα παρέχει τη δυνατότητα εκμετάλλευσης όλων των υπηρεσιών που θα διέθετε αν ήταν ενσύρματα συνδεμένος σε ένα δίκτυο. Η κινητικότητα επιτρέπει στους χρήστες να είναι συνδεδεμένοι στο δίκτυο οπουδήποτε και αν βρίσκονται μέσα στην ακτίνα κάλυψης του δικτύου. Για παράδειγμα, αν τα δεδομένα μιας βάσης δεδομένων είναι αποθηκευμένα κεντρικά, η κινητικότητα επιτρέπει στους χρήστες να έχουν πρόσβαση σε αυτά όπου και αν βρίσκονται.

9.5.2 Περιαγωγή (Roaming)

Όταν μια φορητή ασύρματη συσκευή βρεθεί εντός εμβέλειας ενός ή περισσοτέρων σημείων πρόσβασης (AP), διαλέγει εκείνο το AP το οποίο έχει ισχυρότερο σήμα ή την καλύτερη ποιότητα επικοινωνίας. Στη συνέχεια, γίνεται η συσχέτιση της φορητής συσκευής με το επιλεγμένο AP και είναι πλέον δυνατή η ασύρματη επικοινωνία. Περιοδικά γίνεται ανίχνευσή των διαθέσιμων σημάτων και στην περίπτωση που βρεθεί σήμα με καλύτερα χαρακτηριστικά, γίνεται επανασυσχέτιση με το καινούργιο AP και συντονισμός της συσκευής στην καινούρια συχνότητα.

Επίσης επανασυσχέτιση με άλλον σημείο πρόσβασης μπορεί να γίνει λόγω μετακίνησης της φορητής συσκευής ή μπορεί να γίνει σαν αποτέλεσμα υψηλού φόρτου στο δίκτυο, ώστε να βρεθεί καλύτερο AP. Με τον τρόπο αυτό υλοποιείται ένα από τα βασικά χαρακτηριστικά του προτύπου που είναι η κινητικότητα των χρηστών.

9.6 Ασφάλεια στα Ασύρματα Δίκτυα

Τα ασύρματα δίκτυα γενικότερα είναι περισσότερο ευαίσθητα σε επιθέσεις υποκλοπής, καθώς οι σταθμοί βάσης δέχονται και επεξεργάζονται αιτήματα συσχέτισης από όλες ανεξαιρέτως τις συσκευές-σταθμούς που βρίσκονται εντός εμβέλειας. Για παράδειγμα ένα ασύρματο δίκτυο που σχεδιάστηκε καλύπτει τις ανάγκες ενός κτιρίου, μπορεί η εμβέλειά του να βρίσκεται και εκτός αυτού, επιτρέποντας σε έναν εξωτερικό και πιθανά μη εξουσιοδοτημένο χρήστη να επιχειρήσει να συνδεθεί σε αυτό.

Για αυτό το λόγο και για την προστασία των δεδομένων που διακινούνται σε ένα ασύρματο δίκτυο εφαρμόζονται συνδυαστικά ορισμένες τεχνικές ασφαλείας, οι οποίες διαμορφώνουν συγκεντρωτικά πρότυπα ασφαλείας ειδικά για την ασύρματη επικοινωνία.

9.6.1 Τεχνικές Ασφάλειας με χρήση προτύπων WEP και WPA/WPA2

9.6.1.1 Πρότυπο ασφαλείας WEP

Το πρότυπο ασφαλείας WEP (Wired Equivalent Privacy), χρησιμοποιείται από τις συσκευές-σταθμούς που συνδέονται σε ένα δίκτυο για να προστατευτούν τα δεδομένα που διασχίζουν την απόσταση από αυτές μέχρι το σημείο εκπομπής. Σχεδιάστηκε για να εξασφαλίζει όλες τις διεργασίες που απαιτούνται σε ένα ασύρματο δίκτυο για να καλυφθούν οι ανάγκες της εμπιστευτικότητας (υποκλοπή δεδομένων), της ακεραιότητας (αλλοίωση δεδομένων) και της αυθεντικοποίησης (πιστοποίηση ταυτότητας χρηστών). Επίσης προσφέρει στα σημεία πρόσβασης ισχυρή αυθεντικοποίηση των συνδεόμενων σταθμών μέσω διαμοιραζόμενου κλειδιού.

Για την προστασία της κίνησης δεδομένων από επιθέσεις αποκρυπτογράφησης ωμής βίας (brute-force attacks), το WEP χρησιμοποιεί ένα σετ από τέσσερα προκαθορισμένα κλειδιά ή και εφαρμόζει ζεύγη κλειδιών, τα οποία ονομάζονται χαρτογραφημένα κλειδιά (mapped keys). Τα προκαθορισμένα κλειδιά διαμοιράζονται μεταξύ των συσκευών-σταθμών με ένα πακέτο υπηρεσίας και από τη στιγμή που θα πάρει μια συσκευή-σταθμός ένα κλειδί τότε μπορεί να επικοινωνήσει μέσω του WEP. Αντίστοιχα τα ζεύγη κλειδιών μοιράζονται μεταξύ δύο συσκευών-σταθμών δημιουργώντας μεταξύ τους μια χαρτογραφημένη σχέση κλειδιών (key mapping relationship).

Ωστόσο στην πράξη το WEP δεν ικανοποίησε στον απαιτούμενο βαθμό τις ιδιότητες της εμπιστευτικότητας, της ακεραιότητας και της αυθεντικοποίησης, καθώς:

- Ο RC4 αλγόριθμος κρυπτογράφησης που χρησιμοποιεί έχει αδυναμίες.
- Ο έλεγχος ακεραιότητας μέσω του αλγορίθμου CRC (Cyclic Redundancy Check) ήταν αναποτελεσματικός, αφού δεν προσέφερε σε ικανοποιητικό βαθμό εγγύηση των πακέτων που διαχειριζόταν.
- Η αυθεντικοποίηση δεν χρησιμοποιεί τους χρήστες αλλά τις διευθύνσεις υλικού MAC, οι οποίες είναι εύκολο να υποκλαπούν.
- Αν ένας εισβολέας ανακαλύψει το κλειδί WEP, τότε μπορεί να συνδεθεί με το δίκτυο ως ένας κανονικά πιστοποιημένος χρήστης.

9.6.1.2 Πρότυπο ασφαλείας WPA

Το πρότυπο WPA (Wi-Fi Protected Access) είναι ένα πρότυπο ασφαλείας του Wi-Fi που σχεδιάστηκε και έγινε διαθέσιμο το 2003 για να αντικαταστήσει το WEP, βελτιώνοντας τις αδυναμίες που υπήρχαν. Συγκεκριμένα:

- Βελτίωσε την κρυπτογράφηση μέσω του πρωτοκόλλου TKIP (Temporal Key Integrity Protocol), αυξάνοντας τα μεγέθη των κλειδιών από 40-bit ή 104-bit σε 128-bit και μετατρέποντας τα από μόνιμα για κάθε σύνδεση σε δυναμικά για κάθε πακέτο.
- Βελτίωσε το βαθμό ακεραιότητας των δεδομένων με τη χρήση του αλγόριθμου Michael για τον έλεγχο της ακεραιότητας των πακέτων.
- Η αυθεντικοποίηση του χρήση έγινε μέσω του πρωτοκόλλου EAP (Extensible Authentication Protocol). Το ΕΑΠ είναι χτισμένο σε ένα πιο ασφαλές σύστημα κρυπτογράφησης δημοσίου κλειδιού που εξασφαλίζει πρόσβαση στο δίκτυο μόνο τους πιστοποιημένους χρήστες.

Το πρότυπο αυτό αποτελεί έναν ενδιάμεσο σταθμό μεταξύ του WEP και του προτύπου ασφαλείας IEEE 802.11i ή αλλιώς γνωστό ως WPA2.

9.6.1.3 Πρότυπο ασφαλείας WPA2

Το πρότυπο **WPA2** (Wi-Fi Protected Access II) ή αλλιώς **IEEE 802.11i** έγινε διαθέσιμο το 2004 και είναι στην ουσία το ολοκληρωμένο πρότυπο WPA. Το WPA2 χρησιμοποιεί επιπλέον για την κρυπτογράφηση τους αλγόριθμους **CCMP** (CCM Mode Protocol) και **AES** (Advanced Encryption Standard) που ενισχύουν ακόμα περισσότερο την ασφάλειά του, υπερκεράζοντας τις αδυναμίες που διαπιστώθηκαν στον αλγόριθμο Michael. Σήμερα είναι πλέον υποχρεωτική η υποστήριξή του από τις συσκευές που φέρουν το λογότυπο του προτύπου Wi-Fi.

Υπάρχουν δύο τύποι του προτύπου WPA2:

- Το προσωπικό WPA2 (WPA2-Personal) ή αλλιώς WPA2-PSK.
- Το επιχειρησιακό WPA2 (WPA2-Enterprise), που πιστοποιεί τους δικτυακούς χρήστες μέσω ενός επιχειρησιακού διακομιστή αυθεντικοποίησης, όπως ο RADIUS Server.

Το **προσωπικό WPA2,** προστατεύει από τη μη εξουσιοδοτημένη χρήση χρησιμοποιώντας ένα προκαθορισμένο κλειδί (Pre-Shared Key, PSK), μήκους από 8 ως 63 χαρακτήρες. Χρησιμοποιεί το πρωτόκολλο TKIP (Temporal Key Integrity Protocol) και συνδυάζει το συνθηματικό και το δικτυακό όνομα SSID (Service Set Identifier ή Network Name), ώστε να δημιουργήσει ένα μοναδικό κλειδί κρυπτογράφησης.

Το SSID (Service Set Identifier ή Network Name) είναι το όνομα του ασύρματου τοπικού δικτύου (WLAN). Αποτελείται από μια σειρά από αλφαριθμητικούς χαρακτήρες με μέγιστο μήκος τους 32 χαρακτήρες. Όλες οι ασύρματες συσκευές σε ένα WLAN πρέπει να χρησιμοποιούν το ίδιο SSID για να μπορούν να επικοινωνήσουν μεταξύ τους.

Το **επιχειρησιακό WPA2,** που πιστοποιεί τους δικτυακούς χρήστες μέσω ενός επιχειρησιακού διακομιστή αυθεντικοποίησης, όπως ο RADIUS Server. Πιστοποιεί τους μεμονωμένους χρήστες με τη χρήση *όνομα χρήστη* και *συνθηματικού* και δίνει και κάθε συνδέει ένα μοναδικό κλειδί κρυπτογράφησης, το οποίο δεν γνωρίζει ο χρήστης

9.6.2 Χρήση Διακομιστή Radius (Radius Server)

Στα εταιρικά περιβάλλοντα η προστασία που προσφέρεται από το WPA/WPA2 δεν είναι επαρκής. Είναι χαρακτηριστικό ότι όλοι οι χρήστες που συνδέονται σε ένα ασύρματο δίκτυο με τέτοιου τύπο ασφάλεια χρησιμοποιούν το ίδιο κλειδί. Αυτή η προσέγγιση έχει σημαντικά μειονεκτήματα:

- Αυξάνει την πιθανότητα υποκλοπής του κλειδιού και χρήσης του από μη εξουσιοδοτημένα πρόσωπα.
- Στην περίπτωση που συμβεί κάτι τέτοιο θα πρέπει να γίνει αλλαγή του κλειδιού σε όλες τις συσκευές της ασύρματης υποδομής (δρομολογητές, σημεία πρόσβασης, επαναλήπτες), αλλά και σε όλες τις συσκευές των χρηστών που συνδέονται στο ασύρματο δίκτυο (υπολογιστές, κινητά τηλέφωνα, Tablets, εκτυπωτές κ.α.)
- Μη εξουσιοδοτημένοι χρήστες που μπορεί να υποκλέψουν το κλειδί, αλλά και οι κανονικοί χρήστες του ασύρματου δικτύου μπορούν να υποκλέψουν τη δικτυακή δραστηριότητα (με χρήση λογισμικού συλλογής πακέτων), αφού όλοι χρησιμοποιούν το ίδιο κλειδί για κρυπτογράφηση και αποκρυπτογράφηση.

