ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΤΗΛΕΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Εγκατάσταση και διαχείριση ενός FTP Server

Όνομα :Κωνσταντίνου Ιωάννα

Επιβλέπον καθηγητής :Παπαμώκος Γεώργιος

ΑΡΤΑ

Ιούνιος 2005

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

1. ΕΙΣΑΓΩΓΗ 3
   1.1 Η Ανάγκη Μεταφοράς Αρχείων 3
   1.2 Εισαγωγή στο πρωτόκολλο FTP 4
   1.3 Συμπεράσματα 8
2. ΕΦΑΡΜΟΓΕΣ FTP 9
   2.1 Τα Εργαλεία του FTP 9
   2.2 Πελάτες (Clients) FTP 11
   2.3 Συμπεράσματα 22
3. ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΔΙΑΔΙΚΤΥΟΥ – ΠΡΩΤΟΚΟΛΛΑ 23
   3.1 Διαδίκτυο (Internet) 23
   3.2 Αρχιτεκτονικές Δικτύων 25
   3.3 Το Μοντέλο Αναφοράς OSI 25
   3.4 Τα Επίπεδα του Διαδικτύου 27
   3.5 Εισαγωγή στην Τεχνολογία Πελάτη / Διακομιστή 35
   3.6 Συμπεράσματα 39
4. ΑΣΦΑΛΕΙΑ ΕΝΟΣ ΔΙΑΚΟΜΙΣΤΗ FTP 40
   4.1 Τι εννοούμε με τον όρο Ασφάλεια 40
   4.2 Συστήματα Ασφάλειας Firewalls 45
   4.3 Συμπεράσματα 51
5. ΕΓΚΑΤΑΣΤΑΣΗ ΕΝΟΣ ΔΙΑΚΟΜΙΣΤΗ FTP 52
   5.1 Εγκατάσταση του FTP Server του IIS των Windows 52
   5.2 Συμπεράσματα 65
6. ΔΙΑΧΕΙΡΙΣΗ ΕΝΟΣ ΔΙΑΚΟΜΙΣΤΗ 66
   6.1 Διαχείριση του Internet Information Services των Windows 66
   6.2 Οι Μελλοντικές Εξελίξεις των Servers 71
   6.3 Συμπεράσματα 72
7. ΕΙΔΙΚΟ ΘΕΜΑ ΔΙΑΧΕΙΡΙΣΗΣ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΕΝΟΣ ΔΙΑΚΟΜΙΣΤΗ 73
   7.1 10 Πρακτικές Ασφαλούς Διαχείρισης ενός διακομιστή FTP 73
   7.2 Secure File Transfer Protocol 83
   7.3 Ασφάλεια δεδομένων 83
   7.4 Εγκατάσταση SFTP 87
   7.2 Συμπεράσματα 90
8. Βιβλιογραφία 91

1. ΕΙΣΑΓΩΓΗ

1.1 Η Ανάγκη Μεταφοράς Αρχείων

Η επικοινωνία δεδομένων και η αναγκαιότητα για μεταφορά αρχείων έχει αναχθεί σε πρωταρχικής σημασίας κομμάτι της πληροφορικής. Δίκτυα εγκατεστημένα σε όλο το κόσμο, χρησιμοποιούνται για την συλλογή και διανομή δεδομένων πάνω σε ποικίλα θέματα. Από καιρό έχει κατανοηθεί η αναγκαιότητα διασύνδεσης όλων αυτών των επιμέρους δικτύων σε ένα ευρύτερο σύνολο, διευκολύνοντας και επιταχύνοντας την επικοινωνία. Οι προσπάθειες της κατασκευής αυτού του υπέρ – δικτύου ήταν επιτυχημένες και το αποτέλεσμα ήταν αυτό που σήμερα ξέρούμε σαν Internet. Το Internet (ή Διαδίκτυο) παρουσιάζει μεγάλη αποδοχή, πράγμα που οδηγεί στην συνεχή εξέλιξη και αναδιαμόρφωση του.

Ένα από τα μεγαλύτερα προβλήματα που έπρεπε να λυθούν ώστε το Διαδίκτυο να γίνει πραγματικότητα, ήταν η ύπαρξη πολλών τεχνολογιών δικτύων, καθεμιά από τις οποίες εξυπηρετεί μια συγκεκριμένη ομάδα ανθρώπων. Οι χρήστες του δικτύου διαλέγουν την τεχνολογία που είναι κατάλληλη για τις επικοινωνιακές τους ανάγκες. Η χρήση μίας και μόνο τεχνολογίας για την δημιουργία ενός παγκόσμιου δικτύου είναι αδύνατη, γιατί δεν υπάρχει τεχνολογία που να ικανοποιεί όλες τις απαιτήσεις. Για παράδειγμα, μερικοί χρήστες χρειάζονται δίκτυα υψηλών ταχυτήτων που καλύπτουν μικρές αποστάσεις. Για άλλους πάλι, πιο εξαπλωμένα δίκτυα, χαμηλών ταχυτήτων είναι πιο χρήσιμα.

Το Διαδίκτυο, παρ' όλα αυτά, καταφέρνει να συνενώσει όλες αυτές τις διαφορετικές τεχνολογίες, παρέχοντας ένα σύνολο συμβάσεων. Κρύβει τις λεπτομέρειες της υποκείμενης δικτυακής τεχνολογίας και επιτρέπει σε υπολογιστές από όλο τον κόσμο να βρίσκονται σε επαφή ανεξάρτητα από το δίκτυο στο οποίο συνδέονται. Το Διαδίκτυο βασίζεται σε μια συλλογή από τυποποιήσεις που καλούνται πρωτόκολλα. Τα πρωτόκολλα (π.χ. TCP και IP) παρέχουν τους κανόνες για την επικοινωνία. Περιέχουν τις λεπτομέρειες των ανταλλασσόμενων μηνυμάτων, περιγράφουν πως ανταποκρίνεται ο υπολογιστής όταν λαμβάνει κάποιο μήνυμα και ορίζει πως διαχειρίζεται ο υπολογιστής της καταστάσεις λάθους. Κατά μία έννοια, τα πρωτόκολλα είναι για την επικοινωνία ότι είναι οι αλγόριθμοι για τον

προγραμματισμό. Ένας αλγόριθμος επιτρέπει την κατανόηση της λογικής του προγράμματος, χωρίς να χρειάζεται να ξέρει την δομή και κατασκευή της CPU. Ομοίως, ένα πρωτόκολλο επιτρέπει στον χρήστη να καταλάβει τα δεδομένα χωρίς να έχει γνώση του δικτυακού υλικού.

Το FTP ήταν η πρώτη υπηρεσία για την ανάκτηση και μεταφορά πληροφορίας και αρχείων που χρησιμοποιήθηκε στο Διαδίκτυο. Η βασική λειτουργία του είναι η αξιόπιστη μεταφορά αρχείων από υπολογιστή σε υπολογιστή και επιτρέπει στους χρήστες να στήνουν μια σύνδεση ελέγχου μεταξύ του FTP client και του FTP server. Η σύνδεση αυτή τους επιτρέπει να ψάχνουν στους καταλόγους του server και να μεταφέρουν τα αρχεία που επιθυμούν από τον server προς τον δικό τους υπολογιστή. Για την μεταφορά των αρχείων δημιουργείται αυτόματα μια νέα ανεξάρτητη σύνδεση.

1.2 Εισαγωγή στο πρωτόκολλο FTP

Το FTP (File Transfer Protocol) επιτρέπει τη μεταφορά αρχείων ανάμεσα σε δύο υπολογιστές, που είναι συνδεμένοι στο Internet. Είναι ένα πρωτόκολλο μεταφοράς αρχείων σε περιβάλλον TCP/IP που στηρίζεται στις από άκρο σε άκρο (end-to-end) αξιόπιστες υπηρεσίες μεταφοράς που παρέχει το TCP/IP.

Μέσω του FTP μπορούμε να μεταφέρουμε αρχεία από έναν απομακρυσμένο υπολογιστή στο δικό μας και αντίστροφα. Όταν χρησιμοποιούμε το FTP, εκτελείται στο δικό μας υπολογιστή ένα πρόγραμμα που ονομάζεται πελάτης FTP (FTP client) για να συνδεθούμε με τον απομακρυσμένο υπολογιστή, στον οποίο εκτελείται ένα άλλο πρόγραμμα που ονομάζεται FTP διακομιστής (FTP server).

Εφόσον η μεταφορά αρχείων με το πρωτόκολλο FTP είναι του τύπου πελάτης-διακομιστής πρέπει πάντα, για την υλοποίηση της μεταφοράς, να υπάρχει ένας διακομιστής FTP, με τον οποίο θα συνδέονται ως πελάτες οι άλλοι υπολογιστές. Ο διαχειριστής του διακομιστή καθορίζει ποιοι υπολογιστές έχουν δικαίωμα σύνδεσης, καθώς και τι μπορούν να κάνουν, αφού συνδεθούν. Μπορεί έτσι να καθορίσει ξεχωριστά για κάθε υπολογιστή το είδος της πρόσβασης (πλήρης, μόνο για ανάγνωση κ.λπ.), ενώ το ίδιο μπορεί να κάνει και για κάθε φάκελο του διακομιστή. Μπορεί δηλαδή ο διαχειριστής του διακομιστή να κρύψει κάποιους φακέλους του συστήματός του, κάποιους άλλους να τους κάνει μόνο για ανάγνωση κ.λπ. Κατά τη σύνδεση ενός πελάτη με το διακομιστή, ο διακομιστής ζητεί από αυτόν το όνομα χρήστη και τον

κωδικό πρόσβασης, ενώ του δίνει τα δικαιώματα πρόσβασης που έχουν καθοριστεί για το συγκεκριμένο όνομα χρήστη. Στη συνέχεια, και με τη χρήση συγκεκριμένων εντολών FTP, ο πελάτης μπορεί να κατεβάσει ή να ανεβάσει αρχεία στο διακομιστή. Όλα τα μοντέρνα λειτουργικά συστήματα υποστηρίζουν εγγενώς τις εντολές FTP, αλλά ο περισσότερος κόσμος κάνει τη δουλειά του χρησιμοποιώντας τα ειδικά προγράμματα πελάτη FTP, τα οποία προσφέρουν γραφικό περιβάλλον, ευχρηστία, μεγάλες ευκολίες και αυτοματισμούς.

Το FTP χρησιμοποιεί 3 τρόπους μεταφοράς:

- stream: είναι ο default τρόπος και δεν αλλάζει τίποτε στα μεταφερόμενα αρχεία
- block: διαμερίζει τα μεταφερόμενα αρχεία σε block
- compressed: συμπιέζει τα αρχεία

FTP servers υπάρχουν διάσπαρτοι σε διάφορα μέρη σε ολόκληρο τον κόσμο και χιλιάδες από αυτούς υποστηρίζουν μια ειδική υπηρεσία τύπου FTP, το anonymous FTP, η οποία και χρησιμοποιείται συνήθως. Anonymous FTP σημαίνει ότι μπορούμε να συνδεθούμε με τον απομακρυσμένο υπολογιστή και να ανακτήσουμε αρχεία χωρίς να είμαστε υποχρεωμένοι να έχουμε λογαριασμό στον υπολογιστή αυτό. Στην προτροπή για το όνομα χρήστη (username) δίνουμε τη λέξη anonymous και στην προτροπή για το σύνθημα (password) δίνουμε την προσωπική μας διεύθυνση E-mail.

Το FTP χρησιμοποιεί δυο συνδέσεις TCP: μια για εντολές / απαντήσεις και μια για μεταφορές / αναγνωρίσεις δεδομένων. Ένας FTP server έχει ανοικτή την πόρτα 21 κι όταν έρχεται αίτημα σύνδεσης από έναν πελάτη (client) μπορεί να ζητήσει πιστοποίηση κωδικού (password) ή να επιτρέπει ανώνυμη μεταφορά.

Για να συνδεθούμε με ένα διακομιστή FTP, πρέπει να γνωρίζουμε την πλήρη διεύθυνσή του στο Internet, ενώ κατά τη σύνδεση ο διακομιστής θα μας ζητήσει όνομα χρήστη και κωδικό πρόσβασης. Το όνομα χρήστη και ο κωδικός πρόσβασης που θα δώσουμε πρέπει να είναι καταχωρισμένα στη βάση δεδομένων του διακομιστή, να είμαστε δηλαδή εξουσιοδοτημένος χρήστης των υπηρεσιών του εν λόγω διακομιστή. Εκτός όμως από τους εξουσιοδοτημένους χρήστες, οι περισσότεροι διακομιστές FTP μπορούν να δεχτούν και όλους τους άλλους, **δίνοντάς τους**

βεβαίως πολύ λιγότερα δικαιώματα πρόσβασης στα αρχεία και στους φακέλους που διαθέτουν.

Στην περίπτωση των διακομιστών FTP ελεύθερης πρόσβασης, για να ξεπεραστεί το εμπόδιο της διαδικασίας πιστοποίησης του ονόματος χρήστη και του κωδικού πρόσβασης, χρησιμοποιείται ως όνομα χρήστη το anonymous και ως κωδικό πρόσβασης δίνεται η διεύθυνση της ηλεκτρονικής μας αλληλογραφίας. Η σύνδεση αυτού του είδους λέγεται **anonymous FTP**, και για να επιτευχθεί στους διακομιστές FTP που την υποστηρίζουν, έχει δημιουργηθεί ειδικός λογαριασμός, στον οποίο, όπως είπαμε, το όνομα χρήστη είναι anonymous, ενώ ο κωδικός πρόσβασης είναι οποιαδήποτε διεύθυνση ηλεκτρονικής αλληλογραφίας (ακόμη και μη υπαρκτή). Ο κυριότερος προορισμός των διακομιστών FTP ελεύθερης πρόσβασης ή ανώνυμης πρόσβασης είναι η διανομή αρχείων, τα οποία προσφέρονται δωρεάν, όπως, για παράδειγμα, κάποια προγράμματα ελεύθερης χρήσης ή τα αρχεία διόρθωσης και ανανέωσης διαφόρων πακέτων λογισμικού.

Ο κανόνας στους ανώνυμους διακομιστές FTP, ο οποίος έχει βεβαίως και τις εξαιρέσεις του, θέλει το φάκελο που περιέχει τα ελεύθερα για κατέβασμα αρχεία να λέγεται pub, ενώ στους διακομιστές FTP που μας επιτρέπουν να ανεβάσουμε και τα δικά μας αρχεία, ο φάκελος λέγεται upload ή incoming. Υπάρχουν και κάποιοι άλλοι γραπτοί ή άγραφοι κανόνες στον κόσμο του FTP, όπως τα αρχεία κειμένου (.txt), τα οποία περιλαμβάνουν τα περιεχόμενα του διακομιστή ή του φακέλου στον οποίο βρίσκονται, καθώς και τα αρχεία κειμένου τα οποία περιέχουν τους κανόνες χρήσης του διακομιστή.

1.2.1 Τα Πλεονεκτήματα του FTP

Η περιήγηση στον κόσμο του FTP μοιάζει λιγάκι σαν να ψάχνεις μια βιβλιοθήκη με χιλιάδες βιβλία που κάποια από αυτά είναι ενδιαφέροντα και κάποια αδιάφορα. Για παράδειγμα σε FTP Servers μπορούμε να βρούμε τους τελευταίους οδηγούς της κάρτας γραφικών του συστήματός μας. Βέβαια, πολλά από αυτά τα αρχεία μπορούμε να τα βρούμε και στις ιστοσελίδες του Παγκόσμιου Ιστού, αλλά δεν είναι το ίδιο πράγμα. Το FTP διαφέρει σε ποσότητα, ταχύτητα κατεβάσματος, δυνατότητες και πάνω από όλα, διαφέρει σε αίσθηση. Είναι διαφορετικό να έχεις μπροστά σου μια ιστοσελίδα με κάποιους λιγοστούς δεσμούς (links) σε μερικά αρχεία

και άλλο να έχεις μπροστά σου ένα χορταστικό τραπέζι, παραγεμισμένο με όποιο λογισμικό τραβά η όρεξή σου. Γιατί αυτό είναι οι περισσότεροι διακομιστές FTP: τράπεζες λογισμικού, νόμιμου αλλά πολλές φορές και παράνομου. Ειδικά για αυτούς που ψάχνουν παράνομο λογισμικό το FTP είναι ο παράδεισος. Το γεγονός ότι το FTP δεν είναι τόσο δημοφιλές όσο ο λεγόμενος Παγκόσμιος Ιστός (οι ιστοσελίδες δηλαδή) κάνει την αδύνατη την αστυνόμευσή του από τους απανταχού διώκτες της πειρατείας. Οι περισσότεροι διακομιστές πειρατικού λογισμικού και παράνομων τραγουδιών MP3 είναι διακομιστές FTP. Ειδικά όσον αφορά στα τελευταία (τα τραγούδια MP3 δηλαδή), οι διακομιστές FTP είναι το αγαπημένο μέσο των πειρατών, ακριβώς για τα προτερήματά τους που είναι πολλά, όπως είπαμε.

Το FTP είναι το κατεξοχήν πρωτόκολλο μεταφοράς αρχείων, είναι δημιουργημένο γι' αυτόν το σκοπό και παρ' όλες τις προσθήκες που κατά καιρούς έχει δεχτεί ο σταρ του Internet, το HTTP (το πρωτόκολλο μεταφοράς ιστοσελίδων), δεν μπορεί σε τίποτα να υποκαταστήσει τον πραγματικό μεταφορέα των αρχείων. Μέσα από έναν πελάτη FTP βλέπουμε τους φακέλους του διακομιστή FTP σαν να ήταν κοινόχρηστοι φάκελοι του τοπικού μας δικτύου. Μπορούμε λοιπόν να δούμε τα περιεχόμενά τους, να αντιγράψουμε στο σκληρό μας τα αρχεία που μας ενδιαφέρουν κ.λπ.

Μια σημαντική δυνατότητα, την οποία δυστυχώς δεν υποστηρίζουν όλοι οι διακομιστές FTP, είναι ότι σε περίπτωση διακοπής της σύνδεσής μας με το Internet (αν, π.χ., πέσει η γραμμή), μπορούμε να ανακτήσουμε το αρχείο που μεταφέραμε και να συνεχίσουμε τη μεταφορά του από το σημείο όπου ήταν τη στιγμή της διακοπής. Αυτή η δυνατότητα είναι πραγματικά σωτήρια, ειδικά κατά τη μεταφορά αρχείων μεγάλου μεγέθους. Ας αναλογιστούμε την περίπτωση ότι κατεβάζουμε ένα αρχείο 30MB, να έχουμε κατεβάσει τα 29MB και πέφτει η γραμμή του τηλεφώνου. Εάν συμβεί αυτό όταν κατεβάζουμε το αρχείο μέσω browser από το διαδίκτυο οι περισσότερες πιθανότητες είναι να χάσουμε το αρχείο. Εάν όμως χρησιμοποιούμε FTP Server και ο διακομιστής FTP, από τον οποίο κατεβάζουμε το αρχείο, υποστηρίζει ανάκτηση (το ίδιο φυσικά πρέπει να ισχύει και για το πρόγραμμα πελάτη που χρησιμοποιούμε), τότε, με το που καταφέρνουμε να ξανασυνδεθούμε με το διακομιστή FTP, το κατέβασμά μας συνεχίζεται από το σημείο που διακόπηκε, από τα 29MB δηλαδή.

Ένα άλλο πλεονέκτημα της μεταφοράς αρχείων με FTP είναι η δυνατότητα της μαζικής μεταφοράς. Μαρκάρουμε τα αρχεία που θέλουμε να ανεβάσουμε ή να κατεβάσουμε και το πρόγραμμα πελάτη αναλαμβάνει τη μεταφορά τους είτε σειραϊκά (το ένα μετά το άλλο) είτε ακόμη και ταυτόχρονα. Σε περίπτωση που δοκιμάσουμε κάτι αντίστοιχο χρησιμοποιώντας HTTP για τη μεταφορά πολλών αρχείων είτε θα μας πάρει αρκετό χρόνο η μεταφορά είτε θα κολλήσει το μηχάνημά μας λόγω του μεγάλου όγκου των αρχείων που κατεβαίνουν εκείνη την στιγμή. Δεν είναι τυχαίο άλλωστε ότι ο Microsoft Internet Explorer ένας από τους πιο δημοφιλής internet browsers περιορίζει τους χρήστες στο ταυτόχρονο κατέβασμα τριών μόνο αρχείων και επιτρέπει το κατέβασμα το τέταρτου μόνο σε περίπτωση που έχει τελειώσει το κατέβασμα ενός από τα προηγούμενα αρχεία. Το HTTP είναι άριστο για ιστοσελίδες, αλλά για τη μεταφορά αρχείων ο αδιαμφισβήτητος κυρίαρχος είναι το FTP.

1.3 Συμπεράσματα

Σε αυτό το κεφάλαιο αναφερθήκαμε στην ολοένα και αυξανόμενη ανάγκη που έχει δημιουργηθεί για την ανάγκη μεταφοράς αρχείων μέσω του διαδικτύου γρήγορα και με ασφάλεια. Παρουσιάσαμε μια εισαγωγή στην υπηρεσία του FTP και δώσαμε μια πρώτη επεξήγηση των εννοιών πίσω από αυτή την υπηρεσία. Τέλος καταγράψαμε τα πλεονεκτήματα του FTP και τους λόγους γιατί είναι ο αδιαμφισβήτητος κυρίαρχος στην μεταφορά αρχείων. Στο επόμενο κεφάλαιο θα αναφερθούμε στους πελάτες FTP, στις κυριότερες εντολές του και στην διαδικασία μεταφοράς αρχείων από ένα FTP server τόσο από περιβάλλον γραμμής εργαλείων όσο και μέσω εφαρμογών.

2. ΕΦΑΡΜΟΓΕΣ FTP

2.1 Τα Εργαλεία του FTP

Όπως αναφέραμε και στο προηγούμενο κεφάλαιο υπάρχουν οι διακομιστές (server) FTP και οι πελάτες (client) FTP. Σε αυτό το κεφάλαιο θα ασχοληθούμε με τους πελάτες FTP καθώς είναι απαραίτητοι για την σύνδεση και τη μεταφορά αρχείων από τους FTP servers. Οι FTP servers παρουσιάζονται αναλυτικά σε επόμενα κεφάλαια.

Ο καθένας μπορεί να στήσει το δικό του FTP server και έτσι κάθε φορά που συνδεόμαστε στο Internet να μπορούν άλλοι χρήστες να κατεβάζουν ή να ανεβάζουν αρχεία από και προς τον υπολογιστή μας. Βέβαια, πρέπει κάθε φορά να τους παρέχεται η διεύθυνσή IP μας, διότι στους απλούς λογαριασμούς dialup η διεύθυνση IP είναι δυναμική (dynamic) και αλλάζει κάθε φορά που συνδεόμαστε με το Internet. Από εκεί και πέρα, ή θα έχουμε δημιουργήσει «ανώνυμο» λογαριασμό, ο οποίος, όπως είπαμε, επιτρέπει ελεύθερη πρόσβαση σε όλους, ή θα δημιουργήσουμε κανονικούς λογαριασμούς με όνομα χρήστη και κωδικό πρόσβασης, επιτρέποντας έτσι την πρόσβαση μόνο σε εξουσιοδοτημένους από εμάς χρήστες. Υπάρχουν πάρα πολλά προγράμματα που δίνουν στον υπολογιστή μας τη δυνατότητα να είναι FTP Server, αρκετά από αυτά μάλιστα είναι και δωρεάν, όπως τα παρακάτω:

ArGoSoft FTP Server (http://www.argosoft. com/applications/ftpserver.html)

FDaemon (http://www.fictional.net/ software/fdaemon)

GuildFTPD (http://gftpd.dhs.org/)

NiteServer http://come.to/niteserversite

WAR FTP Daemon (http://home.sol.no/ jgaa/tftpd.htm)

Μπορούμε λοιπόν να στήσουμε εύκολα και εντελώς ανέξοδα το δικό μας FTP Server, ακόμη και μέσα από τα Windows χρησιμοποιώντας την υπηρεσία IIS όπως περιγράφεται στο πέμπτο κεφάλαιο. Εκτός από τα παραπάνω προγράμματα,

υπάρχουν πολλά άλλα shareware, τα οποία μπορούμε να τα βρούμε στους δικτυακούς τόπους διανομής λογισμικού δοκιμαστικής χρήσης, όπως είναι ο Tucows. Στους ίδιους τόπους μπορούμε να βρούμε και έναν πραγματικά τεράστιο αριθμό προγραμμάτων πελάτη FTP, τα οποία θα μας επιτρέψουν να ξεκινήσουμε την μεταφορά αρχείων στους FTP servers του Διαδικτύου. Τα πιο γνωστά και διαδεδομένα προγράμματα πελάτη FTP είναι το WS-FTP (http://www.ipswitch.com/products/WS_FTP) το οποίο και περιγράφουμε στη συνέχεια, το CuteFTP (http://www.cute ftp.com), καθώς και το περιβόητο GetRight http://www.getright.com. Αυτή την στιγμή σχεδόν όλα τα προγράμματα περιήγησης στο Internet (browsers) διαθέτουν τις στοιχειώδεις δυνατότητες πελάτη FTP. Απλώς δίνουμε τη διεύθυνση του FTP server στην μπάρα διευθύνσεων του προγράμματος περιήγησης μας στο Internet και αυτό θα φροντίσει τα υπόλοιπα.

2.1.1 Ανέβασμα Αρχείων με FTP

Όπως είπαμε, με FTP μπορούμε να κατεβάσουμε αρχεία στον υπολογιστή μας, που τα βρίσκουμε στους πολυάριθμους FTP server ανά την υφήλιο. Μπορούμε όμως και να ανεβάσουμε τα δικά μας αρχεία στους διακομιστές αυτούς. Είτε απλώς για να μπορέσουν να τα πάρουν από εκεί κάποιοι άλλοι χρήστες, είτε επειδή, για να μας επιτρέψει ο διαχειριστής του FTP server να κατεβάσουμε στον υπολογιστή μας κάποια αρχεία του, πρέπει εμείς να ανεβάσουμε κάποια δικά μας για αντάλλαγμα, είτε για να δημοσιεύσουμε στην προσωπική μας ιστοσελίδα. Όλοι μας, όταν φτιάχνουμε τις προσωπικές μας ιστοσελίδες, τις δημιουργούμε στον υπολογιστή μας. Για να είναι όμως προσιτές σε όλους και όλες τις ώρες (και όχι μόνο τις ώρες που ο υπολογιστής μας είναι συνδεδεμένος με το Internet), πρέπει οι ιστοσελίδες μας να μεταφερθούν σε κάποιο διακομιστή ιστοσελίδων (Web Server). Η πλέον δημοφιλής μέθοδος μεταφοράς των ιστοσελίδων από τον υπολογιστή στον οποίο κατασκευάστηκαν, στον υπολογιστή που τελικά θα τις φιλοξενεί (Web Server) είναι με FTP. Αυτός είναι πραγματικά ο πιο απλός και καθαρός τρόπος. Είναι σαν να μεταφέρουμε αρχεία από το σκληρό μας δίσκο σε κάποιον κοινόχρηστο σκληρό του τοπικού μας δικτύου, ασχέτως αν στην πραγματικότητα ο διακομιστής Web στον οποίο στέλνουμε τις ιστοσελίδες μας μπορεί να βρίσκεται στην άλλη άκρη του κόσμου.

2.2 Πελάτες (Clients) FTP

Για τη μεταφορά αρχείων μέσω FTP, υπάρχουν αρκετά προγράμματα τα οποία μπορούμε να χρησιμοποιήσουμε. Τα προγράμματα αυτά είτε τρέχουν από τη γραμμή εντολών του λειτουργικού συστήματος, όπως το πρόγραμμα FTP των Windows 2000, είτε αποτελούν ολοκληρωμένες παραθυρικές εφαρμογές, δοκιμαστικές εκδόσεις των οποίων μπορούν να κατεβούν από το Internet, όπως το **WS-FTP** το οποίο περιγράφεται παρακάτω και το **CuteFTP.**

2.2.1 Το πρόγραμμα FTP των Windows

Οι FTP servers εκτελούνται συνήθως σε μηχανές UNIX. Το λογισμικό του αντίστοιχου πελάτη έχει κατασκευαστεί για διάφορες κατηγορίες μηχανών. Έτσι, σε προσωπικό υπολογιστή τύπου συμβατού IBM, οι πελάτες FTP ενεργοποιούνται από αντίστοιχο εικονίδιο μέσα από τα Windows ή από τη γραμμή εντολής (*Run*) πληκτρολογώντας:

ftp <*όνομα_μηχανής*>

Οι εφαρμογές αυτές εκτελούνται σε **περιβάλλον κειμένου** και οι λειτουργίες τους πραγματοποιούνται από εντολές σε μορφή κειμένου. Οι λειτουργίες παρουσιάζονται παρακάτω και συμπίπτουν με τις λειτουργίες που χρησιμοποιούνται σε περιβάλλον UNIX.

Ο ακόλουθος πίνακας περιέχει τις βασικές εντολές:

open <*όνομα_μηχανής*>	Αίτηση για σύνδεση με την απομακρυσμένη μηχανή <*όνομα_μηχανής*> (αφού έχουμε κάνει **close** στην προηγούμενη σύνδεση).
close <*όνομα_μηχανής*>	Τερματισμός τρέχουσας σύνδεσης.
help	Εμφάνιση της λίστας των διαθέσιμων εντολών. Με **help** <*όνομα_εντολής*> παίρνουμε μια σύντομη εξήγηση της εντολής <*όνομα_εντολής*>.

pwd	Εμφάνιση του τρέχοντος καταλόγου στο δίσκο της απομακρυσμένης μηχανής.
dir <*dir* >	Εμφάνιση των περιεχομένων του καταλόγου <*dir*> της απομακρυσμένης μηχανής.
cd <*dir* >	Αλλαγή τρέχοντος καταλόγου στο δίσκο της απομακρυσμένης μηχανής.
lcd <*dir*>	Αλλαγή τρέχοντος καταλόγου στο δίσκο της δικής μας μηχανής.
ascii	Μετάβαση σε κατάσταση ascii για τη μεταφορά αρχείων. Τα αρχεία μεταφέρονται σαν αρχεία κειμένου.
binary	Μετάβαση σε κατάσταση binary για τη μεταφορά αρχείων. Τα αρχεία μεταφέρονται σαν δυαδικά αρχεία.
type	Εμφάνιση της τρέχουσας κατάστασης μεταφοράς αρχείων.
get <*file*>	Αίτηση για μεταφορά του αρχείου <*file*> από τον τρέχοντα κατάλογο της απομακρυσμένης μηχανής στον τρέχοντα κατάλογο της δικής μας. **Προσοχή:** αν προϋπάρχει αρχείο με το ίδιο όνομα αντικαθίσταται από το μεταφερόμενο χωρίς προειδοποίηση.
put <*file*>	Αίτηση για μεταφορά του αρχείου <*file*> από τον τρέχοντα κατάλογο της δικής μας στον τρέχοντα κατάλογο της απομακρυσμένης μηχανής, αν βέβαια έχουμε αυτό το δικαίωμα. Η σύσταση της προηγούμενης εντολής ισχύει κι εδώ.
mget <*file1*> <*file2*> ...	Όμοια με την **get**, με τη διαφορά ότι γίνεται αίτηση για μεταφορά πολλών αρχείων (των <*file1*>, <*file2*>, κλπ.)

mput *<file1> <file2> ...*	Όμοια με την **put**, με τη διαφορά ότι γίνεται αίτηση για μεταφορά πολλών αρχείων (των *<file1>*, *<file2>*, κλπ.)
bye	Έξοδος από το περιβάλλον του ftp.

Έστω ότι θέλουμε να συνδεθούμε με τον FTP server Serv_X. Εφόσον ξέρουμε ότι το όνομα της μηχανής είναι: http://www.serv_x.gr/ftp/. Δίνουμε:

open http://www.serv_x.gr/ftp/

Εναλλακτικά, θα μπορούσαμε να είχαμε πληκτρολογήσει κατευθείαν από τη γραμμή εντολής του UNIX:

ftp http://www.serv_x.gr/ftp/

Μετά από λίγο, αν βέβαια το όνομα μηχανής που δώσαμε είναι σωστό και η αντίστοιχη μηχανή σε λειτουργία, παίρνουμε μήνυμα που μας προτρέπει να δώσουμε όνομα χρήστη (user name) και σύνθημα (password). Θα κάνουμε anonymous FTP. Δίνουμε σαν όνομα χρήστη "anonymous" και σαν σύνθημα την E-mail διεύθυνσή μας.

Αν υποθέσουμε ότι η αναγνώρισή μας από τη μηχανή είναι επιτυχής και βρισκόμαστε έτσι σε ένα περιβάλλον όπου μπορούμε να εξετάσουμε τα περιεχόμενα του δίσκου της και να τα μεταφέρουμε στο δίσκο της δικής μας μηχανής. Η μηχανή με την οποία συνδεθήκαμε, όπως και οι περισσότεροι FTP servers, είναι συνήθως μια μηχανή UNIX. Πληροφορούμαστε επίσης ότι τα αρχεία μεταφέρονται σαν δυαδικά αρχεία (binary).

Το FTP υποστηρίζει δύο καταστάσεις μεταφοράς αρχείων: σαν **αρχεία κειμένου (ascii)** και σαν **δυαδικά αρχεία (binary)**. Χρησιμοποιούμε την πρώτη μόνον για απλά αρχεία χαρακτήρων και τη δεύτερη για δυαδικά αρχεία (προγράμματα, έγγραφα από επεξεργαστές κειμένου, αρχεία γραφικών, συμπιεσμένα αρχεία, κλπ.), δηλαδή πρακτικά για όλα τα υπόλοιπα είδη αρχείων.

