ΚΕΦΑΛΑΙΟ 2ο

Υπηρεσίες του Διαδικτύου

Στο προηγούμενο κεφάλαιο κάναμε μια εισαγωγή στο Διαδίκτυο (Internet) και γνωρίσαμε αρκετές από τις πτυχές που είναι άρρηκτα συνδεδεμένες με αυτό. Στο παρόν κεφάλαιο θα επιχειρήσουμε να αναλύσουμε ορισμένες από τις πιο βασικές και διαδεδομένες υπηρεσίες που μας προσφέρει το Διαδίκτυο με έμφαση κυρίως στον Παγκόσμιο Ιστό (World Wide Web). Επίσης, στο προηγούμενο κεφάλαιο αναλύθηκε η χρήση της διεύθυνσης IP για τον προσδιορισμό ενός υπολογιστή στο Διαδίκτυο.

2.1. Υπηρεσία Μητρώου Ονομάτων DNS

Για τους ανθρώπους η χρήση διευθύνσεων του τύπου 197.21.4.56 ή 203.12.54.233 δεν οδηγεί απ' ευθείας στο δίκτυο ή τον υπολογιστή στον οποίο αναφέρεται. Για το λόγο αυτό έχει βρεθεί ένας τρόπος διευθυνσιοδότησης που σαν χαρακτηριστικό έχει κοινές λέξεις ή ακρώνυμα λέξεων με σκοπό από το ανάγνωσμα και μόνο των λέξεων αυτών να είναι κατανοητή η λειτουργία ή η προέλευση του υπολογιστή που φέρει τη διεύθυνση αυτή.

Το σύστημα ονοματοδοσίας στο Internet είναι το DNS (Domain Name Service – Υπηρεσία Ονοματοδοσίας Περιοχής). Σύμφωνα με αυτό κάθε όνομα περιέχει μια ακολουθία από αλφαριθμητικά τμήματα που χωρίζονται από τελείες. Παραδείγματος χάριν, ένας υπολογιστής στο τμήμα Πληροφορικής του Πανεπιστημίου Πειραιώς έχει το όνομα πεδίου (Domain name): rainbow.cs.unipi.gr.

Η χρήση των διευθύνσεων και η απαραίτητη επεξεργασία τους σαν δυαδικοί αριθμοί είναι εύκολη από ένα μηχάνημα, όπως είναι ένας δρομολογητής, αλλά είναι πολύ δύσκολη και συχνά ακατανόητη από ανθρώπους και ιδιαίτερα από χρήστες που δεν είναι εξοικειωμένοι με την αρίθμηση αυτή. Επιπλέον, οι αριθμοί αυτοί δεν δίνουν άμεσα καμία πληροφορία για τη γεωγραφική θέση του οργανισμού ή κάποια άλλη σχετική πληροφορία. Για το λόγο αυτό χρησιμοποιούνται συμβολικά ονόματα τα οποία πρέπει μετά να περάσουν από επεξεργασία από τους υπολογιστές. Τα συμβολικά αυτά ονόματα χρησιμοποιούνται από τα προγράμματα εφαρμογής και μεταφράζονται σε αριθμούς από τα χαμηλότερα επίπεδα. Οι χρήστες δεν συμμετέχουν τις περισσότερες φορές σε αυτή τη διαδικασία, όλα γίνονται διάφανα για αυτούς.

Η διαδικασία μετάφρασης συμβολικών ονομάτων σε διευθύνσεις IP χρησιμοποιεί το μοντέλο πελάτη – εξυπηρετητή. Η βάση δεδομένων, όμως, δεν είναι τοποθετημένη σε κάποιο κεντρικό σημείο του δικτύου αλλά χρησιμοποιείται ένας κατανεμημένος τρόπος πρόσβασης στην πληροφορία μέσω ενός εξυπηρετητή ονοματοδοσίας (naming server).

Το Internet είναι χωρισμένο νοητά σε εκατοντάδες διαφορετικές **περιοχές (domains) υψηλού επιπέδου**, καθεμία από τις οποίες καλύπτει πολλούς host. Κάθε περιοχή διαιρείται σε **υπό-περιοχές (sub-domains)**, που διαιρούνται παραπέρα, κ.ο.κ.

Οι περιοχές υψηλού επιπέδου είναι δύο ειδών: γένη και χώρες. Οι περιοχές γενών είναι:

- com (εμπορικές)
- edu (εκπαιδευτικοί οργανισμοί)
- gov (κυβερνητικές οργανώσεις)
- int (συγκεκριμένες διεθνείς οργανώσεις)
- mil (στρατιωτικές υπηρεσίες)
- net (παροχείς δικτύου)
- org (μη κερδοσκοπικοί οργανισμοί)

Οι **περιοχές χωρών** περιλαμβάνουν μία καταχώριση για κάθε χώρα, που αποτελείται από δυο γράμματα. Για παράδειγμα η Γαλλία έχει το .fr, η Ιρλανδία το .ie κλπ.

Τα ονόματα περιοχών μπορεί να είναι είτε απόλυτα είτε σχετικά. Ένα απόλυτο όνομα περιοχής τελειώνει με μία τελεία, ενώ μια σχετική ονομασία όχι. Οι **ονομασίες περιοχών** δεν εξαρτώνται από τα κεφαλαία ή πεζά γράμματα, έτσι edu και EDU είναι το ίδιο πράγμα.

Για να δημιουργηθεί μία καινούργια περιοχή απαιτείται άδεια από την περιοχή στην οποία θα περιληφθεί. Για παράδειγμα, όταν ξεκινάει μία ομάδα COMP στο Πανεπιστήμιο Πειραιά και θέλει να γίνει γνωστή ως comp.cs.unipi.gr, χρειάζεται άδεια από αυτόν που διαχειρίζεται το cs.unipi.gr. Με τον τρόπο αυτό αποφεύγονται οι συγκρούσεις των ονομάτων και κάθε περιοχή είναι σε θέση να κρατά λογαριασμό με όλες τις υπο-περιοχές της.

Πλέον έχουν εισαχθεί και καινούργια ονόματα περιοχών. Μερικά από αυτά δίνονται παρακάτω:

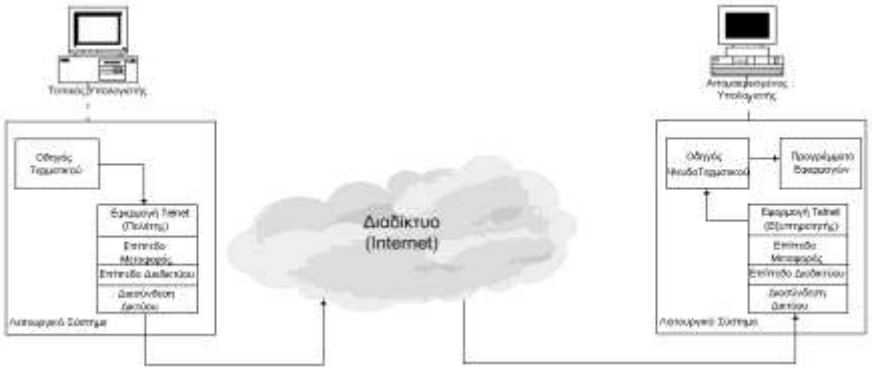
- .web
- .shop
- .site
- .hotel
- .blog
- .news
- .music
- .art
- .equipment

Στην παραπάνω λίστα προστίθενται καθημερινά καινούργιες καταλήξεις.

2.2. Υπηρεσία Απομακρυσμένου Τερματικού - TELNET (TERMINAL NETWORK)

Το Telnet είναι ένα πρωτόκολλο που επιτρέπει στο χρήστη – πελάτη να συνδεθεί με ένα απομακρυσμένο ηλεκτρονικό υπολογιστή, δίνοντας του τη δυνατότητα να τον διαχειριστεί σαν να ήταν το δικό του μηχάνημα.

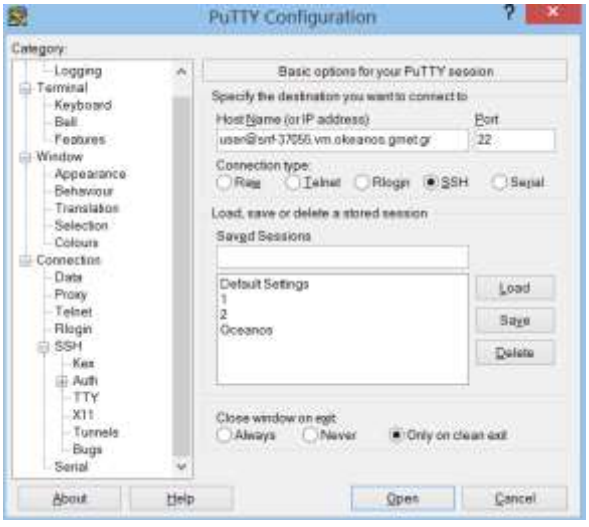
Υπάρχουν διάφοροι τρόποι σύνδεσης με κάποιο μηχάνημα. Ο πρώτος τρόπος αφορά τη σύνδεση με κάποιο τοπικό τερματικό (Local Login). Ο δεύτερος είναι η σύνδεση με απομακρυσμένο τερματικό (Remote Login). Στην περίπτωση αυτή χρησιμοποιείται ένας πελάτης TELNET, ο οποίος μπορεί να συνδεθεί με το απομακρυσμένο μηχάνημα – εξυπηρετητή, διαμέσου του Διαδικτύου.



Εικόνα 2.2.1. *Το πρωτόκολλο TELNET*

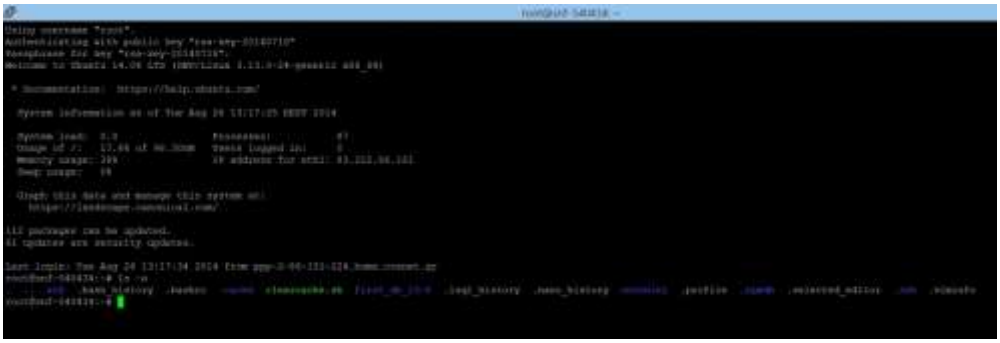
Ένα παράδειγμα πελάτη TELNET είναι το Putty. Αποτελεί ένα από τα πιο δημοφιλή βοηθητικά προγράμματα για τη σύνδεση με Linux εξυπηρετητές από υπολογιστές που τρέχουν ένα λειτουργικό σύστημα Microsoft Windows. Συχνά χρησιμοποιείται για να δημιουργήσει συνδέσεις SSH για την απομακρυσμένη υποστήριξη γραφικών, παρέχοντας οθόνες σε απομακρυσμένα συστήματα.

Για να ανοίξει το Putty σε λειτουργικό σύστημα Windows ο χρήστης πρέπει να επιλέξει να εκτελέσει το πρόγραμμα μέσα από το αντίστοιχο παράθυρο εκτέλεσης (Start, Run) και στο αναδυόμενο παράθυρο να πληκτρολογήσει «putty». Στο πεδίο «Host Name» ο χρήστης πρέπει να συμπληρώσει το όνομα του υπολογιστή στον οποίο θέλει να συνδεθεί. Για παράδειγμα user@snf-37055.vm.okeanos.grnet.gr και στη συνέχεια επιλέγει το Open (βλέπε εικόνα 2.2.2).



Εικόνα 2.2.2. *Αρχικό παράθυρο σύνδεσης εφαρμογής*

Γίνεται προτροπή για να εισαγάγει το όνομα χρήστη (login as). Στη συνέχεια ο χρήστης επιλέγει Enter για να εισάγει και τον κωδικό του. Για λογούς ασφαλείας, όσο ο χρήστης πληκτρολογεί τον κωδικό, δεν εμφανίζεται κάτι στην οθόνη, οπότε μόλις ολοκληρωθεί η εισαγωγή του κωδικού ο χρήστης επιλέγει Enter. Αν όλα έχουν πάει καλά τότε θα εμφανιστεί μια οθόνη όπως η παρακάτω:

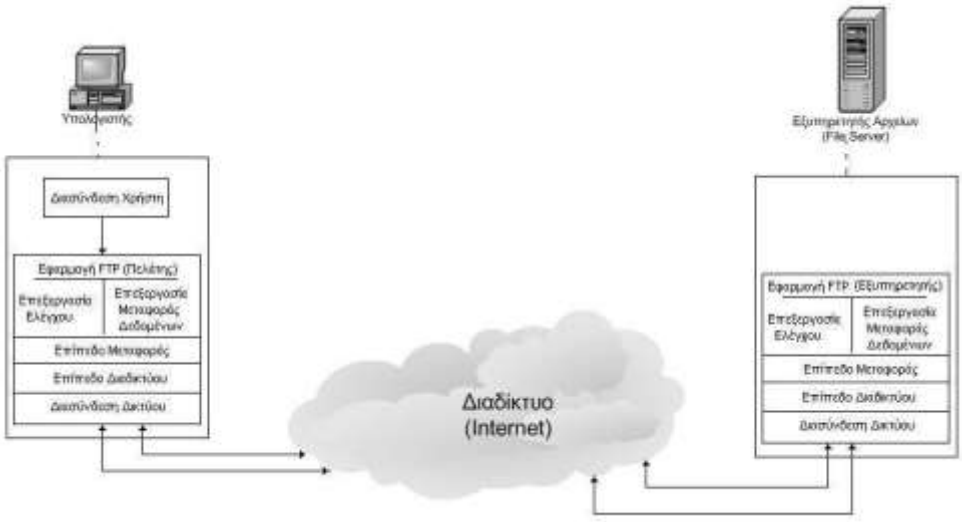


Εικόνα 2.2.3. *Οθόνη σύνδεσης μέσω «putty»*

2.3. Υπηρεσία Μεταφοράς Αρχείων – FTP (FILE TRANSFER PROTOCOL)

Το FTP επιτρέπει στον πελάτη να αντιγράψει και να μεταφέρει αρχεία από τον ένα υπολογιστή στον άλλο, διαμέσου του Διαδικτύου. Το FTP διαφέρει από τις άλλες εφαρμογές Διαδικτύου στο ότι δημιουργεί δύο τύπων συνδέσεις, μεταξύ του πελάτη και του εξυπηρετητή. Η πρώτη χρησιμοποιείται για τη μεταφορά του αρχείου, ενώ η δεύτερη για τον έλεγχο της επικοινωνίας μεταξύ των δύο υπολογιστών (Εντολές και αποκρίσεις).

Το έργο του FTP δεν είναι τόσο απλό όσο δείχνει, γιατί τα 2 διαφορετικά συστήματα μπορεί να χρησιμοποιούν διαφορετικό τρόπο αρχειοποίησης και αναπαράστασης των αρχείων τους. Έτσι, το FTP αναλαμβάνει τις απαραίτητες μετατροπές των αρχείων για την πιο αποτελεσματική μεταφορά.



Εικόνα 2.3.1. *Το Πρωτόκολλο Μεταφοράς Αρχείου (FTP).Υπάρχουν 2 συνδέσεις TCP, μια για την επεξεργασία ελέγχου (θύρα 21) και μια για την επεξεργασία Μεταφοράς των Δεδομένων (Θύρα 20)*

Πίνακας 2.3.1. *Οι βασικές εντολές του FTP*

Εντολή	***Επεξήγηση***
ftp	Η κλήση του ftp client γίνεται με την εντολή́ ftp από τη γραμμή́ εντολών
Pwd	Με την εντολή́ pwd εμφανίζουμε το όνομα του τρέχοντος καταλόγου (φακέλου).
Lcd	Με την εντολή́ lcd βλέπουμε ποιος είναι ο τρέχων τοπικός μας κατάλογος.
Dir	Με την εντολή́ dir εμφανίζουμε τα περιεχόμενα του τρέχοντος καταλόγου (φακέλου).
Cd	Με την εντολή́ cd και το όνομα του φακέλου ή́ τη διαδρομή́ οπού βρίσκεται.
cd/	Η μετάβαση στον αρχικό́ κατάλογο (root) γίνεται με την εντολή́ cd \ από́
	οποιονδήποτε κατάλογο και αν βρίσκομαι.
mkdir	Με την εντολή́ mkdir και το όνομα του νέου καταλόγου,

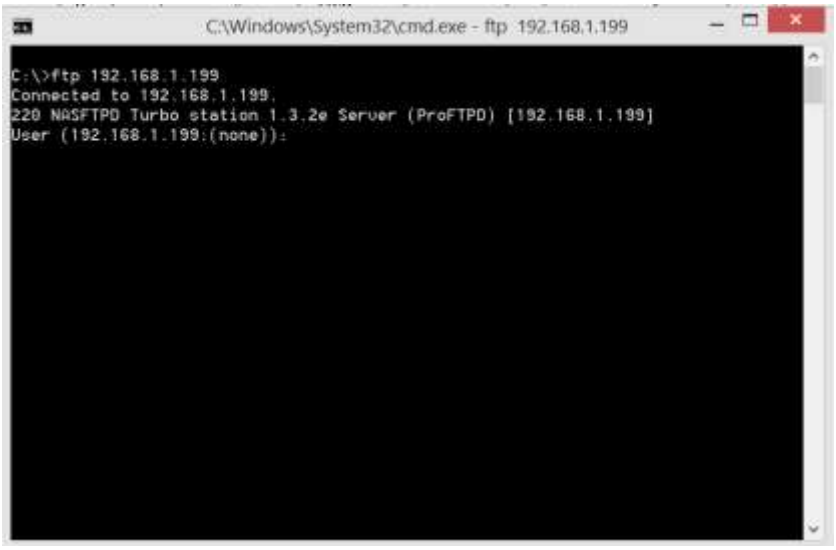
	δημιουργούμε το νέο κατάλογο μέσα στον τρέχοντα κατάλογο.
delete	Με την εντολή delete και το όνομα του αρχείου , επιτυγχάνουμε τη διαγραφή του.
mdelete	Για τη διαγραφή όλων των αρχείων χρησιμοποιούμε την mdelete * Για την επιβεβαίωση διαγραφής κάθε αρχείου πληκτρολογούμε yes.
prompt	Με την εντολή prompt ενεργοποιούμε/απενεργοποιούμε τη διαδραστική λειτουργία, ώστε οι εντολές για πολλαπλά αρχεία να εκτελούνται χωρίς επιβεβαίωση του χρήστη.
rmdir	Εφ' όσον ο κατάλογος είναι άδειος μπορούμε να τον διαγράψουμε με την εντολή rmdir και το όνομα ή τη διαδρομή οπού βρίσκεται ο κατάλογος.
Ren	Με την εντολή ren μετονομάζουμε ένα αρχείο ή έναν κατάλογο.
Put	Για την αποστολή ενός αρχείου στον τρέχοντα κατάλογο του ftp server από τον τρέχοντα τοπικό μας κατάλογο, χρησιμοποιούμε την εντολή put και το όνομα του αρχείου που θέλουμε να ανεβάσουμε.
mput *	Με την εντολή mput * αποστέλλουμε ούλα τα αρχεία του τρέχοντος καταλόγου του ftp server στον τρέχοντα τοπικό μας κατάλογο.
Get	Για τη λήψη ενός αρχείου από τον ftp server στον τρέχοντα τοπικό μας κατάλογο , χρησιμοποιούμε την εντολή get και το όνομα του αρχείου που θέλουμε να κατεβάσουμε.
mget*	Με την εντολή mget * κάνουμε λήψη όλων των αρχείων του τρέχοντος καταλόγου του ftp server στον τρέχοντα τοπικό μας κατάλογο.
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>.
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.
Hash	Αλλάζει το hash mark stats indicator.
Tick	Αλλάζει byte counter indicator.
Prom	Θέτει το interactive mode για κατέβασμα αρχείων.
Quit	Αποσυνδέεται από τον server.