Ενώ λοιπόν αυτό το σχήμα μπορεί να είναι αποδεκτό για προσωπική/οικιακή χρήση, στα εταιρικά περιβάλλοντα, αλλά και σε οποιαδήποτε περίπτωση η ασφάλεια είναι ο πιο σημαντικός παράγοντας, χρειάζεται μια μέθοδος με την οποία να μπορεί να γίνει πιστοποίηση του κάθε χρήστη ξεχωριστά, καθώς και ανεξάρτητη κρυπτογράφηση των μεταδιδόμενων πακέτων του κάθε χρήστη.

Ένας διακομιστής RADIUS διαχειρίζεται την πρόσβαση στα δίκτυα. Το όνομα RADIUS προκύπτει από τα αρχικά των λέξεων "Remote Authentication Dial-in User Service" και προέρχεται από την εποχή που οι χρήστες συνδέονταν στα εταιρικά συστήματα μέσω τηλεφωνικών κλήσεων. Από τότε βέβαια έχει υποστεί πολλές βελτιώσεις και σήμερα και έχει κερδίσει ευρεία υποστήριξη ανάμεσα ακόμα και στους παρόχους υπηρεσιών (ISPs).

Ένας RADIUS Server επιτελεί τρεις βασικές λειτουργίες:

- **Πιστοποίηση (Authentication):** Είναι η διαδικασία με την οποία καθορίζεται ποιος έχει πρόσβαση σε ένα δίκτυο. Συνήθως γίνεται με χρήση μιας βάσης δεδομένων που αποτελείται από ονόματα χρηστών (usernames) και συνθηματικά (passwords) στο διακομιστή πρόσβασης, υπάρχουν όμως και πιο εξελιγμένα συστήματα. Ωστόσο το γεγονός ότι η ταυτότητα κάποιου χρήστη πιστοποιήθηκε δε σημαίνει ότι αυτός έχει αποκτήσει πρόσβαση σε όλες τις υπηρεσίες του δικτύου—είναι πιθανό να του ζητηθεί εκ νέου κάποιος κωδικός αν θελήσει να κάνει χρήση κάποιας συγκεκριμένης υπηρεσίας.
- **Εξουσιοδότηση (Authorization):** Πρόκειται για την ικανότητα του περιορισμού των δικτυακών υπηρεσιών σε διαφορετικούς χρήστες βάση μιας δυναμικά εφαρμοζόμενης λίστας πρόσβασης (access list), που μερικές φορές αναφέρεται και ως "προφίλ χρήστη" και που βασίζεται στο συνδυασμό όνομα χρήστη/συνθηματικού. Το χαρακτηριστικό αυτό επιτρέπει στο διαχειριστή του δικτύου να επιτρέπει ή να απαγορεύει την πρόσβαση σε υπηρεσίες ανάλογα π.χ. με την τοποθεσία που βρίσκεται ο χρήστης ή με τον τρόπο με τον οποίο έχει συνδεθεί.
- **Κοστολόγηση (Accounting):** Ο διακομιστής παρακολουθεί και καταγράφει τη δραστηριότητα των χρηστών ώστε αυτοί να μπορούν π.χ. να χρεωθούν για το χρόνο που χρησιμοποίησαν κάποια υπηρεσία ή τον όγκο δεδομένων που διακίνησαν.

Λόγω ακριβώς των Αγγλικών λέξεων που περιγράφουν τις βασικές λειτουργίες των RADIUS Server, πολλές φορές αυτοί ονομάζονται και AAA Server. Αξίζει να τονισθεί ότι οι RADIUS Server δεν χρησιμοποιούνται μόνο σε συνδυασμό με ασύρματα δίκτυα, αλλά οπουδήποτε κρίνονται απαραίτητες οι λειτουργίες που προσφέρουν.

Ερωτήσεις Ανακεφαλαίωσης

1. Τι είναι ένα ασύρματο δίκτυο;
2. Ποια είναι τα βασικά πλεονεκτήματα της ασύρματης δικτύωσης;
3. Ποια είναι τα βασικά μειονεκτήματα της ασύρματης δικτύωσης;
4. Ποιες είναι οι δύο βασικές τοπολογίες ασύρματων δικτύων;
5. Ποια είναι τα βασικά χαρακτηριστικά ενός ασύρματου ad hoc δικτύου;
6. Ποιες είναι οι τρεις ταξινομήσεις με βάση την εφαρμογή των ασύρματων ad hoc δικτύων;
7. Ποια είναι τα πλεονεκτήματα και ποια τα μειονεκτήματα των ασύρματων ad hoc δικτύων;
8. Ποια είναι τα βασικά χαρακτηριστικά ενός ασύρματου δικτύου υποδομής (Infrastructure);
9. Τι καλύπτει στη λειτουργία των ασύρματων δικτύων η οικογένεια πρωτοκόλλων IEEE 802.11;
10. Ποιες είναι οι βασικές διαφορές των προτύπων 802.11a, 802.11b, 802.11g, 802.11n;
11. Τι είναι το Wi-Fi;
12. Τι είναι ένα Ασύρματο Σημείο Πρόσβασης (Access Point, AP);
13. Τι είναι ένα hotspot ή ελεύθερο σημείο ασύρματης πρόσβασης;

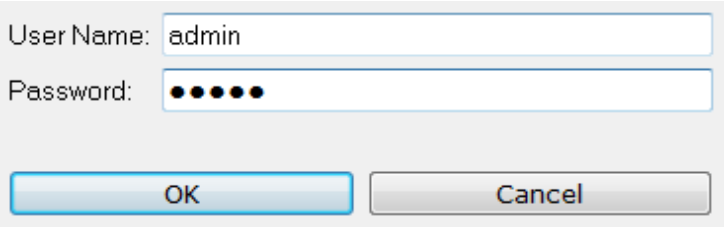
14. Σε τι διαφέρει ένα Ασύρματο Σημείο Πρόσβασης με ένα hotspot;
15. Τι είναι μια επέκταση ασύρματου σήματος (range extender ή range expander);
16. Τι είναι μια κεραία και ποιος είναι ο βασικός ρόλος της;
17. Ποιες είναι οι βασικές αρχές εγκατάστασης ενός ασύρματου δικτύου;
18. Τι είναι η κινητικότητα;
19. Τι είναι η περιαγωγή;
20. Ποιες ήταν οι αδυναμίες του προτύπου ασφαλείας WEP;
21. Τι βελτίωσε το πρότυπο ασφαλείας WPA σε σχέση με τον προκάτοχό του WEP;
22. Ποιες ήταν οι βελτιώσεις του WPA2 σε σχέση με το WPA;
23. Ποιοι είναι οι δύο τύποι του προτύπου ασφαλείας WPA2;
24. Ποιες είναι οι βασικές λειτουργίες που επιτελεί ο διακομιστής RADIUS;

Ασκήσεις

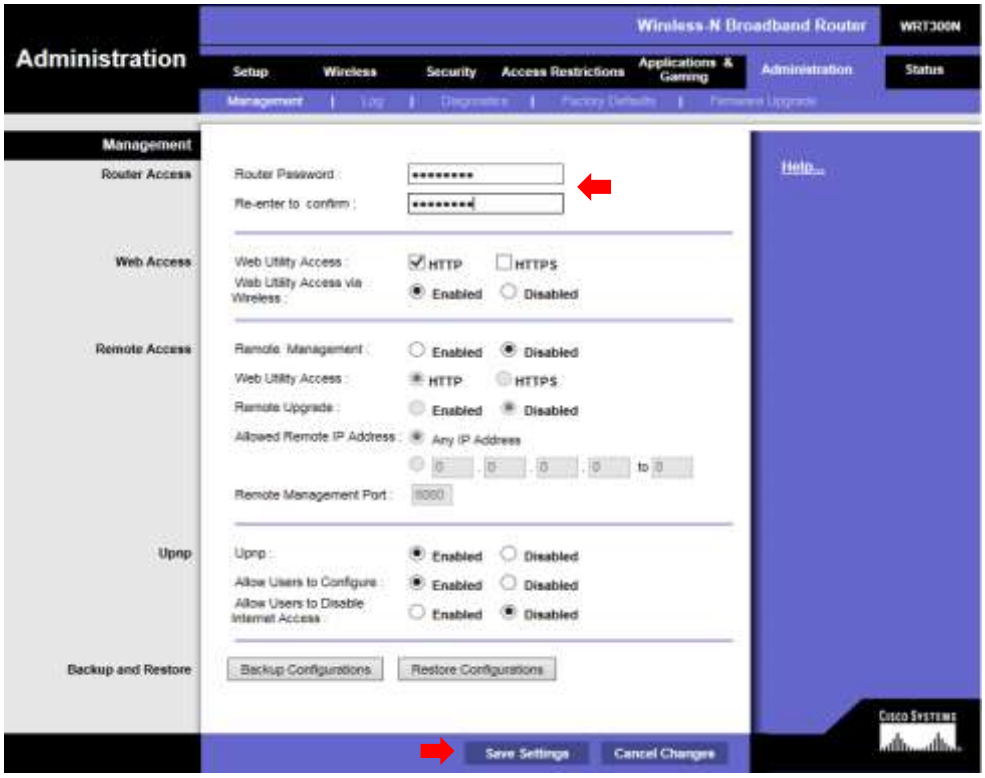
1η Άσκηση (Σε εργαστηριακό περιβάλλον)

Στην άσκηση αυτή θα διαμορφώσετε μία συσκευή πολλαπλών λειτουργιών (router – switch – wireless) για σύνδεση ασύρματων συσκευών σε ελεύθερο δίκτυο wi-fi.

1. Από έναν υπολογιστή που είναι συνδεδεμένος ενσύρματα στο τοπικό σας δίκτυο ανοίξτε έναν browser και δώστε τη διεύθυνση 192.168.1.1
2. Θα σας ζητηθεί να δώσετε όνομα χρήστη και κωδικό για σύνδεση στο μενού της συσκευής. Δώστε και στα δύο πεδία τη λέξη «admin». Θα εμφανισθεί η αρχική σελίδα της εφαρμογής ρύθμισης παραμέτρων της συσκευής.



3. Το πρώτο πράγμα που πρέπει να γίνει είναι η αλλαγή του κωδικού με τον οποίο γίνεται η σύνδεση. Πατήστε στην καρτέλα «Administration» και αλλάξτε τον κωδικό στα δύο πρώτα πεδία σε κάτι άλλο, π.χ. password. Πατήστε [Save Changes] για να αποθηκευθούν οι αλλαγές.



4. Μεταβείτε στην καρτέλα Wireless → Basic Wireless Settings και αλλάξτε το όνομα του δικτύου (SSID) σε MyWirelessNet. Πατήστε [Save Changes|.

5. Από έναν υπολογιστή που διαθέτει κάρτα ασύρματου δικτύου ή από μία άλλη συσκευή (π.χ. Smartphone ή Tablet) δοκιμάστε να συνδεθείτε με το ασύρματο δίκτυο που δημιουργήσατε.
6. Από τη γραμμή εντολών (για υπολογιστή) ή από αντίστοιχα εργαλεία για άλλες συσκευές δώστε την εντολή με την οποία θα βρείτε την IP διεύθυνση της ασύρματης σύνδεσης. Καταγράψτε την εντολή που δώσατε και το αποτέλεσμα που πήρατε.
7. Από τη γραμμή εντολών (για υπολογιστή) ή από αντίστοιχα εργαλεία για άλλες συσκευές δώστε την εντολή με την οποία θα επιβεβαιώσατε ότι υπάρχει επικοινωνία με τη συσκευή πολλαπλών λειτουργιών. Σημειώστε την εντολή που δώσατε, καθώς και το χρονικό διάστημα που χρειάστηκε για να πάρετε απάντηση.
8. Ποιοι οι κίνδυνοι όταν συνδέεστε σε ένα ασύρματο δίκτυο που δεν έχει ασφάλεια;

2η Άσκηση (Σε εργαστηριακό περιβάλλον)

Ένα ασύρματο δίκτυο χωρίς ασφάλεια είναι εκτεθειμένο σε υποκλοπή δεδομένων, καθώς οι πληροφορίες μεταδίδονται χωρίς καμία απολύτως κωδικοποίηση και μπορεί ο οποιοσδήποτε να τις διαβάσει με ένα πρόγραμμα συλλογής πακέτων. Στην άσκηση αυτή θα υλοποιήσετε ένα σχήμα ασφάλειας στο ασύρματο σημείο πρόσβασης έτσι ώστε οι πληροφορίες να μεταδίδονται κωδικοποιημένες.