Όταν ένα αρχείο μεταφέρεται σαν αρχείο κειμένου μεταξύ δύο διαφορετικών τύπων μηχανών, υφίσταται κάποιες μετατροπές για να καταλήξει σε αναγνώσιμη μορφή στη μηχανή προορισμού. Ένα δυαδικό αρχείο μεταφέρεται πάντοτε χωρίς να υποστεί μετατροπές.

Πριν από μια μεταφορά αρχείου πρέπει να βεβαιωνόμαστε ότι βρισκόμαστε στη σωστή κατάσταση μεταφοράς. Εάν μετά από μια μεταφορά το αρχείο που παίρνουμε είναι κατεστραμμένο (π.χ. ένα αρχείο κειμένου φαίνεται ολόκληρο σαν μια γραμμή ή ένα πρόγραμμα που κανονικά θα έπρεπε να εκτελείται στη μηχανή μας, δεν εκτελείται), πρέπει να υποψιαστούμε ότι επιλέξαμε λανθασμένο τρόπο μεταφοράς. Όταν κάνουμε FTP μεταξύ δύο μηχανών του ίδιου τύπου, όπως στην περίπτωσή μας, μπορούμε να μεταφέρουμε όλα τα αρχεία σε δυαδική μορφή.

Για να κατεβάσουμε ένα αρχείο δίνουμε την εντολή **pwd** και βλέπουμε ότι βρισκόμαστε στον κατάλογο ρίζα στο δίσκο της απομακρυσμένης μηχανής. Με **dir** παίρνουμε μια λίστα των περιεχομένων του καταλόγου.

Συνήθως τα αρχεία που είναι δημόσια διαθέσιμα για **anonymous FTP** βρίσκονται σε έναν κατάλογο με ονομασία **"pub"**. Δίνουμε λοιπόν **cd pub** και στη συνέχεια **dir.**

Έστω ότι μας ενδιαφέρει να βρούμε εκτελέσιμα αρχεία για **UNIX**. Δίνουμε **cd unix** και στη συνέχεια **dir**. Αρχεία με ονόματα όπως INDEX, README, κλπ. συνήθως περιέχουν εξηγήσεις για τα περιεχόμενα του καταλόγου (μπορούμε να δούμε το αρχείο INDEX, δίνοντας την εντολή: get INDEX "|more"). Σε περίπτωση που θέλουμε να μεταφέρουμε στη μηχανή μας το αρχείο temp.txt. Δίνουμε την εντολή: get temp.txt

2.2.2 Χρήσιμες Συμβουλές για Αποτελεσματική Μεταφορά Αρχείων

Για να μεταφέρουμε το αρχείο <file1> από την απομακρυσμένη στη δική μας μηχανή μετονομάζοντάς το ταυτόχρονα σε <file2>, δίνουμε:

get <file1> <file2>

Για να δούμε τα περιεχόμενα του αρχείου κειμένου <file> χωρίς να το μεταφέρουμε στη μηχανή μας, δίνουμε:

get <file> "|more"

Δεν συνιστάται η ανάγνωση μεγάλων αρχείων με αυτόν τον τρόπο γιατί εξακολουθούμε να παραμένουμε συνδεδεμένοι με την απομακρυσμένη μηχανή. Είναι προτιμότερο να μεταφέρουμε ένα μεγάλο αρχείο στο μηχάνημά μας και να το διαβάσουμε εκεί.

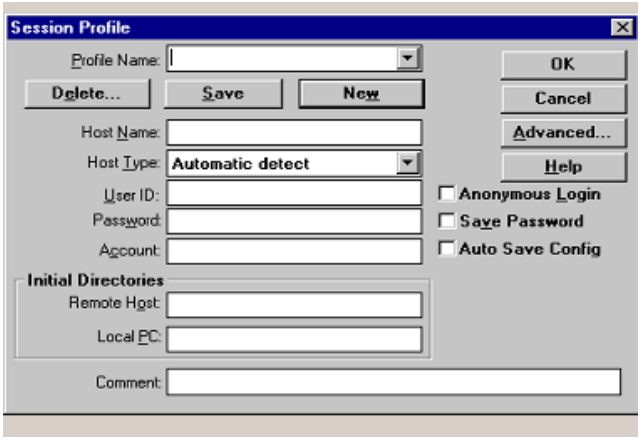
Για να διακόψουμε μια μεταφορά αρχείου πατάμε **[CTRL]+C**. Το μερικό αρχείο που δημιουργείται δεν σβήνεται αυτόματα.

Για να εντοπίσουμε σε ποιον κατάλογο της απομακρυσμένης μηχανής βρίσκεται κάποιο αρχείο που ψάχνουμε, μπορούμε να συμβουλευτούμε αρχεία με ονόματα όπως README, INDEX, κλπ. που βρίσκονται συνήθως στον κατάλογο ρίζα του δίσκου της και περιγράφουν την τρέχουσα δομή καταλόγων. Επίσης, αρχεία με όνομα ls-lR που περιέχουν την έξοδο που προκύπτει από την εκτέλεση της εντολής ls -lR του UNIX, δηλ. μια λίστα των περιεχομένων όλων των καταλόγων. Μπορούμε να μεταφέρουμε τα αρχεία αυτά στη μηχανή μας και να εξετάσουμε τα περιεχόμενα τους. Στην επόμενη σύνδεσή μας θα ξέρουμε σε ποιόν κατάλογο να αναζητήσουμε το αρχείο που μας ενδιαφέρει.

2.2.3 Ο πελάτης WS_FTP

Το πρόγραμμα WS-FTP παρέχει υπηρεσίες μεταφοράς αρχείων χρησιμοποιώντας ένα φιλικό **γραφικό περιβάλλον** προς τον χρήστη. Οι εντολές είναι σε μορφή γραφικών (κουμπιά), πολύ πιο εύχρηστες και κατανοητές όπως στο δημοφιλές πρόγραμμα WS_FTP (public domain για PCs), το οποίο περιγράφουμε στη συνέχεια.

Εκτελούμε την εφαρμογή με διπλό κλικ στο αντίστοιχο εικονίδιο και εμφανίζεται ένα παράθυρο με τίτλο **Session Profile** (Προφίλ Σύνδεσης):



Το αρχικό παράθυρο του WS_FTP

Το WS_FTP δίνει τη δυνατότητα να δημιουργούνται και να αποθηκεύονται "προφίλ σύνδεσης", δηλ. σύνολα από πληροφορίες που σχετίζονται το καθένα με μια σύνδεση που πρέπει να πραγματοποιηθεί (π.χ. όνομα απομακρυσμένης μηχανής, τύπος μηχανής, όνομα χρήστη).

Έτσι, δεν χρειάζεται να εισαχθούν ξανά οι πληροφορίες αυτές κάθε φορά που χρειάζεται να η σύνδεση με μια συγκεκριμένη μηχανή. Απλά επιλέγεται το αντίστοιχο προφίλ από τη λίστα που εμφανίζεται πατώντας το βελάκι στο πεδίο **Profile Name** και στη συνέχεια το κουμπί **OK**.

Ο ακόλουθος πίνακας περιγράφει τα πεδία του αρχικού παραθύρου του WS-FTP:

Profile Name	Όνομα προφίλ. Μπορούμε να δώσουμε ό,τι θέλουμε.
Host Name	Όνομα της απομακρυσμένης μηχανής.
Host Type	Τύπος της απομακρυσμένης μηχανής, συνήθως UNIX. Εάν δεν τον γνωρίζουμε, επιλέγουμε **Automatic detect** (αυτόματη ανίχνευση).
User ID	Όνομα χρήστη. Εάν δεν έχουμε λογαριασμό στη μηχανή, τσεκάρουμε το κουτί **Anonymous Login**.
Password	Σύνθημα που χρησιμοποιούμε για το όνομα χρήστη που δώσαμε. Αν επιλέξαμε Anonymous Login δίνουμε την E-mail διεύθυνσή μας.
Account	Λογαριασμός που χρησιμοποιούμε για το όνομα χρήστη που

	δώσαμε (αν απαιτείται από την απομακρυσμένη μηχανή). Συνήθως το αφήνουμε κενό.
Initial Directories: Remote Host	Ο κατάλογος του δίσκου της απομακρυσμένης μηχανής που θέλουμε να είναι τρέχον όταν αποκαθίσταται η σύνδεση. **Προσοχή:** στο UNIX, το σύμβολο που χωρίζει τα ονόματα των καταλόγων σε μια διαδρομή είναι το "/". Π.χ. /pub/win95.
Local PC	Ο κατάλογος του δίσκου του τοπικού μηχανήματος που θέλουμε να είναι επιλεγμένος όταν αποκαθίσταται η σύνδεση.
Comment	Σχόλια (προαιρετικά) που περιγράφουν τη σύνδεση.
Anonymous Login	Όταν είναι τσεκαρισμένο, στο πεδίο **User ID** μπαίνει η λέξη "anonymous" και στο πεδίο **Password** η E-mail διεύθυνσή μας.
Save Password	Όταν είναι τσεκαρισμένο, το σύνθημά μας αποθηκεύεται στο αρχείο ws_ftp.ini. Καλό είναι να το αφήνουμε κενό, γιατί κάποιος με πρόσβαση στον υπολογιστή μας θα μπορούσε να κλέψει το συνθηματικό μας.
Auto Save Config	Όταν είναι τσεκαρισμένο, το προφίλ σύνδεσης αποθηκεύεται αυτόματα με το πάτημα του **OK** και τη σύνδεση με την απομακρυσμένη μηχανή.

Τα πεδία του αρχικού παραθύρου του WS_FTP

Τα κουμπιά **Delete, Save** και **New** χρησιμεύουν για την διαχείριση των προφίλ σύνδεσης. Με το **New** δημιουργούμε ένα νέο προφίλ. Επιλέγοντας από τη λίστα ένα προφίλ και μετά πατώντας **Delete**, το σβήνουμε. Με το **Save** αποθηκεύουμε ένα προφίλ χωρίς να χρειαστεί να συνδεθούμε άμεσα με την απομακρυσμένη μηχανή.

Αφού συνδεθούμε περνάμε στο παράθυρο εργασίας της εφαρμογής WS_FTP το οποίο χωρίζεται σε δυο πανομοιότυπες ζώνες. **Αριστερά** βλέπουμε τα περιεχόμενα του δίσκου του **τοπικού μηχανήματος** (προσωπικού υπολογιστή), ενώ **δεξιά** βλέπουμε τα περιεχόμενα του δίσκου του FTP server με τον οποίο συνδεόμαστε.

Τα μέσα αποθήκευσης του FTP server (σκληρός δίσκος, cd-rom, κλπ.) είναι οργανωμένα με τη λογική μορφή ενός “δέντρου”. Κάθε κλαδί του δέντρου είναι ένας κατάλογος (directory) που περιέχει αρχεία (files) και άλλους καταλόγους

(subdirectories). Ο κατάλογος που βρίσκεται στην κορυφή του δέντρου ονομάζεται ρίζα (root). Το όνομα ενός αρχείου ή καταλόγου έχει μήκος μέχρι 14 χαρακτήρες, οι οποίοι μπορεί να είναι: i) τα γράμματα του λατινικού αλφάβητου a-z, A-Z, ii) οι αριθμοί 0-9**,** iii) οι ειδικοί χαρακτήρες: ".", "_", ",", "-", "+". Το όνομα έχει μόνο έναν τρόπο γραφής. Αν τα ίδια γράμματα αλλάξουν από πεζά σε κεφαλαία ή αντίστροφα, τότε έχουμε διαφορετικό όνομα. Π.χ.: τα INDEX, Index και index είναι τρία διαφορετικά ονόματα αρχείων.

Σε κάθε ζώνη της οθόνης, επάνω εμφανίζεται σε μια γραμμή η πλήρης διαδρομή του τρέχοντος καταλόγου και από κάτω δύο πλαίσια.

Στο **επάνω πλαίσιο** εμφανίζονται οι **υποκατάλογοι** του τρέχοντος καταλόγου, ενώ στο **κάτω** τα **αρχεία** του τρέχοντος καταλόγου. Σέρνοντας με το ποντίκι τη μπάρα που χωρίζει τα δύο πλαίσια, μπορούμε να αυξομειώνουμε το μέγεθός τους.

Με το ποντίκι μπορούμε να επιλέγουμε αρχεία και καταλόγους.

Όταν ένα αρχείο μεταφέρεται σε έναν κατάλογο όπου προϋπάρχει αρχείο με το ίδιο όνομα, το υπάρχον αρχείο αντικαθίσταται από το μεταφερόμενο χωρίς να ερωτηθούμε. Για να έχουμε τη δυνατότητα να δώσουμε άλλο όνομα στο μεταφερόμενο αρχείο, μπορούμε να τσεκάρουμε την επιλογή Options → Session Options → Prompt For Destination File Names. Εναλλακτικά, μπορούμε να καθορίσουμε η δική μας ή η απομακρυσμένη μηχανή να αποδίδει αυτόματα άλλο όνομα στο μεταφερόμενο αρχείο (επιλογές Options → Session Options → Receive Unique και Options → Session Options → Send Unique αντίστοιχα).

Όταν μεταφέρεται ένα αρχείο, εμφανίζεται ένα κουτί διαλόγου που δείχνει την πρόοδο της μεταφοράς. Αν για οποιονδήποτε λόγο θέλουμε να διακόψουμε τη μεταφορά, πατάμε **Cancel**. Το μερικό αρχείο που δημιουργείται δεν σβήνεται αυτόματα.

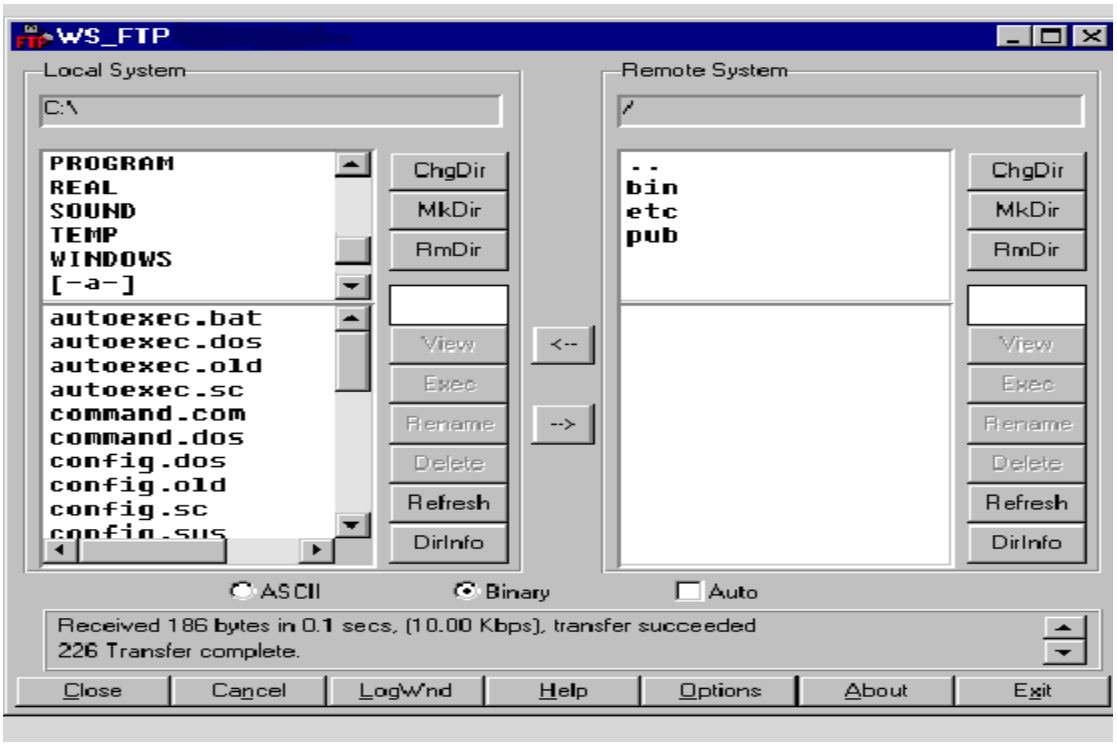
Για να μεταφέρουμε πολλά αρχεία, τα επιλέγουμε με το ποντίκι έχοντας πατημένο το πλήκτρο **[CTRL]** και στη συνέχεια πατάμε ← ή →**.**

Όταν κάνουμε διπλό κλικ πάνω σε ένα όνομα καταλόγου, εμφανίζονται τα περιεχόμενά του (ισοδυναμεί με επιλογή του καταλόγου και πάτημα του κουμπιού ChgDir). Μέσω του Options → Program Options μπορούμε να καθορίσουμε και το αποτέλεσμα που θα έχει το διπλό κλικ πάνω σε ένα όνομα αρχείου, σαν ένα από τα παρακάτω: α) Transfer (το αρχείο μεταφέρεται στην απέναντι πλευρά), β) View (ισοδυναμεί με επιλογή του αρχείου και πάτημα του κουμπιού View) και γ) Nothing (δεν συμβαίνει τίποτα).

Κατά τη διάρκεια της εκτέλεσης του προγράμματος, στις γραμμές κατάστασης (Log Window) του κάτω μέρους της οθόνης εμφανίζονται μηνύματα από τα οποία μπορούμε να παρακολουθούμε την πορεία της "συνδιαλλαγής" του υπολογιστή μας με τον FTP server.

Πατώντας το κουμπί DirInfo, δημιουργείται αυτόματα ένα αρχείο κειμένου στο πρόγραμμα Notepad. Περιέχει μια λίστα με τα περιεχόμενα του επιλεγμένου καταλόγου. Αν πρόκειται για κατάλογο του UNIX, κάθε γραμμή της λίστας έχει την εξής δομή: ο πρώτος χαρακτήρας μας πληροφορεί για το αν πρόκειται για αρχείο ή κατάλογο (ένα - σημαίνει αρχείο κι ένα d σημαίνει κατάλογος), οι επόμενοι 9 χαρακτήρες δείχνουν τα δικαιώματα προσπέλασης του αρχείου ή καταλόγου, ακολουθεί ο αριθμός των συνδέσμων του αρχείου ή καταλόγου, ο ιδιοκτήτης του, η ομάδα στην οποία ανήκει ο ιδιοκτήτης, το μέγεθος, η ημερομηνία τελευταίας τροποποίησης και τέλος, το όνομα του αρχείου ή καταλόγου.

Μόλις ολοκληρώσουμε την μεταφορά των αρχείων που επιθυμούμε δίνουμε close για να αποσυνδεθούμε από τη μηχανή και στη συνέχεια είτε open <όνομα_άλλης_μηχανής> για να συνδεθούμε με μια άλλη μηχανή είτε bye για να βγούμε από το περιβάλλον του πελάτη FTP.



Το παράθυρο εργασίας του WS_FTP

Τα κουμπιά που βρίσκονται δεξιά από κάθε ζώνη υλοποιούν τις αντίστοιχες εντολές κειμένου του πελάτη FTP για UNIX:

ChgDir	Αλλαγή τρέχοντος καταλόγου. (Εναλλακτικά, κάνουμε double click πάνω στο όνομα του καταλόγου).
MkDir	Δημιουργία νέου κενού καταλόγου.
RmDir	Διαγραφή τρέχοντος καταλόγου.
View	Εμφάνιση περιεχομένων του επιλεγμένου αρχείου κειμένου με χρήση της εφαρμογής που προσδιορίζεται στο **Options □Program Options □Text Viewer.**

Exec	Εκτέλεση επιλεγμένου αρχείου σύμφωνα με τις συνδέσεις επέκτασης που προσδιορίζονται στο **Options □Associations**. Όταν επιλέγεται αρχείο του δίσκου της απομακρυσμένης μηχανής, πρώτα μεταφέρεται αυτόματα στο PC μας (στον προσωρινό κατάλογο των Windows) και κατόπιν εκτελείται. Η μεταφορά γίνεται σε δυαδική κατάσταση.
Rename	Μετονομασία επιλεγμένου αρχείου.
Delete	Διαγραφή επιλεγμένου αρχείου.
Refresh	Ανανέωση της πληροφορίας των παραθύρων.
DirInfo	Εμφάνιση περιεχομένων επιλεγμένου καταλόγου.

Οι εντολές του WS_FTP

Τα κουμπιά ← και → που βρίσκονται ανάμεσα στις δύο ζώνες, πραγματοποιούν τις εντολές **get** (μεταφορά αρχείου από την απομακρυσμένη μηχανή) και **put** (μεταφορά αρχείου προς την απομακρυσμένη μηχανή) αντίστοιχα. Το όνομα των μεταφερόμενων αρχείων εμφανίζεται στο πλαίσιο της απέναντι περιοχής αμέσως μόλις τελειώσει η μεταφορά.

Τα κουμπιά **ASCII**, **Binary** και **Auto** που βρίσκονται κάτω από τις δύο ζώνες καθορίζουν την **κατάσταση μεταφοράς** των αρχείων:

ASCII	Μετάβαση σε ascii κατάσταση μεταφοράς αρχείων. Τα αρχεία μεταφέρονται σαν αρχεία κειμένου.
Binary	Μετάβαση σε binary κατάσταση μεταφοράς αρχείων. Τα αρχεία μεταφέρονται σαν δυαδικά αρχεία.
Auto	Όταν είναι τσεκαρισμένο, όλα τα αρχεία μεταφέρονται σε binary κατάσταση, εκτός εάν η επέκτασή τους έχει καταχωρηθεί στο **Options → Extensions**, οπότε μεταφέρονται σε ascii κατάσταση. Η επεκτάσεις μπορεί να έχουν μήκος μέχρι 10 χαρακτήρες και να περιέχουν και τελείες, π.χ.: .TXT, .ME, INDEX,.BAT, .HTM,

	.HTML, README, .LST, κλπ.

Τα κουμπιά ASCII, Binary και Auto

Στο κάτω μέρος της οθόνης υπάρχει μια σειρά από κουμπιά που εκτελούν τις εξής βασικές λειτουργίες:

Connect/Close	Σύνδεση / αποσύνδεση με την απομακρυσμένη μηχανή.
Cancel	Ακύρωση σύνδεσης ή μεταφοράς αρχείων.
LogWnd	Εμφάνιση παραθύρου κατάστασης (συνομιλία πελάτη-εξυπηρετητή).
Help	Εμφάνιση της βοήθειας.
Options	Εμφάνιση επιλογών παραμέτρων του προγράμματος.
Exit	Έξοδος από το πρόγραμμα.

Κουμπιά στο κάτω μέρος του του WS_FTP

Πάνω από τη σειρά αυτή, εμφανίζονται δύο γραμμές κατάστασης. Πατώντας το κουμπί **LogWnd**, εμφανίζεται ένα παράθυρο με περισσότερες γραμμές κατάστασης.

2.3 Συμπεράσματα

Σε αυτό το κεφάλαιο αναφερθήκαμε στους πελάτες FTP, στις κυριότερες εντολές του και στην διαδικασία μεταφοράς αρχείων από ένα FTP server τόσο από περιβάλλον γραμμής εργαλείων όσο και μέσω εφαρμογών. Στο επόμενο κεφάλαιο θα αναφερθούμε στην αρχιτεκτονική του Διαδικτύου και στα Πρωτόκολλα λειτουργίας του. Θα παρουσιάσουμε το μοντέλο αναφοράς OSI σε σχέση με τα επίπεδα του Διαδικτύου καθώς και την αρχιτεκτονική και τις λειτουργίες του μοντέλου πελάτης διακομιστής (client – server) στην οποία βασίζεται και η λειτουργία του FTP.

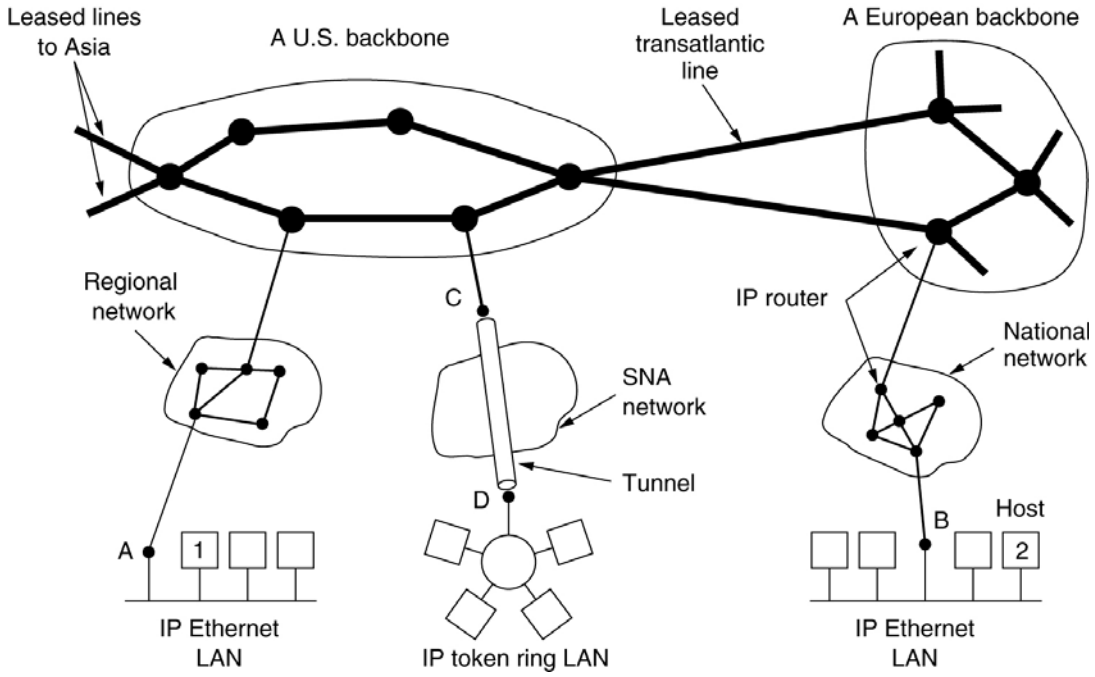
3. ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΔΙΑΔΙΚΤΥΟΥ – ΠΡΩΤΟΚΟΛΛΑ

3.1 Διαδίκτυο (Internet)

Το Internet, ένα από τα πιο συναρπαστικά και συνάμα ουσιαστικά δημιουργήματα του ανθρώπινου νου, δίκαια θεωρείται από πολλούς ως ένα σύγχρονο κουτί της Πανδώρας, που ανοίγοντας το, ξεπετάχτηκε ένας θαυμαστός κόσμος που μόλις πριν από λίγα χρόνια η ύπαρξη του ήταν αδιανόητη. Το μόνο πράγμα που χρειάζεται να έχει για αυτή την συναρπαστική περιπλάνηση, είναι μόνο ένας καλός υπολογιστής, εξοπλισμένος με ένα modem ή μια κάρτα δικτύου, καθώς και το κατάλληλο λογισμικό, που θα του επιτρέψει να επικοινωνήσει με τον έξω κόσμο.

Τι είναι όμως το Internet; Αν και δεν υπάρχει ίσως κάποιος γενικός αποδεκτός ορισμός, το Internet ορίζεται ως το μεγαλύτερο δίκτυο υπολογιστών και διασυνδεδεμένων δικτύων (LANs και WANs) του πλανήτη μας. Εάν μάλιστα θελήσουμε να ακριβολογήσουμε, το Internet δεν είναι ένα δίκτυο αλλά ένα διαδίκτυο, δηλαδή ένα δίκτυο που αποτελείται από άλλα δίκτυα. Έτσι κάθε χρήστης, οποιουδήποτε υπολογιστή και οποιουδήποτε συνδεδεμένου δικτύου, μπορεί να επικοινωνήσει και να μοιραστεί πληροφορίες, γνώσεις, και γενικά κάθε είδους δεδομένα, με οποιονδήποτε άλλο χρήστη, σε ένα από τα άλλα συνδεδεμένα δίκτυα.

Η εξάπλωση που έχει γνωρίσει το Internet τα τελευταία χρόνια, δεν έχει ιστορικό προηγούμενο. Ο αριθμός των υπολογιστών που συνδέονται με αυτό αυξάνεται με ρυθμό γεωμετρικής προόδου και οι πάσης φύσεως χρήστες είναι κάθε είδους, από καθηγητές, ερευνητές και επιστήμονες μέχρι επιχειρηματίες, τεχνικοί, ή ακόμα και μικρά παιδιά. Μέσω του Internet μπορεί να πραγματοποιηθεί κάθε είδους δραστηριότητα, από τη δημοσίευση επιστημονικών εργασιών και ερευνητικών αποτελεσμάτων, μέχρι τη διεξαγωγή εμπορικών συναλλαγών και ηλεκτρονικού εμπορίου. Μια σχηματική αναπαράσταση του Internet μπορούμε να δούμε στην παρακάτω εικόνα.



Σχηματική αναπαράσταση του Internet

Η ευρεία χρήση του διαδικτύου από δισεκατομμύρια χρήστες σε όλον τον κόσμο, κατέστησε επιτακτική την ανάγκη δημιουργίας κάποιων υπηρεσιών, οι οποίες θα διευκόλυναν τους χρήστες στο έργο τους, εξοικονομώντας με τον τρόπο αυτό χρόνο και χρήμα. Πράγματι, οι υπηρεσίες αυτές, που αναπτύχθηκαν σταδιακά και με την πάροδο του χρόνου, έχουν δώσει τη δυνατότητα σε κάθε χρήστη του δικτύου να εργασθεί με αυτό με έναν απλό και ταυτόχρονα αποδοτικό τρόπο. Στην συνέχεια παρατίθενται μερικές από τις κυριότερες υπηρεσίες του Internet που μια από αυτές είναι και η μεταφορά αρχείων μέσω FTP :

- Ηλεκτρονικό Ταχυδρομείο (e-mail)
- Πρωτόκολλο μεταφοράς αρχείων (FTP)
- Πρόσβαση σε απομακρυσμένο υπολογιστή (telnet)
- Ηλεκτρονικοί πίνακες ανακοινώσεων (USENET)
- Αναζήτηση αρχείων (Archie και Gopher)
- Παγκόσμιος Ιστός (World Wide Web)
- Ηλεκτρονική συνδιάσκεψη (IRC)
- Αναζήτηση χρηστών (Finger)

3.2 Αρχιτεκτονικές Δικτύων

Τα μοντέρνα δίκτυα υπολογιστών έχουν σχεδιαστεί μ' έναν υψηλό βαθμό δόμησης. Για να ελαττώσουν την πολυπλοκότητα της σχεδίασης, τα περισσότερα δίκτυα έχουν οργανωθεί σε σειρές από στρώματα ή επίπεδα (layers ή levels), που το καθένα χτίζεται πάνω στο προηγούμενό του. Ο αριθμός των επιπέδων, τα ονόματά τους, τα περιεχόμενά τους και η λειτουργία του καθενός διαφέρουν από δίκτυο σε δίκτυο. Σε όλα όμως τα δίκτυα ο σκοπός κάθε επιπέδου είναι να προσφέρει συγκεκριμένες υπηρεσίες στα υψηλότερα επίπεδα, απομονώνοντας αυτά τα επίπεδα από τις λεπτομέρειες σχετικά με το πως πραγματικά υλοποιούνται οι παρεχόμενες υπηρεσίες.

Το επίπεδο n μιας μηχανής επικοινωνεί με το επίπεδο n μιας άλλης μηχανής. Οι κανόνες και οι συνθήκες που χρησιμοποιούνται σ'αυτή την επικοινωνία είναι γνωστές ως το πρωτόκολλο του επιπέδου n (layer n protocol). Οι οντότητες που περιλαμβάνονται στα αντίστοιχα επίπεδα σε διαφορετικά μηχανήματα ονομάζονται ομότιμες διεργασίες (peer processes). Με άλλα λόγια, οι ομότιμες διεργασίες είναι αυτές που επικοινωνούν χρησιμοποιώντας το πρωτόκολλο. Ανάμεσα σε κάθε ζεύγος γειτονικών επιπέδων υπάρχει μια διασύνδεση (interface). Η διασύνδεση αυτή καθορίζει ποιες πρωτογενείς λειτουργίες και υπηρεσίες προσφέρει ένα επίπεδο στο επίπεδο πάνω από αυτό. Το σύνολο των επιπέδων και πρωτοκόλλων ονομάζεται αρχιτεκτονική δικτύου (network architecture).

3.3 Το Μοντέλο Αναφοράς OSI

Το **μοντέλο αναφοράς OSI (Open System Interconnection – Διασύνδεση Ανοιχτών Συστημάτων)** αναπτύχθηκε από τον Διεθνή Οργανισμό Τυποποίηση (ISO – International Standards Organization) και ασχολείται με συνδέσεις ανοιχτών συστημάτων (αυτά τα οποία είναι ανοιχτά για επικοινωνία με άλλα συστήματα).

Το μοντέλο OSI έχει 7 επίπεδα τα οποία φαίνονται στο παρακάτω σχήμα:

7. Επίπεδο Εφαρμογής (Application Layer)
6. Επίπεδο Παρουσίασης (Presentation Layer)

5. Επίπεδο Συνόδου (Session Layer)
4. Επίπεδο Μεταφοράς (Transport Layer)
3. Επίπεδο Δικτύου (Network Layer)
2. Επίπεδο Σύνδεσης Δεδομένων (Data Link Layer)
1. Φυσικό Επίπεδο (Physical Layer)

Το Μοντέλο Αναφοράς OSI

Το **φυσικό επίπεδο (physical layer)** ασχολείται με τη μετάδοση ακατέργαστων bits σε ένα κανάλι επικοινωνίας.

Η κύρια αποστολή του **επιπέδου σύνδεσης δεδομένων (data link layer)** είναι να μετασχηματίσει το ακατέργαστο μέσο μετάδοσης σε μια γραμμή που εμφανίζεται ελεύθερη από σφάλματα μετάδοσης στο επίπεδο δικτύου. Μερικές από τις βασικές λειτουργίες αυτού του επιπέδου είναι η επιβεβαίωση μετάδοσης και λήψης καθώς και η ανίχνευση λαθών.