Το FTP υποστηρίζει τρεις βασικές λειτουργίες: ένας χρήστης μιας μηχανής μπορεί να στείλει ένα αρχείο σε άλλον υπολογιστή, να φέρει αρχείο από αυτόν τον υπολογιστή και να μεταφέρει αρχεία ανάμεσα σε δύο απομακρυσμένα μηχανήματα. Παρέχει ένα μεγάλο αριθμό επιλογών για τη δημιουργία, μεταβολή ή επισκόπηση ενός απομακρυσμένου λογαριασμού χρήστη, σβήσιμο ή ανάκτηση ενός απομακρυσμένου αρχείου, επιλογή του τρόπου μεταφοράς (με ρεύμα, τμήμα ή συμπίεση) και για αποστολή αρχείων.

Ο συνήθης τρόπος αποστολής είναι με ρεύμα (stream). Το αρχείο στέλνεται χωρίς τροποποιήσεις. Ο τρόπος με τμήματα σημαίνει τεμαχισμό του αρχείου και αποστολή του κατά τμήματα. Αυτός ο τρόπος εφαρμόζεται για να διευκολύνει την ανάκτηση σε περίπτωση σφάλματος. Ο συμπιεσμένος τρόπος, τέλος, χρησιμοποιείται για την αποφυγή αποστολής μεγάλων τμημάτων από επαναλαμβανόμενους χαρακτήρες (π.χ. κενά μεταξύ λέξεων).

Όπως ειπώθηκε και προηγουμένως, το FTP χρησιμοποιεί δύο συνδέσεις TCP: μία για τις εντολές και αποκρίσεις και μία άλλη για τις μεταφορές δεδομένων και επιβεβαιώσεις. Ο κάθε κόμβος έχει πάντα μια διεργασία FTP να τρέχει και να είναι έτοιμη να επεξεργαστεί εντολές. Αυτές οι εντολές φτάνουν σε μία σύνδεση TCP, χρησιμοποιώντας έναν ειδικό αριθμό θύρας (το 21) (Βλέπε εικόνα 2.3.1). Η αίτηση FTP από μία άλλη μηχανή μπορεί να απαιτήσει την πιστοποίηση του χρήστη με συνθηματικό.



Εικόνα 2.3.1. *Το περιβάλλον εντολών FTP, όπως εμφανίζεται σε παράθυρο MS-DOS Prompt των WINDOWS 8.1 Pro*

2.3.1 Anonymous FTP

Υπάρχουν FTP εξυπηρετητές διάσπαρτοι σε όλο τον κόσμο και χιλιάδες από αυτούς υποστηρίζουν μια ειδική υπηρεσία τύπου FTP, το anonymous FTP, η οποία χρησιμοποιείται συνήθως.

Anonymous FTP σημαίνει ότι ένας χρήστης μπορεί να συνδεθεί με τον απομακρυσμένο υπολογιστή και να ανακτήσει αρχεία χωρίς απαραίτητα να έχει 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 ηλεκτρονικού ταχυδρομείου (e-mail).

Όταν γίνεται χρήση του anonymous FTP, δεν είναι δυνατή η μεταφορά αρχείων από τον τοπικό στον απομακρυσμένο υπολογιστή και γενικά δεν είναι δυνατή η επέμβαση στα περιεχόμενα του σκληρού του δίσκου (π.χ. διαγραφή ή και μετονομασία αρχείων, δημιουργία νέων καταλόγων κ.λπ.). Στην περίπτωση που ένας χρήστης έχει λογαριασμό στον απομακρυσμένο υπολογιστή, θα υπάρχει προστασία για τα αρχεία και τους καταλόγους του και οι δυνατότητες του κάθε χρήστη εξαρτώνται από τα δικαιώματα που του έχουν εκχωρηθεί.

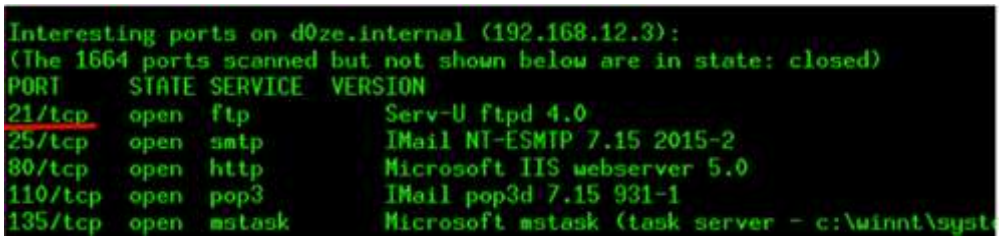
Είναι ευνόητο ότι η υπηρεσία anonymous FTP συμβάλλει στη διαθεσιμότητα της πληροφορίας, έναν από τους πρωταρχικούς σκοπούς ύπαρξης του Internet. Μέσω του anonymous FTP, ο χρήστης μπορεί να ανακτήσει στο σκληρό του δίσκο αρχεία από ολόκληρο τον κόσμο.

Οι εξυπηρετητές FTP 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**. Οι εφαρμογές αυτές εκτελούνται σε περιβάλλον κειμένου και οι λειτουργίες τους πραγματοποιούνται από εντολές σε μορφή κειμένου.

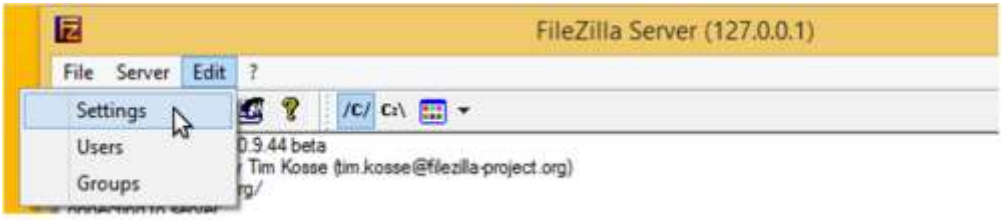
2.3.2 Το πρόγραμμα μεταφοράς αρχείων – Filezilla

Σήμερα, υπάρχουν προγράμματα τα οποία έχουν εύχρηστες διεπαφές για την χρήση του FTP. Ένα από τα πιο δημοφιλή είναι το Filezilla. Το Filezilla είναι ένα πρόγραμμα μεταφοράς αρχείων, το οποίο δίνει τη δυνατότητα στο χρήστη να μεταφέρει εύκολα και γρήγορα τα αρχεία του ιστότοπού του από τον υπολογιστή του, προς τον εξυπηρετητή όπου υπάρχει το πακέτο φιλοξενίας του. Μόλις ο χρήστης εγκαταστήσει και ανοίξει την εφαρμογή θα του ζητηθεί να εισάγει τον εξυπηρετητή/hostname/κόμβο (π.χ. αν το domain είναι το example.gr, ο εξυπηρετητής είναι ο ftp.example.gr), όπως και όνομα χρήστη και συνθηματικό για να γίνει η σύνδεση. Τα στοιχεία αυτά για την πρόσβαση μέσω ftp, θα πρέπει να έχουν δοθεί από τον εκάστοτε πάροχο φιλοξενίας. Σε αυτή την περίπτωση, μπορεί σε αυτό το πεδίο να συμπληρώσει την IP του εξυπηρετητή. Αφού γίνει η σύνδεση μέσω Filezilla στον εξυπηρετητή, ο χρήστης μπορεί να αναζητήσει τα αρχεία για μεταφορά στον υπολογιστή του από το παράθυρο της εφαρμογής, και να τα μεταφέρει (με drag&drop) στον φάκελο που έχει καθορίσει ο εκάστοτε πάροχος φιλοξενίας στον εξυπηρετητή.

Ένα μικρό αλλά ουσιαστικό βήμα για την ασφάλεια του εξυπηρετητή FTP είναι το να αλλάξουμε τη θύρα στην οποία δέχεται συνδέσεις ή αλλιώς "ακούει". Η προεπιλογή είναι η θύρα 21 (ή αλλιώς, η "Original"). Όμως, χιλιάδες hackers τρέχουν προγράμματα που ψάχνουν αυτόματα για οικιακούς FTP Servers στη θύρα 21.



Εικόνα 2.3.3. *Θωρακίζοντας την ασφάλεια του προγράμματος Filezilla*



Εικόνα 2.3.4. *Ρυθμίσεις ασφαλείας του προγράμματος Filezilla*

Για την αλλαγή της θύρας αρκεί να πάει ο χρήστης στο Edit → Settings. Στο πεδίο "Listen on these ports" βάζουμε έναν πενταψήφιο αριθμό μικρότερο από το 65535.

Εικόνα 2.3.5. *Αλλαγή θύρας του προγράμματος Filezilla*

Αυτή η αλλαγή θα αποθαρρύνει τους "τυχαίους" hacker που ψάχνουν για ένα εύκολο θύμα. Ο FileZilla Server διαθέτει και άλλες δυνατότητες ασφαλείας, όπως το IP Filter - που επιτρέπει τη σύνδεση μόνο από συγκεκριμένες IP. Για απλή οικιακή χρήση, όμως, η αλλαγή της θύρας σε συνδυασμό με ένα ισχυρό password είναι παραπάνω από αρκετή.

2.4. Το Ηλεκτρονικό Ταχυδρομείο

Σε κάθε δίκτυο, οποιουδήποτε μεγέθους, μία από τις βασικότερες υπηρεσίες που οι κατασκευαστές του φροντίζουν να υλοποιήσουν και να διαθέσουν στους χρήστες του είναι η δυνατότητα του ηλεκτρονικού ταχυδρομείου.

Το **ηλεκτρονικό ταχυδρομείο** ή κοινώς «**email**» (προερχόμενο από τη συνένωση των λέξεων electronic mail), είναι η πιο χρήσιμη εφαρμογή του Διαδικτύου, η οποία χρησιμοποιείται καθημερινά από εκατομμύρια χρήστες.

Τα πρώτα συστήματα ηλεκτρονικού ταχυδρομείου αποτελούνταν απλώς από πρωτόκολλα μεταφοράς αρχείων, όπου η πρώτη γραμμή κάθε μηνύματος περιείχε τη διεύθυνση του παραλήπτη.

Με αυτήν την προσέγγιση όμως υπήρχαν αρκετοί περιορισμοί και τα μειονεκτήματα άρχισαν να φαίνονται. Οι χρήστες δεν είχαν τη δυνατότητα να στείλουν ένα μήνυμα σε πολλούς αποδέκτες. Τα μηνύματα που έστελναν με αυτόν τον τρόπο δεν είχαν κάποια δομή, με αποτέλεσμα τη δυσκολία στην ανάγνωση. Ο αποστολέας κάποιου μηνύματος δεν μπορούσε να γνωρίζει αν το μήνυμά του έφτασε πράγματι τον παραλήπτη. Επιπλέον, δεν ήταν δυνατή η αποστολή μηνυμάτων που να περιέχουν μαζί σχέδια, ήχο και κείμενο. Και όλα αυτά σε ένα περιβάλλον διεπαφής που δεν διευκόλυνε καθόλου τον χρήστη.

Από το ξεκίνημα του Διαδικτύου, είχαν προταθεί πολλά συστήματα ηλεκτρονικού ταχυδρομείου, που δημοσιεύονταν στα λεγόμενα RFC (Requests for Comments). Γενικά μπορούμε να πούμε ότι το ηλεκτρονικό ταχυδρομείο αποτελεί έναν ταχύτατο, φθηνό και αποδοτικό τρόπο επικοινωνίας μεταξύ χρηστών του Διαδικτύου σε ολόκληρο τον κόσμο. Είναι, ίσως, η μεγαλύτερη καινοτομία που εισήγαγε το Διαδίκτυο στον τρόπο εργασίας, καθώς συμβάλλει στην άμεση πληροφόρηση. Οι χρήστες μπορούν να ανταλλάσσουν μηνύματα, επιστολές, έγγραφα κλπ. Πλέον, υπάρχει πληθώρα προγραμμάτων για αποστολή και λήψη email κάποια από τα οποία θα αναφερθούν σε επόμενη παράγραφο του παρόντος κεφαλαίου.

Το ηλεκτρονικό ταχυδρομείο δημιουργήθηκε σαν μια άμεση επέκταση του εσωτερικού ταχυδρομείου ενός οργανισμού ή μιας εταιρείας. Επιτρέπει τη δημιουργία ενός μηνύματος και την αποστολή αντιγράφων σε άλλους ανθρώπους. Είναι αυτοματοποιημένο και επιτρέπει τη χρήση του από ανθρώπους ή προγράμματα.

Για να σταλεί σε ένα χρήστη ηλεκτρονικό μήνυμα πρέπει να υπάρχει στον δέκτη του μηνύματος μια ηλεκτρονική ταχυδρομική θυρίδα για να κρατάει τα μηνύματα. Η θυρίδα αυτή είναι ιδιωτική. Ο καθένας μπορεί να στείλει κάτι σε αυτήν αλλά μόνο ο εξουσιοδοτημένος χρήστης μπορεί να δει και να διαχειριστεί τα μηνύματα. Συνήθως μία θυρίδα αντιστοιχεί σε ένα λογαριασμό χρήστη στον υπολογιστή.

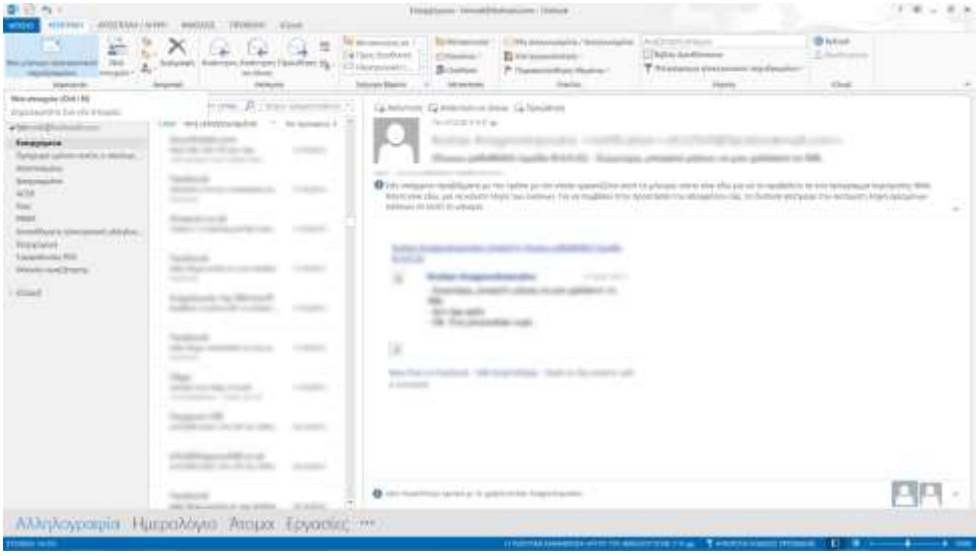
Κάθε ηλεκτρονική θυρίδα έχει μια μοναδική ηλεκτρονική διεύθυνση (email address). Η διεύθυνση αυτή προσδιορίζει την θυρίδα και τον υπολογιστή. Συνήθως είναι της μορφής θυρίδα@υπολογιστή (mailbox@computer). Με το πρώτο συνθετικό ο υπολογιστής γνωρίζει σε ποια θυρίδα θα εναποθέσει το μήνυμα, ενώ το δεύτερο συνθετικό επιτρέπει τη μεταφορά του μηνύματος στον κατάλληλο υπολογιστή.

Συνήθως σαν θυρίδα χρησιμοποιείται το όνομα του λογαριασμού του χρήστη. Παραδείγματος χάρη: christos@unipi.gr, όπου christos είναι το όνομα (username) με το οποίο ο υπολογιστής γνωρίζει το χρήστη και unipi.gr είναι ο υπολογιστής όπου βρίσκεται ο συγκεκριμένος λογαριασμός.

Υπάρχουν συστήματα που δεν επιτρέπουν διαφοροποίηση μεταξύ της θυρίδας και του ονόματος του χρήστη. Τα πιο σύγχρονα συστήματα δίνουν τη δυνατότητα επιλογής κατανοητών ή ομοιόμορφων ονομάτων για τον προσδιορισμό της θυρίδας.

2.4.1. Μορφή Ηλεκτρονικού Μηνύματος

Ένα ηλεκτρονικό μήνυμα περιέχει την επικεφαλίδα και το κυρίως σώμα του μηνύματος. Η επικεφαλίδα περιέχει πληροφορία για τον αποστολέα, τους παραλήπτες και το περιεχόμενο του μηνύματος.



Εικόνα 2.4.1. *Παράδειγμα ηλεκτρονικού μηνύματος, στο πρόγραμμα Outlook*

Στο κυρίως σώμα του μηνύματος μπορεί να περιέχεται οποιαδήποτε πληροφορία. Στην επικεφαλίδα όμως υπάρχει μια προτυποποιημένη μορφή που πρέπει να χρησιμοποιηθεί από το λογισμικό ηλεκτρονικού ταχυδρομείου. Κάθε γραμμή της επικεφαλίδας ξεκινάει με μία λέξη-κλειδί και ακολουθείται από μια άνω τελεία και πρόσθετη πληροφορία. Η λέξη-κλειδί επιτρέπει στο λογισμικό του ηλεκτρονικού ταχυδρομείου να διερμηνεύσει το υπόλοιπο της γραμμής.

Μερικές λέξεις κλειδιά είναι απαραίτητες ενώ άλλες μπορούν να χρησιμοποιηθούν επιλεκτικά. Στην εικόνα 2.4.1 φαίνεται ένα παράδειγμα ηλεκτρονικού μηνύματος γραμμένου σε Outlook Express. Τα From: και To: είναι απαραίτητα για να προσδιοριστεί ο αποστολέας και ο παραλήπτης του μηνύματος. Στα πεδία αυτά φαίνονται οι αντίστοιχες ηλεκτρονικές διευθύνσεις.

Στο σχήμα φαίνονται επίσης γραμμές με την ημερομηνία και το θέμα του μηνύματος. Το λογισμικό εφαρμογής πολλές φορές προσθέτει και άλλες γραμμές στην επικεφαλίδα για λόγους λειτουργικότητας. Μερικές φορές οργανισμοί προσθέτουν κάποιο διαφημιστικό ή ενδεικτικό του οργανισμού τους. Στον πίνακα 2.4.1 φαίνονται μερικές από τις πιο ευρέως διαδεδομένες επικεφαλίδες στο ηλεκτρονικό ταχυδρομείο μέσω του Διαδικτύου.