1. Από έναν υπολογιστή που είναι συνδεδεμένος ενσύρματα στο τοπικό σας δίκτυο ανοίξτε έναν browser και δώστε τη διεύθυνση 192.168.1.1
2. Θα σας ζητηθεί να δώσετε όνομα χρήστη και κωδικό για σύνδεση στο μενού της συσκευής. Δώστε σαν όνομα χρήστη το admin και τον κωδικό που ισχύει.
3. Μεταβείτε στην καρτέλα Wireless → Wireless Security.
4. Ανοίξτε τη λίστα και ανατρέχοντας στη θεωρία, στη βοήθεια που είναι διαθέσιμη από το Setup του Router, αλλά και στο Διαδίκτυο συμπληρώστε τον ακόλουθο πίνακα (με ✓ ή x):

Είδος Ασφάλειας	Προορίζεται για προσωπική χρήση	Προορίζεται για εταιρική χρήση
WEP		
WPA Personal		
WPA2 Personal		
WPA Enterprise		
WPA2 Enterprise		
RADIUS		

5. Από τα είδη ασφάλειας που προορίζονται για προσωπική χρήση, ποιο είναι αυτό που σήμερα θεωρείται πιο ασφαλές;
6. Επιλέξτε από τον κατάλογο την ασφάλεια WPA2 Personal. Χρησιμοποιείστε σαν κρυπτογράφηση τον αλγόριθμο AES και δώστε έναν κωδικό για τιμή του κλειδιού (Pre-Shared Key ή PSK). Ο κωδικός πρέπει να ακολουθεί τους κανόνες για τη δημιουργία ισχυρών κωδικών, αλλά εδώ για ευκολία δώστε τη λέξη password. Πατήστε [Save Changes] για να αποθηκευτούν οι αλλαγές.

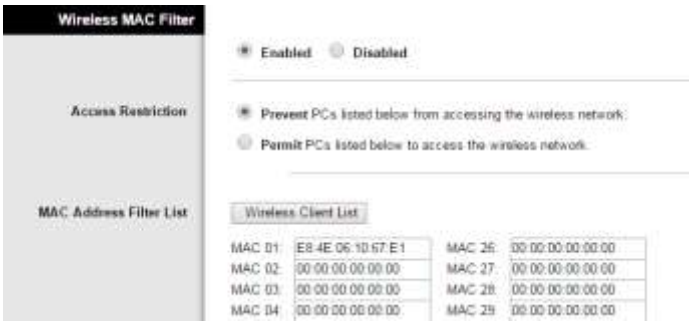
7. Δοκιμάστε πάλι να συνδεθείτε με το ασύρματο δίκτυο. Τι θα σας ζητηθεί πριν να αποκτήσετε πρόσβαση;

3η Άσκηση (Σε εργαστηριακό περιβάλλον)

Στην άσκηση αυτή θα αυξήσετε την ασφάλεια του ασύρματου δικτύου σας με την επιβολή περιορισμών στις φυσικές (MAC) διευθύνσεις των συσκευών που μπορούν να συνδεθούν στο ασύρματο δίκτυο. Οι περισσότεροι δρομολογητές έχουν συνήθως δύο επιλογές:

- Να επιτρέπουν τη σύνδεση συσκευών με οποιαδήποτε MAC διεύθυνση, <u>εκτός</u> από αυτές που περιλαμβάνονται σε μια συγκεκριμένη λίστα,
- Να επιτρέπουν <u>μόνο</u> τη σύνδεση συσκευών με τις διευθύνσεις MAC που περιλαμβάνονται σε μια λίστα.

1. Βρείτε και σημειώστε τη MAC διεύθυνση της συσκευής με την οποία συνδέεστε στο ασύρματο δίκτυο.
2. Από έναν υπολογιστή που είναι συνδεδεμένος ενσύρματα στο τοπικό σας δίκτυο ανοίξτε έναν browser και δώστε τη διεύθυνση 192.168.1.1
3. Θα σας ζητηθεί να δώσετε όνομα χρήστη και κωδικό για σύνδεση στο μενού της συσκευής. Δώστε σαν όνομα χρήστη το admin και τον κωδικό που ισχύει.
4. Μεταβείτε στην καρτέλα Wireless → Wireless MAC Filter.
5. Πατήστε στο στρογγυλό πλήκτρο [Enabled]
6. Βεβαιωθείτε ότι είναι ενεργή η επιλογή «Prevent PCs listed below from accessing the wireless network». Σε ποια από τις περιπτώσεις (α) ή (β) που αναφέρθηκαν παραπάνω αντιστοιχεί αυτή η επιλογή;
7. Στην πρώτη καταχώρηση της λίστας γράψτε την MAC διεύθυνση της ασύρματης σύνδεσης που βρήκατε στο βήμα 1. Προσέξτε να διατηρήσετε τους χαρακτήρες που διαχωρίζουν τα ψηφία της διεύθυνσης. Μην ξεχάσετε να πατήσετε [Save Settings].



8. Προσπαθήστε να συνδεθείτε με το ασύρματο δίκτυο. Τι παρατηρείτε; Τι μήνυμα εμφανίζεται;
9. Αλλάξτε την MAC διεύθυνση της ασύρματης σύνδεσης, αλλάζοντας π.χ. τα δύο τελευταία ψηφία της, όπως στην αντίστοιχη άσκηση του Κεφ 8. Γράψτε την τιμή της νέας MAC διεύθυνσης που θα δώσετε.
10. Μπορείτε τώρα να συνδεθείτε;
11. Συνδεθείτε ξανά στο router και απενεργοποιήστε το Wireless MAC Filter.
12. Αν ο στόχος σας είναι να αποτρέψετε με εξουσιοδοτημένους χρήστες να συνδεθούν σε ένα ασύρματο δίκτυο, ποια από τις μεθόδους (α) ή (β) θα επιλέγατε και γιατί;

4η Άσκηση (Σε εργαστηριακό περιβάλλον)

Πολλές φορές συμβαίνει στην περιοχή που θέλετε να εγκαταστήσετε ένα ασύρματο δίκτυο, να βρίσκονται πολλά άλλα ήδη σε λειτουργία. Στην άσκηση αυτή θα χρησιμοποιήσετε εργαλεία με τα οποία θα μπορέσετε να βρείτε την καλύτερη συχνότητα λειτουργίας για το δικό σας ασύρματο δίκτυο.

1. Ανάλογα με το λειτουργικό σύστημα που χρησιμοποιείτε ανοίξτε την εφαρμογή τύπου wi-fi Scanner, όπως φαίνεται στον παρακάτω πίνακα. Σε κάποιες από αυτές χρειάζεται να πατήσετε σε ένα κουμπί [Start] για να ξεκινήσει η ανίχνευση των συχνοτήτων.

Λειτουργικό Σύστημα	**Εφαρμογή**
Windows XP	InSSIDer 2.1
Windows 7, 8	Acrylic Wi-Fi Free
Linux	LinSSID
Android	Wifi Analyzer

2. Μετακινηθείτε στο σημείο που φαίνεται το γράφημα με τα δίκτυα που εκπέμπουν σε κάθε κανάλι στη συχνότητα των 2,4 GHz.

3. Εντοπίστε κάποια κανάλια που να είναι κατά προτίμηση κενά ή να έχουν όσο το δυνατόν λιγότερα και με χαμηλή ένταση σήματα WiFi.

4. Καταγράψτε τα αποτελέσματά σας. Σε ποιο κανάλι θα τοποθετούσατε το νέο ασύρματο δίκτυο;
5. Από έναν υπολογιστή που είναι συνδεδεμένος ενσύρματα στο τοπικό σας δίκτυο ανοίξτε έναν browser και δώστε τη διεύθυνση 192.168.1.1
6. Θα σας ζητηθεί να δώσετε όνομα χρήστη και κωδικό για σύνδεση στο μενού της συσκευής. Δώστε σαν όνομα χρήστη το admin και τον κωδικό που ισχύει.
7. Μεταβείτε στην καρτέλα Wireless → Basic Wireless Settings.

8. Ορίστε την τιμή του Network Mode ανάλογα με το είδος των καρτών δικτύου που θα συνδεθούν στο ασύρματό σας δίκτυο. Καταγράψτε την επιλογή σας.
9. Προσδιορίστε το κανάλι στο οποίο θα εκπέμπει το δίκτυό σας, σύμφωνα με τα ευρήματα του ερωτήματος 4. Σε δίκτυα 802.11n έχετε τη δυνατότητα να χρησιμοποιήσετε συνδυασμό δύο καναλιών (40 MHz) για να αυξήσετε την ταχύτητα του ασύρματου δικτύου. Καταγράψτε τις επιλογές σας:

   Radio Band: _____

   Standard Channel: _____

   Wide Channel: _____

Βιβλιογραφία

David Tse, P. V. (2005). *Fundamentals of Wireless Communication.* Cambridge : Cambridge University Press.

Gast, M. (2002). *802.11 Wireless Networks: The Definitive Guide.* O'Reilly.

Olenewa, J. L. (2012). *Guide to Wireless Communications, Third Edition.* Cengage Learning.

Oliviero, A., & Woodward, B. (2009). *Cabling - The Complete Guide to Network Wiring, 2nd Ed (Malestrom)* (2 ed.). Indianapolis: Wiley Publishing, Inc.

Waltenegus Dargie, C. P. (2010). *FUNDAMENTALS OF WIRELESS SENSOR NETWORKS.* Wiley.

Κεφάλαιο 10ο

Σύγχρονη καλωδίωση κτιρίου

Εισαγωγή

Η δομημένη καλωδίωση είναι μια εγκατάσταση που στοχεύει να καταστήσει ένα κτίριο λειτουργικό από άποψη εγκατάστασης υπηρεσιών, εφαρμογών και αυτοματισμών. Ο σωστός σχεδιασμός και η εγκατάστασή της καλωδίωσης και των δικτύων επιτρέπουν σε ένα κτίριο να είναι δικτυακά αυτόνομο και λειτουργικό, ενώ παράλληλα εξασφαλίζει τη δυνατότητα επέκτασής του με χαμηλό κόστος και ελάχιστες παρεμβάσεις.

Διδακτικοί Στόχοι

Με την ολοκλήρωση του 10ου κεφαλαίου οι μαθητές θα πρέπει να είναι σε θέση να:

- Περιγράφουν τα βασικά στοιχεία που περιλαμβάνει η τυπική τηλεπικοινωνιακή καλωδίωση ενός κτιρίου.
- Περιγράφουν τις βασικές αρχές σχεδιασμού καλωδίωσης κτιρίου.
- Σχεδιάζουν και να προτείνουν την καλύτερη επιλογή κτιριακής καλωδίωσης ανάλογα με δοσμένες προδιαγραφές.

Διδακτικές Ενότητες

10.1 Σύγχρονη τηλεπικοινωνιακή καλωδίωση κτιρίου.
10.2 Βασικές αρχές σχεδιασμού κτιριακής καλωδίωσης.

10.1 Σύγχρονη τηλεπικοινωνιακή καλωδίωση κτιρίου

Η καλωδίωση κτιρίου ή αλλιώς δομημένη καλωδίωση είναι μια εγκατάσταση, η οποία αποτελείται από ένα σύνολο εξοπλισμού, όπως καλώδια, πρίζες, κατανεμητές, ικριώματα, σχάρες οροφής κ.α. Μέσω αυτής πραγματοποιείται η μετάδοση φωνής/ήχου, η μεταφορά δεδομένων, η μεταφορά πολυμέσων και η διαχείριση άλλων εφαρμογών, όπως η εγκατάσταση συναγερμού, πυρανίχνευσης, κλιματισμός κ.α.