Το **επίπεδο δικτύου (network layer)** ασχολείται με τον έλεγχο της λειτουργίας του υποδικτύου. Παρέχει σύνδεση και δρομολόγηση (routing) ανάμεσα σε δύο κόμβους ενός δικτύου.

Η βασική λειτουργία του **επιπέδου μεταφοράς (transport layer)** είναι η αποδοχή δεδομένων από το επίπεδο συνόδου, η διάσπαση αυτών σε μικρότερες μονάδες αν χρειαστεί, η μεταφορά τους στο επίπεδο δικτύου και η διασφάλιση ότι όλα τα τμήματα φτάνουν σωστά στην άλλη πλευρά.

Το **επίπεδο συνόδου (session layer)** επιτρέπει στους χρήστες διαφορετικών μηχανημάτων να εγκαθιστούν συνόδους (sessions) μεταξύ τους. Μία σύνοδος επιτρέπει μια συνήθη μεταφορά δεδομένων, όπως και το επίπεδο μεταφοράς, αλλά παρέχει και μερικές πρόσθετες υπηρεσίες που είναι χρήσιμες σε πολλές εφαρμογές. Μια σύνοδος, μπορεί να χρησιμοποιηθεί για να επιτρέψει τη σύνδεση ενός χρήστη σ'ένα απομακρυσμένο σύστημα καταμερισμού χρόνου (time-sharing) ή να μεταφέρει ένα αρχείο μεταξύ δύο μηχανών.

Το **επίπεδο παρουσίασης (presentation layer)** εκτελεί συγκεκριμένες λειτουργίες οι οποίες ζητούνται αρκετά συχνά από τους χρήστες, για να

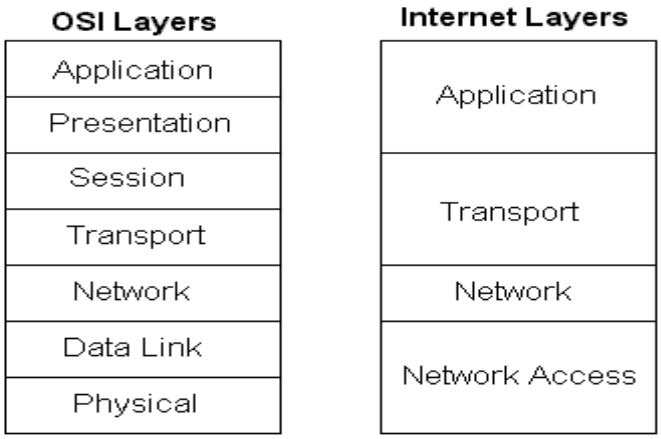
εξασφαλίζουν την εύρεση μιας γενικής λύσης γι' αυτούς, ώστε να μην αφήνεται κάθε χρήστης να λύνει τα προβλήματα μόνος του. Συγκεκριμένα, ενώ όλα τα κατώτερα επίπεδα ενδιαφέρονται μόνο για την αξιόπιστη μεταφορά bits από το ένα μέρος στο άλλο, το επίπεδο παρουσίασης ενδιαφέρεται για το συντακτικό και τη σημασιολογία των πληροφοριών που μεταδίδονται.

Το **επίπεδο εφαρμογής (application layer)** χρησιμοποιεί τις υπηρεσίες του επιπέδου παρουσίασης για την εκτέλεση εφαρμογών των χρηστών. Μερικές χαρακτηριστικές λειτουργίες αυτού του επιπέδου είναι η μεταφορά αρχείων, η εισαγωγή εργασιών από απόσταση, η εμφάνιση καταλόγων (directory) αρχείων, το ηλεκτρονικό ταχυδρομείο.

Σήμερα λίγοι είναι οι υπολογιστές και τα δίκτυα που είναι τελείως συμβατά με όλα τα επίπεδα του μοντέλου αναφοράς OSI.

3.4 Τα Επίπεδα του Διαδικτύου

Ακολούθως θα αναφερθούμε πιο αναλυτικά στα επίπεδα φυσικής πρόσβασης, δικτύου, μεταφοράς και εφαρμογής όπως αυτά φαίνονται στο παρακάτω σχήμα σε σχέση με τα επίπεδα μοντέλου αναφοράς OSI.



Τα επίπεδα του OSI σε σχέση με τα επίπεδα του Διαδικτύου

3.4.1 Επίπεδο Φυσικής Πρόσβασης

Σε αυτό το επίπεδο ανήκουν οι εκάστοτε δικτυακές τεχνολογίες όπως Ethernet, FDDI και Token Ring. Το επίπεδο ασχολείται με την μετάδοση των bit

μέσω διάφορων μέσων και αναλυτικότερα με τα ηλεκτρικά, μηχανικά και λειτουργικά χαρακτηριστικά των διασυνδέσεων. Επίσης ασχολείται με τον τρόπο που γίνεται η πρόσβαση στο φυσικό μέσον και καθορίζει τους κανόνες επικοινωνίας στο τοπικό δίκτυο.

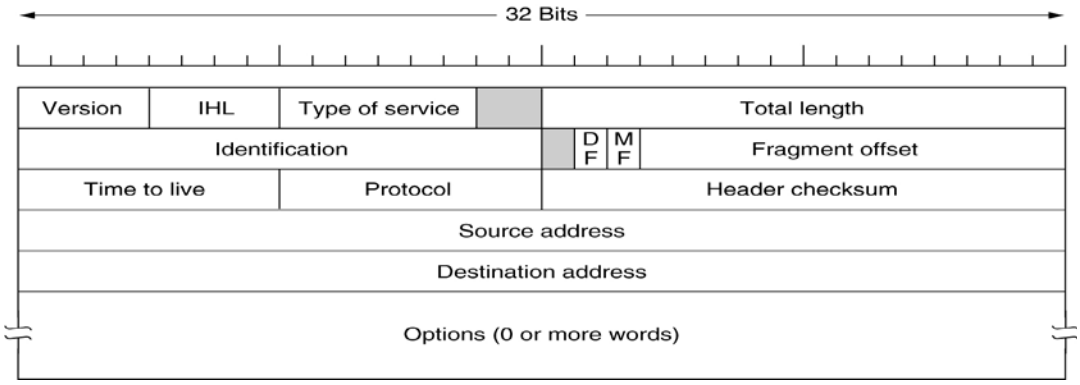
3.4.2 Επίπεδο Δικτύου (IP πρωτόκολλο)

Η μετάδοση στο IP (Internet Protocol) γίνεται με την τεχνική των datagrams. Το κάθε datagram (πακέτο) φθάνει στον παραλήπτη διασχίζοντας ένα η περισσότερα διασυνδεόμενα IP δίκτυα, χωρίς να εξαρτάται από άλλα προηγούμενα ή επόμενα πακέτα.

Το IP, σαν πρωτόκολλο του τρίτου επιπέδου, δεν ασχολείται με τις φυσικές συνδέσεις ή τον έλεγχο των ενδιάμεσων ζεύξεων μεταξύ των κόμβων του δικτύου. Αυτά είναι αρμοδιότητα των χαμηλότερων επιπέδων. Στην ουσία ασχολείται με την διευθυνσιοδότητη, τον τεμαχισμό και την επανασυγκόληση των πακέτων. Το πρωτόκολλο IP δεν είναι αξιόπιστης μεταφοράς (reliable transfer) καθώς δεν εξασφαλίζει την σίγουρη παράδοση των πακέτων με τεχνικές επανεκπομπής και έλεγχο ροής. Επιπλέον είναι connectionless γιατί δεν απαιτεί την αποκατάσταση σύνδεσης μεταξύ των δύο σημείων πριν την ανταλλαγή δεδομένων. Τα IP πακέτα μπορεί να ακολουθήσουν διαφορετικές διαδρομές και να φθάσουν με λανθασμένη σειρά στον αποδέκτη. Προβλήματα σαν αυτό αναλαμβάνουν να διορθώσουν το πρωτόκολλο TCP του ανωτέρου επιπέδου.

Δρομολόγηση

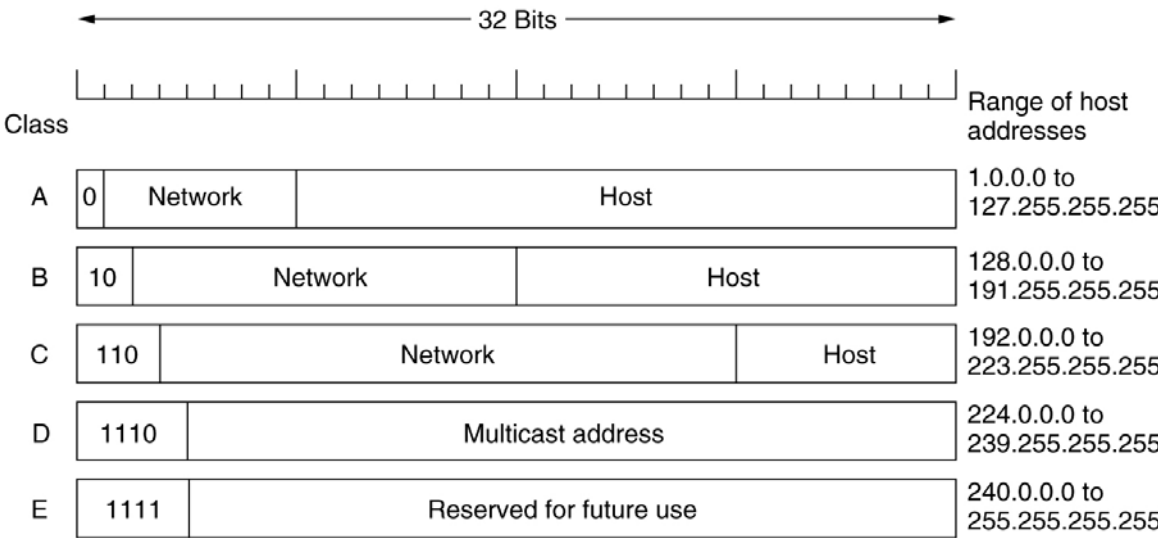
Τα IP πακέτα, όπως αυτά παρουσιάζονται στο παρακάτω σχήμα, διασχίζουν το Διαδίκτυο από δρομολογητή σε δρομολογητή με κατεύθυνση τον τελικό αποδέκτη. Κάθε δρομολογητής διατηρεί πίνακες δρομολόγησης βάσει των οποίων το κάθε πακέτο αποστέλλεται στον επόμενο δρομολογητή που θα αναλάβει να το προωθήσει προς τον αποδέκτη του. Ο καθορισμός του επόμενου δρομολογητή γίνεται με την ανάγνωση της IP διευθύνσεως του παραλήπτη. Ανάλογα με το δίκτυο στο οποίο βρίσκεται ο παραλήπτης, επιλέγεται από τον πίνακα δρομολόγησης διαδεχόμενος router.



Όταν ένα πακέτο φθάσει σε ένα δρομολογητή αποθηκεύεται προσωρινά σε μία ουρά (queue). Τα IP πακέτα επεξεργάζονται με την σειρά άφιξης τους. Κατά την επεξεργασίας τους, διαβάζεται η διεύθυνση του τελικού παραλήπτη. Εάν υπάρχει μποτιλιάρισμα στο δίκτυο, τότε η ουρά των πακέτων μέσα στον δρομολογητή μπορεί να γίνει μεγάλη, αυξάνοντας έτσι τις καθυστερήσεις μετάδοσης. Σε περίπτωση που η ουρά γίνει τόσο μεγάλη που να ξεπερνά τις χωρητικές δυνατότητες του δρομολογητή, τα πακέτα απορρίπτονται και χάνονται.

Διευθυνσιοδότηση

Καθ' ότι το Διαδίκτυο είναι μια εικονική κατασκευή που εφαρμόζεται λογισμικά, οι σχεδιαστές του είναι ελεύθεροι να διαλέξουν σχήμα διευθυνσιοδότησης που να μην σχετίζεται με κανένα υπάρχον δικτυακό υλικό. Το IP λειτουργεί με βάσει ένα νέο σετ διευθύνσεων που είναι ανεξάρτητο από τις υποκείμενες δικτυακές διευθύνσεις των υπολογιστών. Οι νέες αυτές διευθύνσεις καλούνται Internet Addresses ή IP διευθύνσεις.



Οι IP διευθύνσεις, όπως φαίνεται στο παραπάνω σχήμα, είναι φτιαγμένες έτσι ώστε να διευκολύνουν την δρομολόγηση. Κάθε IP πακέτο περιέχει την διεύθυνση του αποστολέα και του παραλήπτη, κάθε μια από τις οποίες έχει μήκος 32 bits. Μια IP διεύθυνση αποτελείται από δύο μέρη: το netid και το hostid. Το netid προσδιορίζει το δίκτυο στο οποίο βρίσκεται ο υπολογιστής, ενώ το hostid προσδιορίζει τον υπολογιστή. Ανάλογα με το μήκος της διευθύνσεως που αφιερώνεται σε κάθε τμήμα αυτής, οι διευθύνσεις διακρίνονται σε τρεις κλάσεις δικτύων:

Κλάση Α: 8 bit διεύθυνση δικτύου / 24 bit διεύθυνση υπολογιστή

Κλάση Β: 16 bit διεύθυνση δικτύου / 16 bit διεύθυνση υπολογιστή

Κλάση Γ: 24 bit διεύθυνση δικτύου / 8 bit διεύθυνση υπολογιστή

Επειδή οι IP διευθύνσεις κωδικοποιούν ένα δίκτυο αλλά και έναν υπολογιστή σε αυτό το δίκτυο, δεν καθορίζουν έναν συγκεκριμένο υπολογιστή, αλλά μία σύνδεση σε ένα δίκτυο.

Στην πράξη η απομνημόνευση των 32 bits είναι εξαιρετικά δύσκολη. Γι' αυτό έχει επινοηθεί η αναπαράσταση της διεύθυνσης με την χρήση δεκαδικών αριθμών. Η διεύθυνση διαχωρίζεται με τελείες σε τέσσερα πεδία των οκτώ bit. Κάθε πεδίο μετατρέπεται στο ισοδύναμο δεκαδικό αριθμό.

Internet Control Message Protocol (ICMP)

Ένα άλλο πρωτόκολλο αυτού του επιπέδου είναι το Internet Control Message Protocol (ICMP). Το ICMP δρα βοηθητικά, παράγοντας και διαχειρίζοντας μηνύματα λάθους για το πακέτο πρωτοκόλλων TCP/IP. Επιτρέπει στους δρομολογητές να επιστρέφουν μηνύματα λάθους σε άλλους δρομολογητές ή υπολογιστές. Για παράδειγμα, εάν ζητηθεί η σύνδεση με υπολογιστή που δεν υπάρχει ή δεν είναι διαθέσιμος προς το παρών, το ICMP σε κάποιον router θα επιστρέψει στον αποστολέα του αρχικού μηνύματος ένα μήνυμα με περιεχόμενο "host unreachable". Επιπλέον, το ICMP μπορεί να χρησιμοποιηθεί για την συλλογή πληροφοριών για ένα δίκτυο και για σκοπούς debugging.

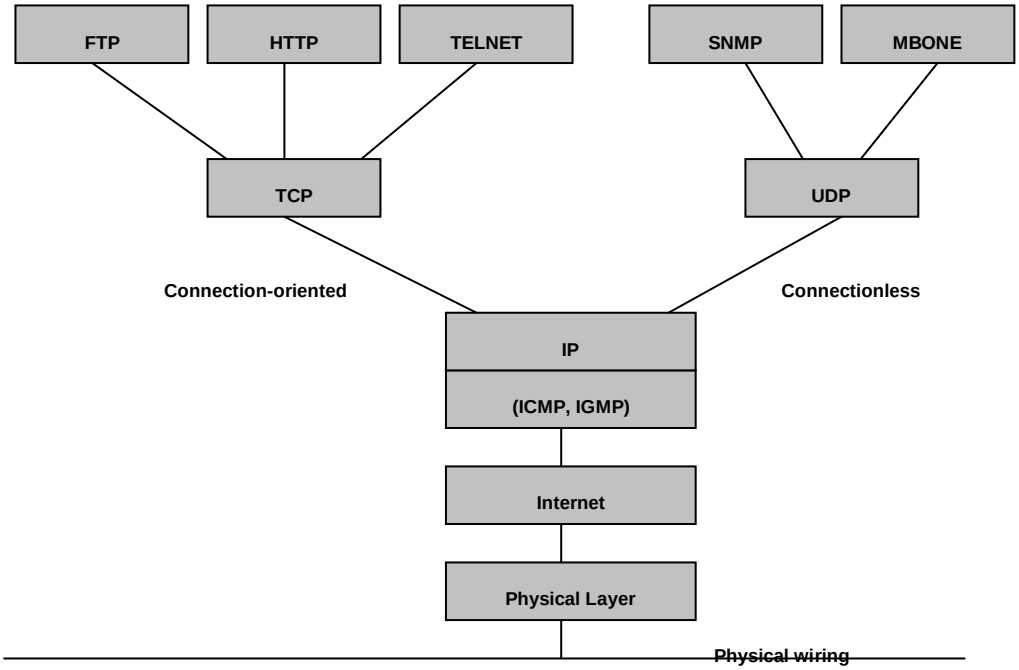
3.4.3 Επίπεδο Μεταφοράς

Transmission Control Protocol (TCP)

Το TCP (Transmission Control Protocol) είναι ένα connection-oriented πρωτόκολλο του επιπέδου μεταφοράς, που είναι υπεύθυνο για την εξασφάλιση αξιόπιστης επικοινωνίας μεταξύ δυο ακραίων υπολογιστών, διαμέσου ενός ή περισσοτέρων δικτύων.

Σε αυτό το επίπεδο επιτυγχάνεται η από άκρου σε άκρου επικοινωνία μεταξύ των χρηστών. Στα χαμηλότερα επίπεδα γινόταν εφικτή η επικοινωνία ενός συστήματος με τον πλησιέστερο δρομολογητή, ώστε διαδοχικές τέτοιες επικοινωνίες να εξασφαλίζουν την σύνδεση των δύο άκρων.

Όπως προαναφέραμε, το IP είναι connectionless πρωτόκολλο. Τις ελλείψεις του IP αναλαμβάνει να καλύψει το TCP: εξασφαλίζει την παράδοση των πακέτων με την σωστή σειρά, ελέγχει την ροή των δεδομένων, διασφαλίζει την αξιοπιστία της σύνδεσης καθώς επίσης ξεκινά και τερματίζει τις συνδέσεις μεταξύ δύο εφαρμογών μέσα στο δίκτυο. Πρωτόκολλα εφαρμογών όπως το FTP για την μεταφορά τον αρχείων και το SMTP για το ηλεκτρονικό ταχυδρομείο, στηρίζονται στις υπηρεσίες που προσφέρει το TCP όπως φαίνεται και στο παρακάτω σχήμα.



Η λογική δομή της οικογένειας πρωτοκόλλων διαδικτύου

Το TCP παραλαμβάνει δεδομένα από την εφαρμογή, τα τεμαχίζει σε τμήματα που δεν υπερβαίνουν τα 64 Kbyte και τα στέλνει στον ανταποκριτή του. Κατά την παραλαβή των πακέτων, ο αποδέκτης επιστρέφει μήνυμα που επιβεβαιώνει την παραλαβή τους. Σε περίπτωση που ο αποστολέας δεν λάβει επιβεβαιωτικό μήνυμα μέσα σε συγκεκριμένο χρονικό διάστημα από την αποστολή του πακέτου, συμπεραίνει ότι το πακέτο δεν παραλήφθηκε και το ξαναστέλνει. Τα πακέτα στέλνονται υπό την μορφή stream, εγκαθιστώντας έτσι μια εικονική σύνδεση μεταξύ των δύο άκρων.

Το TCP έχει τις εξής λειτουργίες:

- Λογική σύνδεση και αποσύνδεση.
- Μετάδοση δεδομένων.
- Έλεγχο ροής.
- Πολύπλεξη εφαρμογών.
- Αξιοπιστία μετάδοσης.
- Υποστήριξη *full duplex* επικοινωνίας.
- Προτεραιότητα και ασφάλεια.

Προκειμένου να επικοινωνήσει το TCP με το ανώτερο επίπεδο εφαρμογών χρησιμοποιείται η έννοια της πόρτας (port). Πόρτα είναι ένας ακέραιος που βρίσκεται στο πεδίο της επικεφαλίδας του πακέτου TCP και της οποίας η τιμή αντιπροσωπεύει την εφαρμογή που χρησιμοποιεί την σύνδεση.

Ο συνδυασμός της διεύθυνσης IP με τον αριθμό της πόρτας του TCP ονομάζεται socket και χαρακτηρίζει με μοναδικό τρόπο την συγκεκριμένη εφαρμογή που τρέχει σε ένα σύστημα. Ένα ζευγάρι από socket χαρακτηρίζει μοναδικά την επικοινωνία μεταξύ των δύο εφαρμογών σε διαφορετικά συστήματα υπολογιστών.

User Datagram Protocol (UDP)

Το **UDP** είναι πρωτόκολλο του επιπέδου μεταφοράς όπως το TCP με την διαφορά ότι είναι connectionless. Είναι εξαιρετικά απλό στην υλοποίηση του, άλλα σε αντίθεση με το TCP, δεν προσφέρει μηχανισμούς επανεκπομπής, αξιοπιστίας και έλεγχου ροής. Μερικές από τις εφαρμογές που στηρίζονται στο UDP είναι η NFS (Network File System) για διαχείριση αρχείων δικτύου και η TFTP (Trivial File

Transfer Protocol) για την μεταφορά αρχείων. Οι ίδιες οι εφαρμογές πρέπει να φροντίζουν για τις λειτουργίες που δεν είναι σε θέση να προσφέρει το UDP.

3.4.4 Επίπεδο Εφαρμογών

Σε αυτό το επίπεδο ανήκουν οι υπηρεσίες του Διαδικτύου. Θα περιγράψουμε τις σημαντικότερες και τις πιο συχνά χρησιμοποιούμενες.

Telnet

Το **Telnet** (ή remote login) είναι μια από τις βασικότερες υπηρεσίες του Διαδικτύου που επιτρέπει σε κάποιον χρήστη να έχει πρόσβαση τερματικού σε ένα μακρινό server. Το Telnet λειτουργεί μεταφέροντας τις εντολές που πληκτρολογεί ο χρήστης στον υπολογιστή του στον απομακρυσμένο υπολογιστή με τον οποίο συνδέεται. Παρ' όλο που στην πραγματικότητα ο χρήστης "μιλάει" με τον υπολογιστή του, το πρόγραμμα καταφέρνει και δίνει την ψευδαίσθηση στον χρήστη ότι επικοινωνεί με τον απομακρυσμένο υπολογιστή.

File Transfer Protocol (FTP)

Το **FTP** ήταν η πρώτη υπηρεσία για την ανάκτηση και μεταφορά πληροφορίας και αρχείων που χρησιμοποιήθηκε στο Διαδίκτυο. Η βασική λειτουργία του είναι η αξιόπιστη μεταφορά αρχείων από υπολογιστή σε υπολογιστή και επιτρέπει στους χρήστες να στήνουν μια σύνδεση ελέγχου μεταξύ του FTP client και του FTP server. Η σύνδεση αυτή τους επιτρέπει να ψάχνουν στους καταλόγους του server και να μεταφέρουν τα αρχεία που επιθυμούν από τον server προς τον δικό τους υπολογιστή. Για την μεταφορά των αρχείων δημιουργείται αυτόματα από ο FTP μια νέα ανεξάρτητη σύνδεση.

Domain Name Service (DNS)

Η υπηρεσία **DNS** χρησιμοποιείται από τους χρήστες του Διαδικτύου για την αντικατάσταση των αριθμητικών IP διευθύνσεων με εύχρηστα ονόματα (domain names). Συγκεκριμένα, το DNS προσφέρει υπηρεσίες μετάφρασης μεταξύ ονομάτων και IP διευθύνσεων. Κάθε υπολογιστής και δρομολογητής στο Διαδίκτυο διαθέτει ένα όνομα. Η ονοματολογία του Διαδικτύου έχει σαν χαρακτηριστικό την ιεράρχηση των ονομάτων. Κατατάσσονται ανάλογα με το εύρος του δικτύου που περιγράφουν και το όνομα ενός μηχανήματος αποτελείται από τόσα επιμέρους ονόματα όσα χρειάζεται για να προσδιοριστεί πλήρως. Τα επιμέρους ονόματα δικτύων διαχωρίζονται μεταξύ

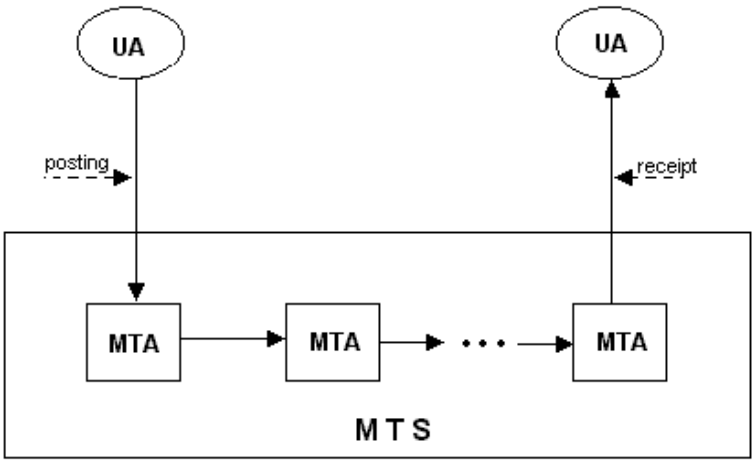
τους με τελείες. Για παράδειγμα, το όνομα saturn.lab.epmhs.gr αντιπροσωπεύει τον υπολογιστή με το όνομα saturn που βρίσκεται στο τοπικό δίκτυο lab.epmhs.gr. Το lab.epmhs.gr ανήκει με την σειρά του στο ευρύτερο δίκτυο epmhs.gr, το οποίο ανήκει στην περιοχή gr, δηλαδή στην Ελλάδα.

Σε ένα δίκτυο που εξυπηρετεί αρκετούς υπολογιστές κάτω από το ίδιο όνομα δικτύου πρέπει να λειτουργεί ένας DNS server που θα παρέχει πληροφορίες για τους υπολογιστές που ανήκουν στο δίκτυο του. Για κάθε επίπεδο αυτής της ιεράρχησης υπάρχει τουλάχιστον ένας DNS server που γνωστοποιεί το όνομα του στον server του αμέσως ανώτερου επιπέδου. Αυτό επαναλαμβάνεται έως ότου να καλυφθεί όλη ιεραρχία ονομάτων.

Η υπηρεσία του DNS χρησιμοποιείται αυτοματοποιημένα και από τις υπόλοιπες εφαρμογές του Διαδικτύου. Όποτε απευθύνεται στον DNS server ερώτημα για κάποιον υπολογιστή από οποιαδήποτε υπηρεσία, αυτός συμβουλεύεται τους πίνακες καταχωρήσεων που διαθέτει και δίνει απάντηση για την IP διεύθυνση που αντιστοιχεί στο όνομα του ζητούμενου υπολογιστή. Σε περίπτωση που ερωτηθεί για υπολογιστή για τον οποίο δεν έχει καταχώρηση, τότε παραπέμπει την αίτηση σε DNS server υψηλότερου επιπέδου.

Ηλεκτρονικό Ταχυδρομείο (E-mail)

Το **ηλεκτρονικό ταχυδρομείο** επιτρέπει την αποστολή μηνυμάτων μεταξύ των χρηστών του Διαδικτύου. Οι διευθύνσεις του ηλεκτρονικού ταχυδρομείου βασίζονται στις διευθύνσεις του Internet και έχουν την μορφή "user@domain", όπου user το όνομα του χρήστη και domain το όνομα του υπολογιστή.



Παρακάτω φαίνεται πως μεταφέρονται τα ηλεκτρονικά μηνύματα. Ο User Agent (UA) είναι το πρόγραμμα client στον υπολογιστή του χρήστη που αναλαμβάνει την διαχείριση και ανάκτηση του ταχυδρομείου. Με την βοήθεια αυτού του προγράμματος ο χρήστης γράφει τα μηνύματα του, τα στέλνει, παραλαμβάνει άλλα μηνύματα και τα διαβάζει. Ο Mail Transfer Agent (MTA) παραλαμβάνει τα μηνύματα από τον UA και τα προωθεί στον επόμενο MTA μέχρι να βρεθεί ο MTA που έχει άμεση σύνδεση με τον υπολογιστή του χρήστη. Ο τελευταίος MTA επικοινωνεί με τον UA του παραλήπτη για την παράδοση των μηνυμάτων. Το σύνολο των MTA καλείται Message Transfer System (MTS).

Η επικοινωνία από MTA σε MTA γίνεται με χρήση του πρωτοκόλλου SMTP (Simple Mail Transfer Protocol, ενώ η επικοινωνία του UA με τον MTA γίνεται με χρήση των πρωτοκόλλων POP (Post Office Protocol) και IMAP (Internet Message Access Protocol). Τα ίδια τα μηνύματα συντάσσονται με βάσει το πρωτόκολλο MIME (Multipurpose Internet Mail Extensions) ή με το RFC822.

Το παραπάνω σύστημα παράδοσης του ηλεκτρονικού ταχυδρομείου επιτρέπει το ηλεκτρονικό ταχυδρομικό του χρήστη να βρίσκεται σε κάποιον server και έτσι δεν είναι απαραίτητο να είναι εν λειτουργία ο υπολογιστή του αποδέκτη κατά την αποστολή του μηνύματος. Ο αποδέκτης θα παραλάβει τα μηνύματα του όταν ανοίξει τον υπολογιστή του και συνδεθεί με τον server (MTA).

3.5 Εισαγωγή στην Τεχνολογία Πελάτη / Διακομιστή

3.5.1 Τι είναι το μοντέλο πελάτη διακομιστή;

Γενικά, το μοντέλο πελάτη / διακομιστή (client /server) αναφέρεται σε μια βασική αλλαγή στο στυλ των υπολογιστών, την αλλαγή από τα συστήματα που βασίζονται στα μηχανήματα στα συστήματα που βασίζονται στον χρήστη.

Ειδικότερα, ένα σύστημα client-server είναι ένα σύστημα στο οποίο το δίκτυο ενώνει διάφορους υπολογιστικούς πόρους, ώστε οι clients (ή αλλιώς front end) να μπορούν να ζητούν υπηρεσίες από έναν server (ή αλλιώς back end), ο οποίος προσφέρει πληροφορίες ή επιπρόσθετη υπολογιστική ισχύ.

Με άλλα λόγια, στο μοντέλο πελάτη / διακομιστή, ο client θέτει μια αίτηση και ο server επιστρέφει μια ανταπόκριση ή κάνει μια σειρά από ενέργειες. Ο server μπορεί να ενεργοποιείται άμεσα για την αίτηση αυτή ή να προσθέτει την αίτηση σε

μια ουρά. Η άμεση ενεργοποίηση για την αίτηση μπορεί, για παράδειγμα, να σημαίνει ότι ο server υπολογίζει έναν αριθμό και τον επιστρέφει αμέσως στον client. Η τοποθέτηση της αίτησης σε μια ουρά μπορεί να σημαίνει ότι η αίτηση πρέπει να τεθεί σε αναμονή για να εξυπηρετηθεί. Ένα καλό παράδειγμα για αυτό είναι όταν εκτυπώνουμε ένα κείμενο σε ένα εκτυπωτή δικτύου. Ο server τοποθετεί την αίτηση σε μια ουρά μαζί με αιτήσεις εκτυπώσεων και από άλλους clients. Μετά επεξεργάζεται την αίτηση με βάση την σειρά προτεραιότητας, η οποία , σε αυτή την περίπτωση, καθορίζεται από τη σειρά με την οποία ο server παρέλαβε την απαίτηση.

Το client-server computing είναι πολύ σημαντικό, διότι επιτυγχάνει τα εξής:

- Αποτελεσματική χρήση της υπολογιστικής ισχύος.
- Μείωση του κόστους συντήρησης, δημιουργώντας συστήματα client-server που απαιτούν λιγότερη συντήρηση και κοστίζουν λιγότερο στην αναβάθμιση.
- Αύξηση της παραγωγικότητας, προσφέροντας στους χρήστες ξεκάθαρη πρόσβαση στις αναγκαίες πληροφορίες μέσω σταθερών και εύκολων στην χρήση διασυνδέσεων.
- Αύξηση της ευελιξίας και της δυνατότητας δημιουργίας συστημάτων που υποστηρίζουν πολλά περιβάλλοντα.

Με βάση αυτούς τους σκοπούς, οι οργανισμοί που κινούνται προς την κατεύθυνση της client-server τεχνολογίας αυξάνουν κατά πολύ την ανταγωνιστική τους θέση.

3.5.2 Το βασικό μοντέλο client-server

Η πλευρά του client πρώτα στέλνει ένα μήνυμα για να καλέσει σε ετοιμότητα τον server. Από τη στιγμή που ο client και ο server έχουν επικοινωνία μεταξύ τους, ο client μπορεί να υποβάλλει την αίτησή του.

Client: Ο client είναι ο αιτών των υπηρεσιών. Ο client δεν μπορεί παρά να είναι ένας υπολογιστής. Οι υπηρεσίες που ζητούνται από τον client μπορεί να υπάρχουν στους ίδιους σταθμούς εργασίας ή σε απομακρυσμένους σταθμούς εργασίας που συνδέονται μεταξύ τους μέσω ενός δικτύου. Ο client ξεκινάει πάντα την επικοινωνία.

Τα συστατικά του client είναι πολύ απλά. Μια client μηχανή πρέπει να μπορεί να κάνει τα ακόλουθα:

- Να τρέχει το λογισμικό των γραφικών διεπαφών χρηστών (GUIs).