Πίνακας 2.4.1. *Επικεφαλίδες στο Ηλεκτρονικό Ταχυδρομείο*

Λέξεις Κλειδιά	**Σημασία**
From	Διεύθυνση Αποστολέα
To	Διεύθυνση Παραλήπτη
Cc	Διευθύνσεις για Ακριβή Αντίγραφα
Date	Ημερομηνία αποστολής μηνύματος
Subject	Το Θέμα που αφορά το μήνυμα
Reply – To	Διεύθυνση όπου αποστέλλεται απάντηση για ένα μήνυμα
X – Charset	Το σύνολο των χρησιμοποιούμενων χαρακτήρων (Συνήθως ASCII).
X – Mailer	Το λογισμικό Ηλεκτρονικού Ταχυδρομείου που χρησιμοποιείται κατά την αποστολή μηνύματος
X – Sender	Διπλό αντίγραφο της διεύθυνσης του αποστολέα
X – Face	Κωδικοποιημένη εικόνα του προσώπου του αποστολέα

Η εντολή Cc μας δίνει τη δυνατότητα να στείλουμε ακριβή αντίγραφα σε περισσότερους από ένα παραλήπτες. Αν θέλουμε να αποκρύψουμε την ταυτότητα των παραληπτών αυτών από άλλους παραλήπτες τότε χρησιμοποιούμε την BCC (Blind Carbon Copy).

2.4.2. Η Μορφή MIME

Το αρχικό πρωτόκολλο ηλεκτρονικού ταχυδρομείου επέτρεπε την αποστολή μόνο κειμένου σε μορφή χαρακτήρων ASCII. Συχνά απαιτείται να σταλούν αρχεία με πληροφορία σε δυαδική (binary) μορφή, αρχεία exe ή αρχεία ήχου ή βίντεο. Για να σταλούν τα αρχεία αυτά μέσω ηλεκτρονικού ταχυδρομείου, απαιτείται η κατάλληλη κωδικοποίησή τους. Έχουν προταθεί διάφοροι μέθοδοι κωδικοποίησης.

Μια τέτοια χρησιμοποιεί το δεκαεξαδικό σύστημα, δηλαδή χαρακτήρες από το 0-9 και από το A-F.

Για να υπάρχει συμβατότητα μεταξύ των διαφόρων κωδικοποιήσεων το IETF έχει εφεύρει το πρωτόκολλο MIME (Multipurpose Internet Mail Extensions). Το πρωτόκολλο αυτό δεν προτείνει μια καινούρια κωδικοποίηση αλλά επιτρέπει στον αποστολέα και τον παραλήπτη να αποφασίσουν μία κοινή μέθοδο κωδικοποίησης. Για το σκοπό αυτό προστίθενται στην επικεφαλίδα και στο σώμα του μηνύματος πρόσθετες γραμμές με πληροφορία που επιτρέπει την αναγνώριση του τύπου των δεδομένων και την κωδικοποίηση. Επίσης επιτρέπει το σπάσιμο ενός μηνύματος σε κομμάτια, ώστε να μπορεί να αποσταλεί ταυτόχρονα κείμενο και εικόνες.

Το MIME προσθέτει δύο γραμμές στην επικεφαλίδα, μια για να δηλώσει την ύπαρξή του και μια για να δείξει με ποιο τρόπο η πληροφορία για το MIME έχει συμπεριληφθεί στο κυρίως σώμα.

Παράδειγμα:

MIME-Version: 1.0

Content-Type: Multipart/Mied; Boundary=Mime_separator

Η πρώτη γραμμή δηλώνει ότι για την αποστολή έχει χρησιμοποιηθεί η έκδοση 1.0 του MIME, ενώ η δεύτερη ότι το μήνυμα έχει πολλά μέρη με μία διαχωριστική γραμμή στο ενδιάμεσο.

Το MIME είναι ένα πρότυπο πολύ ευέλικτο γιατί δεν περιγράφει ένα συγκεκριμένο τρόπο κωδικοποίησης αλλά επιτρέπει την προσθήκη καινούριων μεθόδων.

Οι τύποι MIME και οι αντίστοιχες επεκτάσεις των αρχείων διατηρούνται από το λειτουργικό σύστημα και από τον φυλλομετρητή, ώστε να γνωρίζουν ποιες εφαρμογές θα ενεργοποιήσουν, όταν επιλεχθεί κάποιος τύπος MIME.

Στον πίνακα 2.4.2 παρουσιάζονται μερικοί από τους τύπους MIME με τις αντίστοιχες επεκτάσεις αρχείων.

Πίνακας 2.4.2. *Κυριότεροι τύποι MIME και οι αντίστοιχες επεκτάσεις αρχείων*

ΤΥΠΟΣ MIME	ΕΠΕΚΤΑΣΕΙΣ ΑΡΧΕΙΩΝ
Text/plain	.txt
Text/html	.htm
Application/msword	.doc, .dot
Application/pdf	.pdf
Application/x-compress	.zip
Image/gif	.gif

Image/jpeg	.jpg, .jpe, .pjp
Image/x-ms-bmp	.bmp
Audio/basic	.au
Audio/x-pn-realaudio	.mpa, .abs, .mp2
Audio/x-wav	.wav
Midi/mid	.mid
Midi/rmi	.rmi
Video/mpeg	.mpg, .mpe, .mpv, .vbs
Video/quicktime	.mov
Video/x-msvideo	.avi
x-world/x-vrml	.wrl

2.4.3. Ηλεκτρονικό Ταχυδρομείο: Προγράμματα και Μεταφορά

Το ηλεκτρονικό ταχυδρομείο μπορεί να συνεργαστεί με προγράμματα για μεταφορά και επεξεργασία. Ένα πρόγραμμα μπορεί σαν αποτέλεσμα να στείλει ένα μήνυμα, ή να δεχτεί σαν είσοδο ένα μήνυμα και να αρχίσει να εκτελείται.

Για να λειτουργήσει το ηλεκτρονικό ταχυδρομείο σε ένα υπολογιστή, ο χρήστης συνθέτει το μήνυμα και δηλώνει τους παραλήπτες. Το λογισμικό του ηλεκτρονικού ταχυδρομείου αναλαμβάνει να στείλει το μήνυμα. Οι λειτουργίες αυτές γίνονται με ένα πρόγραμμα διεπαφής, το οποίο αλληλεπιδρά με το χρήστη για τη σύνθεση ή την ανάγνωση ενός μηνύματος. Το πρόγραμμα μεταφοράς ταχυδρομείου (mail transfer program) ασχολείται με τις λεπτομέρειες της αποστολής του αντιγράφου του μηνύματος στον απομακρυσμένο υπολογιστή. Πρώτα δηλαδή γίνεται η σύνθεση του μηνύματος και μετά η εναπόθεσή του σε μια ουρά για αποστολή από το πρόγραμμα αποστολής.

Η αποστολή σε τοπικό υπολογιστή γίνεται αυτόματα με την απλή αντιγραφή του μηνύματος στη θυρίδα του παραλήπτη. Η αποστολή σε απομακρυσμένο υπολογιστή απαιτεί τη χρήση του μοντέλου πελάτη - εξυπηρετητή. Ο εξυπηρετητής βρίσκεται στον παραλήπτη και είναι αυτός που μεταφέρει το μήνυμα στη θυρίδα του παραλήπτη (βλέπε εικόνα 2.4.2).

Η διαδικασία αυτή ακολουθεί το πρωτόκολλο SMTP (Simple Mail Transfer Program). Το πρωτόκολλο αυτό διαχειρίζεται όλες τις λεπτομέρειες της επικοινωνίας και καταφέρνει αξιόπιστη μεταφορά μηνυμάτων. Το SMTP κρατάει αντίγραφο του μηνύματος που αποστέλλεται για να το έχει σε περίπτωση που χαθεί στη μεταφορά, βρίσκει αν υπάρχει ο υπολογιστής του παραλήπτη.

Επίσης, γίνεται διαχείριση του τρόπου αποστολής ώστε σε περιπτώσεις που στέλνεται ένα μήνυμα σε πολλούς παραλήπτες να μην φορτώνεται η σύνδεση του

χρήστη, αλλά να στέλνεται το μήνυμα μια φορά και να αναλαμβάνει το δίκτυο (οι δρομολογητές δηλαδή) την αποστολή του στους πολλαπλούς αυτούς παραλήπτες. Με τον τρόπο αυτό πετυχαίνουμε το μήνυμα να φτάνει περίπου την ίδια ώρα στους διάφορους παραλήπτες και αν κάτι δεν πάει καλά μεταξύ πομπού και δέκτη οι πιθανότητες να λάβει κάποιος το μήνυμα χωρίς να το έχει λάβει κάποιος άλλος να ελαχιστοποιούνται.

Εικόνα 2.4.2. *Το μοντέλο πελάτη – εξυπηρετητή για την αποστολή ηλεκτρονικού ταχυδρομείου*

2.4.4. Λίγα λόγια για το SMTP

Το πρωτόκολλο SMTP (Simple Mail Transfer Protocol) έχει καθιερωθεί για την μετάδοση μηνυμάτων ηλεκτρονικού ταχυδρομείου στο Διαδίκτυο. Περιγράφεται αναλυτικά στα RFC 812 και RFC 1123. Το πρωτόκολλο που χρησιμοποιείται σήμερα αποτελεί επέκταση του αρχικού προτύπου και περιγράφεται στο RFC 2821.

Ας προχωρήσουμε στον τρόπο λειτουργίας του εν λόγω πρωτοκόλλου. Για την αποστολή ενός ηλεκτρονικού μηνύματος θα πρέπει ο χρήστης να έχει πρόσβαση σε ένα εξυπηρετητή SMTP (SMTP server). Όλα τα προγράμματα ηλεκτρονικής αλληλογραφίας (π.χ. Mozilla Thunderbird, Microsoft Outlook κλπ.) θα πρέπει να ρυθμιστούν κατάλληλα από τον χρήστη για να λειτουργήσουν σωστά. Συγκεκκριμένα ο χρήστης θα πρέπει να καθορίσει τον SMTP server που θα χρησιμοποιήσει για να στείλει και να παραλάβει ηλεκτρονική αλληλογραφία. Με τον τρόπο αυτό μπορεί για παράδειγμα ένας χρήστης να ανταλλάξει ηλεκτρονικά μηνύματα χωρίς να είναι συνδεδεμένος στο διαδίκτυο, αν χρησιμοποιεί ένα τοπικό SMTP server.

Οι SMTP servers θα πρέπει να έχουν ανοιχτή τουλάχιστον μια από τις θύρες 25 και 587, ούτως ώστε να μπορέσουν να επικοινωνήσουν με άλλους SMTP servers για

την αποστολή ή παραλαβή ηλεκτρονικών μηνυμάτων. Πολλοί SMTP servers χρησιμοποιούν και τις δυο θύρες για λόγους συμβατότητας.

Μια τυπική παραλαβή ηλεκτρονικού μηνύματος από ένα SMTP server έχει ως εξής: Αρχικά δημιουργείται μια σύνδεση μεταξύ του SMTP server που έχει τον ρόλο του αποστολέα και του SMTP server που έχει τον ρόλο του παραλήπτη. Στην συνέχεια οι δυο SMTP servers «συνομιλούν» ούτως ώστε να επιτευχθεί χωρίς προβλήματα η ανταλλαγή του μηνύματος. Στην συνέχεια παρατίθεται ως παράδειγμα μια υποτυπώδης συνομιλία μεταξύ του αποστολέα (Α) και του παραλήπτη (Π) του μηνύματος. Για την δημιουργία σύνδεσης μεταξύ των δυο υπολογιστών μπορεί να χρησιμοποιηθεί το πρόγραμμα telnet ως εξής:

telnet www.example.com 25

Η παραπάνω εντολή δημιουργεί μια TCP σύνδεση από τον αποστολέα στον παραλήπτη (www.example.com) στην θύρα 25. Αφού γίνει η σύνδεση, ακολουθεί η εξής συνομιλία μεταξύ των δυο υπολογιστών:

Π: 220 www.example.com ESMTP Postfix

Α: HELO mydomain.com

Π: 250 Hello mydomain.com

Α: MAIL FROM: <sender@mydomain.com>

Π: 250 Ok

Α: RCPT TO: <friend@example.com>

Π: 250 Ok

Α: DATA

Π: 354 End data with <CR> <LF>.<CR> <LF>

Α: Subject: test message

Α: From: sender@mydomain.com

Α: To: friend@example.com

Α:

Α: Hello,

Α: This is a test.

Α: Goodbye.

Α: .

Π: 250 Ok: queued as 12345

A: QUIT

Π: 221 Bye

Ουσιαστικά η παραπάνω συνομιλία χρησιμοποιείται για να στείλει το ακόλουθο μήνυμα από τον SMTP server mydomain.com (ηλ. διεύθυνση sender@mydomain.com) στον SMTP server example.com (ηλ. διεύθυνση friend@example.com):

Hello,

This is a test.

Goodbye.

Υπάρχουν φυσικά και αρκετές άλλες επιλογές στην συνομιλία, οι οποίες δεν παρουσιάζονται στο παραπάνω παράδειγμα. Ενδεικτικά αξίζει να αναφερθεί η λέξη SIZE που χρησιμοποιείται από τον αποστολέα για να μάθει το μέγιστο μηνύματος που μπορεί να παραλάβει ο παραλήπτης. Επίσης η λέξη EHLO (αναγραμματισμένο HELO) χρησιμοποιείται αντί της HALLO στην παραπάνω συνομιλία για να ξεκινήσει μια σύνοδο Extended SMTP (ESMTP) αντί για μια σύνοδο απλού SMTP. Παρακάτω φαίνεται ένα παράδειγμα όπου χρησιμοποιούνται οι δυο προαναφερθείσες επιλογές.

Π: 220-serverdomain.com ESMTP {postfix version and date}

Π: 220 NO UCE. {etc., terms of service}

A: EHLO mydomain.com

Π: 250-serverdomain.com Hello mydomain.com [127.0.0.1]

Π: 250-SIZE 14680064

Π: 250-PIPELINING

Π: 250 HELP

Στο παράδειγμα αυτό ο SMTP server serverdomain.com (Παραλήπτης) χρησιμοποιεί την λέξη SIZE για να ενημερώσει τον SMTP server mydomain.com (Αποστολέας) ότι δεν πρόκειται να δεχθεί μηνύματα το μέγεθος των οποίων υπερβαίνει κάποια προκαθορισμένη τιμή. Στην συγκεκριμένη τιμή το μέγεθος αυτό είναι 14.680.064 bytes ή 14 MB. Εάν το μήνυμα που προσπαθεί να μεταδώσει ο αποστολέας είναι μεγαλύτερο από 14 MB, τότε δεν θα γίνει αποδεκτό και η μετάδοση θα αποτύχει.

2.4.4.1 Μοντέλο επεξεργασίας μηνυμάτων στο SMTP

Ένα email υποβάλλεται από ένα πελάτη (mail client ή MUA- mail user agent) σε ένα εξυπηρετητή (mail server ή MSA- mail submission agent) χρησιμοποιώντας το SMTP στην θύρα 587. Οι περισσότεροι πάροχοι ηλεκτρονικών θυρίδων εξακολουθούν να επιτρέπουν την υποβολή στην παραδοσιακή θύρα 25. Από εκεί ο MSA μεταφέρει το μήνυμα στον MTA (mail transfer agent). Συχνά, οι δυο τελευταίοι, είναι απλώς διαφορετικές οντότητες του ίδιου λογισμικού, οι οποίοι εκκινούνται με διαφορετικές επιλογές στην ίδια μηχανή. Η τοπική επεξεργασία μπορεί να γίνει είτε σε μια μόνο μηχανή ή να διασπαστεί και κάθε κομμάτι να επεξεργαστεί από διαφορετικό μηχάνημα. Στην πρώτη περίπτωση οι διαδικασίες που εμπλέκονται μπορούν να μοιραστούν αρχεία μεταξύ τους. Στην δεύτερη περίπτωση το SMTP χρησιμοποιείται για να μεταφέρει το μήνυμα εσωτερικά, με κάθε host να ρυθμίζεται ώστε να χρησιμοποιήσει την επόμενη συσκευή ως smart host. Κάθε διαδικασία σε ένα MTA από μόνη της είναι ορθή-πρόκειται στην ουσία για ένα SMTP server.

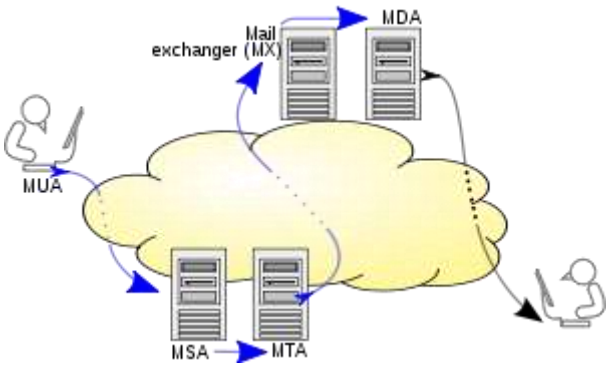
Ο MTA έχει σαν στόχο να εντοπίσει τον target host. Χρησιμοποιεί το DNS για να αναζητήσει την εγγραφή του ανταλλαγέα μηνυμάτων (Mail Exchanger Record, MX record) για την περιοχή του παραλήπτη (το μέρος της διεύθυνσης ηλ. ταχυδρομείου στα δεξιά του @). Η επιστρεφόμενη εγγραφή περιέχει το όνομα του target host. Ο MTA έπειτα συνδέεται στον exchange server σαν πελάτης SMTP. (Το άρθρο σχετικά με τις εγγραφές MX αναλύει όλους τους παράγοντες που καθορίζουν με ποιον εξυπηρετητή θα συνδεθεί κάθε φορά ο MTA, βλ. Wikipedia).

Μόλις ο MX target host αποδεχθεί το εισερχόμενο μήνυμα, το προωθεί σε ένα MDA (mail delivery agent) με στόχο να το αποστείλει στον παραλήπτη. Ένας MDA μπορεί να σώζει μηνύματα σύμφωνα με το σχετικό format που θεσπίζεται από την ηλ. θυρίδα. Και πάλι, η τελική παραλαβή του μηνύματος μπορεί να γίνει χρησιμοποιώντας πολλούς υπολογιστές ή μόνο ένα-το σχήμα απεικονίζει δυο κουτιά το ένα δίπλα στο άλλο για κάθε περίπτωση. Ένας MDA μπορεί να αποστείλει μηνύματα απευθείας στον αποθηκευτικό χώρο ή να τα προωθήσει μέσω ενός δικτύου χρησιμοποιώντας το SMTP ή με οποιανδήποτε άλλο τρόπο συμπεριλαμβανομένου του πρωτοκόλλου LMTP (Local Mail Transfer Protocol), ενός παράγωγου του SMTP που σχεδιάστηκε για αυτό τον σκοπό.

Με το που αποστέλλεται στον local mail server, το μήνυμα αποθηκεύεται σε περίπτωση που χρειαστεί να ανακτηθεί από τους MUAs. Το μήνυμα ανακτάται από τις εφαρμογές των χρηστών, που καλούνται πελάτες ηλ. μηνυμάτων, χρησιμοποιώντας το IMAP (Internet Mail Access Protocol), ένα πρωτόκολλο που διευκολύνει τόσο την πρόσβαση στα μηνύματα όσο και την διαχείριση του συνόλου των αποθηκευμένων μηνυμάτων ή το POP (Post Office Protocol) που χρησιμοποιεί το παραδοσιακό format της θυρίδας των ηλ. μηνυμάτων ή ένα ιδιόκτητο σύστημα όπως το Microsoft Exchange/Outlook ή το Lotus

Notes/Domino. Οι πελάτες μπορούν να χρησιμοποιήσουν οποιαδήποτε μέθοδο, αλλά το πρωτόκολλο που αναλαμβάνει την παραλαβή των μηνυμάτων συνήθως δεν είναι προκαθορισμένο εξ αρχής.