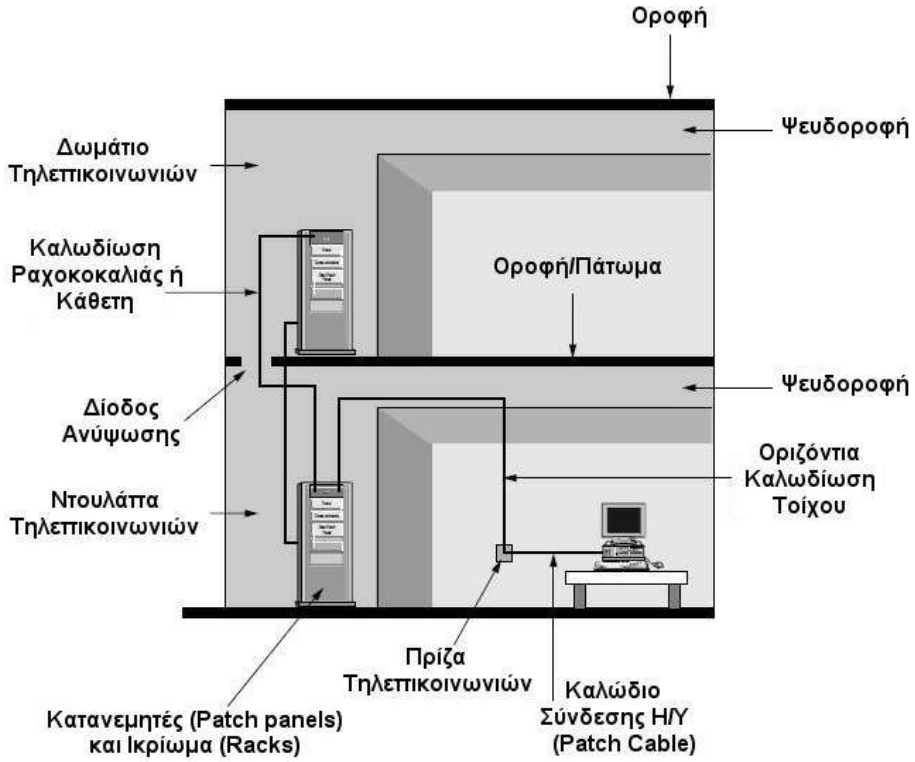
Η βασική καλωδίωση ενός κτιρίου περιλαμβάνει τα εξής στοιχεία:

- Το **ικρίωμα** τηλεπικοινωνιών (Telecommunications closet and racks) που βρίσκεται σε κάθε όροφο που απαιτεί οριζόντια κατανομή δικτύου.
- Την **κάθετη καλωδίωση** ή **καλωδίωση ραχοκοκαλιάς** (backbone), η οποία διατρέχει κάθετα το κτίριο και συνδέεται σε κάθε όροφο με τη ντουλάπα τηλεπικοινωνιών (Telecommunications closet) και τα ράφια τηλεπικοινωνιών (racks).
- Την **οριζόντια καλωδίωση** (horizontal) που διατρέχει οριζόντια έναν όροφο και συνδέει το ικρίωμα τηλεπικοινωνιών με τις πρίζες τηλεπικοινωνιών.

Οι βασικές αρχές και οι οδηγίες για την υλοποίηση της δομημένης καλωδίωσης κτιρίων καταγράφονται αναλυτικά υπό μορφή προτύπων, τα οποία εξασφαλίζουν την ποιότητα λειτουργίας των δικτύων. Τα πιο γνωστά πρότυπα δομημένης καλωδίωσης παγκοσμίως είναι τα:

- ISO/IEC DIS 11801 (Διεθνές) με την πιο πρόσφατη έκδοσή του2.2 το 2010.
- ANSI/TIA/EIA – 568 (Η.Π.Α.) με τις αναθεωρήσεις του 568-A, 568-B και 568-C.
- EN50173-1, EN50174-1, EN 50174-2 (Ευρώπη) που έχουν αναγνωρισμένη την τυποποίησή τους και από τον ελληνικό οργανισμό τυποποίησης (ΕΛΟΤ).

- IEEE-802.3-2012 που ορίζει τις προδιαγραφές για τη λειτουργία διαφόρων τύπων μετάδοσης δικτύων τεχνολογίας Ethernet.

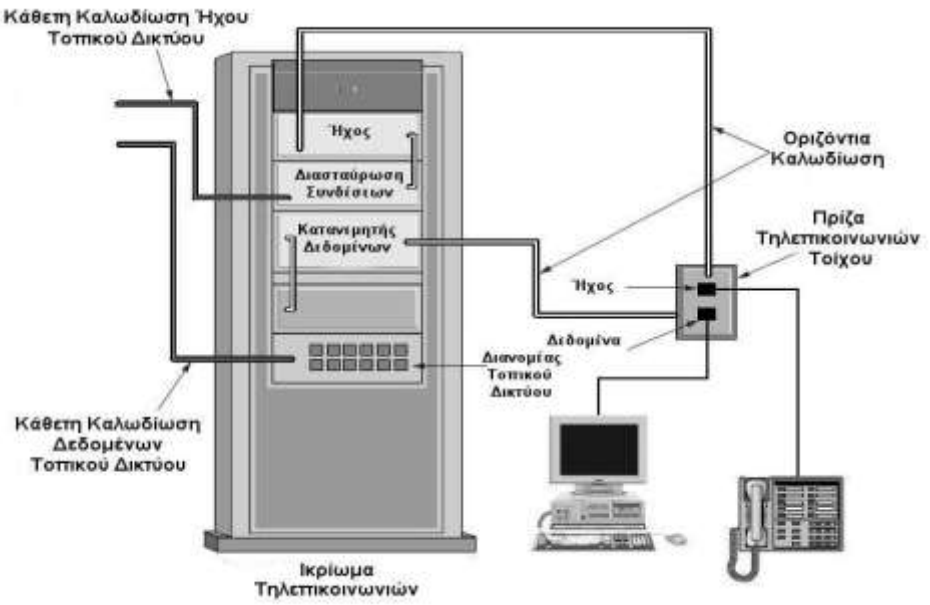


Εικόνα 10.1: Τυπικά στοιχεία που υπάρχουν σε ένα σύστημα δομημένης καλωδίωσης.

(Τροποποιημένη από πηγή: Oliviero, A., & Woodward, B., Cabling - The Complete Guide to Network Wiring)

Τα πρότυπα συνήθως καθορίζουν τις ελάχιστες απαιτήσεις μιας εγκατεστημένης δομημένης καλωδίωσης σε ένα κτίριο ή και σε περισσότερα συνδεδεμένα μεταξύ τους, μέχρι και την τηλεπικοινωνιακή έξοδο τους. Για παράδειγμα το πρότυπο ANSI/TIA/EIA-569-A αναφέρει ότι ένα σύστημα δομημένης καλωδίωσης πρέπει να αποτελείται από τα εξής:

- Εγκατάσταση εισόδου.
- Δωμάτιο εξοπλισμού.
- Καλωδίωση ραχοκοκαλιάς.
- Τηλεπικοινωνιακό ικρίωμα.
- Οριζόντια καλωδίωση.
- Τηλεπικοινωνιακές πρίζες.
- Κατανεμητής ορόφου.
- Κατανεμητής κτιρίου.
- Οδεύσεις οπτικών ινών.
- Οπτικοί κατανεμητές.
- Κατακόρυφη καλωδίωση.
- Γειώσεις.
- Υλικά χώρου εργασίας και δομημένης καλωδίωσης.



Εικόνα 10.2: Τυπικά στοιχεία που υπάρχουν στην οριζόντια καλωδίωση ενός ορόφου.

(Τροποποιημένη από πηγή: Oliviero, A., & Woodward, B., Cabling - The Complete Guide to Network Wiring)

10.2 Βασικές αρχές σχεδιασμού κτιριακής καλωδίωσης

Πριν την έναρξη του σχεδιασμού της καλωδίωση ενός κτιρίου είναι απαραίτητη η σωστή καταγραφή των αναγκών που θα πρέπει να καλυφθούν, ώστε το κτίριο να είναι λειτουργικό και η καλωδίωση που θα κατασκευαστεί να καλύπτει τις ανάγκες για τις οποίες σχεδιάστηκε. Εάν η καλωδίωση ενός κτιρίου δεν είναι σχεδιασμένη και εγκατεστημένη σύμφωνα με τις ανάλογες προδιαγραφές και τη χρήση την όποια προορίζεται να καλύψει, τότε το κόστος από τα προβλήματα που θα προκύψουν είναι πολλές φορές ανυπολόγιστα.

Παρακάτω αναφέρονται συνήθεις καλές πρακτικές που λαμβάνονται υπόψη κατά το **σχεδιασμό** της δομής του συστήματος της καλωδίωσης ενός κτιρίου:

- Είναι προτιμότερο να σχεδιάζεται ένα ενιαίο σύστημα καλωδίωσης που θα καλύπτει τις ανάγκες τόσο σε μετάδοση φωνής, όσο και δεδομένων ή άλλων εφαρμογών.
- Είναι προτιμότερο να χρησιμοποιούνται τα πιο διαδεδομένα πρότυπα δομικής καλωδίωσης και ποιοτικός εξοπλισμός. Εάν η καλωδίωση του κτιρίου είναι ποιοτική, η «ζωή» της μπορεί να ξεπεράσει τα 16 χρόνια.
- Επειδή οι ανάγκες δικτύωσης συνήθως αυξάνονται και τα δίκτυα τείνουν να γίνονται πιο περίπλοκα, σχεδιάζουμε με τέτοιο τρόπο, ώστε να προβλέψουμε και να καλύψουμε και πιθανές μελλοντικές ανάγκες. Πχ. Αφήνουμε επιπλέον πρίζες-απολήξεις σε έναν όροφο από τις τρέχουσες ανάγκες .
- Δίνουμε ιδιαίτερη προσοχή κατά την εγκατάσταση του εξοπλισμού, με συνεχείς ελέγχους.
- Είναι προτιμότερο να χρησιμοποιούνται υποδομές που υποστηρίζουν όσο το δυνατό μεγαλύτερες ταχύτητες δεδομένων, ακόμα και αν οι τρέχουσες προδιαγραφές δεν τις χρειάζονται. Γιατί οι ανάγκες των εφαρμογών για ταχύτητες μετάδοσης αυξάνονται συνεχώς.
- Καταγραφή και έντυπη τεκμηρίωση του συστήματος καλωδίωσης κατά τον έλεγχο της εγκατάστασης. Η αναφορά στα έγγραφα της τεκμηρίωσης οδηγεί σε ταχύτερο εντοπισμό της αιτίας μελλοντικών προβλημάτων που θα προκύψουν.

Μετά το σχεδιασμό της δομημένη καλωδίωσης, λαμβάνει χώρα η **εγκατάσταση** του δικτύου εντός του κτιρίου. Συγκεκριμένα γίνονται τα εξής:

- Η εγκατάσταση των καλωδίων μέσα σε ειδικές σχάρες από τους τηλεπικοινωνιακούς θαλάμους στις τηλεπικοινωνιακές εξόδους – χώρους εργασίας.
- Στήριξη των καλωδίων με μεταλλικούς αγωγούς ή στηρίγματα.
- Ο τερματισμός των καλωδίων, η απογύμνωσή τους από το μονωτικό υλικό και η σύνδεση τους στις κατάλληλες πρίζες-απολήξεις, ανάλογα με τη χρήση του καλωδίου.
- Τοποθέτηση μεταλλικών ικριωμάτων για την εγκατάσταση των τηλεπικοινωνιακών συσκευών, όπως δρομολογητές, διανομείς, κατανεμητές κτλ.
- Σύνδεση των καλωδίων στον κατανεμητή και στις άλλες δικτυακές συσκευές, ανάλογα με το σχεδιασμό του δικτύου.
- Σήμανση των καλωδίων με ευανάγνωστες ετικέτες για καλύτερη διαχείριση της καλωδίωσης από τους διαχειριστές του δικτύου.