- Να δημιουργεί τις αιτήσεις για πληροφορίες και να τις στέλνει στον server.
- Να αποθηκεύει τις επιστρεφόμενες πληροφορίες.

Αυτές οι αιτήσεις καθορίζουν πόση μνήμη χρειάζεται, ποια ταχύτητα επεξεργασίας θα μπορούσε να βελτιώσει τον χρόνο ανταπόκρισης, και πόση χωρητικότητα αποθήκευσης απαιτείται.

Server: Ο server απαντάει στις αιτήσεις που γίνονται από τους clients. Ένας client μπορεί να ενεργεί ως server εάν λαμβάνει και επεξεργάζεται αιτήσεις όπως ακριβώς και τις στέλνει (για παράδειγμα, ένας σταθμός εργασίας που χρησιμοποιείται και ως server εκτυπώσεων από άλλους). Οι server δεν ξεκινάνε τις επικοινωνίες -περιμένουν τις αιτήσεις των clients.

Επιστρέφοντας στο παράδειγμα του server εκτυπώσεων ενός δικτύου, ο client ζητάει από τον server να εκτυπώσει ένα κείμενο σε έναν συγκεκριμένο εκτυπωτή και ο server προσθέτει την εκτύπωση σε μια ουρά και ενημερώνει τον client όταν το κείμενο εκτυπωθεί επιτυχημένα. Η διαδικασία του client μπορεί να ανήκει φυσικά στον ίδιο σταθμό εργασίας με την διαδικασία του server. Στο παράδειγμα εδώ, μια εντολή εκτύπωσης μπορεί να εκδίδεται στον server του σταθμού εργασίας του δικτύου, χρησιμοποιώντας την διαδικασία του server εκτύπωσε αυτόν τον σταθμό εργασίας.

Τα συστατικά του server είναι πολύ απλά. Μια server μηχανή πρέπει να μπορεί να κάνει τα ακόλουθα :

- Να αποθηκεύει, να ανακτά και να προστατεύει πληροφορίες.
- Να επιθεωρεί τις αιτήσεις των clients.
- Να δημιουργεί εφαρμογές διαχείρισης πληροφοριών, όπως δημιουργία αντιγράφων, ασφάλεια κτλ.
- Να διαχειρίζεται πληροφορίες.

Δίκτυα:Τα δίκτυα είναι τα πιο άγνωστα συστατικά στην εξίσωση των client-server. Γενικά οι άνθρωποι δεν ξέρουν πολλά για το πώς λειτουργούν τα δίκτυα στα συστήματα client-server, διότι τα συστήματα αυτά είναι σχεδιασμένα για να κάνουν τα δίκτυα διάφανα στον χρήστη. Επιπλέον, τα δίκτυα πρέπει να είναι αξιόπιστα. Πρέπει να μπορούν να υποστηρίζουν την επικοινωνία, να ελέγχουν σφάλματα και να ξεπερνούν αμέσως τις αποτυχίες.

Τα δίκτυα ελέγχονται από το λογισμικό λειτουργικών συστημάτων και διαχείρισης για να ελέγχουν τις υπηρεσίες επικοινωνίας του server και να

προστατεύουν τα προγράμματα του client και του server από το να έχουν άμεση σύνδεση μεταξύ τους. Το λογισμικό διαχείρισης εστιάζεται στη παροχή αξιόπιστων υπηρεσιών, στην ελαχιστοποίηση των προβλημάτων στο δίκτυο και στην ελαχιστοποίηση των χρόνων «πτώσης» του δικτύου.

Η τεχνολογία των υπολογιστών αναπτύχθηκε βαθμιαία, με τέτοιο τρόπο που κάθε καινούργια αρχιτεκτονική έπαιρνε τα πλεονεκτήματα από τις τεχνικές που ήδη υπήρχαν, ώστε να εκμεταλλεύεται όλες τις δυνατότητες των υπολογιστών. Σήμερα οι υπολογιστές είναι μικρότεροι, γρηγορότεροι και φθηνότεροι από ότι παλιότερα. Σαν αποτέλεσμα, η γενική κατεύθυνση είναι η διανομή της επεξεργασίας της πληροφορίας αλλά και της ίδιας της πληροφορίας σε ένα πλήθος αυτών των νέων υπολογιστών.

Ο όρος αρχιτεκτονική συνήθως χρησιμοποιείται για να περιγράφει συστήματα διαχείρισης βάσεων δεδομένων, λειτουργικά συστήματα και άλλους υπολογιστικούς μηχανισμούς λογισμικού και υλικού. Οι αρχιτεκτονικές περιγράφουν πως οι συσκευές και τα λογισμικά πακέτα ταιριάζουν για να φτιάξουν είναι εύκολο στην χρήση και στην διαχείριση σύνολο.

Η κλασσική αρχιτεκτονική αποτελείται από έναν υπολογιστή μεγάλης ισχύος, (που παίζει το ρόλο του οικοδεσπότη) με ένα ή περισσότερα απλά τερματικά. Οι εφαρμογές ελέγχονται και διανέμονται από τον υπολογιστή-«οικοδεσπότη». Σε αυτόν πραγματοποιούνται όλες οι διαχειρίσεις πληροφοριών, η λογική των εφαρμογών και η μορφοποίηση της εμφάνισης τους. Οι χρήστες αλληλεπιδρούν με το κεντρικό σύστημα μέσω των τερματικών, τα οποία εμφανίζουν μόνο πληροφορίες. Αυτή είναι η πιο συνηθισμένη αρχιτεκτονική σήμερα.

Ένα καλά οργανωμένο σύστημα που χρησιμοποιεί αυτήν την κλασσική αρχιτεκτονική προσφέρει τις ακόλουθες δυνατότητες:

- Ένα υψηλό επίπεδο αξιοπιστίας .
- Κεντρικό έλεγχο και κεντρική διαχείριση των πληροφοριών.
- Ισχυρή διαχείριση των πληροφοριών και δυνατότητα αποθηκεύσεων .

Πάντως, οι κλασικές εφαρμογές περιορίζουν την ευελιξία των τελικών χρηστών. Η διασύνδεση των χρηστών δεν είναι γραφική, κάτι που κάνει το σύστημα δυσκολότερο στη χρήση και σημαίνει ότι ο χρήστης πρέπει να μάθει πως να χρησιμοποιήσει την γλώσσα του οικοδεσπότη. Επίσης, οι εφαρμογές εξαρτώνται από μια πλατφόρμα, που σημαίνει ότι εάν κάτι συμβεί στον υπολογιστή-«οικοδεσπότη», ο

χρήστης δεν μπορεί να χρησιμοποιήσει το σύστημα, έως ότου το σύστημα αρχίσει να επαναλειτουργεί.

Στην client-server αρχιτεκτονική, η client εφαρμογή τρέχει σε έναν πλήρη σταθμό εργασίας. Αυτός ο σταθμός μπορεί να είναι ένας προσωπικός υπολογιστής, ένας UNIX σταθμός εργασίας ή ένας Mac. Η client εφαρμογή βασίζεται στις υπηρεσίες που προσφέρει ο server και επικοινωνούν μέσω πρωτοκόλλων, όπως το πρωτόκολλο του Internet (TCP/IP) το οποίο έχει περιγραφεί προηγουμένως.

Το περιβάλλον του client-server έχει πολλά πλεονεκτήματα σε σχέση με τις κλασσικές αρχιτεκτονικές. Η διαχείριση της διασύνδεσης των χρηστών και άλλες επεξεργασίες είναι αποφορτισμένα από τον «οικοδεσπότη», ενώ ο server ακόμη προσφέρει συγκεντρωμένο έλεγχο των κοινών πόρων. Επειδή ο client επικοινωνεί με τον server μέσω ενός καθορισμένου συστήματος διασύνδεσης, δεν χρειάζεται να γνωρίζει που ανήκει ο server ή πως ενεργεί. Ο σταθμός εργασίας τρέχει την εφαρμογή και εμφανίζει τις πληροφορίες στον χρήστη. Μόνο όταν ο client προσπελάζει πληροφορίες, τότε εγκαθίσταται επικοινωνία με τον server. Ο φόρτος εργασίας μειώνεται δραματικά στον υπολογιστή-«οικοδεσπότη» όσο αυξάνεται η ισχύς κάθε σταθμού εργασίας.

Οι οργανισμοί έχουν να κάνουν με συνεχώς περισσότερα δεδομένα, τα οποία πρέπει να τα διαχειρίζονται και να τα εκμεταλλεύονται στις εργασίες τους. Η αύξηση του όγκου των δεδομένων, σε συνδυασμό με την προσπάθεια των οργανισμών να μειώσουν το κόστος, να αυξήσουν την παραγωγικότητα και να βελτιώσουν τις υπηρεσίες των πελατών (με καλύτερη χρήση πληροφοριών και ταχύτερο χρόνο ανταπόκρισης στους πελάτες ταυτόχρονα), έχουν συμβάλει σε μια ώθηση για δημιουργία και χρήση client-server εφαρμογών όπως αυτής για την μεταφορά αρχείων μέσω FTP.

3.6 Συμπεράσματα

Σε αυτό το κεφάλαιο αναφερθήκαμε στην αρχιτεκτονική του Διαδικτύου και στα Πρωτόκολλα λειτουργίας του. Παρουσιάσαμε το μοντέλο αναφοράς OSI σε σχέση με τα επίπεδα του Διαδικτύου καθώς και την αρχιτεκτονική και τις λειτουργίες του μοντέλου πελάτης – διακομιστής. Στο επόμενο κεφάλαιο θα αναφερθούμε σε θέματα ασφαλείας των διακομιστών και θα κάνουμε μια εισαγωγή ειδικότερα στα Firewalls

4. ΑΣΦΑΛΕΙΑ ΕΝΟΣ ΔΙΑΚΟΜΙΣΤΗ FTP

4.1 Τι εννοούμε με τον όρο Ασφάλεια

> *"ασφάλεια υπολογιστικού συστήματος έχουμε όταν μπορούμε να βασιστούμε σε αυτό και στο λογισμικό του να συμπεριφερθεί όπως περιμένουμε από αυτό"*

Στο σημερινό κόσμο της διαδικτύωσης, κάθε υπολογιστικό σύστημα είναι και ένας πιθανός στόχος. Σπάνια περνάει ένας μήνας χωρίς ειδήσεις που να αφορούν την "κατάληψη" και το "τρύπημα" των υπολογιστικών συστημάτων μεγάλων εταιριών και οργανισμών. Αν και λέγεται, από ορισμένους hackers, ότι τέτοιες επιθέσεις αποτελούν παιχνίδια κάποιων εφήβων το φαινόμενο έχει γίνει πιο μεθοδικό και απειλητικό τα τελευταία χρόνια.

Τα τρία βασικά μέρη μιας πληροφοριακής υποδομής ενός FTP Server που αποτελούν αντικείμενο επιθέσεων, δηλαδή προσπαθειών παραβίασης της κανονικής λειτουργίας τους, είναι ο μηχανογραφικός εξοπλισμός (hardware), το λογισμικό (FTP Client/Server Software) και τα δεδομένα. Οι αδυναμίες ασφάλειας των πληροφοριακών συστημάτων οφείλονται στα μέρη αυτά καθ’ αυτά αλλά και στους τρόπους αλληλεπίδρασης και ενοποίησής τους. Πολύ σημαντική εστία δημιουργίας προβλημάτων αποτελούν οι επικοινωνίες μεταξύ των πληροφοριακών συστημάτων. Η γρήγορη εξέλιξη μάλιστα της τεχνολογίας κάνει τα όρια ανάμεσα στην “απομονωμένη” και στη “δικτυακή” χρήση, ακόμη πιο δυσδιάκριτα. Λογισμικό που εκτελείται σε ένα μηχάνημα δεν είναι απαραίτητα αποθηκευμένο σε αυτό. Μπορεί να προέρχεται από έναν τοπικό διακομιστή δικτύου ή ακόμη και από έναν Web διακομιστή. Έτσι οι σύγχρονοι υπολογιστές πλησιάζουν ολοένα και περισσότερο στη λειτουργία ενός στενά συνδεδεμένου δικτύου εξαρτημάτων, καταργώντας στη πράξη και τα όρια ανάμεσα στις απειλές των δικτύων και των μεμονωμένων πληροφοριακών συστημάτων.

Βασικός στόχος της ασφάλειας πληροφοριακών συστημάτων παραμένει η διαφύλαξη της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας όλων των συστατικών τους μερών. Όμως, είναι αλήθεια ότι κάθε εξέλιξη της τεχνολογίας μοιάζει να δημιουργεί νέα προβλήματα ασφάλειας. Η μεγαλύτερη πρόκληση στο

χώρο της ασφάλειας οφείλεται ακριβώς στο ότι απαιτεί την άμεση εκμετάλλευση τεχνολογιών αιχμής για την αντιμετώπιση των νέων προβλημάτων που συνεχώς αναδύονται.

Ο αγγλικός όρος "security", φέρεται να είναι Λατινικής προέλευσης, αφού προέρχεται από της αντίστοιχες λατινικές λέξεις "se" που σημαίνει "χωρίς" και "cura" που σημαίνει "φροντίδα". Δηλαδή η έννοια της ασφάλειας σε ένα σύστημα μπορεί και να ειδωθεί ως μια επιθυμητή ιδιότητα – κατάστασή του, κατά την οποία οι χρήστες του απαλλάσσονται κάθε έγνοιας και φροντίδας ως της τη σωστή λειτουργία του. Της παρόλο που ο όρος ασφάλεια φαίνεται να έχει μια προφανή σημασία, χρειάζεται να καταβληθεί σημαντική προσπάθεια προκειμένου να καταγραφεί το ακριβές της νόημα.

4.1.1 Βασικές έννοιες -Χαρακτηριστικά

Μπορούμε να κατανοήσουμε καλύτερα την έννοια της ασφάλειας αν διακρίνουμε τις τρεις συνεχείς και διαφορετικές μεταξύ τους δράσεις που αυτή απαιτεί:

- *Πρόληψη (prevention): Λήψη μέτρων που μας επιτρέπουν να προλαβαίνουμε τη δημιουργία επικίνδυνων καταστάσεων.*
- *Ανίχνευση (detection): Λήψη μέτρων που μας επιτρέπουν να αντιληφτούμε πως, πότε και από ποιόν έχει προκληθεί κάποια ζημιά.*
- *Αντίδραση (reaction): Λήψη μέτρων που μας επιτρέπουν να αποκαταστήσουμε τις ζημιές που έχουν προκληθεί.*

Και βέβαια χρειάζεται να γίνει περισσότερο σαφής η εικόνα των «επικίνδυνων καταστάσεων» ή «ζημιών». Τι ακριβώς διακυβεύεται; Οι επικρατούσες απόψεις διακρίνουν τις τρεις ακόλουθες βασικές έννοιες σε σχέση με τη διαχείριση ενός ασφαλούς συστήματος:

- **Εμπιστευτικότητα (confidentiality):** Είναι έννοια στενά συνδεμένη με την ιδιωτικότητα (privacy) και τη μυστικότητα (secrecy). Αφορά τη μη αποκάλυψη των ευαίσθητων πληροφοριών σε χρήστες που δεν έχουν τη κατάλληλη εξουσιοδότηση.
- **Ακεραιότητα (integrity):** *Αφορά τη δυνατότητα τροποποιήσεων (προσθήκες, διαγραφές και μεταβολές) των πληροφοριών. Μόνο σε κατάλληλα εξουσιοδοτημένους χρήστες πρέπει το σύστημα να επιτρέπει τέτοιου είδους*

ενέργειες. Έτσι διαφυλάσσεται η ακρίβεια και η πληρότητα των περιεχομένων ενός πληροφοριακού συστήματος.

- **Διαθεσιμότητα (availability):** Αφορά τη δυνατότητα άμεσης πρόσβασης στις πληροφορίες, στις υπηρεσίες και γενικότερα σε όλους τους πόρους πληροφορικής τεχνολογίας (*IT resources*) όταν ζητούνται, χωρίς αδικαιολόγητες καθυστερήσεις.

Ανάλογα με τη φύση τους, τα διάφορα πληροφοριακά συστήματα είναι περισσότερο ή λιγότερο «ευαίσθητα» στη δυνατότητα να υποστηρίξουν τα προαναφερθέντα χαρακτηριστικά της ασφάλειας. Γι' αυτό και η προσέγγιση της ασφάλειας πληροφοριακών συστημάτων ξεκινάει από την ανάλυση των αναγκών και των σχετικών κινδύνων που παρουσιάζονται σε κάθε περίπτωση. Στη συνέχεια υπολογίζονται οι επιπτώσεις που θα έχει η εφαρμογή των μηχανισμών προστασίας των πληροφοριών στην απόδοση του συστήματος (ταχύτητα, κόστος επεξεργασίας, ευκολία στη διαχείριση, φιλικότητα στο χρήστη κλπ.) και τελικά διαμορφώνεται το κατάλληλο επίπεδο ασφάλειας ως η «χρυσή τομή» ανάμεσα στους κινδύνους που αποφεύγονται, στην συνολική απόδοση του συστήματος και στο κόστος ανάπτυξης και εφαρμογής των μηχανισμών ασφάλειας.

Είναι όμως κοινά αποδεκτό ότι δεν υπάρχει πλήρης ασφάλεια, με την έννοια ότι τα μέτρα πρόληψης ποτέ δεν θα είναι ικανά να εμποδίσουν όλων των ειδών τις επικίνδυνες ενέργειες. Προνοώντας λοιπόν για κάθε ενδεχόμενο, μια ακόμη έννοια έρχεται να συμπληρώσει τα χαρακτηριστικά της διαχείρισης ασφάλειας: η υπευθυνότητα (accountability). Πρέπει το σύστημα να είναι ικανό να καταγράφει επιλεκτικά κάποιες ενέργειες των χρηστών, έτσι ώστε να είναι δυνατόν όσες επηρεάζουν την ασφάλειά του να μπορούν να «ερευνηθούν», και να «οδηγήσουν» στο υπεύθυνο μέρος. Οπότε και είναι δυνατή η απόδοση ευθυνών στο κάθε χρήστη ανάλογα με τη δράση του. Ένα χαρακτηριστικό παράδειγμα είναι η καταγραφή των κινήσεων των χρηστών του FTP server όπως παρουσιάζεται στο σημείο 7.1.2.

Ο όρος αδυναμία-απάρνησης (non-repudiation) ως χαρακτηριστικό ασφάλειας, αποτελεί μια ειδική περίπτωση της έννοιας της υπευθυνότητας και αναφέρεται ακριβώς στο ότι ένας χρήστης δεν μπορεί να αρνηθεί την ανάληψη της ευθύνης για κάποια πράξη που έκανε. Τέλος, υπάρχουν και όροι που έχουν κάποια σχέση-αναλογία με την ασφάλεια συστημάτων όπως η αξιοπιστία (reliability) ή σιγουριά

(safety), δηλαδή η ικανότητα των συστημάτων να λειτουργούν σωστά κάτω από αντίξοες συνθήκες, και η εγκυρότητα (dependability) η οποία ενσωματώνει συνήθως τις έννοιες και της ασφάλειας και της αξιοπιστίας.

4.1.2 Ασφάλεια σε περιβάλλον Διαδικτύου

Το Διαδίκτυο (Internet), είναι το μεγαλύτερο σύμπλεγμα διαφορετικών δικτύων (internet of internets) που χρησιμοποιούν ως πρωτόκολλο επικοινωνίας το TCP/IP και βρίσκονται εγκατεστημένα σε κάθε γωνιά του πλανήτη. Επιτυγχάνει τη διασύνδεση ετερογενών δικτύων Η/Υ (INTERnetworking NETworks). Ο ιδιαίτερος χαρακτήρας του προκύπτει από την ανοχή που διαθέτει σε αναξιόπιστες συνδέσεις. Σχεδιάστηκε έτσι ώστε να υποστηρίζει πολλαπλές συνδέσεις μεταξύ των υπολογιστών με αποτέλεσμα να διατηρεί τη λειτουργικότητά του ακόμα και με κατεστραμμένους κλάδους. Πραγματικά είναι πολύ σημαντική η ικανότητά του κάθε υπολογιστή να μπορεί να στέλνει μηνύματα στους άλλους ακολουθώντας οποιοδήποτε διαθέσιμο δρόμο και όχι κάποιο σταθερό και προκαθορισμένο.

Η ομάδα πρωτοκόλλων TCP/IP (Transmission Control Protocol / Internet Protocol), όπως φαίνεται και στο Κεφάλαιο 3, είναι αυτή που κατά κανόνα χρησιμοποιείται ως η προσυμφωνημένη μέθοδος επικοινωνίας και διαμεταγωγής δεδομένων στο Internet, και η οποία καθιέρωσε τη λογική του «πακέτου»: στο κόμβο του αποστολέα το μήνυμα μετάδοσης τεμαχίζεται σε μικρά τμήματα σταθερού μεγέθους τα οποία μεταδίδονται ανεξάρτητα μέσω του δικτύου. Κάθε πακέτο μεταφέρει ζωτικά στοιχεία για τη δρομολόγησή του (όπως πχ. η διεύθυνση προορισμού του) και ακολουθεί τη δική του διαδρομή μέσα στο δίκτυο. Στο κόμβο του παραλήπτη τα πακέτα θα συναρμολογηθούν για να σχηματιστεί το αρχικό μήνυμα. Φυσικά η όλη διαδικασία προϋποθέτει ότι κάθε υπολογιστής στο Διαδίκτυο έχει και τη δική του διεύθυνση επικοινωνίας (IP address). Με τον τρόπο αυτό, επιτεύχθηκε η δημιουργία κατανεμημένων δικτύων (distributed networks) τα οποία δεν εξαρτώνται από ένα κέντρο οργάνωσης – ελέγχου και άρα δεν χρειάζεται να στηρίζονται σε ένα μεμονωμένο κεντρικό υπολογιστή-οικοδεσπότη (single centralized host). Το σημείο αυτό, ενοχλητικό για πολλούς, είναι που εξηγεί και την άναρχη δομή του Internet: κάθε υπολογιστής-οικοδεσπότης είναι ομότιμος μέσα στο δίκτυο χωρίς να υπάρχει κεντρική διαχείριση.

Το Διαδίκτυο αποτελεί σήμερα τη θεμέλια βάση για την παγκοσμίου κλίμακας επικοινωνία και πρόσβαση απομακρυσμένων πόρων που απολαμβάνουν εκατομμύρια χρήστες υπολογιστών. Τα πλεονεκτήματα που προέκυψαν για τη παγκόσμια κοινότητα από τη χρήση του Internet, είναι διαθέσιμα και στις επιχειρήσεις μέσω των intranets, δηλαδή των ιδιωτικών δικτύων υπολογιστών που χρησιμοποιούν το λογισμικό και τα πρότυπα του Διαδίκτυο αλλά δεν προσφέρουν ελεύθερη προσπέλαση σε όλους τους χρήστες. Ένα intranet, χρησιμοποιεί το πρωτόκολλο TCP/IP τόσο για τοπικής εμβέλειας όσο και για ευρείας εμβέλειας μεταφορά πληροφοριών. Χρησιμοποιεί ακόμη τα πρωτόκολλα HTTP, SMTP και άλλα «ανοικτά» Διαδικτυακά πρότυπα, για να μεταφέρει πληροφορίες ανάμεσα στους πελάτες και τους διανομείς, προσανατολισμένο αυστηρά σε χρήστες που ανήκουν στην επιχείρηση ή έχουν κάποια συνεργασία μαζί της. Στη δικτυακή αρχιτεκτονική μιας τέτοιας επιχείρησης, συνήθως περιλαμβάνεται μια σειρά από υπολογιστές-διανομείς (πχ. web server, SQL server, application server και database server), οι οποίοι είναι συνδεδεμένοι μεταξύ τους, όχι απαραίτητα μέσω ενός τοπικού δικτύου.

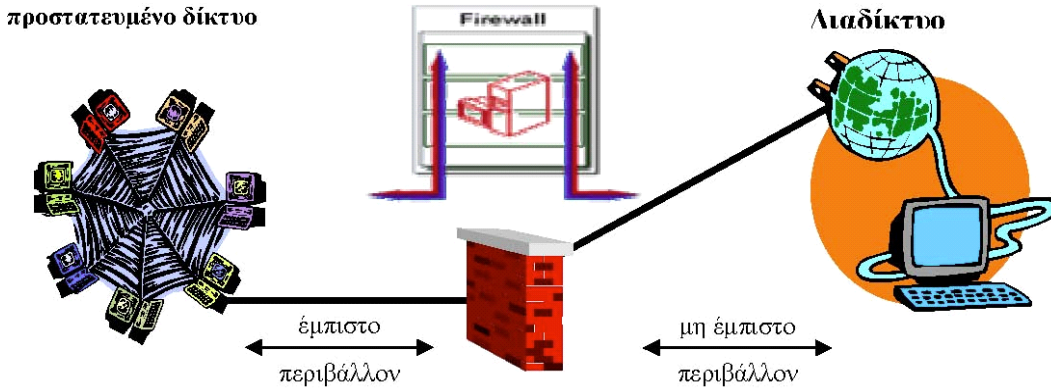
Υπάρχουν όμως ακόμη, θέματα σχετικά με την ασφάλεια στο Internet που κάνουν τους χρήστες να το αποφεύγουν για τη διακίνηση ευαίσθητων δεδομένων. Κλασικό παράδειγμα η εισαγωγή του αριθμού πιστωτικής κάρτας για τη προμήθεια αγαθών ή υπηρεσιών μέσω Διαδικτύου. Είναι γενικά αποδεκτό ότι ο σημαντικότερος παράγοντας που επηρεάζει τη περαιτέρω διάδοση της χρήσης του Internet, είναι αυτός της δημιουργίας κλίματος μεγαλύτερης εμπιστοσύνης και αξιοπιστίας σε αυτό. Σύμφωνα με την επισκόπηση “Third Annual Ernst & Young/Information Week Information Security Survey”, όπως σημειώνεται, το 87% αυτών που χρησιμοποιούν το Διαδίκτυο, το 66% αυτών που δεν το χρησιμοποιούν ακόμη και το 83% αυτών που σκοπεύουν να συνδεθούν μέσα σε ένα χρόνο, δηλώνουν ότι θα χρησιμοποιούσαν το Internet για ανταλλαγές αρχείων αν διευρυνόταν σημαντικά η παρεχόμενη ασφάλεια του.

Ο FTP server για μεταφορά αρχείων μέσω του File Transfer Protocol (FTP) είναι τυπικά προσβάσιμος απ' όλο το Internet. Οι παρακάτω συστάσεις μπορούν να ελαττώσουν τους αντίστοιχους με τους προαναφερθέντες κινδύνους:

- Ο FTP server να μην προσφέρει άλλες υπηρεσίες.

- Ο server να μην προσφέρει ούτε και να περιέχει εμπιστευτικές πληροφορίες (π.χ. αρχείο κωδικών χρηστών).
- Ο FTP server να μη χρησιμοποιεί το ίδιο μηχάνημα με τον Web server. Η πρόσβαση με FTP μπορεί να χρησιμοποιηθεί για τη μεταβολή στοιχείων του Web, ή η πρόσβαση μέσω του Web για την άντληση εμπιστευτικών στοιχείων του FTP.
- Ο server πρέπει να είναι προσεκτικά παραμετροποιημένος και να περιέχει όλες τις τελευταίες αλλαγές του κατασκευαστή.
- Η παραμετροποίηση του server να επιτρέπει πρόσβαση μόνο στην περιοχή των αρχείων.

4.2 Συστήματα Ασφάλειας Firewalls



Σχήμα 3.6 - Σύστημα Firewall

Εφόσον το FTP όπως παρουσιάστηκε και προηγουμένως λειτουργεί με τεχνολογία client – server υπόκεινται στα ίδια προβλήματα ασφαλείας που αντιμετωπίζουν όλοι οι servers οι οποίοι λειτουργούν σε ένα κλειστό δίκτυο υπολογιστών και θέλουν να επικοινωνήσουν με άλλους υπολογιστές στο διαδίκτυο. Ένας από τους ασφαλέστερους τρόπους προστασίας από επιθέσεις μη εξουσιοδοτημένων χρηστών είναι τα τείχη ασφαλείας γνωστά και ως firewalls.

Μόλις ένα δίκτυο αποκτήσει σύνδεση στο Internet, ένα κανάλι αμφίδρομης επικοινωνίας ανοίγει: οι χρήστες του δικτύου (insiders) αποκτούν επαφή με τον έξω κόσμο αλλά ταυτόχρονα και οι outsiders, δηλαδή οι εξωτερικοί χρήστες ως προς αυτό το δίκτυο, αποκτούν πλέον δυνατότητα πρόσβασης. Ο τρομακτικός ρυθμός αύξησης του μεγέθους του Διαδικτύου, προκαλεί ανάλογη αύξηση των πιθανών κινδύνων στα ιδιωτικά (private) δίκτυα που συνδέονται μαζί του. Για τη προστασία τους από

παρακολουθήσεις, εισβολές και άλλες Διαδικτυακές απειλές απαιτείται ένα κατάλληλο φράγμα. Ο φράκτης αυτός που καλείται firewall, πρέπει να είναι ικανός να αναχαιτίζει όλη τη κυκλοφορία μηνυμάτων ανάμεσα σε ένα συγκεκριμένο τοπικό ή ιδιωτικό δίκτυο και στο Internet.

Στη πραγματικότητα ένα σύστημα firewall ανορθώνει ένα εξωτερικό τοίχο ασφάλειας, οριοθετώντας μια περίμετρο προστασίας. Έτσι προκαλεί ένα σαφή διαχωρισμό ανάμεσα στο προστατευμένο-εσωτερικό δίκτυο ενός οργανισμού (το οποίο θεωρείται ασφαλές και έμπιστο) και στο εξωτερικό Διαδίκτυο (το οποίο θεωρείται μη ασφαλές και μη έμπιστο).

Ένα σύστημα firewall ορίζεται ως το λογισμικό και ο εξοπλισμός που τοποθετούμενος ανάμεσα στο Διαδίκτυο και στο υπό προστασία δίκτυο, επιτρέπει τη προσπέλαση των εξωτερικών χρηστών στο προστατευμένο δίκτυο, μόνο εφόσον διαθέτουν συγκεκριμένα χαρακτηριστικά. Έτσι ένα τυπικό σύστημα firewall μπορείνα επιτρέπει επιλεκτικά τη πρόσβαση στους εξωτερικούς χρήστες, βασιζόμενο σε ονόματα χρηστών και συνθηματικά ή σε IP διευθύνσεις ή ακόμη και σε ονόματα επικρατειών (domain names). Αυτός είναι ο κύριος σκοπός του: να κρατήσει τις επικίνδυνες δραστηριότητες μακριά από το προστατευμένο περιβάλλον. Επιπλέον, είναι σε θέση να ρυθμίσει και τις παρεχόμενες Διαδικτυακές υπηρεσίες για τους εσωτερικούς χρήστες. Για τη λειτουργία του αυτή δεν εξετάζει μόνο χαρακτηριστικά των χρηστών, αλλά και στοιχεία σχετικά με το προορισμό των αιτήσεων προσπέλασής τους. Ένα σύστημα λοιπόν firewall έχει σαν στόχο να ελέγχει και να καταγράφει τη πρόσβαση σε προστατευμένες υπηρεσίες, που προέρχονται και από το εσωτερικό και από το εξωτερικό του δικτύου ενός οργανισμού, με το να επιτρέπει, να απαγορεύει ή να ανακατευθύνει τη ροή των δεδομένων μέσω των μηχανισμών του.

Ένα firewall μπορεί να θεωρηθεί σαν ένα ζευγάρι μηχανισμών που ο ένας μπλοκάρει τη κυκλοφορία των δεδομένων και ο άλλος επιτρέπει τη ροή τους. Το ποια δεδομένα επιτρέπονται και ποια απορρίπτονται είναι ζήτημα της πολιτικής (policy) ελέγχου που αυτό υποστηρίζει και εξαρτάται από τη διαμόρφωσή του (firewall configuration). Πραγματικά, ένα σύστημα firewall δεν είναι απλά ένας δρομολογητής (router), ένας διανομέας ή διακομιστής ή εξυπηρετητής (server), ένας οικοδεσπότης (host) ή ένα σύνολο εξοπλισμού και λογισμικού που παρέχει ασφάλεια στα δίκτυα. Οι αληθινές δυνατότητές του γίνονται εμφανείς αν τον θεωρήσουμε ως ένα ισχυρό μέσο υλοποίησης μιας πολιτικής ασφάλειας που καθορίζει τις παρεχόμενες υπηρεσίες και

τις επιτρεπτές προσπελάσεις ανάμεσα σε έμπιστες και μη-έμπιστες επικράτειες. Η υλοποίηση της πολιτικής ελέγχου προσπέλασης δικτύων (network access control policy) γίνεται με την υποχρεωτική κατεύθυνση όλων των επικοινωνιών μέσω του firewall, όπου αποτελούν αντικείμενο εξέτασης και καταγραφής.

4.2.1 Γιατί είναι αναγκαία τα firewalls

Όταν τοπικά δίκτυα (local networks) συνδέονται στο Internet, αποτελεί ζήτημα μεγάλης σημασίας η διασφάλιση της κανονικής λειτουργίας τους από τους νόμιμους και παράνομους χρήστες τους. Η τοποθέτηση ενός firewall συστήματος ανάμεσα στο τοπικό δίκτυο ενός οργανισμού και το Διαδίκτυο, εγκαθιστά δυνατότητες ελέγχου στη ροή των πληροφοριών και διασφαλίζει τη διαδικτυακή σύνδεση (internet link) προστατεύοντας στον οργανισμό:

- τους πόρους του (υλικό, λογισμικό, δεδομένα) από φθορά, κατάχρηση, κλοπή και κατάχρηση.
- την υπόληψή του από τη δημοσιοποίηση αδυναμιών στην ασφάλεια του δικτύου του.
- την επικρατούσα πολιτική ορθής χρήσης των υπηρεσιών του Διαδικτύου από τους εργαζομένους του.