Το SMTP ορίζει την μεταφορά μηνύματος και όχι το περιεχόμενο του μηνύματος. Επομένως ορίζει τον φάκελο του μηνύματος (envelope) και τις παραμέτρους του, όπως τον αποστολέα αλλά όχι την επικεφαλίδα (εκτός από την πληροφορία ίχνους, trace information) ούτε το κυρίως σώμα του μηνύματος. Το STD 10 και το RFC 5321 ορίζουν το SMTP (τον φάκελο), ενώ τα STD 11 και RFC 5322 ορίζουν το μήνυμα (επικεφαλίδα και κυρίως σώμα), που συνήθως αναφέρεται με τον όρο Internet Message Format.



Εικόνα 2.4.3. *Μοντέλο μεταφοράς μηνύματος με το πρωτόκολλο SMTP*

2.4.4.2 Άλλο παράδειγμα επικοινωνίας στο SMTP

Ένα τυπικό παράδειγμα αποστολής ενός μηνύματος μέσω του SMTP σε δυο ηλ. θυρίδες (alice, theboss) που βρίσκονται στην ίδια περιοχή (example.com ή localhost.com) παρουσιάζεται με την βοήθεια της ακόλουθης ανταλλαγής συνόδων. (Σε αυτό το παράδειγμα τα μέρη που συμμετέχουν στην συζήτηση δηλώνονται με τα προθέματα S:, C: για τον εξυπηρετητή και τον πελάτη αντίστοιχα-εντούτοις αυτές οι ετικέτες δεν είναι μέρος της ανταλλαγής).

Αφότου ο αποστολέας του μηνύματος (SMTP client) εγκαταστήσει ένα ασφαλές κανάλι επικοινωνίας με τον αποδέκτη του μηνύματος (SMTP server), η σύνοδος ξεκινάει με ένα χαιρετισμό από τον εξυπηρετητή που συνήθως περιέχει το πλήρες όνομά του (fully qualified domain name, FQDN), σε αυτή την περίπτωση smtp.example.com. Ο πελάτης ξεκινάει τον διάλογο αποκρινόμενος με μια εντολή HELO δηλώνοντας τον εαυτό του στην παράμετρο της εντολής μαζί με το FQDN του (ή με μια έγκυρη διεύθυνση αν δεν υπάρχει κανένα όνομα διαθέσιμο).

S: 220 smtp.example.com ESMTP Postfix

C: HELO relay.example.org

S: 250 Hello relay.example.org, I am glad to meet you

C: MAIL FROM: <bob@example.org>

S: 250 Ok

C: RCPT TO: <alice@example.com>

S: 250 Ok

C: RCPT TO: <theboss@example.com>

S: 250 Ok

C: DATA

S: 354 End data with <CR><LF>.<CR><LF>

C: From: "Bob Example" <bob@example.org>

C: To: "Alice Example" <alice@example.com>

C: Cc: theboss@example.com

C: Date: Tue, 15 January 2008 16:02:43 -0500

C: Subject: Test message

C:

C: Hello Alice.

C: This is a test message with 5 header fields and 4 lines in the message body.

C: Your friend,

C: Bob

C: .

S: 250 Ok: queued as 12345

C: QUIT

S: 221 Bye

{The server closes the connection}

Ο πελάτης γνωστοποιεί την διεύθυνση του αποστολέα του μηνύματος μέσω της εντολής MAIL FROM. Σε αυτό το παράδειγμα το μήνυμα θα σταλεί σε δυο θυρίδες στον ίδιο SMTP server-μια για κάθε παραλήπτη που περιλαμβάνονται στα πεδία επικεφαλίδας To και Cc. Η αντίστοιχη SMTP εντολή είναι RCPT TO (από

το αγγλικό recipient δηλαδή παραλήπτης). Κάθε επιτυχημένη ανάγνωση και εκτέλεση μιας εντολής γίνεται αντιληπτή από τον server με την βοήθεια ενός ειδικού αριθμού που λειτουργεί σαν κωδικός και ενός μηνύματος απόκρισης (π.χ. 250 Ok).

Η μετάδοση του κυρίως σώματος του μηνύματος ξεκινάει με μια εντολή DATA μετά από την οποία μεταδίδεται λέξη προς λέξη και ολοκληρώνεται με μια ακολουθία τύπου «end-of-data» (τέλος δεδομένων). Αυτή η ακολουθία αποτελείται από μια νέα γραμμή (<CR><LF>), μια τελεία (περίοδος) και ακολουθεί νέα γραμμή. Καθώς το κυρίως σώμα ενός μηνύματος μπορεί να περιέχει μια γραμμή με μια μονάχα περίοδο σαν μέρος του κειμένου, ο πελάτης στέλνει δυο περιόδους κάθε φορά που μια γραμμή ξεκινάει με μια περίοδο-επομένως ο server αντικαθιστά κάθε ακολουθία δυο περιόδων στην αρχή μιας γραμμής με μια μόνο. Η μέθοδος αυτή αναφέρεται ως dot-stuffing.

Η θετική απάντηση του εξυπηρετητή στην δήλωση τέλους δεδομένων, όπως φαίνεται από τον κώδικα, υπονοεί ότι ο εξυπηρετητής ανέλαβε την ευθύνη μετάδοσης του μηνύματος. Ένα μήνυμα μπορεί να διπλασιαστεί αν προκύψει εκείνη την στιγμή κάποιο σφάλμα επικοινωνίας, π.χ. εξαιτίας διακοπής ρεύματος. Μέχρι ο αποστολέας να λάβει την απάντηση 250, πρέπει να υποθέσει ότι το μήνυμα δεν στάλθηκε επιτυχώς. Από την άλλη πλευρά, αφότου ο δέκτης αποφάσισε να αποδεχτεί το μήνυμα, πρέπει να υποθέσει ότι το μήνυμα στάλθηκε σε αυτόν. Επομένως κατά την διάρκεια αυτής της χρονικής στιγμής και οι δυο πράκτορες (agents) έχουν ακριβή αντίγραφα του μηνύματος που θα προσπαθήσουν να στείλουν. Η πιθανότητα να συμβεί σφάλμα επικοινωνίας ακριβώς σε αυτό το βήμα είναι ακριβώς ανάλογη με την ποσότητα φιλτραρίσματος που πραγματοποιεί ο εξυπηρετητής στο σώμα του μηνύματος, κυρίως για περιπτώσεις anti-spam. Το προβλεπόμενο χρονικό διάστημα που αναφέραμε πριν υπολογίζεται περίπου στα 10 λεπτά.

Τέλος, η εντολή QUIT ολοκληρώνει (τερματίζει) την σύνοδο. Αν το μήνυμα έχει και άλλους αποδέκτες που βρίσκονται τοποθετημένοι αλλού, ο πελάτης θα τερματίσει την σύνοδο (εντολή QUIT) και θα συνδεθεί σε ένα κατάλληλο SMTP server για τους υπόλοιπους παραλήπτες αφού ο τωρινός προορισμός (ή οι προορισμοί) έχουν εξέλθει της ουράς. Η πληροφορία που στέλνει ο πελάτης στις εντολές HELO και MAIL FROM προστίθεται (δεν φαίνεται αυτό στον κώδικά μας) σαν επιπρόσθετα πεδία επικεφαλίδας στο μήνυμα από τον εξυπηρετητή που το παραλαμβάνει. Προσθέτει τα πεδία επικεφαλίδας Received και Return-path αντίστοιχα.

Μερικοί πελάτες ρυθμίζονται να τερματίζουν την σύνδεση αφότου το μήνυμα γίνει αποδεκτό (250 Ok: queued as 12345), έτσι οι δυο τελευταίες γραμμές μπορούν στην κυριολεξία να παραληφθούν. Αυτό προκαλεί ένα σφάλμα στον εξυπηρετητή όταν προσπαθεί να στείλει την απάντηση 221.

2.4.5. Λίστες και Προωθητές Μηνυμάτων

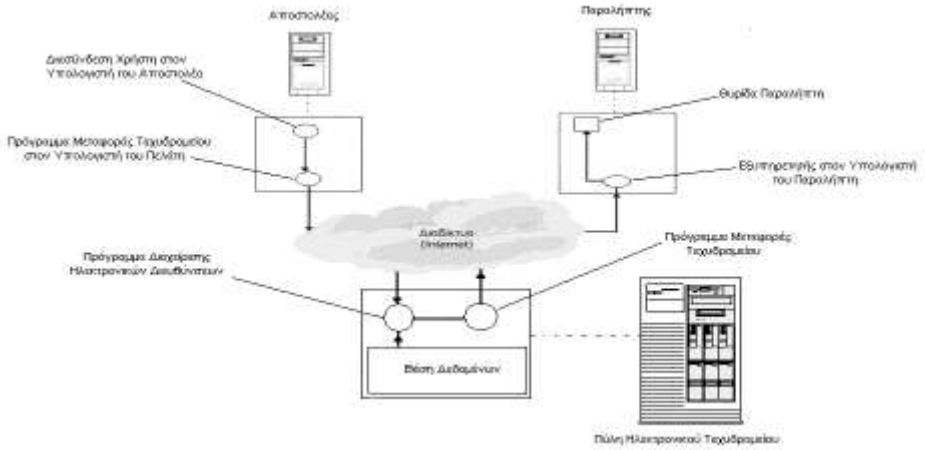
Η διαχείριση και προώθηση μηνυμάτων μπορεί να γίνει από ειδικά προγράμματα. Όταν θέλουμε να στείλουμε ένα μήνυμα σε ομάδες χρηστών μπορούμε να δημιουργήσουμε λίστες, όπου με τη χρήση μιας μόνο διεύθυνσης μπορούμε να στείλουμε το ίδιο μήνυμα σε πολλαπλούς χρήστες. Στο παράδειγμα του πίνακα 2.4.3, αν στείλουμε το μήνυμα μας στη λίστα «Φίλοι» θα το λάβουν και οι πέντε φίλοι μας που ορίζονται στην λίστα. Το σχήμα μας δείχνει μια βάση όπου έχουμε κατατάξει ομάδες θυρίδων σε λίστες.

Υπάρχουν προηγμένα προγράμματα λιστών ή προωθητών ηλεκτρονικού ταχυδρομείου, γνωστά σαν list managers, που επιτρέπουν διαχείριση λιστών με δυνατότητες αυτόματης εγγραφής, διαγραφής, περιορισμών χρήσης, καταγραφής απεσταλμένων μηνυμάτων κ.λπ.

Πίνακας 2.4.3. *Αποστολή ηλεκτρονικού μηνύματος σε ομάδες χρηστών*

Λίστα	**Περιεχόμενα**
Φίλοι	George_Kerk@hotmail.com, Joan@freemail.gr, Peter_Mold@ibm.com, Johny@yahoo.gr, A_S_Gol@unipi.gr
Συγγενείς	Mary@ntua.gr, Mike@microsoft.gr
Καθηγητές	ngali@ntua.gr, pgiann@unipi.gr

Η διαδικασία αποστολής και λήψης μηνυμάτων, ιδιαίτερα αν αυτά απευθύνονται σε πολλούς παραλήπτες, είναι μια χρονοβόρα διαδικασία. Για το λόγο αυτό πολλοί οργανισμοί έχουν αφιερώσει κάποιο μηχάνημα για τη διαχείριση του ηλεκτρονικού ταχυδρομείου. Ένας τέτοιος υπολογιστής είναι γνωστός σαν πύλη ή αναμεταδότης ηλεκτρονικού ταχυδρομείου (email gateway, email relay). Στην εικόνα 2.4.3 φαίνεται η διαδικασία αποστολής ενός μηνύματος με τη χρήση μιας τέτοιας πύλης.



Εικόνα 2.4.3. *Χρήση Πύλης για τη διαχείριση του ηλεκτρονικού ταχυδρομείου*

Η ύπαρξη των πυλών αυτών μας επιτρέπει να χρησιμοποιούμε αντιστοιχίες στις ηλεκτρονικές διευθύνσεις ώστε να διευκολύνουμε τη χρήση τους σε ένα οργανισμό. Μπορούμε παραδείγματος χάριν να αντιστοιχίσουμε την πραγματική διεύθυνση christos@rainbow.cs.unipi.gr που δείχνει που βρίσκεται η θυρίδα του χρήστη christos – δηλαδή, στο μηχάνημα rainbow στο δίκτυο cs.unipi.gr – με την απλούστερη και ευκολότερα διαχειρίσιμη διεύθυνση christos@unipi.gr. Έτσι μπορούμε να πετύχουμε ομοιομορφία στις διευθύνσεις σε ένα οργανισμό και να απαλλάξουμε την άμεση σύνδεση της ηλεκτρονικής διεύθυνσης με κάποια φυσική παρουσία του χρήστη ή με κάποιο συγκεκριμένο μηχάνημα. Έτσι, ένας χρήστης μπορεί να αλλάξει μηχάνημα ή υποδίκτυο χωρίς να είναι απαραίτητη η αλλαγή της ηλεκτρονικής του διεύθυνσης. Για το λόγο αυτό απαιτείται βέβαια η ύπαρξη μιας λίστας αντιστοίχισης στην πύλη του ηλεκτρονικού ταχυδρομείου.

2.4.6. Πρόσβαση στη Θυρίδα

Οι θυρίδες ηλεκτρονικού ταχυδρομείου πρέπει να τοποθετηθούν σε μηχανήματα που έχουν ένα εξυπηρετητή ηλεκτρονικού ταχυδρομείου. Ο υπολογιστής αυτός πρέπει να έχει αρκετή μνήμη και ταχύτητα για να διαχειρίζεται το φόρτο που πιθανόν να φέρει η χρήση του ηλεκτρονικού ταχυδρομείου. Επίσης, θα πρέπει ο υπολογιστής αυτός να είναι ανοικτός συνεχώς και όχι μόνο όταν είναι παρών ο χρήστης.

Το πρωτόκολλο POP (Post Office Protocol) επιτρέπει να τρέχει ένας εξυπηρετητής ηλεκτρονικού ταχυδρομείου σε ένα υπολογιστή και να είναι προσπελάσιμος από πολλούς πελάτες. Έτσι, κεντρικοποιείται η διαχείριση του ηλεκτρονικού

ταχυδρομείου και γίνεται βέλτιστη χρήση πόρων. Οι χρήστες τρέχουν ένα πρόγραμμα πελάτη του εξυπηρετητή POP για πρόσβαση στα μηνύματά τους.

Στην εικόνα 2.4.4 φαίνεται η λειτουργία του ηλεκτρονικού ταχυδρομείου. Ο αποστολέας και ο παραλήπτης είναι χρήστες δύο υπολογιστών που είναι συνδεδεμένοι σε δύο δίκτυα. Τα δύο δίκτυα είναι συνδεδεμένα με τη σειρά τους στο διαδίκτυο (Internet). Η διαδικασία αποστολής – λήψης του ηλεκτρονικού μηνύματος είναι η ακόλουθη:

Ο αποστολέας χρησιμοποιεί ένα πρόγραμμα (Mail User Agent) για να συντάξει και να διαμορφώσει το μήνυμά του.

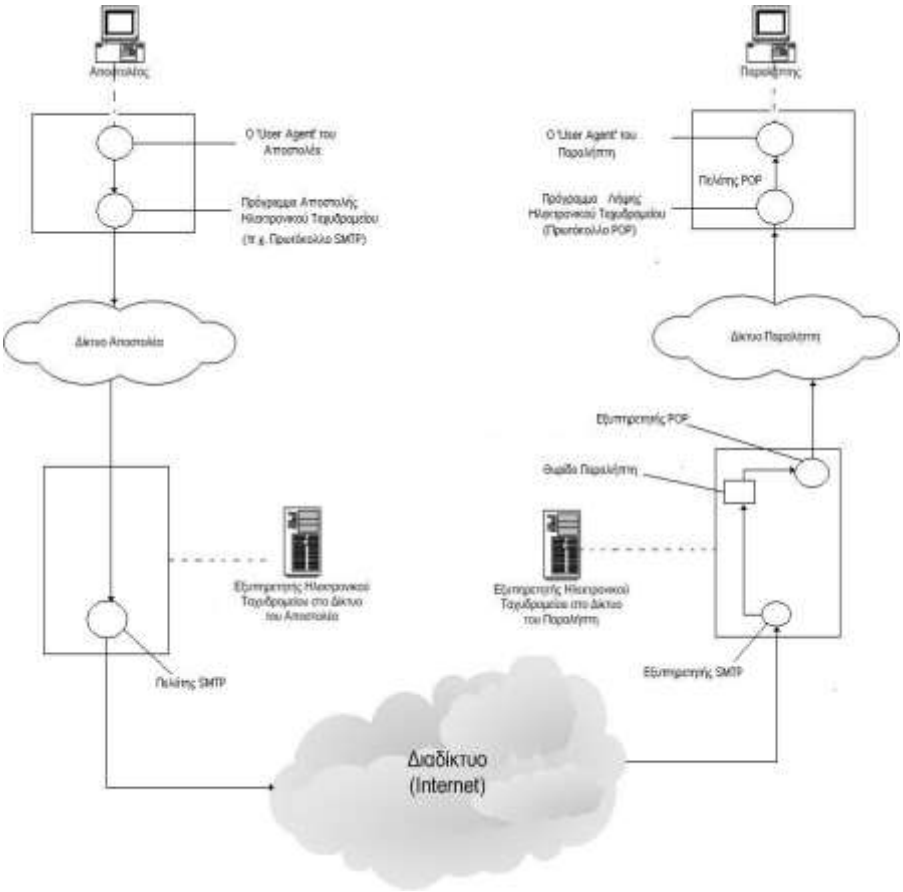
Ο User Agent εναποθέτει το μήνυμα στο πρωτόκολλο SMTP, το οποίο αναλαμβάνει να το στείλει στον εξυπηρετητή ηλεκτρονικού ταχυδρομείου, στο δίκτυο του αποστολέα. Το μήνυμα μπαίνει σε μια ουρά αναμονής, οπού πιθανώς υπάρχουν μηνύματα και από άλλους χρήστες του ίδιου δικτύου.

Ο εξυπηρετητής Ηλεκτρονικού ταχυδρομείου του δικτύου του αποστολέα στέλνει το μήνυμα στον αντίστοιχο εξυπηρετητή του δικτύου του παραλήπτη διαμέσου του Διαδικτύου, με χρήση του πρωτοκόλλου SMTP.

Ο εξυπηρετητής Ηλεκτρονικού Ταχυδρομείου στο δίκτυο του παραλήπτη επεξεργάζεται το μήνυμα που έλαβε και το εναποθέτει στη θυρίδα του παραλήπτη.

Όταν ο παραλήπτης συνδεθεί στο δίκτυό του, μπορεί να «κατεβάσει» το μήνυμα στον υπολογιστή του, με χρήση του πρωτοκόλλου POP (Post Office Protocol).

Οι εξυπηρετητές POP είναι πολύ δημοφιλείς καθώς επιτρέπουν την πρόσβαση σε ηλεκτρονικό ταχυδρομείο και σε χρήστες που συνδέονται με αργές και όχι μόνιμες συνδέσεις στο Διαδίκτυο. Τέτοιοι είναι οι χρήστες οι οποίοι χρησιμοποιούν τηλεφωνικές συνδέσεις και modem.