Επίσης άλλες **συμβουλές** που καλό είναι να ακολουθούνται **κατά την υλοποίηση** μιας δομημένης καλωδίωσης κτιρίου είναι οι ακόλουθες:

- Να χρησιμοποιείται διαφορετικό καλώδιο για τη μετάδοση φωνής και διαφορετικό για τη μετάδοση δεδομένων.
- Να μην καταπονούνται τα καλώδια με συστροφές, τσακίσματα, τεντώματα.
- Να μην τοποθετούνται προεκτάσεις στα χρησιμοποιούμενα καλώδια.
- Να υπάρχει σωστή γείωση για τα θωρακισμένα καλώδια.
- Να μην τοποθετούνται τα καλώδια κοντά σε πηγές υψηλής θερμότητας, π.χ. σωληνώσεις θέρμανσης, γιατί αυξάνονται οι απώλειες στη μετάδοση δεδομένων.
- Να μην τοποθετούνται τα καλώδια κοντά σε καλώδια μεταφοράς ρεύματος υψηλής τάσης, γιατί αυξάνονται οι παρεμβολές στη μετάδοση δεδομένων.
- Να δίνεται ιδιαίτερη προσοχή στον τερματισμό των καλωδίων και στην απογύμνωσή τους από το μονωτικό υλικό.

Σε αυτό το σημείο πρέπει να τονίσουμε ότι όταν κατά την εγκατάσταση της δομημένης καλωδίωσης ενός κτιρίου **αποφασίζεται να μην τηρηθούν όλα τα πλαίσια που ορίζει το πρότυπο** που έχει επιλεγεί, π.χ. να περάσουν οι γραμμές των καλωδίων από σημείο που δεν προβλέπει το πρότυπο ή να χρησιμοποιήσουν υλικά που δεν έχουν την πιστοποίηση του προτύπου, τότε υπάρχει ο κίνδυνος το **δίκτυο να παρουσιάσει προβλήματα κατά την λειτουργία του**.

Επειδή σε ένα κτίριο εκτός από την καλωδίωση δικτύου Η/Υ μπορεί να υπάρχουν και άλλα δίκτυα, όπως το δίκτυο μεταφοράς ρεύματος, οι οδεύσεις του κλιματισμού κτλ., πρέπει να γίνει μια πλήρης και ολοκληρωμένη μελέτη του δικτύου δεδομένων που θα υλοποιηθεί. Κάθε πρότυπο είναι σχεδιασμένο με τέτοιο τρόπο, ώστε να καλύπτει όλες τις πιθανές προβληματικές καταστάσεις που μπορεί να δημιουργηθούν και επομένως, αν δεν τηρηθεί σε όλες του τις προεκτάσεις, δεν μπορεί να εξασφαλιστεί η αποτελεσματικότητα του δικτύου που θα κατασκευαστεί.

Ερωτήσεις Ανακεφαλαίωσης

1. Ποια είναι τα βασικά στοιχεία από τα οποία αποτελείται η δομημένη καλωδίωση ενός κτιρίου;
2. Ποια είναι τα πιο γνωστά πρότυπα δομημένης καλωδίωσης κτιρίων παγκοσμίως;
3. Ποιες είναι οι συνήθεις καλές πρακτικές που λαμβάνονται υπόψη κατά το σχεδιασμό του συστήματος καλωδίωσης ενός κτιρίου;
4. Ποια είναι τα βασικά στάδια υλοποίησης της καλωδίωσης ενός κτιρίου;

5. Τι πρέπει να προσέχουμε κατά την τοποθέτηση των καλωδίων;
6. Τι μπορεί να συμβεί σε ένα δίκτυο, αν κατά την κατασκευή της δομημένης καλωδίωσης του, δεν τηρηθούν όλα τα πλαίσια που ορίζει το πρότυπο που έχει επιλεγεί;

Ασκήσεις

Άσκηση 1η

Εντοπίστε στο Διαδίκτυο τα πιο διαδεδομένα πρότυπα δομημένης καλωδίωση που υπάρχουν παγκοσμίως. Στη συνέχεια απαντήστε στα ακόλουθα ερωτήματα:

1. Ποια είναι τα βασικά χαρακτηριστικά τους;
2. Τι περιλαμβάνουν και ποιες είναι οι υποδιαιρέσεις τους (αν υπάρχουν);
3. Ποια είναι τα κοινά σημεία που έχουν;
4. Ποιες είναι οι βασικές διαφορές τους;

Άσκηση 2η

Αν υποθέσουμε ότι σχεδιάζουμε ένα εργαστήριο Η/Υ, στο οποίο απαιτείται να εγκατασταθεί δομημένη καλωδίωση για δημιουργία δικτύου υπολογιστών.

1. Αναζητήστε τις πληροφορίες που χρειάζεστε και σχετίζονται με τη **σχεδίαση** της δομημένης καλωδίωσης:
   - στο βιβλίο του μαθήματος Υλικό και Δίκτυα Υπολογιστών της Β' Λυκείου ΕΠΑΛ
   - στις σημειώσεις του μαθήματος Δίκτυα Υπολογιστών της Γ' Λυκείου ΕΠΑΛ.
   - στο Διαδίκτυο.
2. Χωριστείτε σε ομάδες εργασίας και κάθε ομάδα ας αναλάβει κάποιες από τις παρακάτω αριθμημένες εργασίες.

   Εργασίες Σχεδιασμού Οριζόντιας Δομημένης Καλωδίωσης:

   i. Να βρείτε την κατάλληλη θέση του ικριώματος για την τοποθέτηση των συσκευών δικτύωσης (router, switch, hubs).
   ii. Να σχεδιάσετε την όδευση των καλωδίων που θα συνδέσουν τους σταθμούς εργασίας με το switch μέσα στο ικρίωμα. Προσοχή να δοθεί στην αισθητική του χώρου, έτσι ώστε τυχόν μελλοντικές επεμβάσεις να υλοποιούνται εύκολα.
   iii. Να επιλέξετε τον κατάλληλο τύπο καλωδίου για την υλοποίηση της διασύνδεσης κάθε σταθμού εργασίας με το switch.
   iv. Να επιλέξετε την κατάλληλη απόληξη (πρίζα) για κάθε σταθμό εργασίας.
   v. Να αποτυπωθούν τα παραπάνω σε ένα σχέδιο που θα αποτελεί σημείο αναφοράς.

Για την εκτέλεση της άσκησης, κάθε ομάδα πρέπει να:

- Μελετήσει το χώρο.
- Καταγράψει τις προτάσεις της.
- Δικαιολογήσει την επιλογής της.
- Παρουσιάσει το αποτέλεσμα της εργασίας της στην ολομέλεια της τάξης σας.

Άσκηση 3η

Αν υποθέσουμε ότι αποφασίζουμε να υλοποιήσουμε το σχέδιο δομημένης καλωδίωσης στο νέο εργαστήριο Η/Υ.

1. Αναζητήστε τις πληροφορίες που χρειάζεστε και σχετίζονται με την **υλοποίηση** της δομημένης καλωδίωσης:
   - Στο βιβλίο του μαθήματος Υλικό και Δίκτυα Υπολογιστών της Β' Λυκείου ΕΠΑΛ

- Στις σημειώσεις του μαθήματος Δίκτυα Υπολογιστών της Γ' Λυκείου ΕΠΑΛ.
- Στο Διαδίκτυο.

2. Χωριστείτε σε ομάδες εργασίας και κάθε ομάδα ας αναλάβει κάποιες από τις παρακάτω αριθμημένες εργασίες.

   Εργασίες Υλοποίησης Οριζόντιας Δομημένης Καλωδίωσης:

   i. Αφού γίνει η εγκατάσταση του ικριώματος, να γίνει ορθή τοποθέτηση των συσκευών δικτύωσης (router, switch, hubs).
   ii. Να εγκαταστήσετε τα καλώδια που επιλέξατε συνδέοντας τη μια άκρη στην αντίστοιχη θύρα του μεταγωγέα (switch) και κλείνοντας τα μέσα στο διάδρομο όδευσης.
   iii. Η άλλη άκρη του κάθε καλωδίου να συνδεθεί με την απόληξη (πρίζα).
   iv. Για τα βήματα 2 και 3, να εισάγετε αρίθμηση στα καλώδια για καλύτερο έλεγχο και εντοπισμό τυχόν λαθών, επισκευής τους ή και αντικατάστασης τους.
   v. Να γίνει έλεγχος μετά την ολοκλήρωση, ώστε κάθε πρίζα να λειτουργεί και να δίνει πρόσβαση στο δίκτυο.

3. Συζητήστε στην τάξη και αναλύστε το βαθμό δυσκολίας που αντιμετωπίσατε σε κάθε βήμα υλοποίησης της οριζόντιας καλωδίωσης.

Βιβλιογραφία

Δημητρόπουλος Β., Βαρβατσουλάκης Μ., Κουτουλάκος Χ., Γεωργάκης Θ., (2001), *Ειδικές Ηλεκτρικές Εγκαταστάσεις, Τεύχος Α*, ΥΠΕΠΘ, Παιδαγωγικό Ινστοτούτο.

Groth, D., McBee, J., & Barnett, D. (2001). *Cabling: The Complete Guide to Network Wiring* (2nd ed.). Alameda: SYBEX Inc.

ISO/IEC 11801, *Information technology ‑ Generic cabling for customer premises*, Reference number ISO/IEC 11801:2002(E), Second edition 2002-09

Oliviero, A., & Woodward, B. (2009). *Cabling - The Complete Guide to Network Wiring*, 2nd Ed (Malestrom) (2 ed.). Indianapolis: Wiley Publishing, Inc.

Κεφάλαιο 11ο

Δικτύωση Powerline

Εισαγωγή

Η τεχνολογία της Powerline δικτύωσης χρησιμοποιεί το ήδη υπάρχον δίκτυο διανομής ηλεκτρικού ρεύματος σε ένα κτίριο ώστε να μεταφέρει δεδομένα μέσω αυτού. Αποτελεί μια πρακτική λύση για την εγκαθίδρυση δικτύου σε κτίρια όπου δεν υπάρχει η δυνατότητα εγκατάστασης νέας καλωδίωσης. Η επιλογή της εγκατάστασής μιας Powerline εφαρμογής δικτύου εξαρτάται πάντα από τη μελέτη των πλεονεκτημάτων που μπορεί να προσφέρει σε αντιστάθμιση με τα μειονεκτήματα που μπορεί να υπάρχουν σε κάθε περίπτωση.

Διδακτικοί Στόχοι

Με την ολοκλήρωση του 11ου κεφαλαίου οι μαθητές θα πρέπει να είναι σε θέση να:

- Περιγράφουν τις βασικές αρχές της τεχνολογίας δικτύωσης Powerline.
- Απαριθμούν τις βασικές μονάδες υλικού που είναι απαραίτητες για την τεχνολογία αυτή.
- Αναφέρουν τα πλεονεκτήματα και τα μειονεκτήματα αυτής της τεχνολογίας
- Τοποθετούν το κατάλληλο υλικό και να υλοποιούν δικτύωση Powerline μέσα στο σχολικό εργαστήριο.

Διδακτικές Ενότητες

11.1 Χρήση υφιστάμενων συστημάτων καλωδίωσης για μεταφορά δεδομένων

Στην παρούσα ψηφιακή εποχή της τεχνολογίας των πληροφοριών, η ζήτηση για την αποστολή ψηφιακών δεδομένων, όπως φωνή, βίντεο και δεδομένων του Διαδικτύου, αυξάνεται συνεχώς. Η εγκατάσταση καλωδίων μεταφοράς δεδομένων για την ικανοποίηση αυτής της ανάγκης είναι μια ακριβή και χρονοβόρα διαδικασία. Για αυτό το λόγο στο πλαίσιο του περιβάλλοντος οικιακής δικτύωσης, ο όρος που έχει επικρατήσει και εφαρμόζεται, ονομάζεται “no new wires”, δηλαδή όχι νέα καλώδια. Δηλαδή, η χρήση τεχνολογιών που χρησιμοποιούν τα υφιστάμενα συστήματα καλωδίωσης για τη διανομή δεδομένων υψηλής ταχύτητας και βίντεο σε όλο το σπίτι ή σε ένα μικρό γραφείο.