Ο πιο συνηθισμένος πάντως λόγος ύπαρξης ενός συστήματος firewall σε έναν οργανισμό είναι η παροχή ενός μηχανισμού ελέγχου προσπέλασης (access control), πρώτου επιπέδου, για τον Web Server. Ένα firewall πρέπει να ελέγχει και να καταγράφει την ροή των επικοινωνιών που διέρχονται μέσα από τον διακομιστή Web. Δηλαδή πρέπει να παρεμβάλλεται και να αποκόβει όλη την κίνηση των δεδομένων ανάμεσα στον Web server και το Internet. Έτσι είναι σε θέση να προστατεύει τα δεδομένα που δημοσιεύονται από ανεπιθύμητες αλλαγές και να ελέγχει τη πρόσβαση στον διακομιστή Web, αποκλείοντας τους μη-εξουσιοδοτημένους χρήστες από ευαίσθητους πόρους του δικτύου.

Ακόμη, ένας οργανισμός μπορεί να χρησιμοποιήσει ένα firewall για να απομονώσει τις επικοινωνίες ανάμεσα στα δίκτυα των επιμέρους τμημάτων του. Για παράδειγμα ένα νοσοκομείο ενδεχομένως να θελήσει να διαχωρίσει το δίκτυο διακίνησης των δεδομένων των ασθενών από το δίκτυο των οικονομικών στοιχείων του. Ένα ή περισσότερα firewalls (intranet firewalls) μπορούν να χρησιμοποιηθούν

για να παρέχουν απομόνωση και ελεγχόμενη προσπέλαση ανάμεσα στα διάφορα μέρη ενός οργανισμού.

Ένα σύστημα firewall λοιπόν μπορεί να αποτελέσει μια διάταξη δρομολόγησης (router), ένας προσωπικός υπολογιστής, ένας διακομιστής, ή ένα σύνολο από διακομιστές, διαμορφωμένοι με τέτοιο τρόπο ώστε να οχυρώνουν μια δικτυακή τοποθεσία (site) ή ένα υποδίκτυο (subnet) από πρωτόκολλα και υπηρεσίες (πχ. υπηρεσίες FTP, HTTP, e-mail κλπ.) οι οποίες μπορούν να προσβληθούν από διακομιστές εκτός του υποδικτύου. Η συνηθισμένη θέση του είναι ως πύλη υψηλού επιπέδου ακριβώς στο σημείο σύνδεσης ενός οργανισμού με το Internet. Όπως όμως έχει ήδη αναφερθεί, μπορεί να τοποθετηθούν και ως πύλες χαμηλότερων επιπέδων πρόσβασης, με σκοπό τη προστασία επιμέρους τμημάτων ενός υποδικτύου.

4.2.2 Πλεονεκτήματα και περιορισμοί από τη χρήση firewalls

Ένα firewall σε λειτουργία, δεν είναι ένα απλό συστατικό του δικτύου αλλά αποτελεί την υλοποίηση μιας στρατηγικής για τη προστασία των συνδεδεμένων στο Διαδίκτυο πόρων ενός οργανισμού. Εξασφαλίζει ότι όλες οι επικοινωνίες από και προς το Internet είναι σύμφωνες με τη προκαθορισμένη πολιτική ασφάλειας του οργανισμού. Πρόκειται για τη πρώτη και σημαντικότερη ωφέλεια. Όμως σπουδαίες είναι και οι υπόλοιπες επιμέρους ωφέλειες που παρέχει ένα σύστημα firewall. Αναλυτικά:

Επιτρέπει αποτελεσματικά την υλοποίηση και διαχείριση μέρους της πολιτικής ασφάλειας (policy enforcement) που θέλουμε να εφαρμόσουμε στο σύστημά μας. Η διαμόρφωση-παραμετροποίηση που υποστηρίζει μας βοηθά να ορίσουμε ποιος χρήστης θα έχει πρόσβαση σε ποιο πόρο. Παράλληλα μέσω των διαθέσιμων εργαλείων του για καταγραφή και επίβλεψη, έχουμε μια πλήρη εικόνα των προσπαθειών (επιτυχών και ανεπιτυχών) σύνδεσης η οποία θα χρησιμεύσει στη συντήρηση ή και μετατροπή της πολιτικής ασφάλειας ειδικότερα πάνω σε χρήστες με «ύποπτη» συμπεριφορά. Χωρίς firewalls, η εφαρμογή της πολιτικής εξαρτάται από τη διάθεση συνεργασίας των χρηστών, αφού η ασφάλεια ενός δικτύου αντιμετωπίζεται ξεχωριστά από το κάθε τμήμα του. Βέβαια, η ασφάλεια ενός οργανισμού λίγο-πολύ εξαρτάται από τους χρήστες του και τη συμμόρφωσή τους στους προβλεπόμενους κανόνες, αλλά με κανένα τρόπο δεν πρέπει να εξαρτάται από τους εξωτερικούς χρήστες του Διαδικτύου.

Προστατεύει από ευπαθείς υπηρεσίες δικτύων (protecting from vulnerable services). Είναι γνωστό ότι τα πρωτόκολλα επικοινωνίας του Διαδικτύου παρουσιάζουν εγγενή προβλήματα ασφάλειας. Η εγκαθίδρυση ενός συστήματος firewall προσφέρει δυνατότητες φιλτραρίσματος που ελαχιστοποιούν τους κινδύνους. Ακόμη μπορεί και καλύπτει γνωστές ρωγμές ασφαλείας (όπως οι επιθέσεις αδυναμίας εξυπηρέτησης) στο κατώτερο επίπεδο των λειτουργικών συστημάτων. Έτσι, κάποια αδύνατα σημεία για την ασφάλεια του δικτύου, που έχουν ήδη εκμεταλλευτεί διάφοροι βάνδαλοι, έρχεται να προστατέψει και να οχυρώσει το firewall.

Αποτελεί μέσο καταγραφής και δημιουργίας στατιστικών στοιχείων για τη χρήση και κατάχρηση του δικτύου (logging-alarming & statistics of network use/misuse). Πρόκειται για πολύτιμες πληροφορίες που λόγω της θέσης του firewall ως το μοναδικό σημείο σύνδεσης με το έξω δίκτυο, είναι ακριβείς και αξιόπιστες. Η χρησιμότητά τους είναι μεγάλη. Τεκμηριώνουν την ικανότητα ή όχι του ίδιου του firewall για αποτροπή των επιθέσεων που συνέβησαν και κρίνουν την καταλληλότητα της πολιτικής ασφάλειας που εφαρμόζεται.

Επιπλέον, τα στατιστικά χρήσης του δικτύου είναι χρήσιμα και στις διαδικασίες ανάλυσης επικινδυνότητας (risk analysis) και ανάλυσης απαιτήσεων δικτύου (network requirement analysis). Ένα firewall μπορεί ακόμη με τις δυνατότητες επεξεργασίας των πληροφοριών αυτών που διαθέτει, να εντοπίσει ύποπτες δραστηριότητες και να αντιδράσει με προαποφασισμένες ενέργειες όπως το κλείσιμο της σύνδεσης ή η ενημέρωση του διαχειριστή ασφάλειας με e-mail.

Επιβάλλει ελεγχόμενη προσπέλαση (controlled access) στους πόρους ενός εσωτερικού δικτύου. Για παράδειγμα, κάποιοι διακομιστές ενδέχεται να προσφέρονται για επικοινωνία με το Internet, ενώ άλλοι όχι.

Προσφέρει διευρυμένη ιδιότητα (enhanced privacy). Για παράδειγμα αποκρύπτει λεπτομέρειες σχετικές με τη διάρθρωση του εσωτερικού δικτύου. Έτσι, οι εξωτερικοί εισβολείς (intruders) δυσκολεύονται στις ενδεχόμενες προσπάθειές τους να «ξεφύγουν» από τα όρια χρήσης του δικτύου που εμείς τους ορίσαμε. Γενικότερα, υπάρχουν πάντοτε πληροφορίες που ενώ θεωρούνται αβλαβείς, περιέχουν σημαντικά στοιχεία για έναν επιδέξιο χρήστη που θέλει να επιχειρήσει επίθεση. Έτσι, μέσω του firewall, πολλοί οργανισμοί σταματούν υπηρεσίες όπως η Finger και η DNS (Domain Name Service). Η πρώτη δίνει πληροφορίες σχετικά με τους χρήστες ενός δικτύου,

όπως το πότε συνδέθηκαν για τελευταία φορά, αν διαβάσανε το ηλεκτρονικό τους ταχυδρομείο κλπ. Έτσι όμως διαρρέουν πληροφορίες στους εισβολείς σχετικές με το πόσο συχνά ένα σύστημα χρησιμοποιείται ή αν εκείνη τη στιγμή υπάρχουν συνδεδεμένοι ενεργοί χρήστες. Η υπηρεσία DNS από την άλλη, παρέχει πληροφορίες για τις δικτυακές τοποθεσίες του συστήματος, όπως τα ονόματα των τόπων και οι IP διευθύνσεις του. Η μη δημοσιοποίησή τους στο Διαδίκτυο, αφαιρεί σίγουρα χρήσιμα στοιχεία από όσους τα επιβουλεύονται.

Συγκεντρώνει υπηρεσίες ασφάλειας σε μια καλά ορισμένη και οχυρωμένη περιοχή (concentrated security). Ελαχιστοποιεί τη ζώνη κινδύνου (zone risk) ενός οργανισμού εφόσον η ευρεία περιοχή των μηχανημάτων του παύει να απειλείται άμεσα. Ουσιαστικά το ίδιο το firewall αποτελεί τη μοναδική ζώνη κινδύνου για τον οργανισμό. Άμεση συνέπεια του γεγονότος αυτού, είναι η ευκολία διαχείρισης ασφάλειας και γενικότερα μια οικονομία κλίμακας αφού δεν χρειάζεται κάθε φορά που χρειάζονται ρυθμίσεις επειδή κάτι αλλάζει στο λογισμικό των εφαρμογών ή της ασφάλειας, να απαιτούνται επεμβάσεις σε όλους τους διακομιστές. Η ενημέρωση-συντήρηση αφορά κυρίως το σύστημα firewall. Για παράδειγμα η εγκατάσταση πρόσθετου λογισμικού πιστοποίησης (όπως τα συστήματα συνθηματικών μιας χρήσης - “authentication using one-time password systems”), δεν χρειάζεται να γίνει σε κάθε διακομιστή ξεχωριστά, αλλά να γίνει μια φορά στο firewall.

Αρκετά σύγχρονα συστήματα firewall προσφέρουν ως μια επιπλέον λειτουργία τους και τις υπηρεσίες τους ως πύλες κρυπτογράφησης (encrypting gateways). Δηλαδή έχουν ταυτόχρονα δυνατότητες κρυπτογράφησης στις επικοινωνίες μεταξύ των διακομιστών που προστατεύουν. Ακόμη και εξωτερικά συστήματα μπορούν να συνομιλήσουν σε κρυπτογραφημένη μορφή, αρκεί να εγκαταστήσουν το ανάλογο λογισμικό πελάτη και να παρουσιάσουν τα σχετικά διαπιστευτήρια που προέρχονται από το διαχειριστή του firewall. Ένας τέτοιος λογικός διαχωρισμός των δικτύων μέσω firewalls και τεχνικών κρυπτογράφησης δημιουργεί τα λεγόμενα εικονικά ιδιωτικά δίκτυα (VPN – Virtual Private Networks). Η κρυπτογράφηση μπορεί να είναι επιλεκτική, ανάλογα με την αιτούμενη από το Διαδίκτυο υπηρεσία και η διαχείρισή της είναι ενσωματωμένη με τα υπόλοιπα χαρακτηριστικά του firewall, έτσι ώστε να είναι δυνατή η εκμετάλλευση όλων των βοηθημάτων που υποστηρίζονται για τη κατασκευή των κανόνων ελέγχου προσπέλασης, τη καταγραφή-παρακολούθηση των ενεργειών κλπ.

4.3 Συμπεράσματα

Σε αυτό το κεφάλαιο αναφερθήκαμε σε θέματα ασφαλείας του διαδικτύου καθώς θεωρούμε ότι είναι από τους περισσότερο κρίσιμους παράγοντες λειτουργίας των servers. Παρουσιάσαμε επίσης και τα Firewalls τα οποία αποτελούν μια αποτελεσματική και αξιόπιστη λύση ασφαλούς διαχείρισης των πληροφοριών που διατηρούμε στον υπολογιστή μας και ειδικότερα στον FTP server μας. Έχοντας λοιπόν τονίσει την σημασία της ασφάλειας είμαστε έτοιμοι ώστε στο επόμενο κεφάλαιο να αναφερθούμε στα βήματα εγκατάστασης ενός FTP server.

5. ΕΓΚΑΤΑΣΤΑΣΗ ΕΝΟΣ ΔΙΑΚΟΜΙΣΤΗ FTP

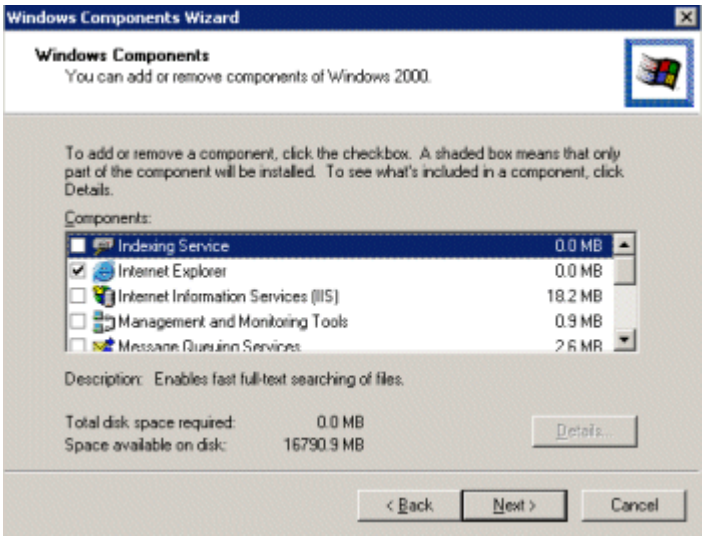
5.1 Εγκατάσταση του FTP Server του IIS των Windows

Σε αυτό το κεφάλαιο θα παρουσιάσουμε την εγκατάσταση και διαχείριση του FTP Server που υπάρχει στην υπηρεσία IIS (Internet Information Services) που παρέχεται δωρεάν από τα Microsoft Windows σε συνδυασμό με τον web server. Ο FTP Server αυτός είναι από τους πιο δημοφιλής στο Διαδίκτυο καθώς παρέχεται δωρεάν με τα Microsoft Windows, είναι πολύ εύκολος στην εγκατάσταση και διαχείριση (όπως θα δούμε και παρακάτω) αλλά συνδυάζεται επίσης και με ένα επιτυχημένο web server.

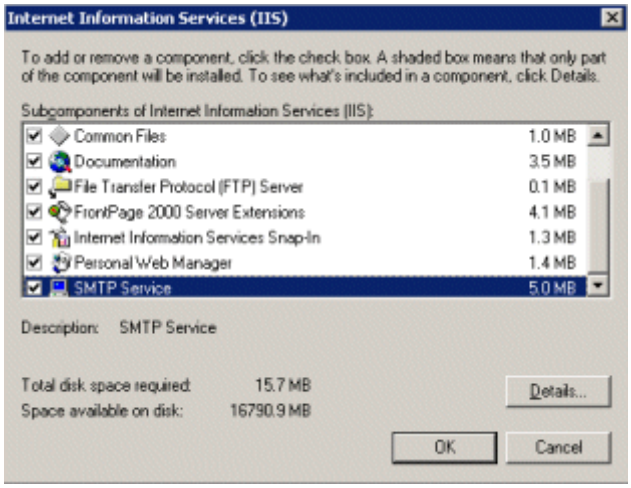
Θα αρχίσουμε με την εγκατάσταση του FTP Server που βρίσκεται μέσα στην υπηρεσία IIS (Internet Information Services) που παρέχεται από τα Microsoft Windows. Όπως φαίνεται και από τον τίτλο η Microsoft παρέχει αυτή την υπηρεσία για να δώσει την δυνατότητα στους χρήστες να εγκαταστήσουν Web αλλά και FTP servers. Συνεπώς η εγκατάσταση του FTP server προϋποθέτει την εγκατάσταση της υπηρεσίας IIS όπως φαίνεται και στα βήματα που ακολουθούν.

Η εγκατάσταση του IIS γίνεται με την χρήση του CD εγκατάστασης των Windows και όλες οι αρχικές και απαραίτητες παραμετροποιήσεις γίνονται στα πρώτα στάδια. Φυσικά ο χρήστης μπορεί να αλλάξει κάποιες από τις παραμέτρους στην πορεία χρήσης του FTP Server.

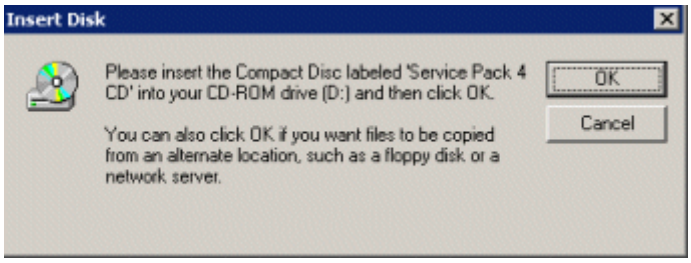
Μέσω του Add or Remove Programs προχωρούμε στην επιλογή Add and Remove Windows Components (Προσθαφαίρεση Προγραμμάτων Windows) και βλέπουμε το παρακάτω παράθυρο από το οποίο και επιλέγουμε την εγκατάσταση του IIS.



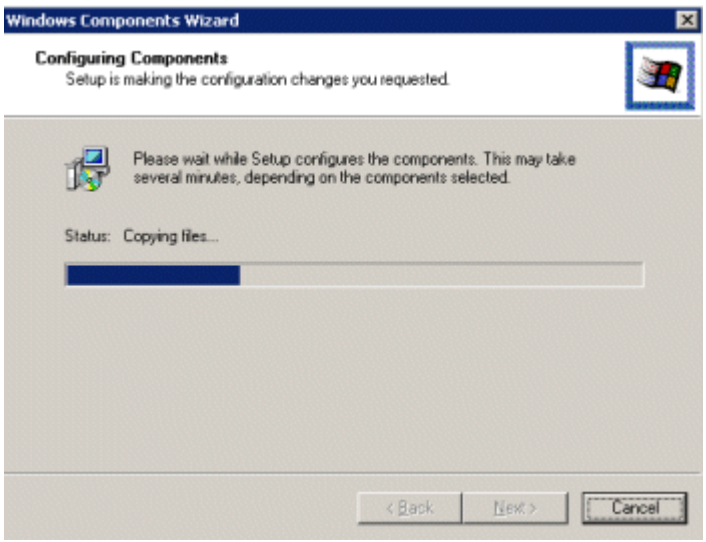
Όταν επιλέξουμε το IIS οδηγούμαστε στο παράθυρο με τις υπο-υπηρεσίες του IIS όπως αυτές φαίνονται στο επόμενο παράθυρο.



Από το παραπάνω παράθυρο μπορούμε να επιλέξουμε τους τύπους των υπηρεσιών που θέλουμε να εγκατασταθούν για την υπηρεσία μας. Η συνήθης πρακτική είναι η επιλογή όλων των υπηρεσιών εκτός από αυτές τις οποίες ο χρήστης είναι σίγουρος πως δεν θα χρειαστούν στην συνέχεια. Εφόσον έχουν επιλεγεί όλες οι απαραίτητες επιλογές πατάμε OK και συνεχίζουμε την εγκατάσταση.



Στο επόμενο παράθυρο θα μας ζητηθεί το CD εγκατάστασης των Windows που είναι εγκατεστημένα στον υπολογιστή. Τοποθετούμε το CD και συνεχίζουμε με OK.



Μόλις βρεθεί το CD από τον οδηγό των Windows τότε θα αρχίσει αυτόματα την εγκατάσταση του IIS. Δεν χρειάζεται κάποια παραμετροποίηση κατά την διάρκεια της εγκατάστασης του IIS, απλά θα αφήσουμε τον οδηγό να ολοκληρώσει την εγκατάσταση.

Μόλις τελειώσει η εγκατάσταση του IIS θα δούμε ένα παράθυρο όπως το παραπάνω (ανάλογα με την έκδοση των Windows που έχουμε εγκατεστημένα στον υπολογιστή) και επιλέγουμε Finish για να συνεχίσουμε.

Τώρα θα πρέπει να διασφαλίσουμε ότι οι δρομολογητές (routers) και τα τείχη προστασίας (firewalls) τα οποία βρίσκονται μπροστά από τους Web και FTP Server είναι παραμετροποιημένοι σωστά ώστε να επιτρέπουν την διακίνηση δεδομένων μέσα και έξω από τους Web και FTP Server.

Η παρακάτω λίστα παρουσιάζει τις πόρτες (ports) οι οποίες πρέπει να είναι ανοιχτές στους δρομολογητές και στα τείχη προστασίας ώστε να μην υπάρχει πρόβλημα διακίνησης της πληροφορίας.

Σύνηθες αριθμοί πόρτας για τις παρακάτω υπηρεσίες:

80 - **HTTPD**

21 – **FTP**

3306 – **MySQL**

110 – **POP3**

25 – **SMTP**

443 – **SSL**

143 – **IMAP**

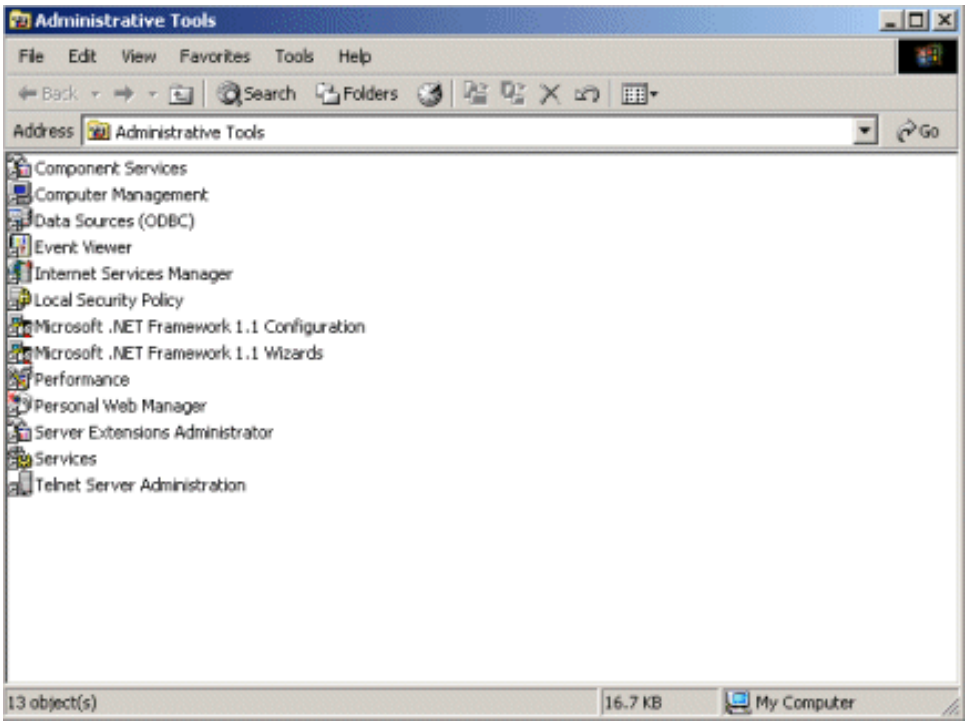
22 – **SSH**

23 – **Telnet**

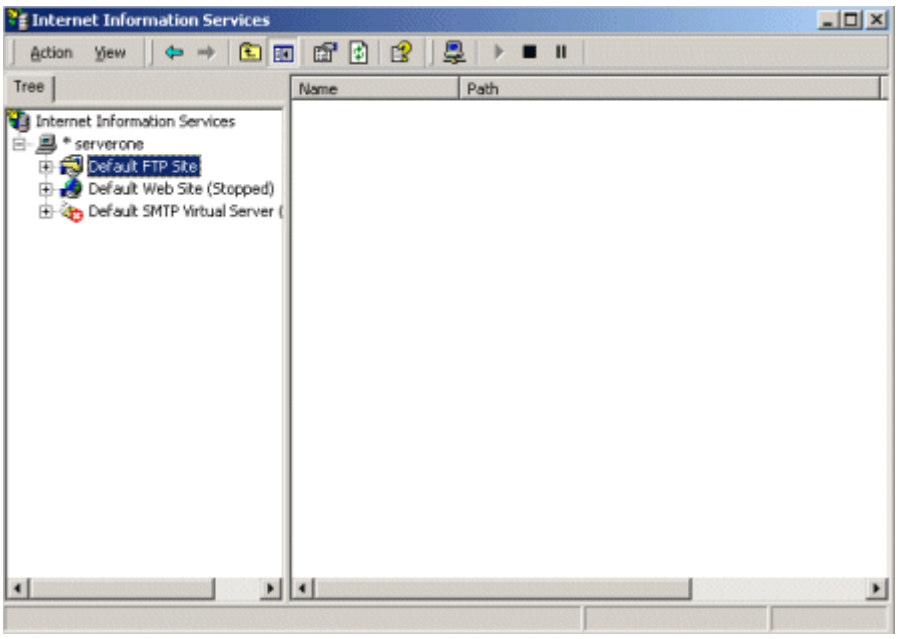
53 – **DNS**

Οι πόρτες που χρειάζονται στην περίπτωση μας είναι η 80 για τον Web Server και η 21 για τον FTP Server.

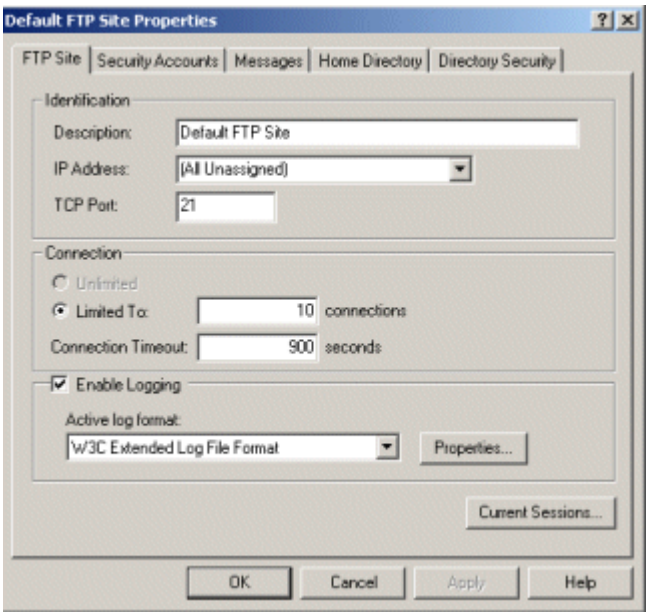
Θα προχωρήσουμε στην εγκατάσταση του FTP Server και ενός τυπικού χρήστη του FTP Server μέσα από την παραμετροποίηση του IIS η οποία βρίσκεται στην επιλογή Administrative Tools του Control Panel.



Η πρώτη κίνηση είναι να επιλέξουμε το παράθυρο "Administrative Tools" το οποίο βρίσκεται στο Control Panel. Από εκεί επιλέγουμε και ανοίγουμε το "Internet Services Manager".



Μόλις ανοίξει το παράθυρο επιλέγουμε την επιλογή "Default FTP Site" και με δεξί κλικ στο ποντίκι επιλέγουμε τις ιδιότητες (properties). Με την επιλογή αυτή θα ανοίξουν οι ιδιότητες παραμετροποίησης του FTP Server.



Μόλις ανοίξει το παράθυρο με τις ιδιότητες παρατηρούμε ότι έχουμε να επιλέξουμε από πέντε ενότητες (tabs). Θα αρχίσουμε από την πρώτη ενότητα που ονομάζεται “FTP Site” και θα προχωρήσουμε προς τα δεξιά μέχρι να ολοκληρώσουμε και τις πέντε.

Η πρώτη ενότητα είναι η “FTP Site”. Σε αυτή την ενότητα μπορούμε να ονομάσουμε τον FTP server. Για χάρη του παραδείγματος τον ονομάζουμε Default FTP Site.

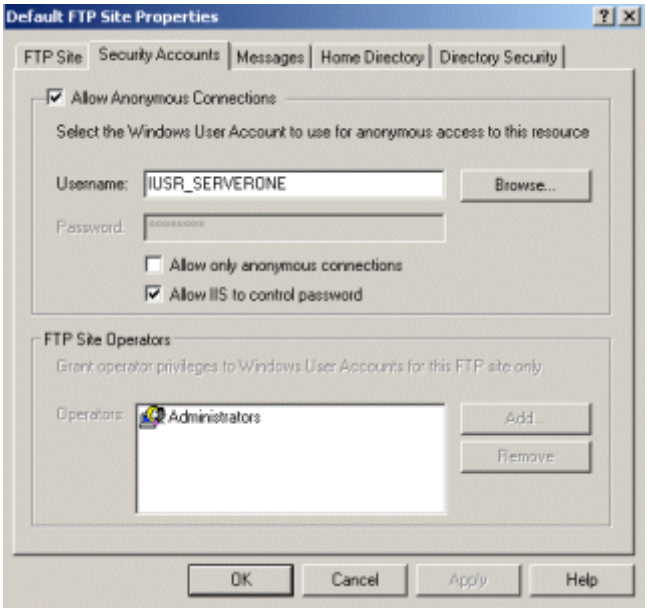
Η επόμενη επιλογή είναι η διεύθυνση IP την οποία αφήνουμε Unassigned εφόσον το IP μας είναι δυναμικό (δηλαδή αλλάζει κάθε φορά που συνδεόμαστε με την εταιρία που μας προμηθεύει την σύνδεση στο Διαδίκτυο). Στην περίπτωση που ο FTP Server πρόκειται να εγκατασταθεί πίσω από ένα δρομολογητή και το πρωτόκολλο DHCP είναι παραμετροποιημένο ώστε να παρέχει στατική IP μέσα στο εσωτερικό δίκτυο τότε η επιλογή Unassigned μπορεί να δουλέψει αλλά ίσως αργότερα χρειαστεί διαφορετικές ρυθμίσεις από πιο εξοικειωμένους χρήστες.

Η επόμενη επιλογή είναι το “TCP Port”. Ως προεπιλογή, όπως είδαμε και προηγουμένως, η πόρτα είναι η 21 η οποία αποτελεί το πρότυπο για την πόρτα του FTP server. Εξαιτίας αυτού του γεγονότος οι περισσότεροι χρήστες δεν αλλάζουν την πόρτα αυτή καθώς είναι κοινώς γνωστή γεγονός όμως που αυξάνει τις πιθανότητες επίθεσης από μη εξουσιοδοτημένους χρήστες στον FTP Server. Υπάρχουν περιπτώσεις που χρήστες θέλουν να δώσουν μια διαφορετική πόρτα ούτως ώστε να

δημιουργήσουν ένα είδος ιδιωτικού FTP Server. Σε αυτό το σημείο ο χρήστης μπορεί να δώσει την πόρτα για παράδειγμα 28. Αυτό σημαίνει ότι όταν θα δίνει την διεύθυνση στους πιθανούς χρήστες του FTP server θα πρέπει να περιλαμβάνει και την πληροφορία ότι θα πρέπει να συνδεθούν με την σωστή πόρτα αλλιώς η σύνδεση θα αποτυγχάνει

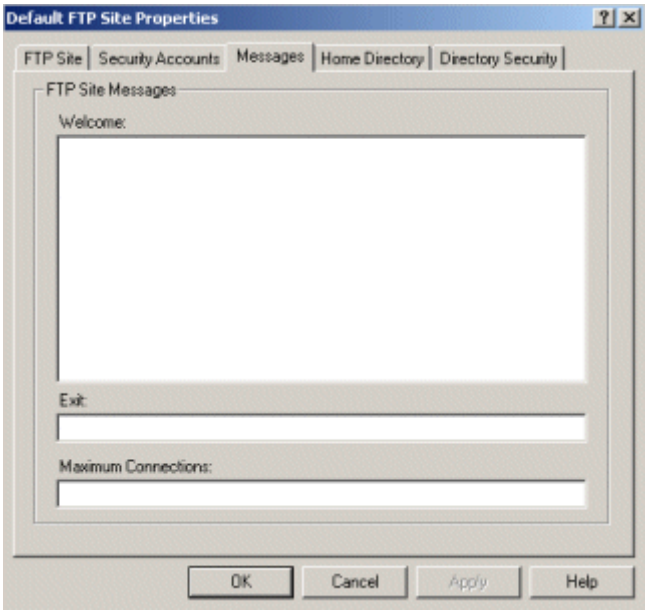
Στην συνέχεια οριοθετούμε τα περιθώρια σύνδεσης (connection limits). Οι περισσότεροι χρήστες οι οποίοι θα στήσουν τον FTP Server για μια απλή χρήση δεν θα χρειαστεί να αλλάξουν τις προεπιλογές καθώς 10 ταυτόχρονοι συνδεδεμένοι χρήστες και 900 δευτερόλεπτα αυτόματος χρόνος αποσύνδεσης (timeout) είναι αρκετά και δεν απαιτούν ιδιαίτερη προσοχή του διαχειριστή του Server.

Σε αυτή την ενότητα έχουμε επίσης την επιλογή της καταγραφής των κινήσεων των συνδεδεμένων χρηστών στον FTP Server. Όπως αναφέρουμε και στην ενότητα για την ασφαλή διαχείριση του FTP Server θα πρέπει να ενεργοποιήσουμε την επιλογή της καταγραφής (εκτός και εάν έχουμε εγκαταστήσει τον FTP Server έτσι ώστε να απευθύνεται σε συγκεκριμένους έμπιστους χρήστες) γιατί είναι θετικό να γνωρίζουμε τις κινήσεις που έχουν γίνει στον FTP Server έτσι ώστε να είμαστε σε θέση να προσδιορίσουμε ανασφαλής κινήσεις για να τις αποφεύγουμε στο μέλλον.