Εικόνα 2.4.4. *Η λειτουργία του ηλεκτρονικού ταχυδρομείου, με χρήση του πρωτοκόλλου POP, για τη λήψη των ηλεκτρονικών μηνυμάτων*

2.4.7. Πρόσβαση στο Ηλεκτρονικό Ταχυδρομείο

Κάθε χρήστης του Internet έχει τη δική του **διεύθυνση ηλεκτρονικού ταχυδρομείου** (**E-mail address**). Αυτό σημαίνει ότι, κάθε χρήστης σε κάποιο από τα δίκτυα που αποτελούν το Internet, έχει τουλάχιστον ένα **λογαριασμό,** αποτελούμενο από το **όνομα χρήστη** (**user name**) και το μυστικό **συνθηματικό** (**password**), καταχωρημένο σε κάποια μηχανή του δικτύου του. Όταν ένας χρήστης αποκτά λογαριασμό σε μια μηχανή, αυτόματα αντιστοιχίζεται σε αυτόν μια διεύθυνση e-mail αποτελούμενη από το όνομα του χρήστη (user name) και τη **διεύθυνση της μηχανής** ενωμένα με το σύμβολο "@". Δηλαδή είναι της μορφής:

όνομα_χρήστη@διεύθυνση μηχανής (όνομα υπολογιστή)

Το όνομα χρήστη μπορεί να είναι το userid με το οποίο κάποιος συνδέεται στον υπολογιστή ή κάποια παραλλαγή του πραγματικού του ονόματος. Σε ορισμένα συστήματα ο χρήστης μπορεί να έχει το πραγματικό του όνομα σαν ταχυδρομικό όνομα ή ακόμη να διαλέξει το όνομα που θέλει.

Όταν κάποιος έχει ηλεκτρονικό ταχυδρομείο, μπορεί να επικοινωνεί με άλλους χρήστες ηλεκτρονικού ταχυδρομείου σ' όλο τον κόσμο. Έτσι, αν συμμετέχει σε διεθνείς ηλεκτρονικές λίστες ή λαμβάνει μέρος σε διεθνή προγράμματα, θα δει ηλεκτρονικές διευθύνσεις από διάφορες χώρες.

Για να εγκαταστήσει κάποιος χρήστης σωστά το ηλεκτρονικό ταχυδρομείο στον υπολογιστή του θα χρειαστεί να γνωρίζει τα εξής :

- Τη διεύθυνση ηλεκτρονικού ταχυδρομείου του
- Τον POP διακομιστή (server) και τον SMTP server στους οποίους συνδέεται
- Τον POP λογαριασμό (account που) κατέχει.

Τα μηνύματα του ηλεκτρονικού ταχυδρομείου διακινούνται στο Διαδίκτυο, σύμφωνα με το πρωτόκολλο **SMTP** (Simple Mail Transfer Protocol). Το πρωτόκολλο αυτό στηρίζεται στην αρχιτεκτονική client-server και χρησιμοποιεί TCP συνδέσεις. Το SMTP δέχεται ένα μήνυμα από το χρήστη μαζί με μια λίστα από προορισμούς. Τότε στέλνεται σε κάθε προορισμό από ένα αντίγραφο, εκτός κι αν οι διαφορετικοί χρήστες είναι στον ίδιο κόμβο. Στην περίπτωση αυτή, το μήνυμα στέλνεται μόνο μία φορά μαζί με τη λίστα προορισμών στον αντίστοιχο κόμβο. Όταν η μεταφορά του μηνύματος δεν είναι επιτυχής, το SMTP επαναλαμβάνει τη μεταφορά για μερικές διαδοχικές μέρες πριν παραιτηθεί και αναφέρει στο χρήστη την αποτυχία της παράδοσης.

Τα παραπάνω ισχύουν στην περίπτωση που δουλεύει κάποιος σαν χρήστης μιας μηχανής συνδεδεμένης με το Internet 24 ώρες το εικοσιτετράωρο. Μπορεί ανά πάσα στιγμή να στείλει ένα μήνυμα και αντίστροφα, αφού η μηχανή του είναι διαρκώς διαθέσιμη να δέχεται μηνύματα που προορίζονται για αυτόν και τους υπόλοιπους χρήστες της. Σε κάθε χρήστη, αντιστοιχεί ένα ξεχωριστό αρχείο στο δίσκο της μηχανής , που φέρει το ίδιο όνομα με το λογαριασμό του χρήστη και λειτουργεί σαν το προσωπικό του **γραμματοκιβώτιο (mailbox)**. Εδώ συγκεντρώνονται τα εισερχόμενα μηνύματα που προορίζονται γι' αυτόν κι έτσι δε συγχέονται με τα μηνύματα που προορίζονται για τους υπόλοιπους χρήστες.

Τι γίνεται όμως στη συνηθέστερη περίπτωση που ο χρήστης δουλεύει στον προσωπικό του υπολογιστή (PC ή MAC) που βεβαίως δε λειτουργεί 24 ώρες το εικοσιτετράωρο;

Τότε, η εισερχόμενη αλληλογραφία του και πάλι αποθηκεύεται στο γραμματοκιβώτιό του σε κάποια μηχανή UNIX του παροχέα υπηρεσιών Internet.

Τώρα, πρέπει να ακολουθήσει ένα πρόσθετο βήμα μεταφοράς της από τη μηχανή UNIX στον προσωπικό του υπολογιστή. Μέσω ενός προγράμματος-πελάτη που εκτελεί στον υπολογιστή του, συνδέεται με τη μηχανή UNIX, στην οποία εκτελείται ένα πρόγραμμα-εξυπηρετητής **POP3** (**P**ost-**O**ffice-**P**rotocol3 server) και ζητάει την αλληλογραφία του η οποία τελικά αποθηκεύεται στο δίσκο του προσωπικού του υπολογιστή.

Όταν θέλει να στείλει ένα μήνυμα από τον προσωπικό του υπολογιστή, αυτό δεν είναι αναγκαίο να αποθηκευτεί στο δίσκο της UNIX μηχανής, μιας και **μπορεί να σταλεί απευθείας**. Στην περίπτωση αυτή, μέσω του προγράμματος-πελάτη, συνδέεται με ένα άλλο πρόγραμμα που εκτελείται στη UNIX μηχανή και ονομάζεται **εξυπηρετητής SMTP** (SMTP server) το οποίο και αναλαμβάνει την αποστολή του μηνύματος του χρήστη.

Επίσης, υπάρχουν πολλές εταιρίες, όπου οι εργαζόμενοι δουλεύουν σε υπολογιστές που δεν είναι συνδεδεμένοι στο Διαδίκτυο και δεν έχουν συνεπώς τη δυνατότητα να στείλουν ή να λάβουν ηλεκτρονικό ταχυδρομείο έξω από την εταιρία. Οι εταιρίες αυτές διαθέτουν έναν ή και περισσότερους εξυπηρετητές ηλεκτρονικού ταχυδρομείου (mail servers) που μπορούν να στείλουν και να λάβουν ηλεκτρονικό ταχυδρομείο. Ο υπολογιστής, λοιπόν, για να στείλει και να λάβει μηνύματα ηλεκτρονικού ταχυδρομείου πρέπει να επικοινωνήσει με τον εξυπηρετητή αυτόν, χρησιμοποιώντας ένα είδος πρωτοκόλλου παράδοσης. Το ταχυδρομικό πρωτόκολλο POP3 είναι ένα απλό πρωτόκολλο το οποίο φέρνει τα μηνύματα από ένα μακρινό γραμματοκιβώτιο και τα αποθηκεύει στον τοπικό υπολογιστή του χρήστη. Το POP3 έχει εντολές που επιτρέπουν στον χρήστη να εισέρχεται στο σύστημα, να φέρνει μηνύματα, να τα διαγράφει και να εξέρχεται από το σύστημα.

2.4.8. Το πρωτόκολλο POP

Το Post Office Protocol (POP) επίσης γνωστό και ως POP3 είναι ένα πρωτόκολλο που χρησιμοποιείται για την παραλαβή των ηλ. μηνυμάτων (email) από ένα απομακρυσμένο εξυπηρετητή (server) χρησιμοποιώντας σύνδεση TCP/IP.

Το POP3 αποτελεί εξέλιξη των προηγούμενων μορφών του πρωτοκόλλου, τα οποία ονομάζονταν ανεπίσημα POP1 και POP2. Ο όρος Post Office Protocol είναι πλέον συνώνυμος με το POP3, καθώς οι προηγούμενες μορφές του πρωτοκόλλου έχουν πλέον καταργηθεί στην πράξη.

Το POP3 είναι σχεδιασμένο με τέτοιο τρόπο ούτως ώστε να επιτρέπει στους χρήστες του διαδικτύου που έχουν προσωρινές συνδέσεις (π.χ. dial-up) να παραλαμβάνουν την ηλεκτρονική τους αλληλογραφία, να την αποθηκεύουν στον τοπικό σκληρό δίσκο και στην συνέχεια να την διαβάζουν χωρίς να χρειάζεται να παραμένουν συνδεδεμένοι στο διαδίκτυο. Παρόλο που υπάρχει η δυνατότητα τα μηνύματα να παραμείνουν στον server ηλ. ταχυδρομείου, οι περισσότερες

εφαρμογές POP3 συνδέονται με τον server, λαμβάνουν όλα τα ηλ. μηνύματα, τα αποθηκεύουν στον υπολογιστή του χρήστη, τα σβήνουν από τον server και αποσυνδέονται.

Σε αντίθεση με το POP3, το πρωτόκολλο Internet Message Access Protocol (IMAP) που εμφανίστηκε αργότερα υποστηρίζει τόσο την online όσο και την offline ανάγνωση μηνυμάτων. Επίσης αφήνει τα μηνύματα στον server έως ότου ο χρήστης αποφασίσει να τα διαγράψει. Η τακτική αυτή δίνει την δυνατότητα σε ένα χρήστη να διαβάζει τα email του από διάφορους υπολογιστές. Αντίθετα το POP3 επιτρέπει την ανάγνωση των email μονάχα από τον υπολογιστή στον οποίο έχουν κατέβει.

Τα περισσότερα προγράμματα διαχείρισης ηλ. αλληλογραφίας (Mozilla Thunderbird, Microsoft Outlook κοκ) υποστηρίζουν και τα δυο πρωτόκολλα και δίνουν στον χρήστη την δυνατότητα να επιλέξει ποιο ταιριάζει καλύτερα στις ανάγκες του. Παρόλα αυτά όμως το πρωτόκολλο IMAP υποστηρίζεται από λιγότερους servers σε σχέση με το πρωτόκολλο POP3.

Το POP3 χρησιμοποιεί την θύρα 110 για να εγκαθιδρύσει μια σύνδεση TCP με τον mail server. Πολλά προγράμματα ηλ. ταχυδρομείου χρησιμοποιούν κρυπτογράφηση ούτως ώστε τα δεδομένα που διακινούνται στην σύνδεση αυτή να μην είναι αναγνώσιμα από όλους. Για να αποδεχθεί ο mail server την σύνδεση, θα πρέπει ο χρήστης να δώσει το όνομα χρήστη και τον κωδικό πρόσβασής του. Η αρχική έκδοση του POP3 μετέδιδε τα ευαίσθητα αυτά δεδομένα σε μορφή απλού κειμένου, οπότε οποιοσδήποτε μπορούσε να τα διαβάσει. Στην συνέχεια όμως το πρωτόκολλο βελτιώθηκε και πλέον παρέχει την δυνατότητα κρυπτογραφημένης μετάδοσης του ονόματος χρήστη και του κωδικού. Παρόλα αυτά όμως πολλοί χρήστες δεν γνωρίζουν αυτή την δυνατότητα και συνεπώς δεν την χρησιμοποιούν.

2.4.8.1. POP4

Το POP4 αποτελεί μια νέα έκδοση του πρωτοκόλλου, η οποία έχει προταθεί αλλά δεν έχει γίνει ακόμα επίσημο standard. Το POP4 επιτρέπει στον χρήστη να διαχειρίζεται καταλόγους στον mail server και εισάγει κάποιες βελτιώσεις στο POP3 όσον αφορά την διαχείριση μηνυμάτων MIME. Αν και έχει προταθεί ήδη από το 2003, δεν έχει γίνει κάποια πρόοδος όσον αφορά την επίσημη υιοθέτησή του.

2.4.8.2. Σύγκριση με το IMAP

1. Το POP είναι απλούστερο πρωτόκολλο, καθιστώντας την υλοποίησή του ευκολότερη

2. Ο εξυπηρετητής POP μετακινεί το μήνυμα από τον mail server στην πλευρά του παραλήπτη στον τοπικό υπολογιστή του χρήστη, παρόλο που υπάρχει συνήθως και η επιλογή να αφήσει τα μηνύματα απευθείας στον mail server.

3. Το IMAP έχει σχεδιαστεί ώστε να αφήνει το μήνυμα στο mail server, κατεβάζοντας απλά ένα τοπικό αντίγραφο του μηνύματος.

4. Το POP χειρίζεται το mailbox ως αυτοτελή αποθηκευτική μονάδα και έτσι η απαίτηση για ύπαρξη αρχείων και καταλόγων δεν υφίσταται.

5. Ένας πελάτης IMAP επιχειρεί πολύπλοκα αιτήματα, ρωτώντας τον server για επικεφαλίδες ή για το κυρίως σώμα συγκεκριμένων μηνυμάτων ή ζητάει από τον ίδιο να αναζητήσει μηνύματα που ικανοποιούν συγκεκριμένα κριτήρια. Τα μηνύματα που αποθηκεύονται στην θυρίδα του παραλήπτη μπορούν να σημειωθούν με διάφορες ετικέτες κατάστασης (π.χ. “deleted” ή “answered”) και παραμένουν στην θυρίδα μέχρι να τα παραλάβει τελικά ο χρήστης και να διαγραφούν από εκεί-μια διαδικασία που ενδέχεται να καθυστερήσει. Εν συντομία: Το IMAP σχεδιάστηκε για να επιτρέπει διαχείριση απομακρυσμένων θυρίδων σαν να ήταν τοπικές. Με βάση την υλοποίηση του πελάτη IMAP και την αρχιτεκτονική της πλατφόρμας που επιθυμεί ο διαχειριστής του συστήματος, ο χρήστης μπορεί να αποθηκεύει μηνύματα κατευθείαν στην μηχανή του πελάτη ή να τα σώζει στον εξυπηρετητή ή να έχει την δυνατότητα να κάνει και τα δυο.

6. Το πρωτόκολλο POP απαιτεί από τον πελάτη που εκείνη την στιγμή είναι συνδεδεμένος στο δίκτυό του να είναι ο μόνος που έχει συνδεθεί με την θυρίδα του και έχει πρόσβαση στα περιεχόμενά της. Αντίθετα το πρωτόκολλο IMAP απαιτεί με ρητό τρόπο την ταυτόχρονη πρόσβαση από πολλαπλούς πελάτες και παρέχει μηχανισμούς στους πελάτες να εντοπίζουν αν έχουν γίνει τυχόν αλλαγές στην θυρίδα από άλλους πελάτες που εκείνη την στιγμή είναι ταυτόχρονα συνδεδεμένοι και εκείνοι στο δίκτυο και έχουν πρόσβαση στα περιεχόμενα της θυρίδας. Δείτε για παράδειγμα το RFC 3501, κεφάλαιο 5.2, το οποίο συγκεκριμένα αναφέρει «την δυνατότητα ταυτόχρονης πρόσβασης στην ίδια θυρίδα από πολλαπλούς πελάτες» σαν παράδειγμα.

7. Όταν το POP ανακαλεί ένα μήνυμα, λαμβάνει όλα τα μέρη που το απαρτίζουν, ενώ το πρωτόκολλο IMAP4 επιτρέπει στους πελάτες να ανακαλούν ξεχωριστά οποιοδήποτε από τα μέρη που συγκροτούν ένα μήνυμα MIME-για παράδειγμα ανάκληση του απλού κειμένου χωρίς τυχόν επισυναπτόμενα αρχεία.

8. Το IMAP υποστηρίζει τα flags στον server για να είναι συνεχώς ενήμερο για την κατάσταση των μηνυμάτων: για παράδειγμα αν το μήνυμα διαβάστηκε ή όχι, αν απαντήθηκε ή όχι, αν διαγράφηκε ή όχι.

2.4.8.3. Άλλα στοιχεία για το POP

Πρόκειται για πρωτόκολλο του επιπέδου εφαρμογής (application layer).

Υποστηρίζει δυνατότητες download και delete για πρόσβαση σε απομακρυσμένες θυρίδες (ονομάζονται maildrops στα RFCs). Παρόλο που οι περισσότεροι πελάτες POP έχουν την δυνατότητα να αφήσουν τα μηνύματα στον εξυπηρετητή μετά το κατέβασμα, οι πελάτες ηλ. ταχυδρομείου που χρησιμοποιούν το POP σε γενικές γραμμές συνδέονται, παραλαμβάνουν όλα τα μηνύματα, τα αποθηκεύουν στον τοπικό τους υπολογιστή σαν νέα μηνύματα, τα διαγράφουν από τον εξυπηρετητή και έπειτα αποσυνδέονται. Άλλα πρωτόκολλα, όπως το IMAP παρέχουν περισσότερο πολύπλοκες δυνατότητες απομακρυσμένης πρόσβασης στις ηλ. θυρίδες. Στα τέλη της δεκαετίας του ’90 και στις αρχές του 2000, λιγότεροι ISPs (Internet Service Providers) υποστήριζαν το IMAP εξαιτίας του αποθηκευτικού χώρου που απαιτούνταν στο υλικό του ISP. Σύγχρονοι πελάτες ηλ. ταχυδρομείου υποστήριξαν το POP και έπειτα με την πάροδο του χρόνου δημοφιλή λογισμικά για πελάτες ηλ. ταχυδρομείου εισήγαγαν σαν πρόσθετο γνώρισμα την παροχή του αναγκαίου βαθμού υποστήριξης για το πρωτόκολλο IMAP.

Ένας εξυπηρετητής POP3 «ακούει» στην προκαθορισμένη θύρα 110. Η κρυπτογραφημένη επικοινωνία για το POP3 είτε ζητείται μετά την εκκίνηση του πρωτοκόλλου, χρησιμοποιώντας την εντολή STLS, εάν υποστηρίζεται, είτε παρέχεται μέσω του POP3S που συνδέεται με τον εξυπηρετητή χρησιμοποιώντας είτε το πρωτόκολλο TLS (Transport Secure Layer) είτε το SSL (Secure Socket Layer) στην γνωστή θύρα TCP 995.

Τα διαθέσιμα μηνύματα στον εξυπηρετητή οργανώνονται όταν ένα POP session ανοίγει το maildrop και αναγνωρίζονται από τον αριθμό μηνύματος (message-number) που είναι τοπικός για το συγκεκριμένο session ή εναλλακτικά από ένα μοναδικό αναγνωριστικό που εκχωρείται στο μήνυμα από το POP server. Αυτό το αναγνωριστικό είναι μόνιμο και μοναδικό για το maildrop και επιτρέπει σε ένα πελάτη να προσπελαύνει το ίδιο μήνυμα σε διαφορετικά sessions. Η ηλ. αλληλογραφία ανακαλείται και σημειώνεται προς διαγραφή μέσω του message-number. Όταν ο πελάτης τερματίζει το session, η αλληλογραφία που έχει σημειωθεί προς διαγραφή αφαιρείται από την θυρίδα.