Οι δύο κυρίαρχες τεχνολογίες μετάδοσης δεδομένων που υπακούν στον παραπάνω όρο της μη χρήσης νέων καλωδίων είναι η εκμετάλλευση της υφιστάμενης καλωδίωσης του συστήματος τηλεφωνικής γραμμής και του δικτύου της διανομής του ηλεκτρικού ρεύματος. Ενώ η πρώτη τεχνολογία είναι ιδιαίτερα διαδεδομένη και χρησιμοποιείται ευρέως από τους διανομείς υπηρεσιών Διαδικτύου, η τεχνολογία που χρησιμοποιεί το δίκτυο διανομής ρεύματος έχει αρχίσει και αυτή να κερδίζει έδαφος για οικιακή χρήση και ονομάζεται Powerline.

11.2 Τεχνολογία Δικτύωσης Powerline

11.2.1 Βασικά χαρακτηριστικά

Η τεχνολογία Powerline εκμεταλλεύεται το ήδη εγκατεστημένο δίκτυο διανομής ηλεκτρικού ρεύματος σε ένα σπίτι. Για αν κατανοήσουμε καλύτερα τον τρόπο λειτουργίας της τεχνολογίας αυτής πρέπει να μελετήσουμε τον τρόπο με τον οποίο είναι σχεδιασμένο το δίκτυο αυτό. Για τη διανομή του ηλεκτρικού ρεύματος στον τελικό καταναλωτή υπάρχουν τρία στάδια η παραγωγή, η μεταφορά, και η τοπική διανομή.

Η τοπική διανομή αστικού ηλεκτρικού ρεύματος είναι αυτή που παρουσιάζει τις ευκαιρίες για την παροχή νέων υπηρεσιών, εκτός από την παροχή ηλεκτρικής ενέργειας. Η υπάρχουσα υποδομή καλωδίωσης που βρίσκεται σε κάθε κτίριο ευνοεί και αυτή με τη σειρά της την παροχή ορισμένων υπηρεσιών. Οι διάφοροι τηλεπικοινωνιακοί φορείς, για παράδειγμα, ενδιαφέρονται για ένα αξιόπιστο τρόπο για να διαθέσουν το περιεχόμενο και τις υπηρεσίες τους στις διάφορες συσκευές μέσα στα σπίτια των πελατών τους. Έτσι, τα οικιακά δίκτυα καλωδίωσης ηλεκτρικού ρεύματος ή τηλεφωνίας, αποτελούν έναν τρόπο για να επιτευχθεί αυτό.

Στα συστήματα επικοινωνίας (Powerline Carrier - PLC), η γραμμή χρησιμοποιείται όχι μόνο για τη μεταφορά ενέργειας, αλλά επίσης ως μέσο για τη μεταφορά δεδομένων. Η δικτύωση PLC είναι μια αναδυόμενη τεχνολογία οικιακής δικτύωσης που επιτρέπει στους τελικούς χρήστες να χρησιμοποιήσουν ήδη υπάρχοντα συστήματα ηλεκτρικών καλωδιώσεων για τη σύνδεση οικιακών συσκευών μεταξύ τους αλλά και με το Διαδίκτυο. Ένα οικιακό δίκτυό, χρησιμοποιώντας την υψηλής ταχύτητας τεχνολογία PLC, είναι σε θέση να ελέγξει οτιδήποτε μπορεί να συνδεθεί σε μια οποιαδήποτε πρίζα εναλλασσόμενου ρεύματος. Αυτό περιλαμβάνει τα φώτα, την τηλεόραση, θερμοστάτες, συναγερμούς κ.α.

Αν και δεν υπάρχει ακόμα μια διεθνής προτυποποίηση για την τεχνολογία αυτή, το 2001 ο οργανισμός βιομηχανικών προτύπων HomePlug Powerline Alliance, μέλη του οποίου ήταν εταιρίες όπως η Cisco, η Motorola, η Intel κ.α, ολοκλήρωσε ένα σύνολο προδιαγραφών, το Homeplug 1.0, που υποστήριζε μετάδοση δεδομένων της τάξης των 14Mb/s.

11.2.2 Τρόπος λειτουργίας

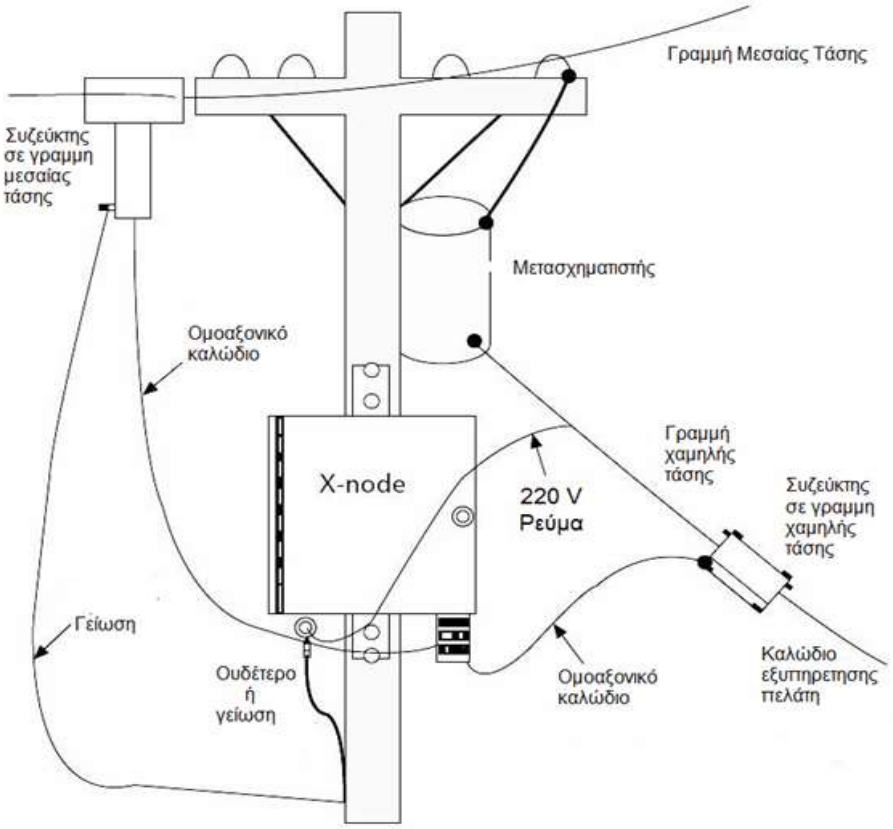
Τα συστήματα πρόσβασης Powerline χρησιμοποιούν τρεις συνιστώσες του δικτύου διανομής ηλεκτρικής ισχύος:

- Η πρώτη συνιστώσα είναι η **γραμμή μέσης τάσης**, που μεταφέρει συνήθως από 1.000 έως 40.000 Volt και μέσω των οποίων μεταφέρεται ρεύμα από έναν υποσταθμό σε μια κατοικημένη περιοχή.
- Η δεύτερη συνιστώσα είναι ο **μετασχηματιστής χαμηλής τάσης** που μετασχηματίζει την τάση στα 220 Volt που απαιτούνται για οικιακή χρήση.
- Η τρίτη συνιστώσα του υπάρχοντος συστήματος διανομής ηλεκτρικής ενέργειας είναι η **διανομή χαμηλής τάσης από το μετασχηματιστή σε ηλεκτρικές υποδοχές** μέσα στα κτίρια, και σε αυτήν συμπεριλαμβάνονται: το καλώδιο παροχής υπηρεσιών, ο πίνακας (panel) διακόπτη κυκλώματος και η εσωτερική καλωδίωση του κτιρίου.

Αντίστοιχα, η τεχνολογία πρόσβασης Powerline ή ευρυζωνικής πρόσβασης μέσω γραμμών ηλεκτρικής ισχύος (BPL πρόσβασης – Broadband over Powerline) είναι η υπεύθυνη για την αποστολή δεδομένων υψηλής ταχύτητας και φωνητικών σημάτων μέσω του δικτύου διανομής, από ένα σημείο όπου υπάρχει μια σύνδεση σε ένα δίκτυο τηλεπικοινωνιών. Αυτό το σημείο της σύνδεσης μπορεί να είναι σε έναν υποσταθμό ηλεκτρικής ενέργειας ή σε ένα ενδιάμεσο σημείο μεταξύ των υποσταθμών, ανάλογα με την τοπολογία του δικτύου. Κοντά

στο σημείο διανομής σε μια γειτονιά, εγκαθίσταται ένας συζεύκτης ή γέφυρα για να επιτρέψει τη μεταφορά ψηφιακών σημάτων υψηλής συχνότητας μέσω του διανομέα χαμηλής τάσης. Ο λόγος για τη χρήση ενός συζεύκτη ή γέφυρας είναι ότι η μετατροπή της μεσαίας τάσης (MV) σε χαμηλή (LV) που προορίζεται για τη μεταφορά σημάτων στα 60 HZ, δεν αποτελεί καλό αγωγό για ψηφιακά σήματα υψηλής συχνότητας.

Επίσης, είναι απαραίτητος ένας μετατροπέας X-Node, οποίος χρησιμοποιείται για τη μεταφορά σημάτων μεταξύ των MV και LV γραμμών και σαν επαναλήπτης (repeater) μεταξύ των MV γραμμών.



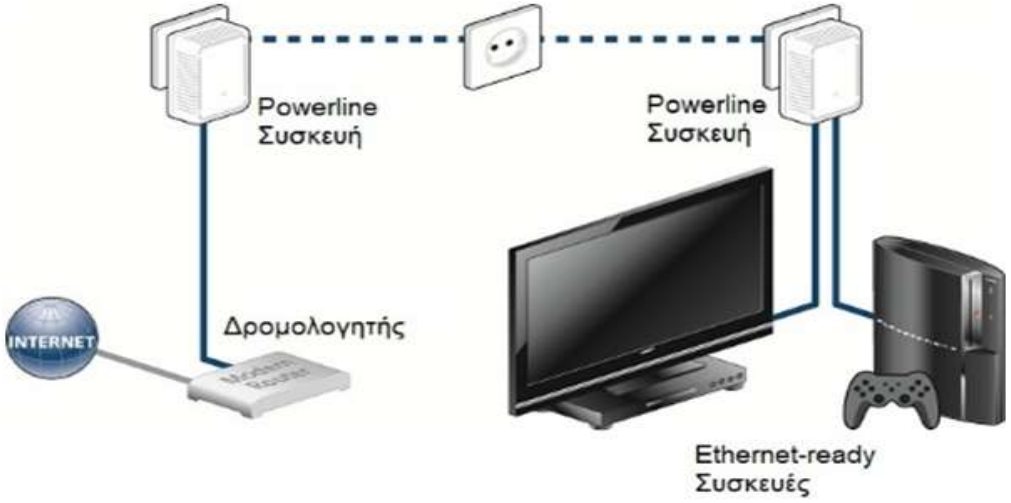
Σχήμα 11.1: Τρόπος εγκατάστασης τεχνολογίας Powerline

11.2.3 Χρήσεις σε τοπικό δίκτυο

Μια τυπική εφαρμογή Powerline δικτύωσης μέσα σε ένα σπίτι (home network) ή σε ένα μικρό γραφείο απαιτεί τουλάχιστον δυο προσαρμογείς Powerline. Ένας προσαρμογέας Powerline διαθέτει τουλάχιστον μια θύρα Ethernet που του επιτρέπει τη σύνδεση με οποιαδήποτε άλλη συσκευή Ethernet. Ο πρώτος προσαρμογέας είναι συνδεδεμένος σε ένα δρομολογητή, όπως οι τυπικοί δρομολογητές τεχνολογίας DSL, σε ένα υπάρχον ενσύρματο τοπικό δίκτυο, μέσω της θύρας δικτύου του. Ο δεύτερος προσαρμογέας θα συνδεθεί σε μια συσκευή Ethernet, όπως είναι ένας υπολογιστής, ένας εκτυπωτής δικτύου ή μια έξυπνη τηλεόραση.