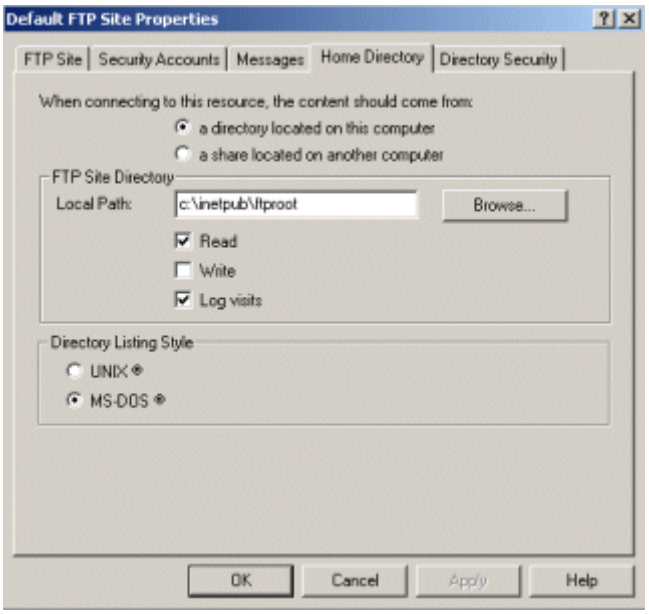


Η επόμενη ενότητα όπως φαίνεται και στο παραπάνω σχήμα είναι της Ασφάλειας. Η ενότητα της Ασφάλειας αποτελείται από δύο μέρη. Το πρώτο μέρος περιέχει τις επιλογές για τις ανώνυμες συνδέσεις (“Anonymous” connections) και η

δεύτερη για τους εξωτερικούς διαχειριστές (“FTP Site Operators”) του FTP Server που είναι οι χρήστες που μπορούν να διαχειριστούν τον FTP Server μέσω μιας εξ’ αποστάσεως σύνδεσης. Σε περίπτωση που ο FTP Server θα χρησιμοποιηθεί για ιδιωτική χρήση μόνο από γνωστούς και εξουσιοδοτημένους χρήστες τότε θα πρέπει να απενεργοποιηθεί η επιλογή για ανώνυμες συνδέσεις, σε κάθε άλλη περίπτωση αφήνουμε τις προεπιλογές ως έχει και προχωρούμε στην επόμενη ενότητα από τις πέντε.



Η ενότητα Μηνύματα (“Messages”) μπορεί να χρησιμοποιηθεί για να την απεικόνιση μηνυμάτων κατά την σύνδεση, αποσύνδεση των χρηστών αλλά και σε περιπτώσεις που ο FTP Server έχει φτάσει στο όριο των συνδεδεμένων χρηστών.

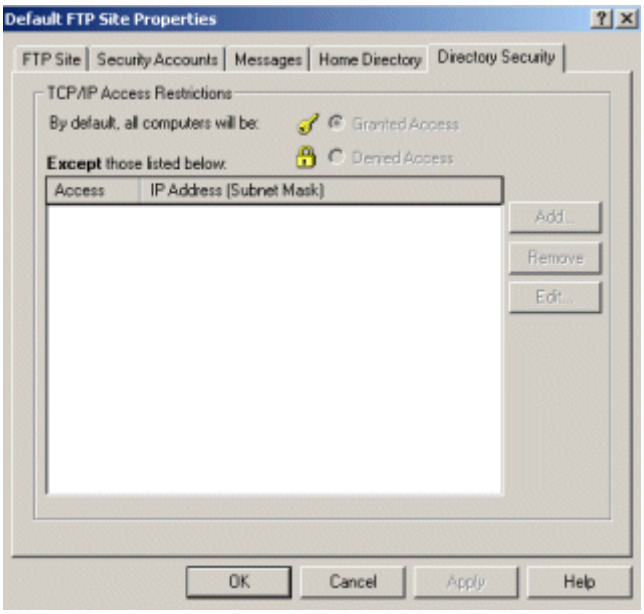


Στην επόμενη ενότητα (“Home Directory”) μπορούμε να επιλέξουμε τον χώρο στο σκληρό δίσκο ο οποίος θα χρησιμοποιείται από τον FTP Server. Η πρώτη επιλογή είναι εάν το home directory θα βρίσκεται στο ίδιο μηχάνημα όπως και ο FTP Server ή σε κάποια άλλη περιοχή σε κοινή χρήση (sharing) ενός άλλου μηχανήματος στο δίκτυο. Η σύνηθες επιλογή είναι η τοποθέτηση του home directory στο ίδιο μηχάνημα που υπάρχει και ο FTP Server.

Στην συνέχεια επιλέγουμε την τοποθεσία (path) του root directory του FTP Server. Για λόγους ασφάλειας, σε περίπτωση που πολλαπλοί χρήστες συνδεθούν μέσω του FTP Server τότε θα πρέπει να αφήσουμε την προεπιλογή ενώ όταν υπάρχει μόνο ένας χρήστης ο οποίος συνδέεται στον FTP Server μπορούμε να αλλάξουμε την τοποθεσία (path) του root directory του FTP Server σε wwwroot που είναι και η προεπιλεγμένη τοποθεσία για όλα τις πληροφορίες του διαδικτύου.

Μπορούμε επίσης να επιλέξουμε και κάποιες από τις παραμέτρους σύνδεσης (read, write, log visits) των χρηστών στο home directory του FTP Server. Αρχικώς θα αφήσουμε τις επιλογές ως έχουν καθώς είναι καλύτερα να γίνεται η παραμετροποίηση των επιλογών αυτών ξεχωριστά για κάθε χρήστη.

Στο τελευταίο τμήμα έχουμε την επιλογή των στυλ εμφάνισης των directory (“Directory Listing Styles”) σύμφωνα με την οποία επιλέγουμε εάν θέλουμε το directory να έχει την μορφή ενός directory σε MS-DOS ή ενός σε UNIX. Στην προκειμένη περίπτωση επιλέγουμε το στυλ εμφάνισης MS-DOS

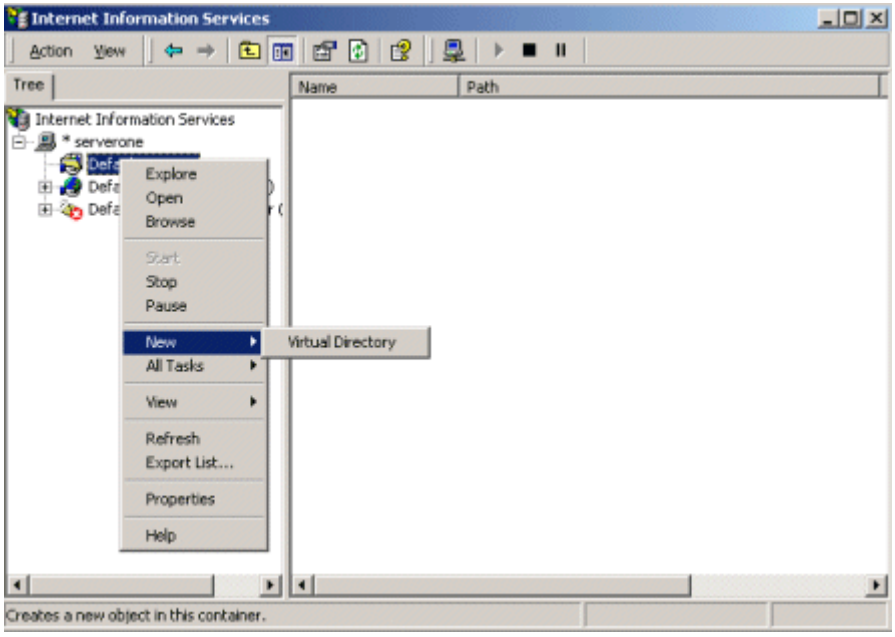


Στην τελευταία ενότητα που υπάρχει γίνεται η επιλογή των αδειών (permissions) των διευθύνσεων IP ή άλλων υπολογιστών από το δίκτυο. Οι απλοί χρήστες δεν χρειάζεται να επέμβουν σε αυτές τις επιλογές.

Τώρα που παραμετροποιήσαμε τον FTP Server το επόμενο βήμα είναι να δημιουργήσουμε ένα χρήστη ο οποίος θα συνδέεται στον FTP Server για να μεταφέρει αρχεία από και προς τον υπολογιστή του χρησιμοποιώντας ένα πρόγραμμα πελάτη FTP όπως αυτά που έχουν παρουσιαστεί νωρίτερα.

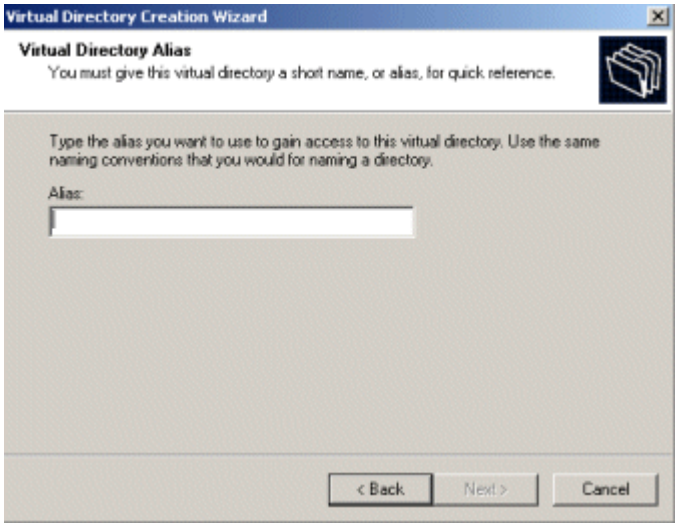
Κάτι πολύ σημαντικό που πρέπει να σημειωθεί σε αυτό το σημείο είναι το γεγονός ότι με την χρήση του IIS για το στήσιμο του FTP Server ό,τι αλλαγές γίνονται επηρεάζουν όλο το σύστημα. Κατά συνέπεια εφόσον ένας χρήστης θέλει να έχει την δυνατότητα να χρησιμοποιεί τον FTP Server ή όποιο άλλο τμήμα του server επιθυμεί χωρίς να αντιμετωπίσει κάποιο πρόβλημα θα πρέπει να προστεθεί ως χρήστης στο σύστημα. Οι χρήστες μπορούν να προστεθούν μέσω της ενότητας "Users and Passwords" που βρίσκεται στο Control Panel.

Όταν ολοκληρωθεί η διαδικασία που προβλέπεται για την πρόσθεση ενός νέου χρήστη στο σύστημα τότε μόνο μπορούμε να τον στήσουμε ως χρήστη του FTP Server ο οποίος είτε θα έχει το δικό του directory για να παίρνει ή να αφήνει αρχεία είτε θα έχει πρόσβαση στο αρχικό (root account) directory. Στην συγκεκριμένη περίπτωση θα στήσουμε ένα λογαριασμό χρήστη (account) ο οποίος θα έχει πρόσβαση στο root access.

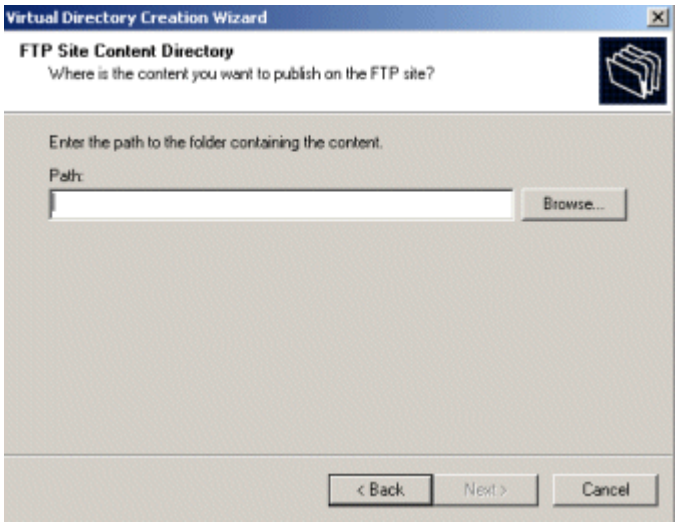


Όπως φαίνεται και στο παραπάνω παράθυρο του IIS στην επιλογή "Default FTP Site" πατάμε δεξί κλικ και στην επιλογή New διαλέγουμε το Virtual Directory.

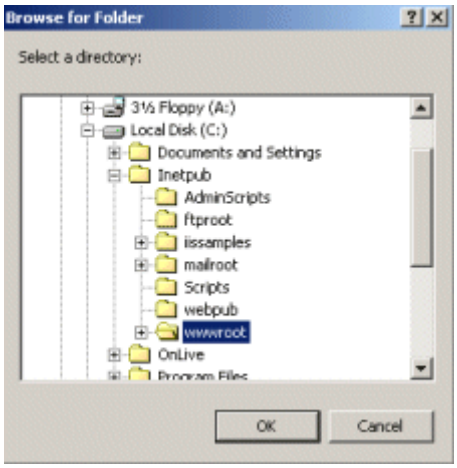
Στην περίπτωση αυτή εμφανίζεται ένας οδηγός ο οποίος θα μας οδηγήσει στην εγκατάσταση του Virtual Directory.



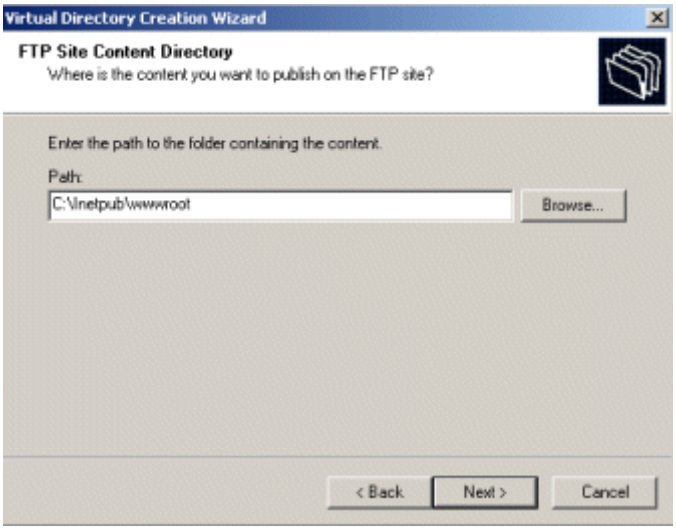
Αρχικώς όπως φαίνεται και στην παραπάνω οθόνη επιλέγουμε το όνομα του Virtual Directory.



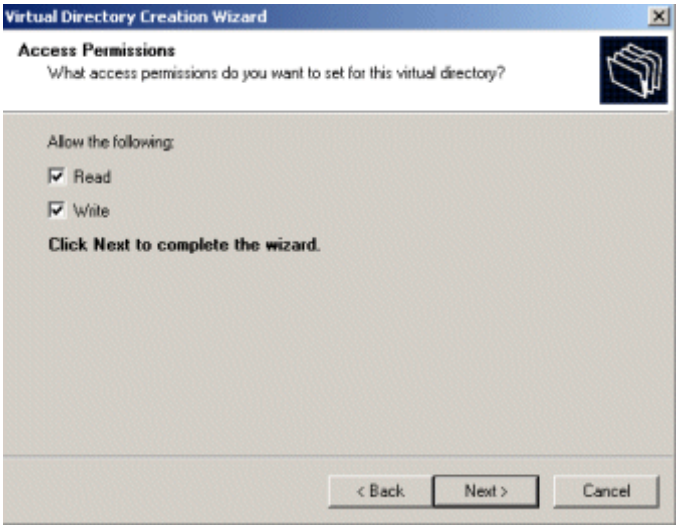
Στη συνέχεια επιλέγουμε το directory στο οποίο θα έχει πρόσβαση ο χρήστης.



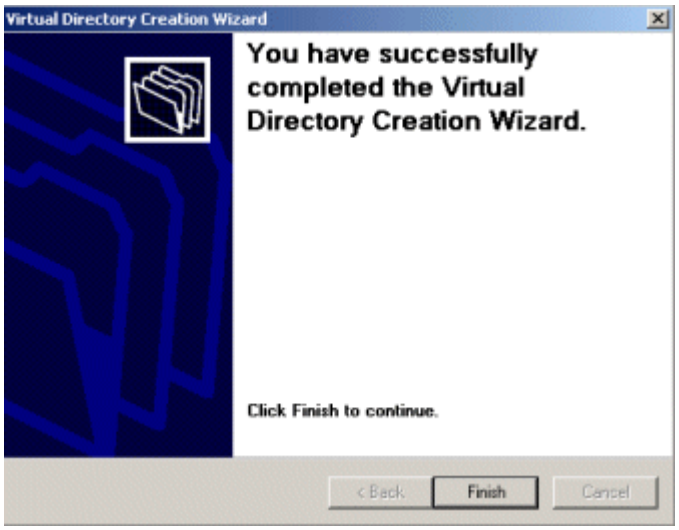
Επιλέγουμε το directory που όπως προαναφέραμε θέλουμε να είναι το wwwroot.



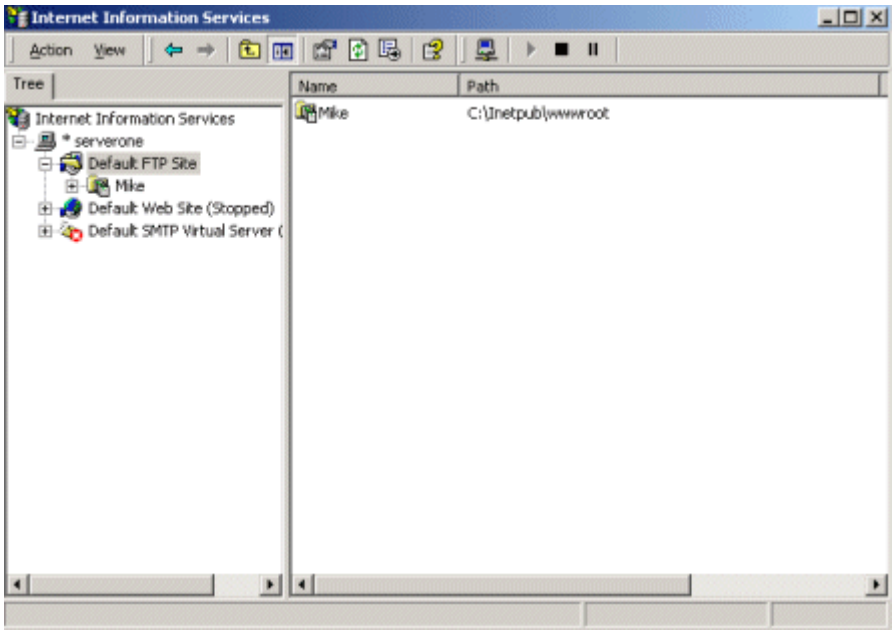
Τώρα η τοποθεσία του νέου directory φαίνεται στο κουτί επιλογής τοποθεσίας. Μετά επιλέγουμε next έτσι ώστε να ολοκληρώσουμε την προσθήκη ενός χρήστη του FTP Server.



Στην συνέχεια θα πρέπει να δώσουμε στον νέο χρήστη τις κατάλληλες άδειες χρήσης σύμφωνα με τις εργασίες που θέλουμε να εκτελεί ο χρήστης στον FTP Server. Επιλέγουμε “Read & Write” κάτι που σημαίνει ότι οι χρήστες έχουν πλήρης δυνατότητες μέσα στον φάκελο αλλά και στους υποφακέλους που τους έχει δοθεί πρόσβαση αρά μπορούν να γράψουν, να σβήσουν αλλά και να αλλάξουν οποιοδήποτε αρχείο βρίσκεται στον φάκελο που έχουν πρόσβαση.



Στο τέλος εμφανίζεται η παραπάνω εικόνα που σηματοδοτεί την επιτυχή ολοκλήρωση της προσθήκης του χρήστη στον FTP Server.



Τώρα μπορούμε να δούμε ότι ο χρήστης του FTP Server έχει προστεθεί στο σύστημα και έτσι τώρα μπορούμε να αλλάξουμε όποια στιγμή θέλουμε τις ιδιότητες αυτού του χρήστη με δεξί κλικ και επιλέγοντας ιδιότητες.

Σημειώνουμε ότι οι χρήστες που πρόκειται να χρησιμοποιήσουν ένα πελάτη FTP για να συνδεθούν στον FTP Server θα πρέπει να επιλέξουν τον τύπο σύνδεσης port και όχι τον passive. Ο FTP Server των Windows δεν λειτουργεί καλά με passive συνδέσεις και οι περισσότεροι χρήστες ενδέχεται να λάβουν ένα μήνυμα λάθους όταν προσπαθήσουν να συνδεθούν.

5.2 Συμπεράσματα

Σε αυτό το κεφάλαιο αναφερθήκαμε στα βήματα εγκατάστασης ενός FTP server. Η εγκατάσταση ενός FTP server αποτελεί μόνο το πρώτο βήμα της λειτουργίας ενός FTP server καθώς πάντα θα πρέπει να αναφερόμαστε και σε θέματα διαχείρισης ώστε να προσεγγίζουμε ολοκληρωμένα το θέμα. Πέραν αυτών στο επόμενο κεφάλαιο να παρουσιάσουμε και τις λογικές επόμενες εξελίξεις στον τομέα των servers καθώς τα μέχρι στιγμής δείγματα γραφής της τεχνολογίας προμηνύουν σημαντικές εξελίξεις.

6. ΔΙΑΧΕΙΡΙΣΗ ΕΝΟΣ ΔΙΑΚΟΜΙΣΤΗ

6.1 Διαχείριση του Internet Information Services των Windows

Όπως είδαμε και στο προηγούμενο κεφάλαιο χρησιμοποιήθηκε η υπηρεσία Internet Information Services (IIS) των Windows ώστε να εγκαταστήσουμε τον FTP server. Σε αυτό το κεφάλαιο εξετάζουμε ορισμένες παραμέτρους διαχείρισης του server μας.

Η προτεραιότητα των νέων εκδόσεων του IIS δίνει μεγαλύτερη βάση στην ευκολότερη διαχείριση του Web και FTP server. Αρχικά όπως είδαμε και στο προηγούμενο κεφάλαιο η διαδικασία της εγκατάστασης έγινε πιο εύκολη και χτίστηκε πάνω στα Windows 2000 Server. Επιπλέον για να μπορούν να γίνουν πιο εύκολα οι ρυθμίσεις που αφορούν την ασφάλεια (Security), υπάρχουν τρεις νέοι βοηθοί (security wizards) που μας διευκολύνουν να ρυθμίσουμε την ασφάλεια του Server μας.

6.1.1 Ολοκληρωμένη εγκατάσταση και αναβάθμιση (Integrated Setup and Upgrade) .

Η διαδικασία της εγκατάστασης για τις νέες εκδόσεις του IIS είναι ολοκληρωμένη και γίνεται μαζί με την εγκατάσταση των Windows 2000 Server. Ο IIS δηλαδή εγκαθίσταται εξ ορισμού μαζί με τα Windows 2000 Server σαν μια δικτυακή υπηρεσία . Η εύκολη και εύχρηστη εγκατάστασή του μας δίνει την δυνατότητα είτε να κάνουμε εγκατάσταση κάποια νέα έκδοση του είτε να κάνουμε αναβάθμιση σε κάποια παλαιότερη έκδοση που υπάρχει στο σύστημα μας.

Ο IIS δημιουργεί ένα default Web site και ένα FTP site όταν εγκαθίστανται τα Windows 2000 Server. Μπορούμε να προσθέσουμε ή να αφαιρέσουμε τον IIS επιλέγοντας additional components (επιπρόσθετα αντικείμενα) χρησιμοποιώντας την εφαρμογή Add/Remove Programs (Πρόσθεση/αφαίρεση Προγραμμάτων) από τον Control Panel (Πίνακα Ελέγχου) όπως είδαμε και στο προηγούμενο κεφάλαιο.

Εάν κάνουμε αναβάθμιση σε Windows 2000, ο IIS 5.0 είναι διαθέσιμος σε όλες τις εκδόσεις των Windows 2000. Ο IIS 5.0 θα αναβαθμίσει τα υπάρχοντα Web

sites που τρέχουν στο παλιό λειτουργικό μας σύστημα. Οι πελάτες με κάθε υπάρχουσα έκδοση των Windows NT Server 3.51 ή 4.0 θα μπορούν αυτόματα να αναβαθμίσουν τις υπηρεσίες τους στα Windows 2000 Server και θα αποκτήσουν και τα πλεονεκτήματα των νέων χαρακτηριστικών και των νέων υπηρεσιών που υπάρχουν στα Windows 2000 Server και στον IIS. Στην αγορά αυτή την στιγμή υπάρχει διατίθεται και η νέα έκδοση IIS ver 6.0 η οποία διατίθεται με τον Windows Server 2003 αλλά επιλέξαμε να κάνουμε την αναφορά μας στα Windows 2000 που είναι και ευρέως διαδεδομένα.

6.1.2 Centralized Administration (Συγκεντρωμένη Διαχείριση) .

Ο IIS χρησιμοποιεί την κονσόλα Internet Information Services Microsoft Management Console (MMC). Τα εργαλεία του διαχειριστή (administration tool) για τον IIS είναι ενοποιημένα με τις υπόλοιπες λειτουργίες του διαχειριστή των Windows 2000. Σε προηγούμενες αναφορές αυτά τα εργαλεία ονομάζονταν Internet Service Manager. Η προσπέλαση των υπηρεσιών Internet Information Services γίνεται κάνοντας «κλικ» στο **Administrative Tools** , στην συνέχεια κάνοντας «κλικ» στο **Computer Management** και εκεί επιλέγετε **Server Applications and Services** . Το εργαλείο του διαχειριστή που είναι βασισμένο στον browser (browser-based), Internet Services Manager, δεν είναι πλέον διαθέσιμο στο Administrative Tools, αλλά παραμένει ακόμα διαθέσιμο για να μας επιτρέπει η διαχείριση από απομακρυσμένα μέρη του IIS μέσα από μια HTTP σύνδεση. Επιπρόσθετα, μπορούμε να χρησιμοποιήσουμε τις Terminal υπηρεσίες για απομακρυσμένη διαχείριση του IIS .

6.1.3 Απομακρυσμένη διαχείριση .

Η διαχείριση ενός υπολογιστή από διαχειριστή που εργάζεται σε άλλον υπολογιστή, ο οποίος είναι συνδεδεμένος στον άλλο υπολογιστή του δικτύου ονομάζεται απομακρυσμένη διαχείριση. Τα εργαλεία του διαχειριστή που είναι βασισμένα στο δίκτυο (Web based) επιτρέπουν την απομακρυσμένη διαχείριση του server μας από σχεδόν οποιονδήποτε browser από οποιαδήποτε πλατφόρμα. Όπως ακριβώς και στην τοπική διαχείριση, υπάρχουν δύο επιλογές – διεπιφάνειες για απομακρυσμένη διαχείριση του server. Η πρώτη επιλογή είναι η βασισμένη στον browser (browser-based) που γίνεται δια μέσου του MMC snap-in. (Για να χρησιμοποιηθεί το MMC snap-in απομακρυσμένα απαιτείται ο απομακρυσμένος

υπολογιστής να έχει εγκατεστημένα τα Windows 2000). Η δεύτερη επιλογή είναι το browser-based Internet Services Manager (HTMLA) και μας επιτρέπει απομακρυσμένη διαχείριση τον χαρακτηριστικών του IIS από το Internet ή δια μέσου ενός proxy server. Επιπρόσθετα σε αυτές τις δύο επιλογές μπορούμε να χρησιμοποιήσουμε και τις Terminal υπηρεσίες για να προσπελάσουμε είτε με το MMC είτε με το HTMLA εργαλείο διαχείρισης.

6.1.4 Ανάθεση διαχείρισης (Delegated Administration) .

Για να ελαττωθεί ο φόρτος εργασίας στα έργα του διαχειριστή (administrative tasks) με τον IIS ο διαχειριστής μπορεί να δημιουργήσει λογαριασμούς Administration accounts που ονομάζονται Web Site και FTP Operators και αυτοί οι λογαριασμοί να έχουν περιορισμένα διοικητικά δικαιώματα (administration privileges) στα Web sites. Δηλαδή με αυτή την ιδιότητα οι διαχειριστές αναθέτουν την διαχείριση κάποιων Site σε ορισμένους χειριστές για να μην έχουν αυτοί όλο το βάρος της εργασίας. Αυτοί οι χειριστές όμως έχουν δικαιώματα μόνο πάνω στα αντίστοιχα Sites και FTP directories για τα οποία θα είναι υπεύθυνοι. Δεν έχουν δικαιώματα στα χαρακτηριστικά και δεν μπορούν να επηρεάσουν τον IIS ή το δίκτυο .

6.1.5 Process Accounting .

To Process Accounting (μερικές φορές αναφέρεται και ως CPU Usage Logging , CPU Accounting ή Job Object Accounting) είναι ένα νέο χαρακτηριστικό στον IIS με την βοήθεια του οποίου επιτρέπεται στους διαχειριστές να παρακολουθούν και να διαχειρίζονται την χρησιμοποίηση της CPU και των διάφορων πόρων μέσα από τα Web Sites του server. Η υπηρεσία παροχής Internet (ISP), μπορεί να χρησιμοποιήσει αυτές τις πληροφορίες για να καθορίσει ποια sites χρησιμοποιούν μεγάλη επεξεργαστική ισχύ και πολλούς πόρους ή το ποια sites μπορεί να έχουν δυσλειτουργικά scripts ή Common Gateway Interface (CGI) επεξεργασίες . Οι διαχειριστές (IT managers) μπορούν να χρησιμοποιήσουν αυτές τις πληροφορίες για να υπολογίσουν το κόστος της φιλοξενίας του Web Site και των εφαρμογών και να τοποθετούν ανάλογα το Site σε κατάλληλο τμήμα της εταιρίας.

Η υπηρεσία Process Accounting μπορεί να κρατήσει μόνο πληροφορίες γύρω από τις out-of-process εφαρμογές. Η υπηρεσία process accounting είναι διαθέσιμη μόνο για τα Web sites και όχι για τα FTP sites .

Η υπηρεσία Process accounting προσθέτει πεδία στο εκτεταμένο (Extended) W3C log αρχείο. Αυτά τα πεδία καταγράφονται μόνο όταν η δομή W3C Extended log file είναι επιλεγμένη. Οι πληροφορίες process accounting είναι αναμιγμένες με άλλες logging πληροφορίες στο αρχείο .

6.1.6 Βελτιωμένο Command-Line Administration Scripts (Improved Command-Line Administration Scripts) .

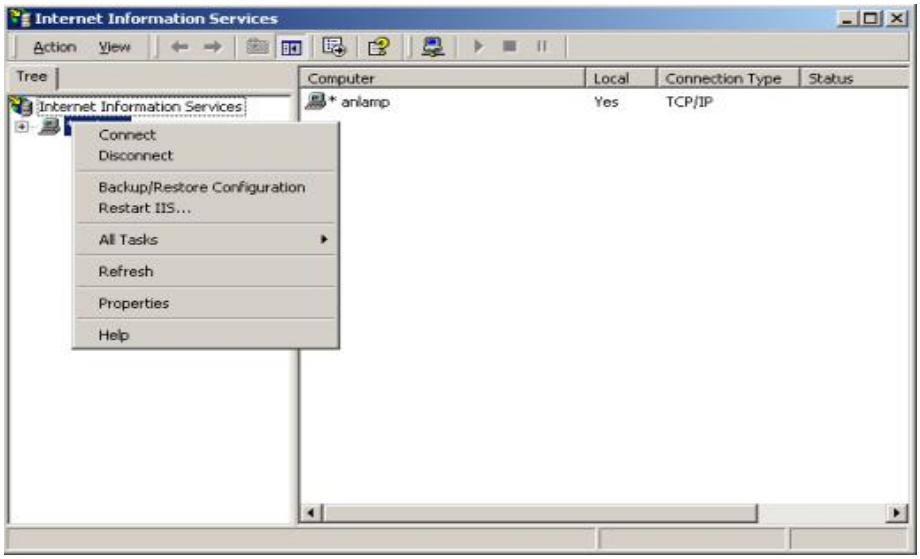
Τα scripts στον IIS μπορούν να εκτελούνται και από το command line για να γίνεται πιο αυτόματη η διαχείριση των συνηθισμένων έργων του Web server. Τα administration scripts αυτοματοποιούν κάποιες από τις περισσότερο συνηθισμένες εργασίες του διαχειριστή. Έτσι μπορούμε να χρησιμοποιήσουμε αυτά τα script για να δημιουργήσουμε και να ελέγξουμε τα Web sites, τις εφαρμογές, τους φακέλους και πολλά άλλα. Οι διαχειριστές επίσης μπορούν να δημιουργήσουν scripts που θα αυτοματοποιούν την διαχείριση του IIS.