Αρχικά το POP3 υποστήριζε ένα μηχανισμό μη κρυπτογραφημένου USER/PASS login ή rlogin (Το rlogin είναι ένα software utility για λειτουργικά συστήματα τύπου Unix που επιτρέπει στους χρήστες να κάνουν log in σε ένα άλλο host μέσω ενός δικτύου, επικοινωνώντας μέσω της TCP θύρας 513). Το POP3 στην τωρινή του μορφή υποστηρίζει διάφορες μεθόδους αυθεντικοποίησης με σκοπό την παροχή διαφόρων επιπέδων προστασίας ενάντια σε οποιαδήποτε μορφή μη εξουσιοδοτημένης πρόσβασης στα ηλ. μηνύματα ενός χρήστη. Οι περισσότερες παρέχονται από τους μηχανισμούς επέκτασης του POP3. Οι πελάτες POP υποστηρίζουν αυθεντικοποίηση SASL (Simple Authentication and Security Layer)

μέσω της επέκτασης AUTH. Το MIT Project Athena πρότεινε επίσης μια παρόμοια έκδοση της προηγούμενης μεθόδου. Το RFC 1460 εισήγαγε το APOP στο κυρίως πρωτόκολλο. Το APOP είναι ένα πρωτόκολλο του τύπου «πρόσκληση/απόκριση» (challenge/response) που χρησιμοποιεί την MD5 hash function με στόχο να αποφύγει τις επιθέσεις αναμετάδοσης (replay attacks) και την αποκάλυψη του διαμοιραζόμενου μυστικού. Πελάτες που υλοποιούν APOP περιλαμβάνουν τους Mozilla Thunderbird, Opera Mail, Eudora, KMail, Novell Evolution, RimArts' Becky!, Windows Live Mail, PowerMail, Apple Mail και Mutt. Το RFC 1460 αναβαθμίστηκε από το RFC 1725 και αυτό εν τέλει από το RFC 1939.

2.4.8.4. Παράδειγμα διαλόγου

Το παράδειγμα το αντλήσαμε από το RFC 1939, σελ. 18. (πρωτόκολλο APOP)

> RFC 1939. Υποστήριξη του APOP μέσω του <1896.697170952@dbc.mtview.ca.us>:
>
> S: <wait for connection on TCP port 110>
>
> C: <open connection>
>
> S: +OK POP3 server ready <1896.697170952@dbc.mtview.ca.us>
>
> C: APOP mrose c4c9334bac560ecc979e58001b3e22fb
>
> S: +OK mrose's maildrop has 2 messages (320 octets)
>
> C: STAT
>
> S: +OK 2 320
>
> C: LIST
>
> S: +OK 2 messages (320 octets)
>
> S: 1 120
>
> S: 2 200
>
> S: .
>
> C: RETR 1
>
> S: +OK 120 octets
>
> S: <the POP3 server sends message 1>
>
> S: .

C: DELE 1

S: +OK message 1 deleted

C: RETR 2

S: +OK 200 octets

S: <the POP3 server sends message 2>

S: .

C: DELE 2

S: +OK message 2 deleted

C: QUIT

S: +OK dewey POP3 server signing off (maildrop empty)

C: <close connection>

S: <wait for next connection>

Οι εξυπηρετητές POP3 χωρίς την εναλλακτική εντολή APOP αναμένουν από τον πελάτη να κάνει log in με τις εντολές USER και PASS:

C: USER mrose

S: +OK User accepted

C: PASS tanstaff

S: +OK Pass accepted

2.4.9. Το Διαλογικό Πρωτόκολλο Ταχυδρομικής Πρόσβασης IMAP (INTERNET MAIL ACCESS PROTOCOL)

Το πρωτόκολλο διαλογικής ταχυδρομικής πρόσβασης IMAP, σχεδιάστηκε ως βελτίωση του POP3. Το κύριο χαρακτηριστικό του είναι ότι ο χρήστης μπορεί να έχει πολλούς φακέλους στον εξυπηρετητή για να αποθηκεύσει τα μηνύματά του. Έτσι, από οπουδήποτε και αν δει τα μηνύματά του χρησιμοποιώντας το IMAP, θα έχει πλήρη πρόσβαση σε όλα τα προηγούμενα διαβασμένα και αποθηκευμένα μηνύματά του.

Ένας άλλος περιορισμός του πρωτοκόλλου POP3 είναι ότι δεν κρατάει την κατάσταση των μηνυμάτων στο γραμματοκιβώτιο του χρήστη. Διαφορετικά μηνύματα μπορεί να έχουν διαφορετικές καταστάσεις, όπως διαβασμένο, αδιάβαστο ή προς διαγραφή. Έτσι, οι περισσότεροι πελάτες POP3 (clients) κατεβάζουν όλα τα μηνύματα στο γραμματοκιβώτιο του χρήστη. Το IMAP

αντίθετα κατεβάζει μόνο τις επικεφαλίδες όλων των μηνυμάτων και κατεβάζει μόνο το μήνυμα που έχει επιλεχθεί.

2.4.9.1. Επιπρόσθετες πληροφορίες για το πρωτόκολλο IMAP

Το Internet Message Access Protocol ή IMAP είναι ένα διαδικτυακό πρωτόκολλο, το οποίο συνδυάζει μερικές από τις δυνατότητες που προσφέρουν το πρωτόκολλο POP3 (Post Office Protocol) και το ηλεκτρονικό ταχυδρομείο μέσω Παγκόσμιου Ιστού (Webmail), αφού επιτρέπει την προαιρετική αποθήκευση μηνυμάτων στον υπολογιστή του χρήστη. Ταυτόχρονα διατηρείται και ένα αντίγραφο της αλληλογραφίας στον διακομιστή (server). Η πρόσβαση σε ένα λογαριασμό ηλεκτρονικού ταχυδρομείου πραγματοποιείται μέσω ενός ειδικού προγράμματος αλληλογραφίας (προγράμματος-πελάτη, όπως π.χ. το Mozilla Thunderbird). Συνήθως τα προγράμματα που υποστηρίζουν το POP3 υποστηρίζουν και το IMAP. Σε οποιονδήποτε υπολογιστή και αν βρίσκεται ο χρήστης και οποιοδήποτε πρόγραμμα ηλεκτρονικής αλληλογραφίας και αν χρησιμοποιεί για να έχει πρόσβαση στον λογαριασμό του, το IMAP τα «βλέπει» όλα με την ίδια δομή.

Το IMAP είναι πρωτόκολλο επιπέδου εφαρμογών (κατά μοντέλο αναφοράς OSI) το οποίο επιτρέπει σε ένα λογισμικό πελάτη (client) να προσπελάσει ένα λογαριασμό ηλεκτρονικού ταχυδρομείου σε ένα απομακρυσμένο διακομιστή (server). Η έκδοση IMAP που χρησιμοποιείται σήμερα είναι η έκδοση 4, αναθεωρημένη 1 (IMAP4rev1) η οποία ορίζεται από το RFC 3501. Ένας διακομιστής IMAP στην πράξη δέχεται επικοινωνία από την port 143. Το IMAP όταν χρησιμοποιείται με Secure Sockets Layer είναι γνωστό ως IMAPS και δέχεται επικοινωνία από την port 993.

Το IMAP λειτουργεί και με σύνδεση και χωρίς σύνδεση. Τα προγράμματα-πελάτες τα οποία χρησιμοποιούν το IMAP συνήθως αφήνουν τα μηνύματα να υπάρχουν και στον διακομιστή, εκτός αν ο χρήστης επιλέξει την διαγραφή τους. Αυτό είναι ένα από τα χαρακτηριστικά της λειτουργίας IMAP το οποίο επιτρέπει περισσότερους από ένα χρήστες να διαχειρίζονται τον ίδιο λογαριασμό ηλ. ταχυδρομείου. Τα περισσότερα λογισμικά ηλ. ταχυδρομείου (πελάτες) υποστηρίζουν το IMAP (πέρα από το POP), όμως είναι λιγότεροι οι διακομιστές ηλ. ταχυδρομείου οι οποίοι υποστηρίζουν το IMAP. Το πρωτόκολλο IMAP παρέχει πρόσβαση στον λογαριασμό ηλ. ταχυδρομείου. Το λογισμικό-πελάτης μπορεί να αποθηκεύει τοπικά αντίγραφα των μηνυμάτων, αλλά αυτά θεωρούνται ως προσωρινή αποθηκευμένη μνήμη των emails (που βρίσκονται αποθηκευμένα στο διακομιστή).

2.4.9.2. Παράδειγμα διαλόγου

Ακολουθεί ένα παράδειγμα σύνδεσης IMAP (βλ. RFC 3501, section 8).

C: <open connection>

S: * OK IMAP4rev1 Service Ready

C: a001 login mrc secret

S: a001 OK LOGIN completed

C: a002 select inbox

S: * 18 EXISTS

S: * FLAGS (\Answered \Flagged \Deleted \Seen \Draft)

S: * 2 RECENT

S: * OK [UNSEEN 17] Message 17 is the first unseen message

S: * OK [UIDVALIDITY 3857529045] UIDs valid

S: a002 OK [READ-WRITE] SELECT completed

C: a003 fetch 12 full

S: * 12 FETCH (FLAGS (\Seen) INTERNALDATE "17-Jul-1996 02:44:25 -0700"

RFC822.SIZE 4286 ENVELOPE ("Wed, 17 Jul 1996 02:23:25 -0700 (PDT)"

"IMAP4rev1 WG mtg summary and minutes"

(("Terry Gray" NIL "gray" "cac.washington.edu"))

(("Terry Gray" NIL "gray" "cac.washington.edu"))

(("Terry Gray" NIL "gray" "cac.washington.edu"))

((NIL NIL "imap" "cac.washington.edu"))

((NIL NIL "minutes" "CNRI.Reston.VA.US")

("John Klensin" NIL "KLENSIN" "MIT.EDU")) NIL NIL

„<B27397-0100000@cac.washington.edu>")

BODY („TEXT" "PLAIN" ("CHARSET" "US-ASCII") NIL NIL "7BIT" 3028 92))

S: a003 OK FETCH completed

C: a004 fetch 12 body[header]

S: * 12 FETCH (BODY[HEADER] {342}

S: Date: Wed, 17 Jul 1996 02:23:25 -0700 (PDT)

S: From: Terry Gray <gray@cac.washington.edu>

S: Subject: IMAP4rev1 WG mtg summary and minutes

S: To: imap@cac.washington.edu

S: cc: minutes@CNRI.Reston.VA.US, John Klensin <KLENSIN@MIT.EDU>

S: Message-Id: <B27397-0100000@cac.washington.edu>

S: MIME-Version: 1.0

S: Content-Type: TEXT/PLAIN; CHARSET=US-ASCII

S:

S:)

S: 004 OK FETCH completed

C: a005 store 12 +flags \deleted

S: * 12 FETCH (FLAGS (\Seen \Deleted))

S: a005 OK +FLAGS completed

C: a006 logout

S: * BYE IMAP4rev1 server terminating connection

S: a006 OK LOGOUT completed

2.4.9.3. Μειονεκτήματα

Αν και το IMAP εξαλείφει πολλά από τα προβλήματα που δημιουργεί το POP, αυτό με την σειρά του εισάγει επιπρόσθετη πολυπλοκότητα. Το μεγαλύτερο μέρος αυτής της πολυπλοκότητας (π.χ. πολλαπλοί πελάτες προσπελαύνουν το ίδιο «γραμματοκιβώτιο» την ίδια χρονική στιγμή) αντισταθμίζεται από τεχνικές από την πλευρά του διακομιστή (π.χ. Maildir) ή με την αξιοποίηση βάσεων δεδομένων.

Το IMAP έχει συχνά επικριθεί ότι είναι ανεπαρκώς «αυστηρό» (strict), καθώς πολλές φορές είναι ανεκτικό σε συμπεριφορές που με ενεργό τρόπο βλάπτουν το ίδιο και υποβαθμίζουν την χρησιμότητά του. Για παράδειγμα στην τυποποίηση του πρωτοκόλλου τονίζεται ότι κάθε μήνυμα που αποθηκεύεται στον διακομιστή έχει «ένα μοναδικό id» που επιτρέπει στους πελάτες να αναγνωρίζουν τα μηνύματα που έχουν ήδη δει οι ίδιοι μεταξύ των διαφόρων sessions. Παρόλα αυτά, όμως, η

τυποποίηση επιτρέπει επίσης την ακύρωση χωρίς περιορισμούς αυτών των Ids, που πρακτικά ακυρώνει τον σκοπό για τον οποίο αυτά δημιουργήθηκαν.

Αν δεν υπάρχει προσεκτική υλοποίηση τόσο του ίδιου του αποθηκευτικού χώρου για τα μηνύματα όσο και των αλγορίθμων αναζήτησης στον διακομιστή, ένας πελάτης μπορεί εν δυνάμει να «καταναλώσει» μεγάλες ποσότητες πόρων του διακομιστή ενόσω αναζητά μεγάλα σε όγκο «γραμματοκιβώτια» (mailboxes).

Οι πελάτες του IMAP4 χρειάζεται να διατηρούν μια σύνδεση TCP/IP με τον διακομιστή για να μπορούν να ενημερώνονται για την άφιξη κάθε νέου μηνύματος. Η ενημέρωση αυτή πραγματοποιείται με το λεγόμενο in-band signaling, που μειώνει κατά τι τον βαθμό πολυπλοκότητας του πρωτοκόλλου. Μια ιδιωτική λύση που έχει προταθεί, το push IMAP, θα επέκτεινε το πρωτόκολλο IMAP στο να υλοποιήσει το λεγόμενο push-email, στέλνοντας ολόκληρο το μήνυμα αντί μιας απλής ειδοποίησης. Παρόλα αυτά όμως το push IMAP δεν έτυχε ιδιαίτερης αποδοχής και ήδη άλλα projects από το IETF έχουν προταθεί για την αντιμετώπιση του προβλήματος (βλ. Lemonade Profile).

Σε αντίθεση με κάποια ιδιόκτητα πρωτόκολλα που συνδυάζουν τις δυνατότητες αποστολής και ανάκτησης, η αποστολή ενός μηνύματος και το σώσιμο ενός αντιγράφου του σε ένα φάκελο από την πλευρά του διακομιστή με ένα πελάτη IMAP απαιτεί την αποστολή του περιεχομένου του μηνύματος δυο φορές, μια στο SMTP για να στείλει το μήνυμα και μια δεύτερη φορά στο IMAP για να μπορέσει να το αποθηκεύσει σε ένα φάκελο. Αυτό επιλύεται από μια σειρά επεκτάσεων από το IETF LEMONADE Working Group για συσκευές κινητών τηλεφώνων: URLAUTH (RFC 4467) και CATENATE (RFC 4469) στο IMAP και BURL (RFC 4468) για την διαδικασία υποβολής μέσω SMTP. Οι διακομιστές POP δεν υποστηρίζουν φακέλους στην πλευρά του διακομιστή και έτσι οι πελάτες δεν έχουν άλλη επιλογή από το να αποθηκεύσουν τα δεδομένα που τους αποστέλλονται στην μηχανή-πελάτη. Πολλοί πελάτες IMAP μπορούν να ρυθμιστούν ώστε να αποθηκεύουν τα απεσταλμένα emails σε ένα folder στην πλευρά του πελάτη ή να επιλέξουμε την δυνατότητα BCC (blind carbon copy) και ύστερα να φιλτράρουμε το εισερχόμενο μήνυμα αντί να αποθηκεύσουμε ένα αντίγραφο σε ένα folder απευθείας. Εκτός όμως από τις παραπάνω επεκτάσεις, ο Courier Mail Server προσφέρει μια non-standard μέθοδο αποστολής με χρήση του IMAP αντιγράφοντας ένα εξερχόμενο μήνυμα σε ένα προκαθορισμένο εξωτερικό folder.

2.4.9.4. Πλεονεκτήματα έναντι του POP

Καταστάσεις λειτουργίας με και χωρίς σύνδεση: Όταν χρησιμοποιούμε το POP, οι πελάτες τυπικά συνδέονται στον διακομιστή ηλ. ταχυδρομείου και παραμένουν συνδεδεμένοι για όσο χρονικό διάστημα απαιτηθεί προκειμένου να κατεβάσουν τα

νέα μηνύματα που καταφθάνουν. Με την χρήση του IMAP4, οι πελάτες συνήθως μένουν συνδεδεμένοι για όσο η διεπαφή χρήστη είναι ενεργή και κατεβάζουν το περιεχόμενο του μηνύματος κατ' αίτηση. Για χρήστες με πολλά ή μεγάλα μηνύματα, αυτό το πρότυπο χρήσης του IMAP4 μπορεί να οδηγήσει σε γρηγορότερους χρόνους απόκρισης.

Πολλαπλοί χρήστες ταυτόχρονοι συνδεδεμένοι στο ίδιο «γραμματοκιβώτιο»: Το πρωτόκολλο POP απαιτεί από τον τωρινά συνδεδεμένο πελάτη να είναι ο μόνος που συνδέεται και έχει πρόσβαση στην ηλ. θυρίδα του. Αντίθετα, το πρωτόκολλο IMAP ειδικά επιτρέπει την ταυτόχρονη πρόσβαση από πολλαπλούς πελάτες και παρέχει μηχανισμούς για τους πελάτες στο να εντοπίζουν τυχόν αλλαγές που έγιναν στην θυρίδα από άλλους, ταυτόχρονα συνδεδεμένους πελάτες. Αυτό το αναφέρει σαν παράδειγμα το RFC 3501 στην ενότητα 5.2, στο οποίο αναφέρεται συγκεκριμένα «η ταυτόχρονη πρόσβαση στην ίδια θυρίδα από πολλαπλούς πελάτες».

Πρόσβαση στα μέρη του μηνύματος μορφής MIME και μερική ανάκληση: Συνήθως ολόκληρη η αλληλογραφία στο διαδίκτυο μεταδίδεται σε μορφή MIME, επιτρέποντας στα μηνύματα να έχουν μια δενδρική δομή, όπου οι κόμβοι «φύλλα» αναφέρονται σε ένα συγκεκριμένο κομμάτι των δεδομένων του μηνύματος και οι κόμβοι που δεν είναι «φύλλα» μπορεί να συνδυάζουν δεδομένα μεταξύ τους. Το πρωτόκολλο IMAP4 επιτρέπει στους πελάτες να ανακαλούν οποιαδήποτε από τα επιμέρους μέρη του μηνύματος με ξεχωριστό τρόπο και επιπλέον να λαμβάνουν είτε μεμονωμένα μέρη του μηνύματος ή ακόμα ολόκληρο το μήνυμα. Αυτοί οι μηχανισμοί επιτρέπουν στους πελάτες να λαμβάνουν το κυρίως σώμα του μηνύματος χωρίς να ανακαλούν συγχρόνως επισυναπτόμενα αρχεία ή να στριμάρει (strwam) περιεχόμενο καθώς αυτό λαμβάνεται από τον χρήστη.