Έτσι, όταν συνδέσουμε τις δύο Powerline συσκευές σε οποιοδήποτε από τις υποδοχές ηλεκτρικού ρεύματος μέσα στο σπίτι ή στο γραφείο θα υπάρχει δικτυακή σύνδεση μεταξύ τους, με αποτέλεσμα την επέκταση του οικιακού δικτύου, χωρίς την εγκατάσταση νέων καλωδίων. Επιπλέον, υπάρχουν συσκευές Powerline που διαθέτουν ενσωματωμένο σημείο πρόσβασης (access point), ώστε να επιτρέπουν τη δημιουργία ασύρματου τοπικού δικτύου.

Ανεξάρτητα από το αν υλοποιείται ενσύρματη ή ασύρματη Powerline δικτύωση, οι ταχύτητες που επιτυγχάνονται, σύμφωνα με τους κατασκευαστές αυτών των συσκευών κυμαίνονται από 200 Mbps μέχρι πάνω από 1000 Mbps.



Εικόνα 11.1: Τρόπος εγκατάστασης τεχνολογίας Powerline σε ένα σπίτι ή μικρό γραφείο

11.2.4 Πλεονεκτήματα και Μειονεκτήματα

Τα βασικότερο πλεονεκτήματα σε αυτή τη σύζευξη μεταξύ των τηλεπικοινωνιακών σημάτων με τα ηλεκτρικά σήματα είναι το χαμηλό κόστος και η ευκολία προσαρμογής και συντήρησής της. Επίσης, μια τέτοια σύζευξη δεν θα υποβαθμίσει τη συνολική αξιοπιστία του συστήματος διανομής ηλεκτρικού ρεύματος. Άλλα πλεονεκτήματα που ενισχύουν τη χρήση αυτής της τεχνολογίας είναι:

- Μια δικτύωση PLC εκμεταλλεύεται την αχρησιμοποίητη παραγωγική ικανότητα των καλωδίων τροφοδοσίας για τη μετάδοση δεδομένων πάνω από το υπάρχουσα καλωδίωση ηλεκτρικής ενέργειας.
- Η διαθεσιμότητα των πολλαπλών υποδοχών ρεύματος σε κάθε δωμάτιο. Έτσι εξαλείφεται η ανάγκη να γίνει επιπλέον καλωδίωση ή επανακαλωδίωση μέσα στο σπίτι.
- Η δυνατότητα διανομής ήχου, βίντεο, και άλλων υπηρεσιών σε πραγματικό χρόνο μαζί με τα δεδομένα, σε όλο το σπίτι.
- Η δυνατότητα μετάδοσης δεδομένων με ταχύτητες από 40Mbps έως 80 Mbps, και μελλοντικές ταχύτητες μετάδοσης της τάξης των 300 Mbps, γεγονός που καθιστά την προώθηση της τεχνολογίας επιτακτική.

Αντίθετα στα μειονεκτήματα της τεχνολογίας αυτής συγκαταλέγονται:

- Η σχετικά μεγάλη ποσότητα ηλεκτρικού θορύβου στις ηλεκτρικές γραμμές μεταφοράς ηλεκτρικής ενέργειας περιορίζει την πραγματική ταχύτητα μετάδοσης δεδομένων σε χαμηλότερες τιμές από τις ονομαστικές.
- Οι διάφορες πηγές παραγωγής θορύβου, όπως ηλεκτρικές σκούπες, ροοστάτες φώτων, ηλεκτρικοί λαμπτήρες, συσκευές κουζίνας και ηλεκτρικά τρυπάνια, που επηρεάζουν την απόδοση ενός PLC δικτύου.
- Τα πιστοποιημένα προϊόντα HomePlug έχουν ενσωματωμένη κρυπτογράφηση 56-bit DES, ωστόσο δεν είναι ενεργοποιημένη από προεπιλογή. Έτσι, τα κανάλια

επικοινωνίας μέσω Powerline δεν παρέχουν κατ' ανάγκη ένα ασφαλές μέσο μετάδοσης.

- Η παρουσία των διαφόρων στοιχείων (ηλεκτρικές συσκευές όπως ψυγείο, πλυντήριο κ.α) σε ένα δίκτυο Powerline που οδηγεί σε απώλεια δεδομένων είναι ένα σημαντικό ζήτημα στην Powerline δικτύωση.
- Σε σύγκριση με τον εξοπλισμό του δικτύου PSTN, οι συσκευές Powerline δικτύωσης είναι πιο δαπανηρές.
- Η έλλειψη τυποποίησης, καθώς ζητήματα κανονικότητας σε ορισμένες διεθνείς αγορές εμποδίζουν την ανάπτυξη παγκόσμιου προτύπου.

Ερωτήσεις Ανακεφαλαίωσης

1. Ποιες είναι οι τρεις συνιστώσες του δικτύου διανομής ηλεκτρικής ισχύος που χρησιμοποιεί η τεχνολογία Powerline;
2. Πώς ονομάζεται η τεχνολογία που είναι η υπεύθυνη για την αποστολή δεδομένων υψηλής ταχύτητας και φωνητικών σημάτων μέσω του δικτύου διανομής;
3. Ποιες μονάδες υλικού απαιτούνται για την υλοποίηση ενός δικτύου BPL πρόσβασης;
4. Ποιες μονάδες υλικού απαιτούνται για την υλοποίηση ενός τοπικού δικτύου τεχνολογίας Powerline;
5. Ποια είναι τα βασικά πλεονεκτήματα της τεχνολογίας Powerline;
6. Ποια είναι τα βασικά μειονεκτήματα της τεχνολογίας Powerline;

Ασκήσεις

Άσκηση 1η (Σε εργαστηριακό περιβάλλον)

Επίδειξη εφαρμογής Powerline δικτύωσης στο σχολικό εργαστήριο.

Παρακολουθήστε τα παρακάτω βήματα για τη σύνδεση δύο συσκευών με χρήση Powerline τεχνολογίας.

1. Τοποθέτηση μιας συσκευής δικτύωσης Powerline δίπλα στο δρομολογητή ή δίπλα σε μια επιτοίχια πρίζα Ethernet.
2. Σύνδεση της μιας άκρης ενός καλωδίου Ethernet στην πρίζα Ethernet στον τοίχο ή σε μια θύρα του δρομολογητή.
3. Σύνδεση της άλλης άκρης του καλωδίου Ethernet στη θύρα Ethernet της συσκευής Powerline.
4. Τοποθέτηση της 2ης συσκευής στο χώρο που δεν διαθέτει σύνδεση με το τοπικό δίκτυο ή το Διαδίκτυο.
5. Σύνδεση της μιας άκρης ενός καλωδίου Ethernet στη θύρα Ethernet της συσκευής που θα συνδεθεί στο Διαδίκτυο.
6. Σύνδεση της άλλης άκρης του καλωδίου Ethernet στη θύρα Ethernet της συσκευής Powerline.
7. Δοκιμή της σύνδεσης που μόλις δημιουργήθηκε.

Τι συμπεράσματα εξάγετε από τον τρόπο εφαρμογής της συγκεκριμένης τεχνολογίας σε σύγκριση με τους συνηθισμένους τρόπους σύνδεσης συσκευών με Ethernet καλώδιο;

Άσκηση 2η (Στην αίθουσα διδασκαλίας)

Χωριστείτε σε ομάδες εργασίας και συζητήστε ώστε να απαντήστε στα ακόλουθα ερωτήματα:

1. Ποιες ενέργειες θα τροποποιούσατε προκειμένου να συνδέσετε μέσω μιας Powerline συσκευής, περισσότερους σταθμούς εργασίας στο δίκτυο ή στο Διαδίκτυο;
2. Να διερευνήσετε τη δυνατότητα ασύρματης επέκτασης του δικτύου σας με χρήση των Powerline συσκευών.

Να παρουσιάσουν οι ομάδες τα αποτελέσματα της συζήτησής τους στην ολομέλεια της τάξης.

Βιβλιογραφία

Mainardi, E., & Bonfè, M. (2008). Powerline Communication in Home-Building Automation Systems. Στο R. a. Construction, *InTech Europe.*

MCMC. (2005). *GUIDELINES ON BROADBAND OVER POWER LINE COMMUNICATIONS.* Malaysian Communications and Multimedia Commission.

Mulroy, P., & Gilbert, I. (2011). COMPARISON OF COUPLING METHODS IN MV EQUIPMENT FOR POWERLINE COMMUNICATIONS. *21st International Conference on Electricity Distribution.* Frankfurt.

Ορολογία και Ακρωνύμια

Absolute Path	Απόλυτη διαδρομή
Access list	Λίστα πρόσβασης
Access Point, AP	Ασύρματο Σημείο Πρόσβασης
Accounting	Κόστος/κοστολόγηση
Ad-Hoc Wireless Networks	Ασύρματο δίκτυο αυτοοργανωμένο ή κατ' απαίτηση
Advanced Encryption Algorithm, AES	Αλγόριθμος συμμετρικής ή σύνθετης ή εξελιγμένης κρυπτογράφησης
Application layer	Επίπεδο Εφαρμογής
Association Process	Διαδικασία συσχετισμού
Asymmetric Cryptography	Κρυπτογράφηση ασύμμετρου κλειδιού
Attack	Επίθεση
Authentication	Αυθεντικοποίηση/πιστοποίηση ταυτότητας
Authorization	Εξουσιοδότηση
Backbone	Δίκτυο κορμού ή Κάθετη καλωδίωση ή καλωδίωση ραχοκοκαλιάς
Bandwidth	Εύρος ζώνης
Base Clock ή BCLK	Βασικό Ρολόι χρονισμού
Base station	Σταθμός βάσης
Bating	Χρήση δολώματος
Beam	Δέσμη
Benchmark program	Πρόγραμμα μέτρησης επιδόσεων
Bridge, SLI/Crossfire	Γέφυρα τεχνολογίας SLI ή Crossfire
Broadband/Wide band	Ευρεία ζώνη
Broadcast	Εκπομπή
Brute-force attacks	Επιθέσεις ωμής βίας ή εξαντλητική αναζήτηση κλειδιού
CAS (Column Access Strobe) latency	Χρόνος αδρανείας ανάμεσα στην αίτηση της Κ.Μ.Ε. για δεδομένα και στην αποστολή τους από τη μνήμη
Cell	Κυψέλη ή κυψελίδα
Certification Authorities CA	Αρχές Πιστοποίησης
Chiphertext	Κρυπτογράφημα
Chipset	Τσίπσετ ή Σύνολο ολοκληρωμένων κυκλωμάτων
Client	Πελάτης
Client-server	(Μοντέλο) πελάτη-εξυπηρετητή
Closet (Telecommunications)	Ικρίωμα τηλεπικοινωνιών
Cloud	Σύννεφο
Cluster	Συστοιχία
Common Internet File System, CIFS	Κοινό Διαδικτυακό σύστημα αρχείων
Computer cluster	Συστοιχία υπολογιστών
Confidentiality	Εμπιστευτικότητα
Configuration	Παραμετροποίηση
CPU frequency	Συχνότητα χρονισμού Κ.Μ.Ε.
CPU multiplier, CPU Ratio	Ρόλοι-πολλαπλασιαστής Κ.Μ.Ε.
CPU Temp (Temperature)	Θερμοκρασία Κεντρικής Μονάδας Επεξεργασίας
CPU Vcore Voltage	Τάση ηλεκτρικού ρεύματος Κ.Μ.Ε.