Γραμμένα σε Visual Basic Scripting (VBScript), τα Administration Scripts χρησιμοποιούνται μαζί με την υπηρεσία Cscript.exe command-line scripting και λειτουργούν καλύτερα εάν το Cscript είναι ρυθμισμένο να εκτελεί .vbs αρχεία. Μπορούμε να εκτελούμε τα Administration Scripts χρησιμοποιώντας VBScript αρχεία τα οποία μπορούν εξ ορισμού να τρέχουν στον κατάλογο directory Inetpub\adminscripts. Για να βελτιώσουμε την απόδοση, μπορούμε επίσης να χρησιμοποιήσουμε μια έκδοση του adsutil.vbs (adsutil.exe, το οποίο είναι επίσης εγκατεστημένο εξ ορισμού στον φάκελο Inetpub\adminscripts). Αυτή η έκδοση δέχεται τις ίδιες παραμέτρους όπως το adsutil.vbs. Το Adsutil.exe είναι ένα δείγμα το οποίο επιδεικνύει το πώς μεταχειρίζεται η metabase χρησιμοποιώντας την υπηρεσία Active Directory Service Interfaces (ADSI) σε C/C++. (Το Adsutil.exe μπορεί να διαβάσει εντολές από αρχεία ενώ το adsutil.vbs δεν μπορεί)

6.1.7 Backing Up και αποκατάσταση (Restoring) IIS .

Το IIS Microsoft Management Console (MMC) snap-in περιλαμβάνει επιλογές που μας επιτρέπουν να πάρουμε back up τις ρυθμίσεις του IIS μας. Χρησιμοποιώντας αυτή την μέθοδο μας επιτρέπετε να κρατήσουμε back up και να επαναφέρουμε τις ρυθμίσεις του Web Server μας, αλλά όχι και τα αρχεία σας ή εκείνες τις ρυθμίσεις που παραμένουν στην registry. Αυτή η μέθοδος δεν θα λειτουργήσει αν απεγκαταστήσουμε τελείως τον IIS και τα αποτελεσματικά backup αρχεία δεν μπορούν να χρησιμοποιηθούν για να επαναφερθούν οι ρυθμίσεις του IIS σε κάποια άλλα συστήματα που τρέχουν με τα Windows 2000. Μπορούμε να κρατήσουμε back up τις ρυθμίσεις του IIS χρησιμοποιώντας επίσης την υπηρεσία που είναι βασισμένη στον πλοηγό (browser-based) Internet Services Manager (HTMLA), αλλά πρέπει να χρησιμοποιήσουμε το IIS snap-in για να επαναφέρουμε τις ρυθμίσεις του IIS .

Η παρακάτω εικόνα μας δείχνει πως μπορούμε να κάνουμε με τις IIS υπηρεσίες Back Up και Restore .



6.1.8 Συνήθη μηνύματα σφαλμάτων (Custom Error Messages) .

Όταν ένας χρήστης προσπαθεί να συνδεθεί σε ένα Web site και εμφανίζετε ένα HTTP error, ένα μήνυμα αποστέλλεται στον client browser με μια σύντομη περιγραφή για το τι συνέβηκε κατά την διάρκεια της προσπάθειας για σύνδεση με το δίκτυο. Με τον IIS μπορούμε να αποστείλουμε περισσότερα πληροφοριακά μηνύματα

λαθών στον client τα οποία συμβαίνουν στις ASP ή HTML σελίδες. Μπορούμε να χρησιμοποιήσουμε τα καθιερωμένα λάθη που παρέχει ο IIS ή να δημιουργήσουμε δικά μας .

Όλα τα καθιερωμένα μηνύματα λαθών που περιέχει ο IIS εμφανίζουν προκατασκευασμένα (industry) και πρότυπα (standard) κομμάτια HTTP κώδικα, τα οποία εξασφαλίζουν συνοχή και συμβατότητα με τα μηνύματα λαθών του πρωτοκόλλου HTTP. Για παράδειγμα, εάν ένας χρήστης προσπαθήσει να συνδεθεί σε ένα Web site στο οποίο έχουν συνδεθεί ήδη τόσοι χρήστες όσους μπορεί να εξυπηρετήσει το Web Site ένα μήνυμα λάθους θα επιστρέψει σε μια HTML σελίδα που θα λέει " Too many users.".

Με τα Windows 2000 Server επιτρέπεται στον διαχειριστή να χρησιμοποιήσει το εργαλείο για ανάπτυξη και διαχείριση ιστοσελίδων Microsoft FrontPage. Με το εργαλείο FrontPage Server Extensions, οι διαχειριστές μπορούν να βλέπουν και να διαχειρίζονται τα Web site τους μέσα από ένα γραφικό περιβάλλον (graphical interface). Επιπρόσθετα οι δημιουργοί των σελίδων μπορούν να δημιουργήσουν, να διορθώσουν και να δημοσιεύσουν τις σελίδες τους από απομακρυσμένα μέρη.

6.2 Οι Μελλοντικές Εξελίξεις των Servers

Οι μελλοντικές εξελίξεις στον τομέα των Servers που παρέχουν δυνατότητες εγκατάστασης τόσο WEB αλλά και FTP servers επηρεάζονται από την ολοένα και αυξανόμενη χρήση του διαδικτύου από όλο και περισσότερους ανθρώπους. Ο στόχος των εταιριών που παρέχουν εφαρμογές για την εγκατάσταση των WEB και FTP servers από εδώ και στο εξής είναι μαζί με την τρομερή αύξηση των απλών χρηστών του διαδικτύου να αυξηθεί και ο αριθμός των advanced χρηστών. Ο μόνος τρόπος για να επιτευχθεί αυτό είναι η απλούστευση των εφαρμογών εγκατάστασης των WEB και FTP servers. Ήδη η Microsoft έχει σχεδιάσει την έκδοση IIS 7.0 η οποία θα είναι διαθέσιμη μαζί με τα Windows Longhorn τα οποία θα παρουσιαστούν κάποια στιγμή το 2006.

Οι περιοχές οι οποίες πιστεύουμε θα εξελιχθούν σε σχέση με την τωρινή κατάσταση έχουν να κάνουν με δύο γενικές κατηγορίες. Η πρώτη είναι η αναπόφευκτη αύξηση της δυναμικής ισχύος των προσωπικών υπολογιστών τα χρόνια που έρχονται αλλά και η αύξηση των ταχυτήτων μεταφοράς δεδομένων στο διαδίκτυο

όπως έχει ήδη γίνει με την εισαγωγή του ADSL. Το γεγονός αυτό θα οδηγήσει στην μεγαλύτερη εμπορευματοποίηση αλλά και χρήση του διαδικτύου για παροχές τις οποίες αυτή την στιγμή δεν θα μπορούσαμε να σκεφτούμε όπως για παράδειγμα Internet-TV και Internet-Movie Channels.

Είναι φυσικό ότι για την υποστήριξη των παραπάνω νέων υπηρεσιών δεν είναι αρκετή μόνο η αναβάθμιση σε υπολογιστική δύναμη αλλά χρειάζεται και αναβάθμιση των εφαρμογών που παρέχουν υπηρεσίες εγκατάστασης web και ftp servers. Ένα επόμενο βήμα αυτών των εφαρμογών είναι η διάσπαση των επιμέρους λειτουργιών σε ξεχωριστά τμήματα έχοντας την δυνατότητα να χρησιμοποιείς μόνο αυτά που χρειάζονται όπως για παράδειγμα εάν οι εφαρμογές μας δεν χρησιμοποιούν Common Gateway Interfaces (CGI) μπορούμε απλά να τις διαγράψουμε. Με αυτό τον τρόπο μπορούμε να στήσουμε ή την ιστοσελίδα μας ή τον FTP server μας μόνο με τις υπηρεσίες που χρειαζόμαστε αυξάνοντας έτσι και τα επίπεδα διαχείρισης και ασφάλειας εφόσον πλέον ξέρουμε να διαχειριστούμε τις υπηρεσίες που επιλέγουμε.

Τέλος μια άλλη υπηρεσία που σχετίζεται με τους web και ftp server και η οποία εκτιμάται ότι θα πρωταγωνιστήσει στις εξελίξεις είναι η διαχείριση. Όπως προαναφέραμε το μέγεθος και η πολυπλοκότητα των ιστοσελίδων πρόκειται να μεγαλώσει με εκρηκτικούς ρυθμούς τα επόμενα χρόνια. Μαζί με αυτό αυξάνεται και η πολυπλοκότητα (complexity) της διαχείρισης των διαφόρων ιστοσελίδων. Ένας από τους τομείς λοιπόν που θα δούμε πολλές εξελίξεις είναι ο τρόπος διαχείρισης καθώς θα υπάρξουν περισσότερες δυνατότητες διαχείρισης των servers από απόσταση διευκολύνοντας έτσι τρομερά το έργο των διαχειριστών καθώς επίσης θα αυξηθεί η δυνατότητα διαχείρισης πολλαπλών servers ταυτόχρονα.

6.3 Συμπεράσματα

Σε αυτό το κεφάλαιο αναφερθήκαμε σε θέματα διαχείρισης ενός server καθώς και στις προοπτικές εξέλιξης των server τα επόμενα χρόνια. Στο επόμενο και τελευταίο κεφάλαιο θα παρουσιάσουμε ένα ειδικό θέμα διαχείρισης και συγκεκριμένα τους τρόπους ασφαλούς παραμετροποίησης του FTP server μας.

7. ΕΙΔΙΚΟ ΘΕΜΑ ΔΙΑΧΕΙΡΙΣΗΣ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΕΝΟΣ ΔΙΑΚΟΜΙΣΤΗ

7.1 10 Πρακτικές Ασφαλούς Διαχείρισης ενός διακομιστή FTP

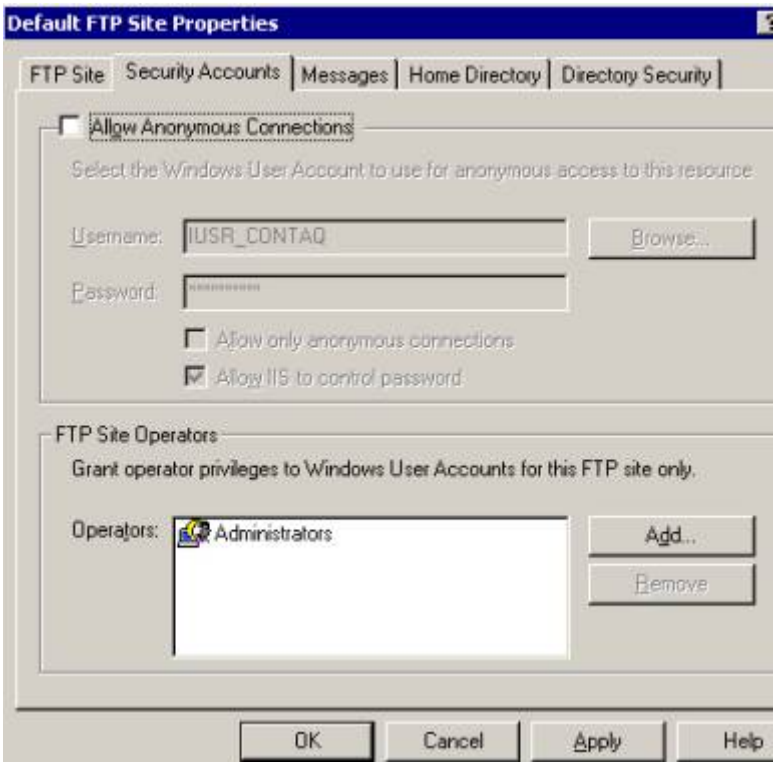
Στην συνέχεια παρατίθενται 10 τρόποι με τους οποίους μπορούν να αποφευχθούν κενά ασφάλειας και να ισχυροποιηθεί η αξιοπιστία του FTP Server μας.

7.1.1 Απενεργοποίηση της Ανώνυμης Πρόσβασης

Η ανώνυμη πρόσβαση είναι προεπιλεγμένη την πρώτη φορά που εγκαθίστανται οι υπηρεσίες του FTP στα Windows 2000. Η ανώνυμη πρόσβαση είναι μια μέθοδος σύμφωνα με την οποία ο κάθε χρήστης μπορεί να έχει πρόσβαση στον FTP Server χωρίς να χρειάζεται λογαριασμό χρήστη.

Υπάρχουν περιπτώσεις που η χρήση ανώνυμης πρόσβασης FTP Server δεν επηρεάζει την ασφάλεια του συστήματός μιας και παρέχει χρήσιμες υπηρεσίες στους επισκέπτες του FTP Server. Η πλειονότητα όμως των ελευθέρου χρόνου ανώνυμων χρηστών ενδέχεται να χρησιμοποιήσουν τον FTP Server με στόχο να αποθηκεύσουν παράνομα αρχεία (π.χ. μουσική, παιχνίδια, εφαρμογές).

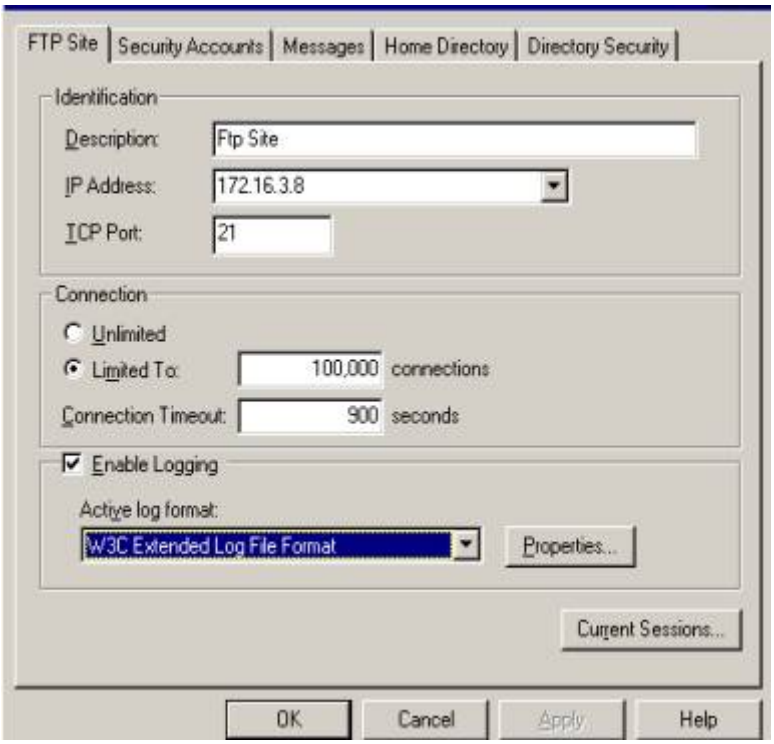
Με την απενεργοποίηση της δυνατότητας ανώνυμης πρόσβασης στον FTP Server περιορίζεται η πρόσβαση σε χρήστες που θα πρέπει να περάσουν πρώτα από μία διαδικασία επικύρωσης και ταυτοποίησης (authentication) του λογαριασμού χρήστη που θα τους έχει δοθεί. Οι δικλείδες ασφαλείας και οι παράμετροι χρήσης της υπηρεσίας του FTP από τους κατόχους λογαριασμών χρηστών παραμετροποιούνται με την χρήση των Λιστών Πρόσβασης (ACLs – Access Control List) όπως αυτά ορίζονται στον αρχικό φάκελο του FTP χρησιμοποιώντας τις παραμέτρους ασφαλούς πρόσβασης του NTFS.



Για τον περιορισμό της ανώνυμης πρόσβασης στον FTP Server θα πρέπει να απενεργοποιηθεί η επιλογή Allow Anonymous Connections όπως φαίνεται και στην παραπάνω εικόνα.

7.1.2 Ενεργοποίηση της Καταγραφής

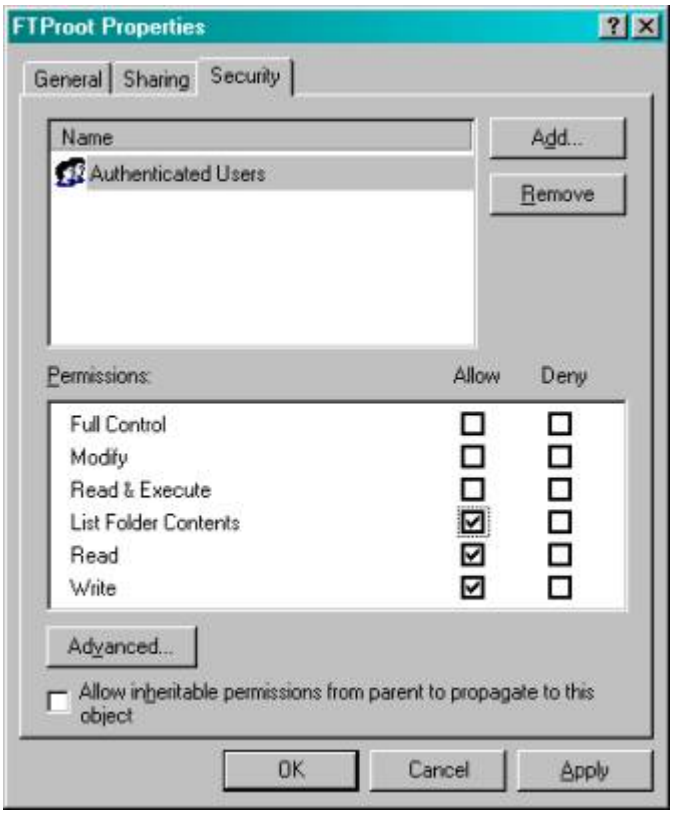
Με την ενεργοποίηση της επιλογής της καταγραφής των κινήσεων των χρηστών του FTP Server μπορεί να διασφαλισθεί ότι θα υπάρχει μια ακριβής καταγραφή των IP διευθύνσεων των χρηστών που χρησιμοποίησαν τον FTP Server. Διατηρώντας αυτές τις πληροφορίες και εξετάζοντας τις ανά τακτά χρονικά διαστήματα μπορούν να διαπιστωθούν παράξενες συμπεριφορές που μπορεί να οδηγήσουν στον προσδιορισμό κενών ή ακόμα και παραβιάσεων ασφάλειας.



Για να ενεργοποιηθεί η καταγραφή στον FTP Server χρησιμοποιείται η επιλογή Enable Logging στο FTP Site όπως φαίνεται στην παραπάνω εικόνα.

7.1.3 Ενίσχυση των Λιστών Πρόσβασης (ACLS)

Η πρόσβαση στον φάκελο του FTP Server θα πρέπει να ελέγχεται με την βοήθεια των λιστών πρόσβασης (ACLs) χρησιμοποιώντας τις παραμέτρους ασφαλούς πρόσβασης του NTFS. Η παράμετρος αυτή είναι τρομερά σημαντική για την ασφάλεια του συστήματος. Ο φάκελος του FTP δεν θα πρέπει να έχει την ομάδα “everyone” με πλήρη δικαιώματα πρόσβασης γιατί αυτό θα περιορίσει σημαντικά την δυνατότητα του διαχειριστή να ελέγχει τις ομάδες χρηστών που θα έχουν πρόσβαση στα στοιχεία και στις πληροφορίες που υπάρχουν μέσα στον FTP server.

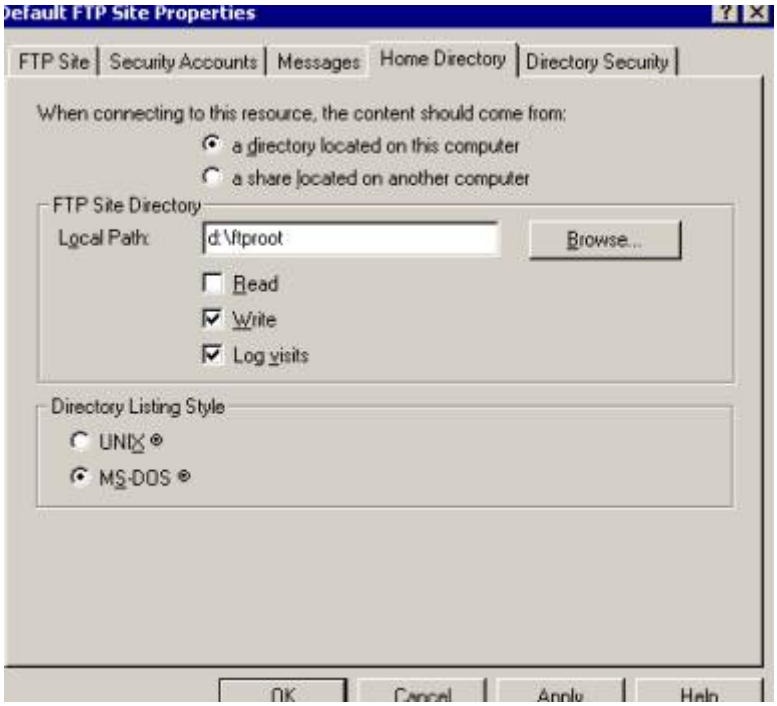


Οι τυπικές επιλογές για τους χρήστες του FTP site θα πρέπει να είναι Read, Write, και List μόνο αλλά στην περίπτωση της τυφλής παραμετροποίησης θα πρέπει να δίνεται πρόσβαση μόνο στην επιλογή Write

7.1.4 Παραμετροποίηση του FTP site ως Blind Put.

Σε περίπτωση που χρειάζεται οι χρήστες του FTP server να μεταφέρουν αρχεία μόνο προς τον FTP server και όχι από αυτόν τότε θα πρέπει να επιλεγεί η παραμετροποίηση του FTP server ως "blind put". Αυτό σημαίνει ότι οι χρήστες θα έχουν την δυνατότητα πρόσβασης στον FTP server αλλά μόνο για να μεταφέρουν αρχεία και όχι για να τα επεξεργάζονται καθώς δεν μπορούν να τα δουν. Με αυτό τον τρόπο διασφαλίζονται τα περιεχόμενα του FTP server σε περίπτωση που κάποιος μη εξουσιοδοτημένος χρήστης προσπαθήσει να επεξεργαστεί αρχεία που βρίσκονται στον FTP server

Η παραμετροποίηση για την δημιουργία των Blind Puts θα πρέπει να γίνει τόσο στον FTP server όσο και στον φάκελο με τις παραμέτρους ασφαλούς πρόσβασης του NTFS.



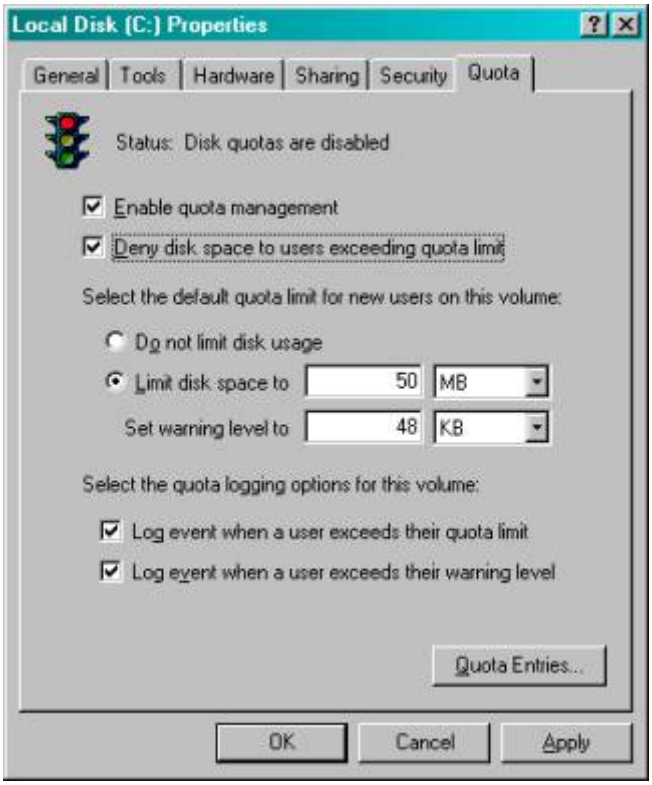
Η παραπάνω εικόνα δείχνει πως αφαιρείται η επιλογή πρόσβασης read από το FTP site χρησιμοποιώντας το Home Directory Tab που βρίσκεται στην παραμετροποίηση του *FTP server*

7.1.5 Ενεργοποίηση Ορίων Χρήσης του Δίσκου (Disk Quotas)

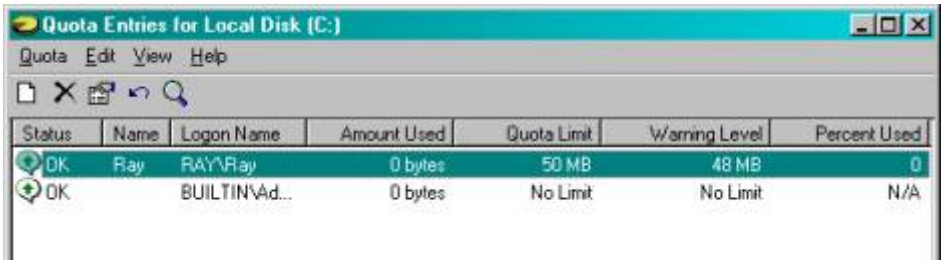
Τα Windows 2000 έχουν μια πολύ καλή εφαρμογή η οποία επιτρέπει την επιβολή ορίων χρήσης του σκληρού δίσκου του υπολογιστή. Η επιβολή ορίων χρήσης στον δίσκο μπορεί να περιορίσει το μέγεθος του διαθέσιμου χώρου στον δίσκο που μπορεί να έχει κάποιος χρήστης του FTP server. Ως προεπιλογή η κυριότητα των πληροφοριών δίδεται σε όποιον χρήστη έχει δημιουργήσει πρώτος το συγκεκριμένο αρχείο. Με την ενεργοποίηση των ορίων χρήσης του σκληρού δίσκου και ενεργοποιώντας την επιλογή άρνησης παραχώρησης περισσότερου χώρου στον σκληρό δίσκο σε όσους έχουν υπερβεί το αρχικό όριο, μπορεί να περιορισθεί η πιθανή ζημιά που θα προκληθεί εάν κάποιος μη εξουσιοδοτημένος χρήστης "καταλάβει" τον σκληρό δίσκο. Μια χειρότερη εκδοχή της παραπάνω περίπτωσης είναι η χρησιμοποίηση του FTP server μέχρι να γεμίσει από δεδομένα ο σκληρός δίσκος. Το γεγονός αυτό φυσικά μπορεί να έχει καταστροφικές συνέπειες και σε άλλες υπηρεσίες που μπορεί να μοιράζονται τον ίδιο χώρο με αυτό του FTP server στον σκληρό δίσκο.

Επιπρόσθετα, με το να περιορισθεί το ποσοστό του σκληρού δίσκου που μπορεί να χρησιμοποιήσει ο κάθε χρήστης, ο FTP server μετατρέπεται σε ένα

καθόλου δημοφιλή στόχο για τους επίδοξους hackers που ψάχνουν κάποιο χώρο για να αποθηκεύσουν τα αρχεία τους.



Η ενεργοποίηση του "Enable Quota Management" που βρίσκεται στο Quota Tab στο παράθυρο των παραμέτρων του NTFS disk partition γίνεται όπως φαίνεται στην παραπάνω εικόνα



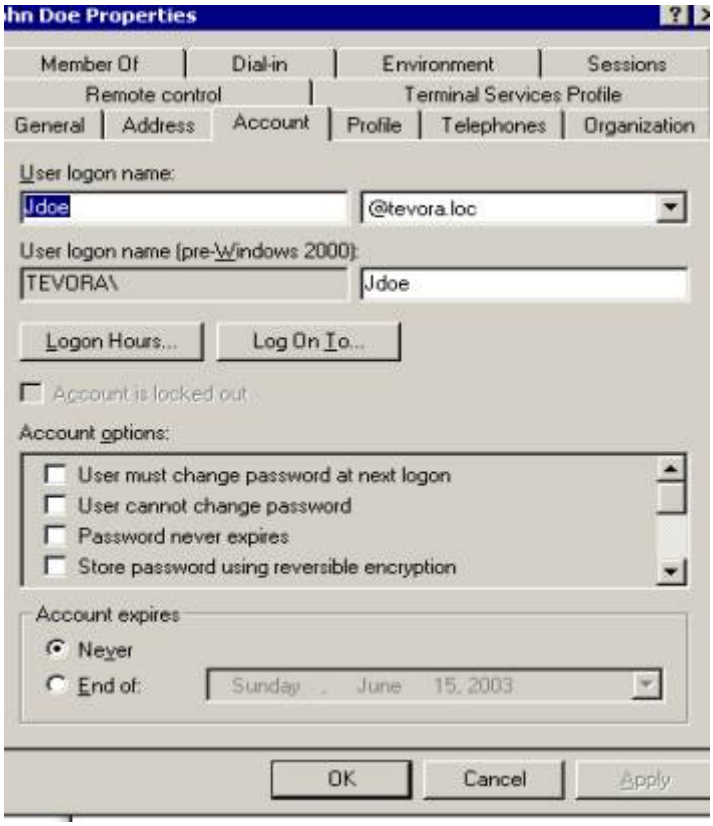
Τα όρια χρήσης του σκληρού δίσκου μπορούν να παραμετροποιηθούν μόνο σε επίπεδο χρήστη.

7.1.6 Ενεργοποίηση Περιορισμού Χρόνου Σύνδεσης (Logon Time)

Τα Windows 2000 έχουν μεταφέρει από τα NT 4.0 την δυνατότητα να περιορίζουν τις ώρες σύνδεσης των χρηστών. Αυτή η επιλογή περιορίζει την σύνδεση του χρήστη μόνο σε συγκεκριμένες ώρες της ημέρας (π.χ. από τις 8 π.μ. μέχρι τις 8 μ.μ.).

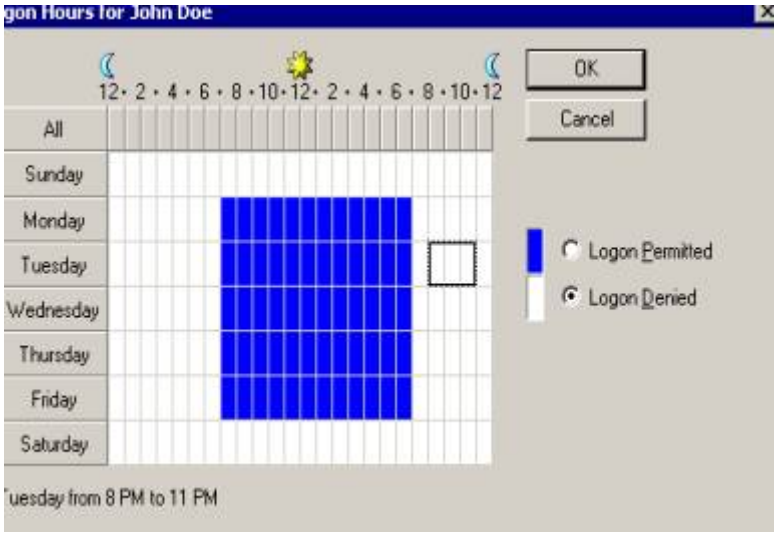
Η δυνατότητα αυτή μπορεί να χρησιμοποιηθεί αποτελεσματικά περιορίζοντας την πρόσβαση στον FTP server μόνο σε εγκεκριμένες ώρες. Έτσι εάν για παράδειγμα

ο FTP server χρησιμοποιείται για επιχειρηματικούς σκοπούς μπορούν να περιορισθούν οι ώρες πρόσβασης ώστε να συμπίπτουν με τις ώρες γραφείου. Με τον τρόπο αυτό προφυλάσσεται ο FTP server από κακόβουλες επιθέσεις σε ώρες που δεν γίνεται να ελέγχεται η κίνηση στον FTP server.



Η παραμετροποίηση των χρόνων σύνδεσης στα Windows 2000 υπάρχουν στο Active Directory Users and Computers όπως φαίνεται στην παραπάνω εικόνα

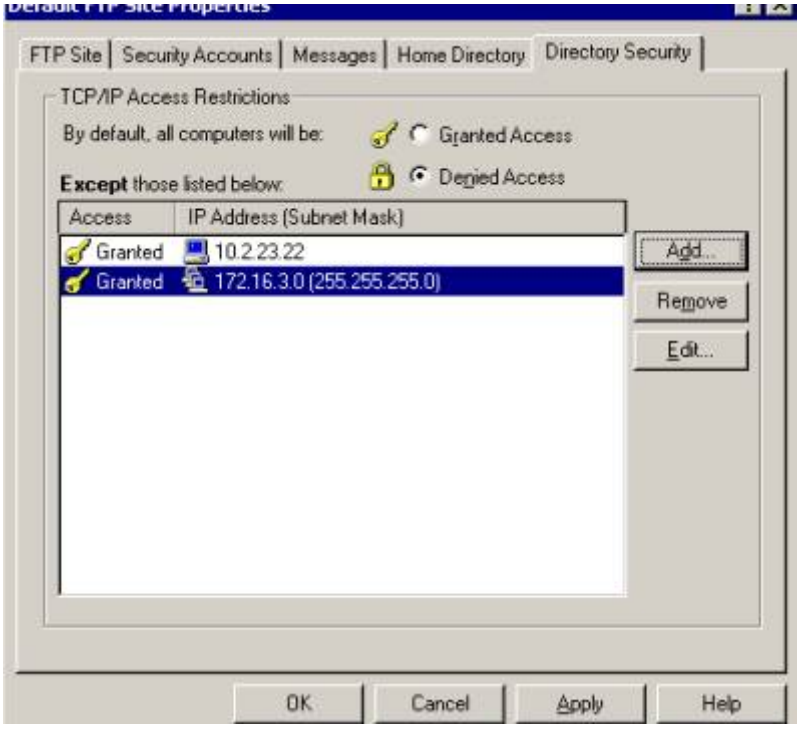
net user <UserName> /times:



** Σημειώνεται ότι οι τοπικοί χρήστες δεν έχουν την δυνατότητα παραμετροποίησης σχετικά με τις ώρες πρόσβασης.*

7.1.7 Περιορισμός Πρόσβασης μέσω IP

Ο FTP server των Windows 2000 μπορεί να παραμετροποιηθεί ώστε να δέχεται συγκεκριμένες διευθύνσεις IP. Περιορίζοντας την πρόσβαση με αυτό τον τρόπο στον FTP server μπορεί να μειωθεί σημαντικά η έκθεση του FTP server σε χρήστες με μη εξουσιοδοτημένη πρόσβαση.