Πληροφορίες κατάστασης μηνυμάτων: Μέσω της χρήσης των λεγόμενων σημαιών (flags) που ορίζονται στο πρωτόκολλο IMAP4, οι πελάτες μπορούν να ενημερώνονται για την κατάσταση των μηνυμάτων: για παράδειγμα αν το μήνυμα διαβάστηκε, απαντήθηκε, διαγράφηκε ή όχι. Αυτές οι σημαίες αποθηκεύονται στον διακομιστή, έτσι διαφορετικοί χρήστες που προσπελαύνουν την ίδια θυρίδα σε διαφορετικές χρονικές στιγμές μπορούν να εντοπίσουν τυχόν αλλαγές στην κατάσταση από άλλους πελάτες. Το POP δεν παρέχει κανένα μηχανισμό για τους πελάτες ώστε να αποθηκεύουν τις συναφείς με την κατάσταση των μηνυμάτων πληροφορίες στον διακομιστή έτσι αν ένας χρήστης προσπελαύνει την θυρίδα με δυο διαφορετικούς πελάτες POP (σε διαφορετικές στιγμές), οι πληροφορίες κατάστασης-για παράδειγμα αν ένα μήνυμα προσπελάστηκε ή όχι-δεν μπορούν να συγχρονιστούν μεταξύ των πελατών. Το πρωτόκολλο IMAP4υποστηρίζει και τις δυο προκαθορισμένες σημαίες του συστήματος και τυχόν λέξεις κλειδιά που ορίζονται για τους πελάτες. Αυτά τα flags υποδηλώνουν τις πληροφορίες κατάστασης, για παράδειγμα αν ένα μήνυμα διαβάστηκε ή όχι. Οι λέξεις κλειδιά, που δεν υποστηρίζονται από όλους τους διακομιστές IMAP, επιτρέπουν στο να

δίνονται στα μηνύματα ένα ή περισσότερα tags (ετικέτες), των οποίων η ερμηνεία επαφίεται στην πλευρά του πελάτη. Οι λέξεις κλειδιά στο IMAP δεν θα πρέπει να συγχέονται με ιδιόκτητες ετικέτες υπηρεσιών web-based e-mail που μερικές φορές μεταφράζονται σε καταλόγους IMAP από τους αντίστοιχους διακομιστές.

Πολλαπλά «γραμματοκιβώτια» στον διακομιστή: Οι πελάτες IMAP4 μπορούν να δημιουργήσουν, να μετονομάσουν και/ή να διαγράψουν θυρίδες (συνήθως παρουσιάζονται στον χρήστη ως κατάλογοι) στον διακομιστή και να αντιγράφουν μηνύματα μεταξύ θυρίδων. Η ύπαρξη πολλαπλών θυρίδων επίσης επιτρέπει στους διακομιστές να παρέχουν πρόσβαση σε διαμοιραζόμενους και δημόσιους καταλόγους. Η επέκταση ACL (Access Control List) του IMAP4 (RFC 4314) μπορεί να χρησιμοποιηθεί για την διαχείριση των δικαιωμάτων πρόσβασης.

Αναζητήσεις από την πλευρά του διακομιστή: Το IMAP4 παρέχει ένα μηχανισμό για ένα πελάτη ώστε να «ρωτήσει» τον διακομιστή να αναζητήσει μηνύματα με βάση συγκεκριμένα κριτήρια. Αυτός ο μηχανισμός αποφεύγει την αναγκαιότητα οι πελάτες να πρέπει να κατεβάσουν κάθε μήνυμα στον τοπικό υπολογιστή με στόχο να πραγματοποιήσει αυτές τις αναζητήσεις.

Άλλοι μηχανισμοί επέκτασης: Αντανακλώντας την εμπειρία από προηγούμενα δικτυακά πρωτόκολλα, το IMAP4 ορίζει ένα μηχανισμό με βάση τον οποίο μπορεί να επεκταθεί. Πολλές επεκτάσεις του IMAP4 στο βασικό πρωτόκολλο έχουν προταθεί και χρησιμοποιούνται σήμερα συχνά. Το IMAP2bis δεν είχε κάποιο μηχανισμό επέκτασης και το POP διαθέτει τώρα ένα που ορίζεται στο RFC 2449.

2.4.9.5. Λίγα λόγια για τις διάφορες εκδόσεις του πρωτοκόλλου

Αρχικό πρωτόκολλο: Το αρχικό πρωτόκολλο που ονομαζόταν Interim Access Mail Protocol αρχικά υλοποιήθηκε σαν πελάτης για μηχανές Xerox που έτρεχαν γλώσσα Lisp όπως επίσης και σαν διακομιστής TOPS-20. Δεν υπάρχουν τυχόν αντίγραφα για το πώς σχεδιάστηκε το πρωτόκολλο ή πληροφορίες για το λογισμικό του. Αν και μερικές εντολές του έμοιαζαν με αυτές του IMAP2, το πρωτόκολλο αυτό παρουσίαζε διάφορες άλλες σημαντικές ελλείψεις και επομένως το συντακτικό του δεν ήταν συμβατό με άλλες εκδόσεις του IMAP.

IMAP2: Το αρχικό πρωτόκολλο αντικαταστάθηκε γρήγορα από την έκδοση 2 του IMAP (IMAP2) που ορίζεται στο RFC 1064 (1988) και αναβαθμίστηκε αργότερα από το RFC 1176 (1990). Το IMAP2 εισήγαγε το command/response tagging που δεν διέθετε το αρχικό πρωτόκολλο και ήταν η πρώτη δημόσια διανεμημένη έκδοση.

IMAP3: Το IMAP3 είναι μια εξαιρετικά σπάνια παραλλαγή του IMAP. Δημοσιεύτηκε στο RFC 1203 το 1991. Γράφτηκε ειδικά ως μια εντελώς αντίθεση πρόταση στο RFC 1176, το οποίο πρότεινε συγκεκριμένες τροποποιήσεις στο

IMAP2. Το IMAP3 δεν έγινε ποτέ αποδεκτό από την αγορά εργασίας. Το IESG (Internet Engineering Steering Group) επαναταξινόμησε το RFC 1203 "Interactive Mail Access Protocol-Version 3" ως ένα ιστορικό πρωτόκολλο το 1993. Το IMAP Working Group χρησιμοποίησε το RFC 1176 (IMAP2) αντί του RFC 1203 (IMAP3) σαν το σημείο εκκίνησής του.

IMAP2bis: Με την έλευση του MIME, το IMAP2 επεκτάθηκε για να υποστηρίξει το format που προέβλεπε το MIME και μεταξύ άλλων εισήγαγε την χρήσιμη λειτουργία της διαχείρισης της ηλ. θυρίδας (δημιουργία, διαγραφή, μετονομασία, μεταφόρτωση μηνύματος) που έλειπε από το IMAP2. Αυτή η πειραματική αναθεώρηση ονομάστηκε IMAP2bis. Η τυποποίησή του ωστόσο ποτέ δεν δημοσιεύτηκε σε επίσημη μορφή. Ένα διαδικτυακό προσχέδιο του IMAP2bis δημοσιεύτηκε από το IETF IMAP Working Group τον Οκτώβριο του 1993. Το προσχέδιο αυτό βασιζόταν στις ακόλουθες τυποποιήσεις: μη δημοσιευθέν έγγραφο IMAP2bis.TXT, RFC 1176 και RFC 1064 (IMAP2). Το προσχέδιο IMAP2bis.TXT κατέγραφε την κατάσταση των επεκτάσεων στο πρωτόκολλο IMAP2, όπως αυτό είχε αρχίσει από τον Οκτώβριο του 1992. Οι αρχικές εκδόσεις του Pine υποστήριζαν σε μεγάλο βαθμό το IMAP2bis (Pine 4.00 αργότερα υποστήριζε και IMAP4rev1). Ο Pine είναι ένας πελάτης ηλ. ταχυδρομείου (e-mail client) που είναι τόσο freeware όσο και text-based. Αναπτύχθηκε στο Πανεπιστήμιο της Ουάσιγκτον. Η πρώτη έκδοση γράφτηκε το 1989 και δημοσιοποιήθηκε το Μάρτιο του 1992. Ο πηγαίος κώδικας ήταν διαθέσιμος μόνο για έκδοση Unix και υπόκειντων σε άδεια (license) που προβλεπόταν από το Πανεπιστήμιο της Ουάσιγκτον. Ο Pine έχει σταματήσει πλέον να σχεδιάζεται και να χρησιμοποιείται και έχει αντικατασταθεί από ένα άλλο e-mail client, τον Alpine, που είναι διαθέσιμος κάτω από Apache License.

IMAP4: Μια ομάδα εργασίας του IMAP που δημιουργήθηκε εντός του IETF στις αρχές του 1990 ανέλαβε την ευθύνη για την σχεδίαση του IMAP2bis. Αποφάσισε την μετονομασία του IMAP2bis σε IMAP4 για να αποφύγει την σύγχυση με μια αντίστοιχη πρόταση για το IMAP3 από άλλη ομάδα εργασίας και να μην δημιουργηθούν περιπτώσεις ακραίου ανταγωνισμού. Η επέκταση του ακρωνυμίου IMAP άλλαξε επίσης σε Internet Message Access Protocol. Η τελευταία έκδοση, IMAP4, επιτρέπει σε ένα e-mail client να χειρίζεται τα μηνύματα ηλ. ταχυδρομείου που είναι αποθηκευμένα σε ένα διακομιστή με τον ίδιο τρόπο όπως ένας πελάτης χρησιμοποιεί τοπικούς καταλόγους. Αυτή η δυνατότητα επιτρέπει σε πολλαπλούς πελάτες για ένα και μόνο χρήστη να βλέπουν την ίδια κατάσταση της ηλ. θυρίδας. Για παράδειγμα εάν ένας χρήστης μετακινήσει ένα μήνυμα από το INBOX σε κάποιο άλλο κατάλογο (φάκελο) χρησιμοποιώντας μόνο ένα πελάτη, όταν αργότερα προσπελάσει την θυρίδα του από άλλο πελάτη το μήνυμα φαίνεται στον κατάλογο (φάκελο) στον οποίο είχε μετακινηθεί προηγουμένως.

2.4.10. Προγράμματα Αποστολής και Λήψης Ηλεκτρονικού Ταχυδρομείου

Πλέον έχουν αναπτυχθεί πολλά προγράμματα αποστολής και λήψης ηλεκτρονικού ταχυδρομείου για όλα τα λειτουργικά συστήματα. Η αποστολή και η ανάγνωση των μηνυμάτων γίνεται σε πλήρως γραφικό-παραθυρικό περιβάλλον πολύ φιλικό προς το χρήστη.

Ένα πρόγραμμα-πελάτης για την υπηρεσία e-mail, συνήθως, αποτελείται από έναν συντάκτη (editor) για τη σύνταξη των εξερχόμενων μηνυμάτων και μια υπηρεσία μεταφοράς αρχείων. Ένα σύγχρονο πρόγραμμα, εκτός της δυνατότητας αποστολής μηνυμάτων και ελέγχου της εισερχόμενης αλληλογραφίας, παρέχει επίσης τις δυνατότητες:

- Δημιουργίας ατζέντας με τις συχνότερα χρησιμοποιούμενες διευθύνσεις
- Οργάνωσης-ταξινόμησης των μηνυμάτων σε καταλόγους
- Επισύναψης αρχείων στα μηνύματα

Οι δύο πρώτες δυνατότητες είναι κατανοητές. Σε αυτό το σημείο θα αναλυθεί λίγο περισσότερο η τελευταία δυνατότητα: Το πρωτόκολλο SMTP είχε σχεδιαστεί για την αποστολή μηνυμάτων αποτελούμενων από απλούς χαρακτήρες ASCII, δηλαδή απλών μηνυμάτων κειμένου. Αυτό σημαίνει ότι για παράδειγμα ένα έγγραφο του Word που περιείχε ειδικούς χαρακτήρες διαμόρφωσης δεν μπορούσε να διακινηθεί μέσω του SMTP.

Τα σύγχρονα προγράμματα για e-mail υποστηρίζουν την κωδικοποίηση δυαδικών αρχείων (για παράδειγμα ενός εγγράφου του Word) σε απλό κείμενο, ώστε να είναι δυνατή η διακίνησή τους από το SMTP.

Με τον τρόπο αυτό, μέσω του ηλεκτρονικού ταχυδρομείου, ο χρήστης μπορεί να στέλνει και να λαμβάνει έγγραφα του MS Office, αρχεία εικόνας, ήχου ή βίντεο, συμπιεσμένα Zip αρχεία, αρχεία του Autocad, αρχεία προγραμμάτων και γενικά αρχεία οποιασδήποτε μορφής και μάλιστα όχι ένα κάθε φορά, αλλά πολλά μαζί.

Πώς όμως επιτυγχάνεται αυτό; Στο μήνυμα του εκάστοτε χρήστη, το σώμα του οποίου αποτελείται από απλό κείμενο, επισυνάπτονται τα αρχεία. Έτσι, το μήνυμά του τελικά μοιάζει με ένα φάκελο που περιέχει ένα κύριο έγγραφο (το σώμα του μηνύματος) και ένα ή περισσότερα συνημμένα έγγραφα. Αυτή η δυνατότητα ανταλλαγής αρχείων είναι ίσως η πολυτιμότερη από τις υπηρεσίες που προσφέρει το ηλεκτρονικό ταχυδρομείο.

Η υπηρεσία **webmail** προσφέρει όλες τις παραπάνω υπηρεσίες ενός πελάτη ηλεκτρονικού ταχυδρομείου (mail client), μέσω διεπαφής διαδικτύου. Ο χρήστης συνδέεται με τον φυλλομετρητή του σε έναν ιστότοπο το οποίο του παρέχει πλήρη διαχείριση στην ηλεκτρονική του αλληλογραφία (βλέπε εικόνα 2.4.5).

Εικόνα 2.4.5. *Σύνδεση στην υπηρεσία Webmail*

Μετά από ένα στάδιο αυθεντικοποίησης εμφανίζεται η ηλεκτρονική θυρίδα του χρήστη μέσω της οποίας μπορεί να αποστείλλει ότι μηνύματα επιθυμεί. Η εφαρμογή webmail συνδέεται με το πρωτόκολλο POP3 ή IMAP με τη θυρίδα του χρήστη (η οποία μπορεί να βρίσκεται σε απομακρυσμένο διακομιστή) και αποστέλλει μέσω τοπικού SMTP εξυπηρετητή τα μηνύματα στους διάφορους παραλήπτες τους (βλέπε εικόνα 2.4.6).

Εικόνα 2.4.6. *Ηλεκτρονική Θυρίδα της Υπηρεσίας Webmail*

Η υπηρεσία webmail λοιπόν αποτελεί μια πολύ καλή λύση για χρήστες ηλεκτρονικού ταχυδρομείου που ταξιδεύουν συχνά, καθώς απαιτεί από το μηχάνημα του χρήστη μοναχά την ύπαρξη ενός φυλλομετρητή, ο οποίος είναι συχνά διαθέσιμος στα διάφορα Net-café ανά τον κόσμο. Παρακάτω δίνονται μερικά παραδείγματα από τα πιο κοινά χρησιμοποιούμενα προγράμματα αποστολής και λήψης ηλεκτρονικού ταχυδρομίου.

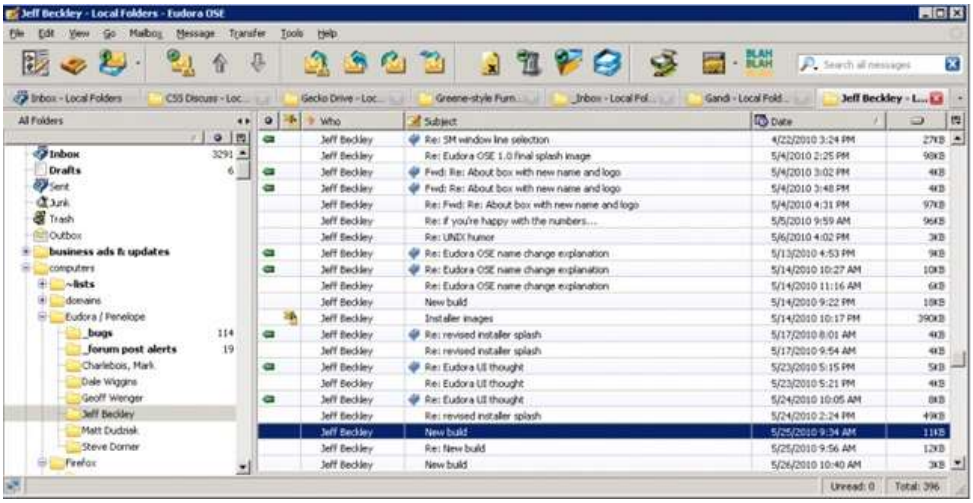
2.4.10.1 Gmail Notifier Pro

Όταν ο χρήστης εγκαταστήσει το Gmail Notifier Pro λαμβάνει ενημερώσεις κάθε φορά που έρχονται καινούργια μηνύματα στο λογαριασμό του στο gmail. Το πρόγραμμα εγκαθίσταται στη γραμμή εργασιών των Windows και δίνει επισημάνσεις όταν υπάρχει κάτι νέο. Εκτός του gmail υποστηρίζει και πολλά άλλα συστήματα, email και όχι μόνο.

Εικόνα 2.4.7. *Gmail Notifier Pro*

2.4.10.2 Eudora OSE

Εφαρμογή ηλεκτρονικού ταχυδρομείου βασισμένη στον κώδικα του Mozilla ThunderBird, η οποία χρησιμοποιεί περιβάλλον εργασίας του πασίγνωστου Eudora Mail. Πρόκειται για ένα ολοκληρωμένο πελάτη ηλεκτρονικού ταχυδρομείου με περιβάλλον εργασίας το οποίο θα ικανοποιήσει τους περισσότερους χρήστες.



Εικόνα 2.4.8. *Eudora OSE*

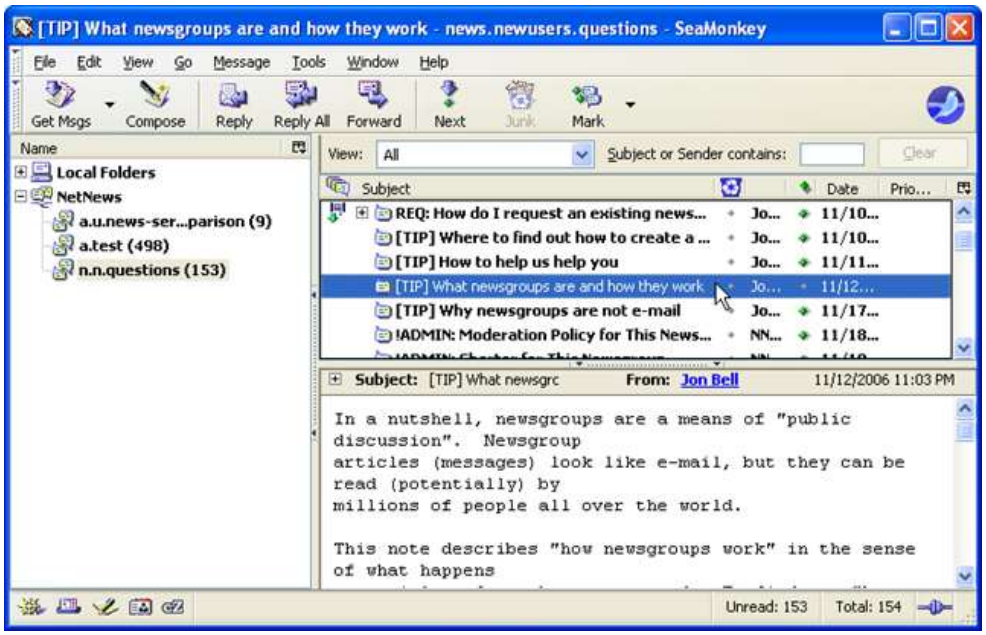
2.4.10.3 SpiceBird

Εφαρμογή Ηλεκτρονικού Ταχυδρομείου βασισμένη στις τεχνολογίες του Mozilla και διαφόρων άλλων διαδικτυακών υπηρεσιών. Απευθύνεται κυρίως σε ανάγκες ομάδων χρηστών που χρειάζονται ένα μείγμα από εργαλεία που μπορούν να μοιράζονται και να χειρίζονται συγχρόνως. Οι χρήστες μιας ομάδας έχουν τη δυνατότητα να μοιράζονται ημερολόγια καθώς και ένα σύστημα διαχείρισης ενεργειών και αποτελεσμάτων, ιδανικό για τον συντονισμό των μελών της ομάδας. Υποστηρίζει λειτουργικά συστήματα Linux και Windows.