Crossfire	Τεχνολογία διπλών καρτών γραφικών της AMD
Cryptography	Κρυπτογράφηση
Cyclic Redundancy Check, CRC	Έλεγχος κυκλικού πλεονασμού (αλγόριθμος)
Data frame	Πλαίσιο δεδομένων
Denial of Service, DoS	Άρνηση Εξυπηρέτησης
Digest	Σύνοψη
Direct Attached Storage, DAS	Απ' ευθείας ή άμεση σύνδεση αποθηκευτικού μέσου
Directional antenna	Κατευθυντική κεραία
Distributed Denial of Service, DDoS	Κατανεμημένη Άρνηση Εξυπηρέτησης
Domain	Περιοχή
Download	Λήψη ή κατέβασμα αρχείων
Drivers	Οδηγοί συσκευών
Dynamic configuration	Δυναμική ρύθμιση/παραμετροποίηση
Encrypted File System, EFS	Κρυπτογραφημένο σύστημα αρχείων
Extender, Range extender ή Range expander	Επέκταση ασύρματου σήματος ή ασύρματος επαναλήπτης
Extensible Authentication Protocol, EAP	Πρωτόκολλο επεκτεινόμενης αυθεντικοποίησης
Failover Cluster	Συστοιχία Υψηλής Διαθεσιμότητας
Fiber/Fiber optic	Οπτική ίνα
File Transfer Protocol, FTP	Πρωτόκολλο μεταφοράς αρχείων
Firewall	Τείχος προστασίας
Format	Μορφοποίηση
Frame	Πλαίσιο
Frequency Control (Panel)	Πίνακας ελέγχου συχνοτήτων
Geoblocking	Γεωγραφικός αποκλεισμός
Graphics processing unit ,GPU	Μονάδα επεξεργασίας γραφικών
Hacker, Cracker , Vandal, Hacktivist	Εξωτερικός εισβολέας
Hacking	Παράνομη πρόσβαση
Hash Function	Συνάρτηση Κερματισμού
High Availability Cluster	Συστοιχία Υψηλής Διαθεσιμότητας
High definition TV HDTV	Τηλεόραση υψηλής ευκρίνειας
High Performance Cluster, HPC	Συστοιχία Υψηλής Απόδοσης
Home Page	Αρχική σελίδα
Hop	Άλμα (μεταξύ δρομολογητών)
Host	Υπολογιστής/δέκτης
Host ID – suffix	Αναγνωριστικό υπολογιστή στο δίκτυο
Hotspot	Σημείο ασύρματης πρόσβασης στο Διαδίκτυο
Hub	Διανομέας
Hypertext Markup Language, HTML	Γλώσσα Σήμανσης Υπερκειμένου
Identification	Αναγνώριση
Inbound (traffic)	Εισερχόμενη κίνηση
Infrastructure	Υποδομή
Infrastructure Wireless Networks	Ασύρματα δίκτυα υποδομής
Institute of Electrical and Electronic Engineers, IEEE	Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών
Integrity	Ακεραιότητα
Interface	Διεπαφή

International Organization for Standardization, ISO	Διεθνής Οργανισμός Τυποποίησης
Internet	Διαδίκτυο
Internet Assigned Numbers Authority, IANA	Αρχή που αντιστοιχίζει της θύρες σε υπηρεσίες (0 μέχρι 1024)
Internet Engineering Task Force, IETF	Τακτική Δύναμη Μηχανικών Διαδικτύου
Internet Protocol Security, Ipsec	Πρωτόκολλο ασφάλειας Διαδικτύου
Internet Protocol, IP	Πρωτόκολλο Διαδικτύου
Internet Service Provider, ISP	Πάροχος υπηρεσιών Διαδικτύου
Just a Bunch Of Disks, JBOD	Τεχνολογία της απλού συνόλου δίσκων
Key mapping relationship	Χαρτογραφημένη σχέση κλειδιών
Laptop	Φορητός ηλεκτρονικός υπολογιστής
Layer 2 Tunneling Protocol, L2TP	Πρωτόκολλο σηράγγων δευτέρου επιπέδου
Link	Σύνδεση ή ζεύξη
Load Balancing Cluster	Συστοιχία Εξισορρόπησης Φορτίου
Local Area Network, LAN	Τοπικό δίκτυο
Log-in	Διαδικασία εισόδου
Login name	Όνομα χρήστη
MAC Address	Διεύθυνση υλικού ή φυσική διεύθυνση
Mail Server	Διακομιστής ηλεκτρονικού ταχυδρομείου
Man in the Middle, MitM	Διαμεσολαβητής
Manual configuration	Μη αυτόματη ρύθμιση
Mapped key	Χαρτογραφημένο κλειδί
Master	Κύριος ή Βασικός
Media Access Control, MAC	Επίπεδο ή υποεπίπεδο Ελέγχου Πρόσβασης στο Μέσο
Members	Μέλη
Memory bus	Δίαυλος μνήμης
Memory multiplier	Πολλαπλασιαστής Κύριας Μνήμης (RAM)
Message Digest	Σύνοψη Μηνύματος
Metropolitan Area Network, MAN	Μητροπολιτικό δίκτυο
Microdots	Μικροκουκκίδες ή Μικροσκοπικές φωτογραφίες σε μέγεθος κουκκίδας (dot)
Mirroring	Κατοπτρισμός
Mobile Ad hoc NETwork, MANET	Κινητό ασύρματο δίκτυο αυτοοργανωμένο ή κατ' απαίτηση
Mobile Base Host, MBS	Ασύρματος Σταθμός Βάσης
Mobility	Κινητικότητα
Monitoring program	Πρόγραμμα παρακολούθησης
Multimedia sensor	Αισθητήρας πολυμέσων
Multiple-input and multiple-output, MIMO	Τεχνολογίας πολλαπλών συχνοτήτων και κεραιών
Network Attached Storage, NAS	Δικτυακό μέσο αποθήκευσης
Network File Systems, NFS	Δικτυακό σύστημα αρχείων
Network, Computer	Δίκτυο υπολογιστών
Node	Κόμβος
Omnidirectional antenna	Πανκατευθυντική κεραία
One-way	Μονόδρομος

Orthogonal Frequency Division Multiplexing, OFDM	Πολυπλεξία ορθογώνιου διαχωρισμού συχνοτήτων
Outbound (traffic)	Εξερχόμενη κίνηση
Overclocking	Υπερχρονισμός
Parity	Δυαδικά ψηφία ισοτιμίας
Partition	Διαμέρισμα
Password	Συνθηματικό
PCI Express slots	Υποδοχές τύπου PCI
Phishing	Παραπλανητική αλληλογραφία ή ηλεκτρονικό «ψάρεμα»
Plugin	Πρόσθετο
Point to point, P2P	Σημείο της σημείο
Point-to-Point Tunneling Protocol, PPTP	Πρωτόκολλο σήραγγας σημείου της σημείο
Port	Θύρα
Port Forwording	Προώθηση θύρας
Powerline / Broadband over Powerline, BPL	Τεχνολογία ευρυζωνικής πρόσβασης μέσω γραμμών ηλεκτρικής ισχύος
Powerline Carrier, PLC	Φέρον σήμα τεχνολογίας Powerline
Pre-Shared Key, PSK	Προκαθορισμένο κλειδί
Pretexting	Δημιουργία Σεναρίου
Private key	Ιδιωτικό κλειδί
Proxy server	Διακομιστής μεσολάβησης
Public key	Δημόσιο κλειδί
Public Key Cryptography	Κρυπτογράφηση δημοσίου κλειδιού
Public Key Infrastructure, PKI	Υποδομή δημόσιου κλειδιού
Public key servers	Εξυπηρετητές δημοσίων κλειδιών
Quality of service, QoS	Ποιότητα υπηρεσίας
Quid pro quo	Κάτι για κάτι ή «Δούναι και λαβείν»
Racks (Telecommunications)	Ράφια τηλεπικοινωνιών
RADIUS Server	Διακομιστής αυθεντικοποίησης
RAID Controller	Ελεγκτής Πλεονάζουσας Συστοιχία Ανεξάρτητων Δίσκων
Redundant Array of Independent Disks, RAID	Πλεονάζουσα Συστοιχία Ανεξάρτητων Δίσκων
Relative Path	Σχετική διαδρομή
Remote Authentication Dial-in User Service, RADIUS	Υπηρεσία απομακρυσμένης πιστοποίησης χρήστη εισερχόμενης κλήσης
Repeater	Επαναλήπτης
Roaming	Περιαγωγή
Router	Δρομολογητής
Scalable Link Interface, SLI	Τεχνολογία διπλών καρτών γραφικών της NVIDIA
Secret key	Μυστικό κλειδί
Secure Sockets Layer, SSL	Επίπεδο ασφαλών θυρών
Security	Ασφάλεια
Server	Εξυπηρετητής ή Διακομιστής
Server clustering	Συστοιχίες Εξυπηρετητών/διακομιστών
Service Set Identifier, SSID/ Network Name	Όνομα ή αναγνωριστικό ασύρματου δικτύου
Settings	Παράμετροι

Shared medium	Διαμοιραζόμενο μέσο
Shut down	Τερματισμός λειτουργίας
Site	Τοποθεσία
Slave	Δευτερεύον
Smartphone	Έξυπνο τηλέφωνο
Social Engineering	Κοινωνική Μηχανική
Sockets	Υποδοχές ή πρίζες
Spoofing	Πλαστοπροσωπία ή μεταμφίεση
Storage Area Network, SAN	Δικτυακή περιοχή αποθήκευσης
Stress Test	Στρες-τεστ ή δοκιμή αντοχής λειτουργίας ενός Η/Υ
Stress Tool	Εργαλείο για εκτέλεση στρες-τεστ ή δοκιμής αντοχής λειτουργίας Η/Υ
Striping	Διαγράμμιση
Symmetric key	Συμμετρικό κλειδί
Tablet	Ηλεκτρονικός υπολογιστής ταμπλέτα
Temporal Key Integrity Protocol, TKIP	Πρωτόκολλο ακεραιότητας προσωρινού κλειδιού
Terminal Adaptor, TA	Τερματικός προσαρμογέας
The onion router, Tor	Κρυπτογράφηση πολλών επίπεδων και υπολογιστών διαμεσολαβητών
Thread	Νήμα
Threat	Απειλή
Upload	Ανέβασμα αρχείων
Username	Όνομα χρήστη
Validity	Εγκυρότητα
Virtual LANs, VLAN	Εικονικά τοπικά δίκτυα
Virtual Private Networks, VPN	Εικονικά Ιδιωτικά Δίκτυα
Voltage Control (Panel)	Πίνακας ελέγχου ηλεκτρικής τάσης
Vulnerability	Αδυναμία
Web browser	φυλλομετρητής/πλοηγός
Web of Trust, WoT	Δίκτυο Εμπιστοσύνης
Web server	Διακομιστής/εξυπηρετητής του παγκόσμιου ιστού
Web Site	Ιστότοπος
Wide Area Networks, WAN	Δίκτυα ευρείας περιοχής
Wi-Fi multimedia, WMM	Πρότυπο πολυμέσων Wi-Fi
Wi-Fi Network Interface Controller, Wi-Fi NIC	Ασύρματη κάρτα δικτύου ή ελεγκτής ασύρματου δικτύου
Wi-Fi Protected Access II, WPA2 / IEEE 802.11i	Προστατευμένη πρόσβαση τεχνολογίας Wi-Fi $2^{η}$ έκδοση
Wi-Fi Protected Access, WPA	Προστατευμένη πρόσβαση τεχνολογίας Wi-Fi
Wired Equivalent Privacy, WEP	Ιδιωτικότητα ισοδύναμη ενσύρματου (δικτύου)
Wireless Ethernet Compatibility Alliance, WECA	Συμμαχία ασύρματης συμβατότητας Ethernet
Wireless Fidelity Wi-Fi	Πρότυπο ασύρματης πιστότητας
Wireless Local Area Network, WLAN	Ασύρματο τοπικό δίκτυο
Wireless Mesh Networks, WMN	Ασύρματα δίκτυα πλέγματος
Wireless Sensor Networks, WSN	Ασύρματα δίκτυα αισθητήρων
Workstation	Τερματικό ή προσωπικός υπολογιστής ή σταθμός εργασίας

World Wide Web, WEB	Παγκόσμιος Ιστός
Worm	Σκουλήκι
WPA2-Enterprise	Επιχειρησιακή προστατευμένη πρόσβαση τεχνολογίας Wi-Fi
WPA2-Personal, WPA2-PSK.	Προσωπική προστατευμένη πρόσβαση τεχνολογίας Wi-Fi
ZombiePC	Υπολογιστές ανυποψίαστων χρηστών μολυσμένοι με προγράμματα ιών