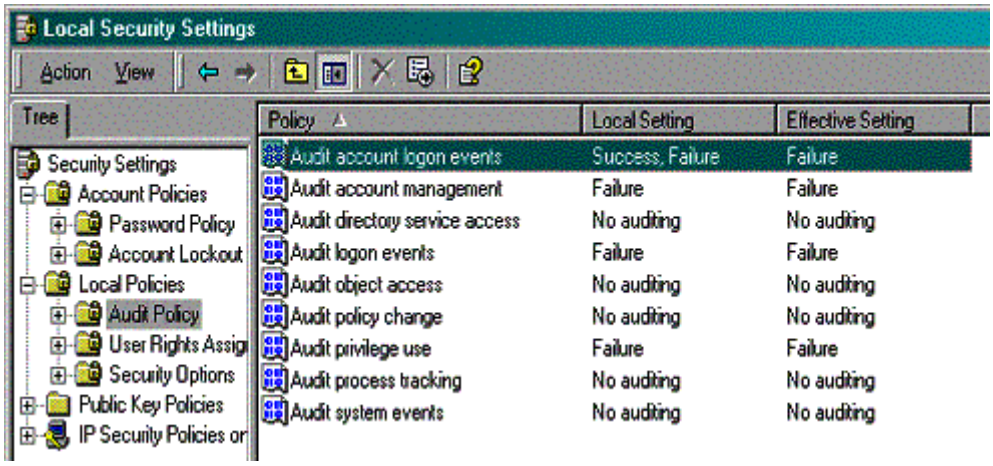
Για να περιοριστεί η πρόσβαση στο FTP μέσω IP θα πρέπει να χρησιμοποιηθεί η επιλογή Directory Security όπως φαίνεται στην παραπάνω εικόνα που βρίσκεται στις επιλογές παραμετροποίησης του FTP Server

7.1.8 Έλεγχος και Καταγραφή των Προσπαθειών Σύνδεσης (Logon Events)

Με την ενεργοποίηση του ελέγχου και καταγραφής των προσπαθειών σύνδεσης μπορεί να εξετάζονται οι επιτυχής ή ανεπιτυχής προσπάθειες σύνδεσης χρηστών με τον FTP server στο Security Log του Event Viewer

Τακτική εξέταση αυτής της καταγραφής μπορεί να προειδοποιήσει για ύποπτη συμπεριφορά όπως αυτή ενός μη εξουσιοδοτημένου χρήστη που προσπαθεί να εισέλθει στον FTP server. Μπορεί επίσης να χρησιμοποιηθεί ως μια αποτελεσματική μέθοδος ανίχνευσης επιθέσεων (IDS Intrusion Detection System) παρέχοντας

ιστορική πληροφόρηση για τις επιτυχής ή ανεπιτυχής προσπάθειες σύνδεσης χρηστών με τον FTP server.



Τα Audit Account Logon Events μπορούν να ενεργοποιηθούν χρησιμοποιώντας το εργαλείο παραμετροποίησης Local Security Policy όπως φαίνεται στην παραπάνω εικόνα.

7.1.9 Ενεργοποίηση Επιλογής Χρήσης Ισχυρών Συνθηματικών (Strong Password)

Η χρήση ισχυρών συνθηματικών είναι μια βέλτιστη πρακτική σε περιπτώσεις που γίνονται συναλλαγές με χρήστες και ζητείται η επικύρωση και ταυτοποίηση της ταυτότητας τους. Στην περίπτωση του FTP server αποτελεί ένα κρίσιμο σημείο για την διασφάλιση της ακεραιότητας του FTP server.

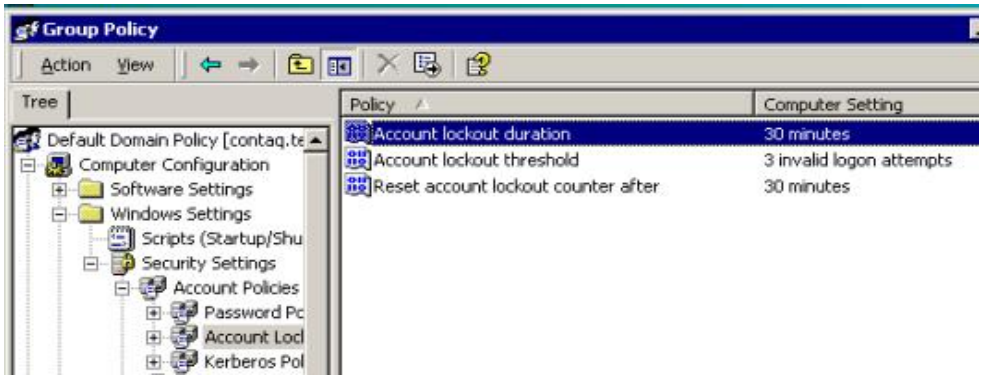
Τα Windows 2000 επιτρέπουν στον διαχειριστή του συστήματος να επιβάλει στους χρήστες την συμμόρφωση με την επιλογή χρήσης ισχυρών συνθηματικών. Με την ενεργοποίηση της επιλογής 'Passwords Must Meet Complexity Requirements' που βρίσκεται στο Local Security Policy ή στο Group Policy, οι λογαριασμοί χρηστών του FTP server θα πρέπει να συμμορφωθούν με τους παρακάτω περιορισμούς όταν επιλέγουν τα συνθηματικά τους.

- Δεν θα πρέπει να περιέχει όλο ή μέρος του ονόματος του λογαριασμού χρήστη
- Θα πρέπει να έχει τουλάχιστον 6 χαρακτήρες
- Θα πρέπει να περιέχει χαρακτήρες από 3 από τις παρακάτω 4 κατηγορίες:
    - Κεφαλαία Γράμματα
    - Μικρά Γράμματα
    - Αριθμοί
    - Χαρακτήρες εκτός από γράμματα και αριθμούς (!, $, #, %)

Τα συνθηματικά θα πρέπει να ακολουθούν πολυσύνθετες προδιαγραφές οι οποίες μπορούν να ενεργοποιηθούν χρησιμοποιώντας το εργαλείο παραμετροποίησης *Local Security Policy*.

7.1.10 Ενεργοποίηση Αυτόματου Κλειδώματος Λογαριασμού

Οι λογαριασμοί FTP είναι πολύ πιθανοί στόχοι προγραμμάτων ανίχνευσης συνθηματικών που τρέχουν μια τεράστια λίστα με συνθηματικά σε μια προσπάθεια να μαντέψουν ή να σπάσουν λογαριασμούς πρόσβασης χρηστών. Οι πολιτικές ασφάλειας των Windows 2000 επιτρέπουν στους διαχειριστές να κλειδώσουν τον αριθμό των ανεπιτυχών προσπαθειών που μπορούν να επιχειρηθούν πριν κλειδωθεί ο λογαριασμός. Με την ενεργοποίηση αυτής της επιλογής και παραμετροποιόντας το περιθώριο των ανεπιτυχών προσπαθειών προτού κλειδώσει το σύστημα ο διαχειριστής μπορεί να περιορίσει την έκθεση του FTP server σε προγράμματα ανίχνευσης συνθηματικών



Οι επιλογές Account Lockout Duration και Threshold μπορούν να ενεργοποιηθούν χρησιμοποιώντας το εργαλείο παραμετροποίησης *Local Security Policy*.

.

7.2 SECURE FILE TRANSFER PROTOCOL

Η σύνδεση του υπολογιστή με το δίκτυο εμπεριέχει κινδύνους ως προς τη διαφύλαξη των δεδομένων στον υπολογιστή μας. Το κεφάλαιο της ασφάλειας ειναι από τα πιο δύσκολα για τον διαχειριστή δικτύων. Ποτέ δεν μπορούμε να πούμε ότι είμαστε απολύτως ασφαλής από κακόβουλες επιθέσεις από το δίκτυο. Μπορούμε όμως να πάρουμε ορισμένες βασικές προφυλάξεις που μειώνουν τον κίνδυνο να βρεθούμε προ δυσάρεστων εκπλήξεων. Μια καλή πολιτική δημιουργίας αντιγράφων (backups) των κρίσιμων δεδομένων μας μπορεί να φανεί σωτήρια τη δύσκολη στιγμή.

7.3 Μπορούμε να πούμε πως η ασφάλεια μπορεί να χωριστεί στους εξής τομείς:

- Φυσική Ασφάλεια: Αυτή αφορά τον τομέα της φυσικής πρόσβασης στους υπολογιστές μας και το δίκτυο. Ποιος λ.χ. θα εχει πρόσβαση στο χώρο που βρίσκονται οι υπολογιστές, οι απολήξεις δικτύου κλπ.
- Εσωτερική Ασφάλεια: Αυτή αφορά την προστασία από κακόβουλη η αθέλητη καταστροφή / πρόσβαση δεδομένων από τους ίδιους του χρήστες του τοπικού δικτύου. Πρέπει να προσέχουμε τις άδειες πρόσβασης στα αρχεία του συστήματος (και των χρηστών), να θέτουμε πολιτική δεκτών μυστικών κωδικών (να περιέχουν αριθμούς / σύμβολα, όχι λέξεις από λεξικό) και να ενημερώνουμε τους χρήστες σχετικά με αυτήν. Οι χρήστες πρέπει από μόνοι τους να διέπονται από μια σωστή ηθική, σε σχέση με την ιδιωτικότητα των υπόλοιπων χρηστών, και να υπάρχει πολιτική αντιμετώπισης παραβιάσεων των ηθικών αυτών κανόνων.
- Εξωτερική Ασφάλεια: Αυτή αφορά την προστασία των δεδομένων μας από κακόβουλες επιθέσεις από το εξωτερικό δίκτυο. Ο διαχειριστής του δικτύου πρέπει να απομονώσει τις επισφαλείς υπηρεσίες όπως του ftp και το telnet και να τις αντικαταστήσει με άλλες ασφαλής όπως το ssh. Η παρακολούθηση των αναβαθμίσεων του λογισμικού που έχουμε εγκαταστήσει και η εγρήγορση σχετικά με την ανακοίνωση ελαττωμάτων ασφάλειας του λογισμικού μας ειναι απαραίτητη για την ασφάλεια του δικτύου μας. Η ανίχνευση εισβολέων με κατάλληλο λογισμικό, η τακτική ανάγνωση των logs του συστήματος και η παρακολούθηση των θυρών του δικτύου μας ειναι απαραίτητη. Επίσης ειναι

απαραίτητο να θέσουμε firewalls στο δίκτυο μας που να ελέγχουν τις επιτρεπτές υπηρεσίες δικτύου. Πολλά δίκτυα θέτουν την πρόσβαση στο ευρύτερο δίκτυο μέσω υπολογιστών proxy που προστατεύουν από την άμεση πρόσβαση του εξωτερικού δικτύου στους υπολογιστές μας.

Πλεονεκτήματα ασφαλούς μεταφοράς αρχείων:

- Μεταφορά ασφαλούς δεδομένων μεταξύ δύο θέσεων
- Απαιτούν μόνο έναν web browser
- Παρέχουν την προστασία του κωδικού πρόσβασης της ταυτότητας του χρήστη και την κρυπτογραφημένη διαδικασία
- Μεταφέρουν στοιχεία σχεδόν σε οποιοδήποτε τύπο υπολογιστή συμπεριλαμβανομένης της IBM DIS υπολογιστών Unisys.

Όταν χρησιμοποιείται ένα πρόγραμμα FTP (όπως WS_FTP) για να έχουμε πρόσβαση σε έναν κεντρικό υπολογιστή δικτύου, στέλνουμε τα στοιχεία μεταξύ της τοπικής μηχανής μας και του κεντρικού υπολογιστή " κάπου εκεί έξω ". Αυτές οι πληροφορίες μπορούν να παρεμποδιστούν από τους αδίστακτους χάκερ Ιστού. Αυτό σημαίνει ότι, οτιδήποτε στέλνουμε μέσω του web, που περιλαμβάνει το όνομα χρήστη (username) μας και τον κωδικός πρόσβασης μας (password), μπορεί να αντιμετωπισθεί από τον καθέναν με τα σωστά εργαλεία. Τα τελευταία χρόνια, οι διοικητές κεντρικών υπολογιστών δικτύου ενδιαφέρονται όλο και περισσότερο για την ασφάλεια των πληροφοριών των πελατών τους, και των σελίδων του παγκόσμιου ιστού.

Εάν χρησιμοποιούμε τον ίδιο κωδικό πρόσβασης και όνομα χρήστη για το ηλεκτρονικό μας ταχυδρομείο, στον online τραπεζικό λογαριασμό μας, κ.λπ., διατρέχουμε τον κίνδυνο κάπου να ανακαλύπτει το όνομα και ο κωδικός πρόσβασής μας.

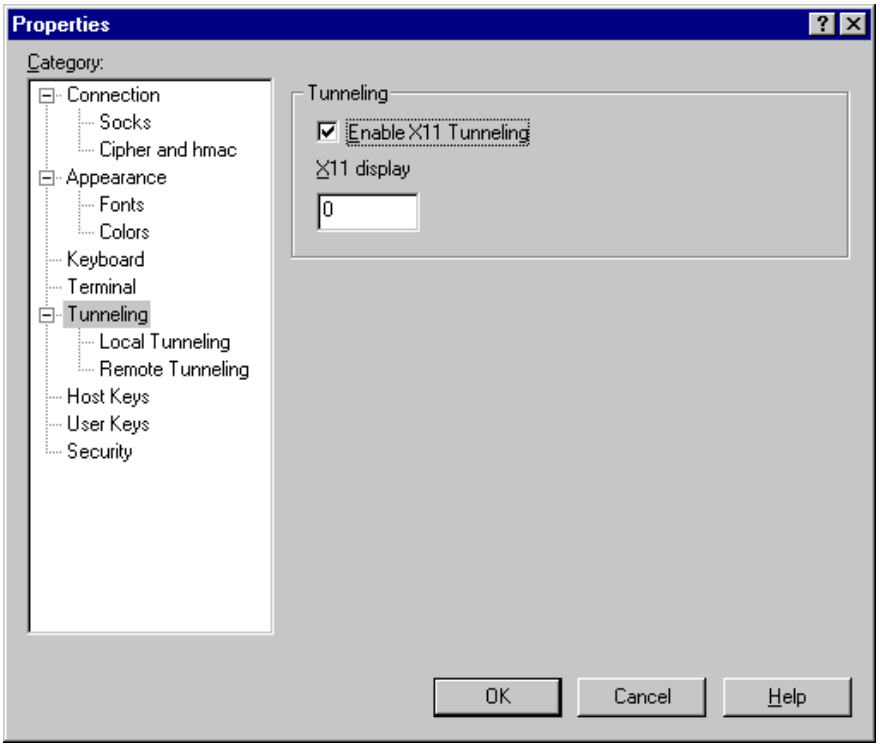
Συνήθως, το ηλεκτρονικό ταχυδρομείο και οι απευθείας τραπεζικές συναλλαγές είναι "ασφαλή," που σημαίνει ότι κανένας δε μπορεί να παρεμποδίσει το όνομα χρήστη και τον κωδικό πρόσβασής μας όπως εργαζόμαστε, πέρα από τον Ιστό. Αυτό

δεν ισχύει απαραιτήτως για τη σύνδεση με έναν κεντρικό υπολογιστή δικτύου όταν φορτώνουμε ή κατεβάζουμε αρχεία.

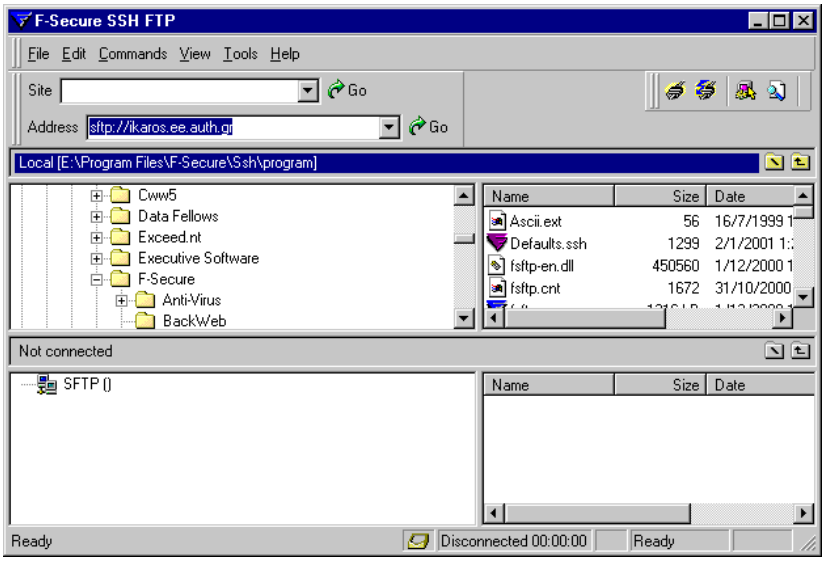
Η χρήση του SSH συνιστάται για την ασφαλή πρόσβαση σε συστήματα UNIX από σταθμούς Microsoft Windows. Το F-Secure SSH της Datafellows παρέχει την δυνατότητα ασφαλούς πρόσβασης αντικαθιστώντας τα συμβατικά πρωτόκολλα telnet, rlogin, ftp, κλπ. Το πακέτο δεν κάνει τίποτε παραπάνω από το να κρυπτογραφεί passwords, remote login sessions και X11 sessions.

Σημεία που θα πρέπει να προσεχθούν κατά την διάρκεια της εγκατάστασης είναι:

1. Επιλέξτε ως γλώσσα ENGLISH και μετά INSTALL
2. Ακολουθήστε τις οδηγίες (φάκελος εγκατάστασης, κλπ.)
3. Την πρώτη φορά που θα τρέξετε την εφαρμογή θα σας ζητηθεί να μετακινήσετε το mouse τυχαία (αυτό θα χρησιμοποιηθεί για την δημιουργία του F-Secure SSH's random number generator)
4. Η επιλογή EDIT > Properties > Tunneling θα πρέπει να έχει πάντα ενεργοποιημένο το check box: Enable X11 Tunneling, όπως φαίνεται παρακάτω (για την κρυπτογράφηση των X11 sessions).



Το πακέτο περιλαμβάνει και γραφικό κρυπτογραφημένο περιβάλλον sftp για μετακίνηση αρχείων από και προς ssh servers.

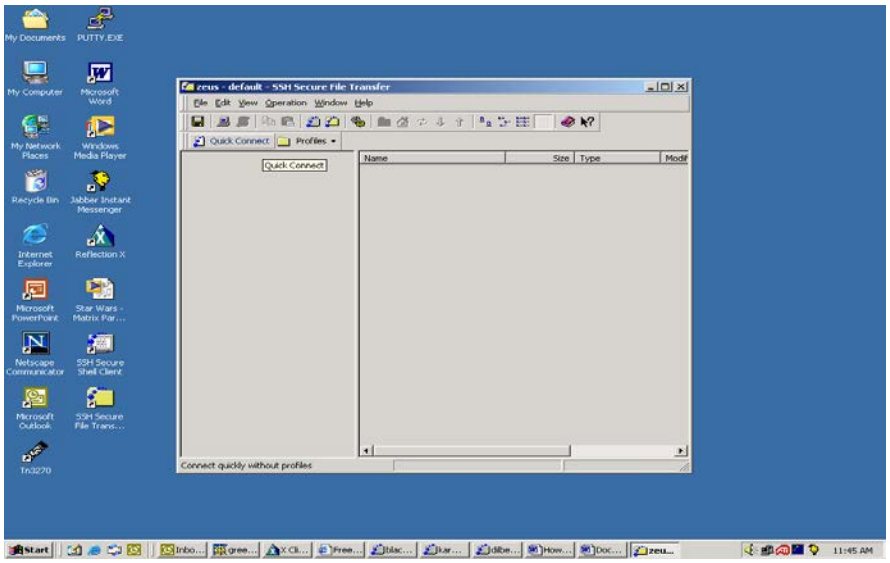


ΠΡΟΣΟΧΗ! Η κρυπτογράφηση του X11 session προϋποθέτει το παραπάνω βήμα 4, αλλά και την σχετική ενεργοποίηση του ssh server (X11forwarding yes στο αρχείο /etc/sshd2_config). Η μη ενεργοποίησή τους οδηγεί σε αποτυχημένες συνδέσεις X11 (μηνύματα X connection broken, cannot open display, κλπ.). Επίσης ο ορισμός του DISPLAY θα πρέπει να γίνεται αυτόματα. Ο manual ορισμός του (π.χ. setenv DISPLAY localhost:0.0) απενεργοποιεί την κρυπτογράφηση!

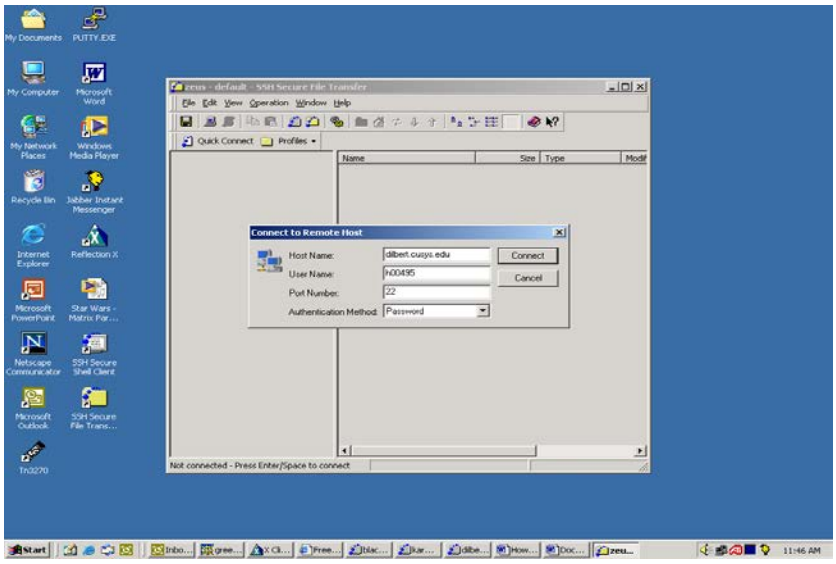
Το κρυπτογραφημένο FTP είναι ο γρήγορος και εύκολος τρόπος να σταλούν και να παραληφθούν αρχεία από και προς το PC σας. Είναι μια τριανταδυάμπιτη (32bit) εφαρμογή πελατών /κεντρικών υπολογιστών, (δύο προγράμματα σε ένα). Ενσωματώνει τον αλγόριθμο κρυπτογράφησης 448bit Blowfish και το πρωτόκολλο FTP (εφαρμογή RFC 959) για να παρέχει τις ασφαλείς μεταφορές αρχείων πέρα από το TCP/ IP που παρέχει την ισχυρή κρυπτογράφηση όταν οι μακρινοί και τοπικοί οικοδεσπότες το χρησιμοποιούν.

7.4 Πώς να χρησιμοποιήσουμε το ασφαλές πρωτόκολλο μεταφοράς αρχείων (SFTP)

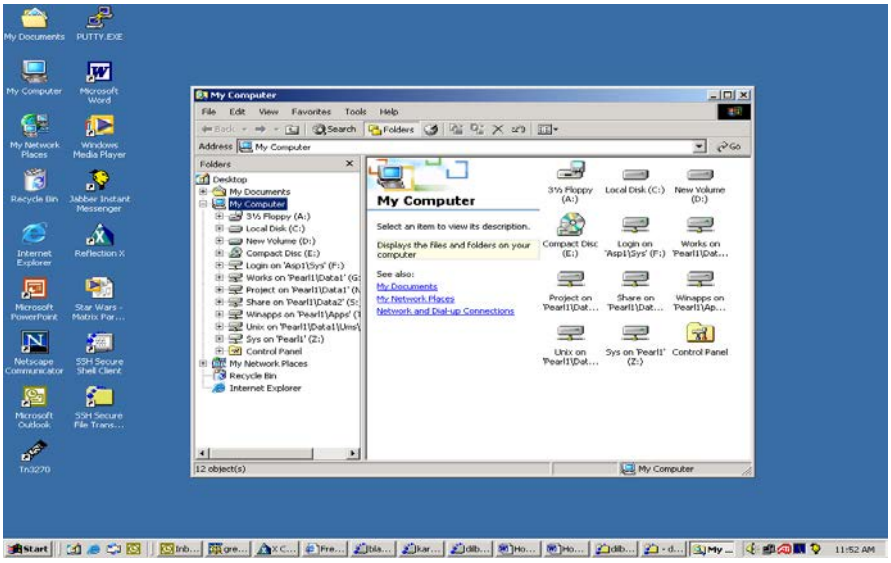
1. Κάνουμε δύο φορές κλικ στην ασφαλή εικόνα πελατών μεταφοράς αρχείων SSH στον υπολογιστή γραφείου μας...



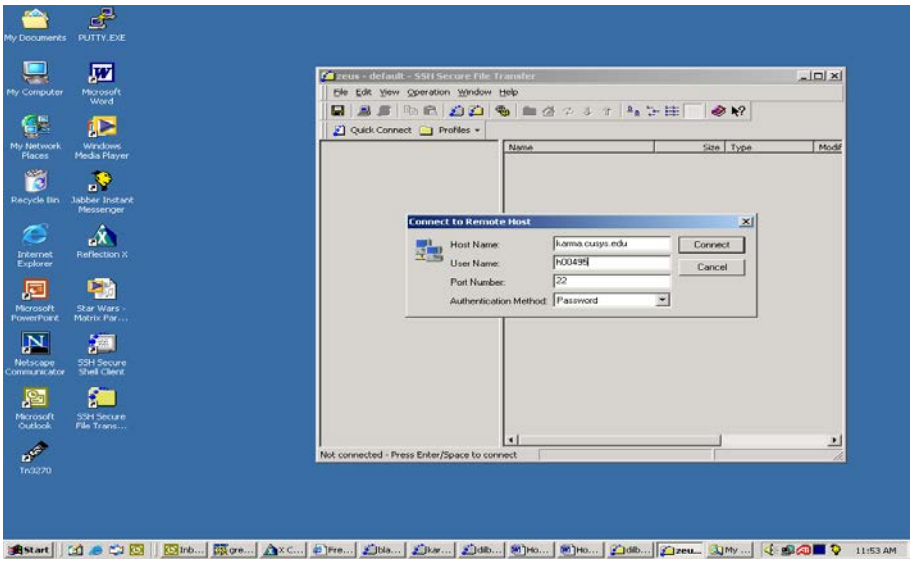
2. Χρησιμοποιούμε την επιλογή quick connect. Γράφουμε το host name " που επιθυμούμε να συνδεόμαστε. Γράφουμε το user name και πατάμε connect.



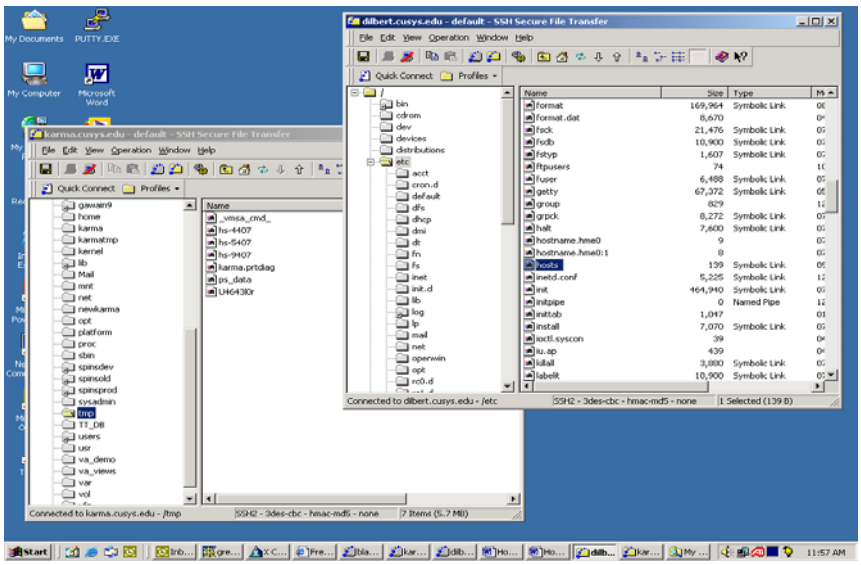
3. Εάν το αρχείο που επιθυμούμε να μεταφέρουμε προέρχεται από το pc μας ανοίγουμε το windows explorer, και βρίσκουμε τον κατάλληλο φάκελο όπου βρίσκετε το αρχείο.



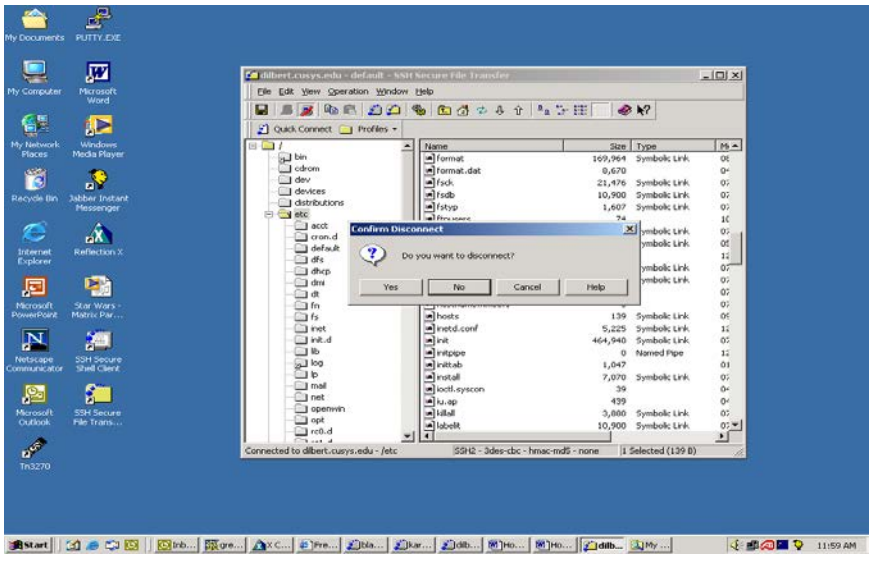
4. Διαφορετικά ανοίγουμε έναν άλλο ασφαλή πελάτη μεταφοράς αρχείων SSH κάνοντας διπλό κλικ στην εικόνα στον υπολογιστή γραφείου μας και επαναλαμβάνουμε το βήμα 2.



5. Βάζουμε το αρχείο στον κατάλληλο κατάλογο



6. Αποσυνδέουμε τη σύνδεσή SFTP όταν ολοκληρώσουμε τη μεταφορά αρχείων



7.5Συμπεράσματα

Σε αυτό το κεφάλαιο παρουσιάσαμε ένα ειδικό θέμα διαχείρισης και συγκεκριμένα τους τρόπους ασφαλούς παραμετροποίησης του FTP server. Ακολουθεί η βιβλιογραφία από την οποία αντλήθηκαν και προσαρμόσθηκαν στις προηγούμενες σελίδες αρκετές ενδιαφέρουσες πληροφορίες

8. Βιβλιογραφία

Δίκτυα:

- «Μετάδοση Δεδομένων και Δίκτυα Υπολογιστών» ΤΕΕ, Τσιλιγκιρίδης – Αλεξίου Αθήνα (2000)
- "Computer Networks", Andrew S Tabenbaum, 1999 Prentice Hall, England Hasall F,"Data Communications, Computer Networks and Open Systems"Addison (1996)
- "TCP/IP Tutorial and Technical Overview", Martin W. Murhammer, Orcun Atakan, Stefan Bretz, Larry R. Pugh, Kazunari Suzuki, David H. Wood International Technical Support Organization
- Computer networks : a systems approach / Larry L. Peterson & Bruce S. Davie. - 2nd Peterson, Larry L. (2000)
- Practical TCP/IP and Ethernet networking / Deon Reynders, Edwin Wright Reynders, Deon (2003)
- TCP/IP network administration. - 2nd ed Hunt, Craig (1998)

SSL, IIS, web servers:

- "E-Commerce with ASP", Stephen Walther – Jonathan Levine, 2000 Sams Publishing, USA
- Microsoft IIS 6.0 Web Page: http://www.microsoft.com/windowsserver2003/technologies/webapp/default.mspx
- Windows 2000 Server Web site: http://www.microsoft.com/windows/server/
- Introduction to IIS 5.0 features: http://www.microsoft.com/windows/server/Overview/features/web.asp
- Microsoft Security, Best Practices and Tools Related to IIS http://www.microsoft.com/security
- Microsoft Developer Network Online Library IIS SDK: http://msdn.microsoft.com/library/psdk/iisref/psdkwelc.htm
- Microsoft TechNet IIS site: http://www.microsoft.com/technet/iis/
- *Microsoft Interactive Developer Journal*: *Internet Information Services 5.0*: http://www.microsoft.com/Mind/0499/IIS5/IIS5.HTM
- Windows 2000 Web and Application Services: http://www.microsoft.com/windows2000/guide/server/features/appsvcs.asp

- IIS 7.0 http://www.ftponline.com/reports/vslivesf/2005/ruest/

WWW:

- Kennedy J. A.: "The Internet and the World Wide Web", Published By: Rough Guides Ltd., Third Edition, UK (1998)
- Thomas J. B.: "The Internet for Scientists and Engineers", Second Edition, Oxford University Press U.K (1996)

Security

- Network and Internetwork Security", W. Stallings, Prentice Hall
- "Network Security: Private Communication in a Public World", C.Kaufman, R.Perlman, M.Speciner, PTR Prentice Hall, 1995
- Network security essentials : applications and standards Stallings, William (2000)
- http://www.redbooks.ibm.com
- "Third Annual Ernst & Young/Information Week Information Security Survey" Ernst & Young

Firewalls

- Firewalls FAQ: http://www.interhack.net/pubs/fwfaq/
- http://www.cisco.com
- RSA-Security Protocols Overview – Ipsec
- http://www.rsa.com/standards/protocols/ipsec.html

Network Management Security

- "SNMP and SNMPv2: The Infrastructure for Network Management."
- Stallings, W. , IEEE Commun. Mag., March 1998.