Εικόνα 2.4.9. *SpiceBird*

2.4.10.4 SeaMonkey

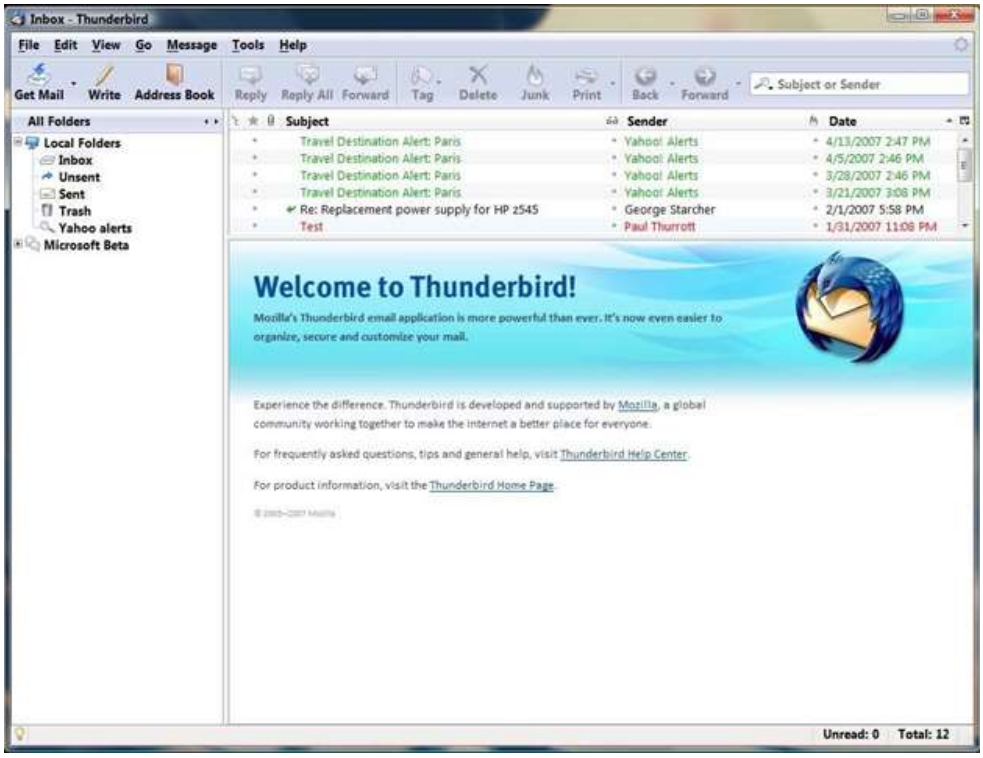
Ένα fork του Mozilla που προσφέρει διαδικτυακό περιηγητή, διαχείριση ηλεκτρονικού ταχυδρομείου, ανάγνωση RSS (newsfeeds), χρήση IRC και περιορισμένες δυνατότητες επεξεργασίας HTML. Παρόλο που δεν προσφέρει κάτι το καινούργιο, το πακέτο είναι καλοδουλεμένο και οι εφαρμογές του εκτελούνται σαφώς πιο γρήγορα από αυτές στις οποίες είναι βασισμένες. Επίσης ο συνδυασμός των εφαρμογών το κάνουν μια ενδιαφέρουσα εναλλακτική λύση για το FireFox / Thunderbird.



Εικόνα 2.4.10. *SeaMonkey*

2.4.10.5 Thunderbird

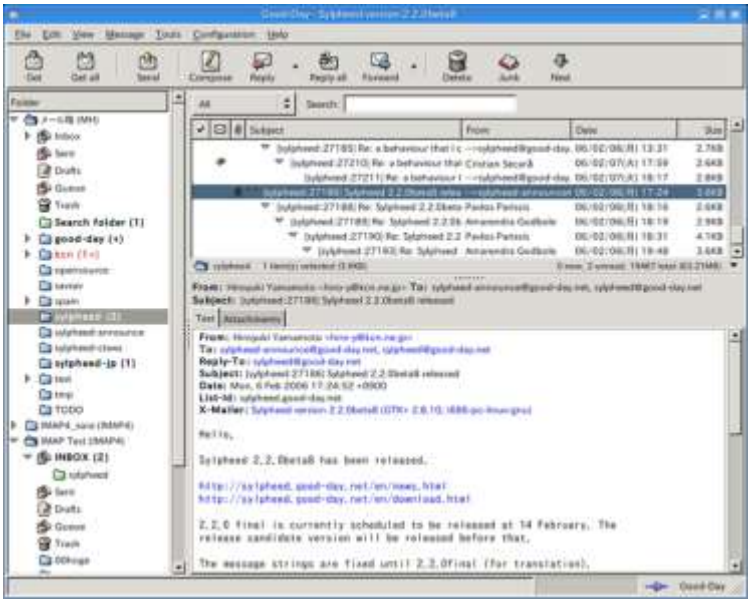
Από του δημιουργούς του εξαιρετικού Mozilla Firefox έρχεται ένα εξίσου καλό εργαλείο για τη χρήση υπηρεσιών ηλεκτρονικού ταχυδρομείου. Προσφέρει τις περισσότερες λειτουργίες των ανταγωνιστών του και συνοδεύεται και από μια πληθώρα πρόσθετων λειτουργιών (add-ons) δημιουργημένα από την κοινότητα των χρηστών του. Υποστηρίζει τις περισσότερες γλώσσες και λειτουργικά συστήματα που υπάρχουν.



Εικόνα 2.4.11. *ThunderBird*

2.4.10.6 Sylpheed

Μια απλή και εύχρηστη εφαρμογή διαχείρισης ηλεκτρονικού ταχυδρομείου. Πρόκειται για μια απλοποιημένη λύση, για αυτούς που θέλουν να ασχολούνται μόνο με το mail τους, χωρίς επιπλέον λειτουργίες. Είναι ελαφρύ, αποτελεσματικό και προσφέρει ένα εύχρηστο περιβάλλον εργασίας. Ιδιαίτερα καλό είναι το σύστημα αναζήτησης των μηνυμάτων που είναι αποθηκευμένα σε αυτό.



Εικόνα 2.4.12. *Sylpheed*

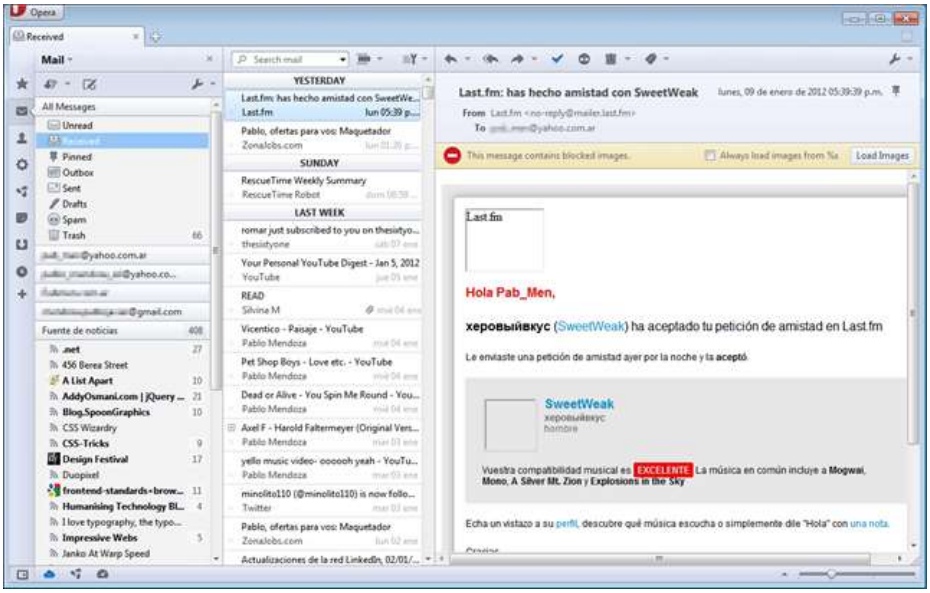
2.4.10.7 Pegasus Mail

Μια από τις παλαιότερες εφαρμογές ηλεκτρονικού ταχυδρομείου που εξελίσσεται διαρκώς τα τελευταία δεκαεννέα χρόνια. Προσφέρει εξαιρετικά συνοδευτικά εργαλεία και υψηλό βαθμό ασφάλειας. Υποστηρίζει λειτουργικά συστήματα των Windows. Μια πραγματικά ολοκληρωμένη εφαρμογή ικανή να καλύψει τις ανάγκες ιδιωτών ή και ολόκληρων οργανισμών.

Εικόνα 2.4.13. *Pegasus Mail*

2.4.10.8 Opera Mail

Εφαρμογή χρήσης ηλεκτρονικού ταχυδρομείου από τους δημιουργούς του γνωστού φυλλομετρητή Opera. Πρόκειται για ένα πολύ εύχρηστο εργαλείο που προσφέρει όλες τις τυπικές διεργασίες των μοντέρνων πελατών ηλεκτρονικού ταχυδρομείου. Οι ιδιαίτερες δυνατότητες ταξινόμησης και αναζήτησης, σε συνδυασμό με ένα πολύ ισχυρό anti-spam φίλτρο το καθιστούν μια πολύ καλή εναλλακτική λύση στα καθιερωμένα προγράμματα του χώρου.



Εικόνα 2.4.14. *Opera Mail*

2.4.10.9 Outlook

Το Microsoft Outlook XP είναι ένα πρόγραμμα που βρίσκεται ενσωματωμένο στην σουίτα Office XP και χρησιμοποιείται από χρήστες οι οποίοι επιθυμούν να κάνουν χρήση της υπηρεσίας ηλεκτρονικού ταχυδρομείου σε συνδυασμό με προγράμματα χρήσης ημερολογίου, διαχείριση εργασιών και επαφών καθώς παρέχεται η δυνατότητα προγραμματισμού συσκέψεων και συναντήσεων.

Εικόνα 2.4.15. *Outlook*

2.4.11. Προϋποθέσεις για τη Χρήση του Ηλεκτρονικού Ταχυδρομείου

Εξοπλισμός: Ο χρήστης χρειάζεται να έχει πρόσβαση σε μία συσκευή, συνδεδεμένο στο δίκτυο και στον οποίο υπάρχει εγκατεστημένο πρόγραμμα ταχυδρομείου (mail program).

Εγγραφή: Πρέπει να εγγραφεί στο τοπικό κέντρο διαχείρισης υπολογιστών ως χρήστης e-mail. Κατά την εγγραφή θα του δοθεί μια θυρίδα και τα μηνύματα που του στέλνονται θα αποθηκεύονται εκεί. Επίσης θα πρέπει να χρησιμοποιεί ένα πρόγραμμα ταχυδρομείου, όπως έχει ήδη αναφερθεί, για να διαβάζει τα μηνύματα. Θα του δοθεί επίσης μια διεύθυνση e-mail, που πιθανότατα θα έχει την παρακάτω μορφή: όνομα_χρήστη@όνομα_υπολογιστή. Με αυτόν τον τρόπο, μολονότι υπολογίζεται ότι υπάρχουν δεκάδες εκατομμυρίων χρηστών στο Internet, το e-mail είναι μοναδικό και μηνύματα γραμμένα σωστά που απευθύνονται σε κάποιο συγκεκριμένο χρήστη, φυσιολογικά θα βρουν το δρόμο τους για τη θυρίδα αυτού του χρήστη. Γίνεται τώρα κατανοητό γιατί όταν στέλνει κάποιος ένα e-mail είναι πολύ σημαντικό να γράφει τη διεύθυνση με ακρίβεια.

2.4.12. Προτερήματα του Ηλεκτρονικού Ταχυδρομείου

Ελαχιστοποίηση Κόστους: Για τις ακαδημαϊκές και ερευνητικές κοινότητες, δεν υπάρχει προς το παρόν άμεσο κόστος για την αποστολή ή την παραλαβή μηνυμάτων μέσω e-mail. Στην πραγματικότητα, η χρήση του e-mail συμβάλλει στην εξοικονόμηση χρημάτων.

Άμεση Αποστολή: Τα μηνύματα μεταφέρονται συνήθως σε διάστημα λίγων λεπτών. Η απόσταση δεν αποτελεί κριτήριο για την παράδοση του μηνύματος. Ένα μήνυμα μπορεί να μεταδοθεί στην άλλη πλευρά του κόσμου σχεδόν τόσο γρήγορα όσο και στην άλλη πλευρά της πανεπιστημιούπολης.

Πλεονέκτημα έναντι Κανονικού Ταχυδρομείου και Τηλεφώνου: Η επικοινωνία με e-mail είναι απλώς θέμα χρήσης του πληκτρολογίου. Δεν χρειάζεται να μετακινηθεί ο χρήστης για να στείλει ή να λάβει e-mail, ούτε απαιτείται χαρτί, φάκελοι ή γραμματόσημα. Επιπλέον σε αντίθεση με το τηλέφωνο, δεν είναι ανάγκη ο συνομιλητής να είναι διαθέσιμος κατά τη διάρκεια της επικοινωνίας. Ένα e-mail μπορεί να περιμένει στο mailbox μέχρι να ανοιχθεί και να διαβαστεί.

Ευκολία: Ένα μήνυμα μπορεί να σταλεί σε ένα πρόσωπο ή σε πολλά. Εκτός αυτού, οτιδήποτε είναι σε ψηφιακή μορφή (εικόνα, μουσική, video) μπορεί να σταλεί με e-mail.

Επικοινωνία – Συνεργασία: Το e-mail είναι ένας από τους πιο αποτελεσματικούς και αποδοτικούς τρόπους επικοινωνίας με τους συνεργάτες σε ολόκληρο τον κόσμο, γιατί είναι γρήγορο, φθηνό και ανεπίσημο. Ενισχύει τη συνεργασία, προσφέροντας έναν εύκολο τρόπο για επικοινωνία σε ατομικό ή ομαδικό επίπεδο. Επίσης, παρέχει πολλές διευκολύνσεις στην ανταλλαγή εγγράφων.

Διοίκηση: Παίρνοντας ως δεδομένο ότι η πλειοψηφία των ανθρώπων που συμμετέχουν σε ένα συνέδριο ή σύσκεψη, έχουν διευθύνσεις e-mail, το e-mail μπορεί να χρησιμοποιηθεί για τις αρχικές ανακοινώσεις, για το σχεδιασμό των προγραμμάτων, για το κλείσιμο θέσεων, για την παραλαβή των ανακοινώσεων, για την έκδοση των πρακτικών.

Ανταλλαγή Εγγράφων – Αποστολή Αρχείων μέσω E-mail: Τα έγγραφα μπορούν εύκολα να αποσταλούν, να τυπωθούν και να επιστραφούν με e-mail. Το χαρακτηριστικό αυτό κάνει το e-mail γρήγορο και αποτελεσματικό μέσο σε περιπτώσεις κοινής συγγραφής κειμένων από συγγραφείς σε διαφορετικά μέρη του κόσμου και εξ αποστάσεως επίβλεψη διδακτορικών διατριβών.

2.4.13. Ασφάλεια στο Ηλεκτρονικό Ταχυδρομείο

Ανάμεσα στα περιβάλλοντα κατανεμημένων συστημάτων, το ηλεκτρονικό ταχυδρομείο είναι η περισσότερο χρησιμοποιούμενη δικτυακή εφαρμογή. Με την ανερχόμενη εξάρτηση της χρήσης του ηλεκτρονικού ταχυδρομείου για οποιοδήποτε σκοπό μπορεί κανείς να αντιληφθεί ότι υπάρχει μια αυξανόμενη ανάγκη για υπηρεσίες **αυθεντικοποίησης,** να γνωρίζουμε δηλαδή ποιος είναι ο πραγματικός αποστολέας ενός μηνύματος**,** και **εμπιστευτικότητας,** να είμαστε σίγουροι δηλαδή για το ότι το μήνυμά μας δεν έχει διαβαστεί ή αλλοιωθεί. Στον τομέα της ασφάλειας στο ηλεκτρονικό ταχυδρομείο κυριαρχούν: το **Pretty Good Privacy (PGP)** και το **Private-Enhanced Mail (PEM).**

2.4.13.1 PGP (Pretty Good Privacy)

Το PGP εφευρέθηκε από τον Phil Zimmerman και παρέχει τις υπηρεσίες της εμπιστευτικότητας και της αυθεντικοποίησης. Το PGP χρησιμοποιείται ευρύτατα εξαιτίας των παρακάτω λόγων:

- Είναι διαθέσιμο παντού και μπορεί να τρέξει σε οποιαδήποτε πλατφόρμα.
- Βασίζεται σε αλγορίθμους που είναι ευρέως αποδεκτοί σαν απόλυτα ασφαλείς.
- Είναι κατάλληλο για ένα ευρύ φάσμα εφαρμογών.
- Δεν αναπτύχθηκε, ούτε ελέγχεται από κυβερνητικό ή άλλο οργανισμό για τυποποιήσεις.

Το PGP συμπιέζει από μόνο του το μήνυμα πριν κρυπτογραφηθεί και αφού τοποθετηθεί η απαραίτητη υπογραφή για αυθεντικοποίηση. Έτσι εξοικονομείται χώρος κατά τη μετάδοση και κατά την αποθήκευση του μηνύματος. Ο αλγόριθμος που χρησιμοποιείται είναι ο ZIP.

Όταν χρησιμοποιείται το PGP, ολόκληρο ή τουλάχιστον ένα μέρος του block που αποστέλλεται είναι κρυπτογραφημένο και αποτελείται από μία σειρά από τυχαία 8-bit octets. Λόγω του περιορισμού που υπάρχει σε ορισμένα συστήματα ηλεκτρονικού ταχυδρομείου για μόνο μηνύματα κειμένου χαρακτήρων ASCII, το PGP παρέχει μία υπηρεσία που μετατρέπει τη σειρά αυτή σε εκτυπώσιμους χαρακτήρες ASCII. Το PGP ακόμα, μπορεί να μετατρέπει μόνο το μέρος όπου υπάρχει η υπογραφή, ώστε ο αποστολέας να μπορεί να διαβάζει τα μηνύματα, χωρίς να χρησιμοποιεί PGP, και μόνο στην περίπτωση που θέλει να πιστοποιήσει την υπογραφή να χρειάζεται το PGP.

Το PGP μπορεί να υποδιαιρεί ένα μήνυμα που είναι πολύ μεγάλο σε μικρότερα τμήματα, ώστε να γίνεται κατάλληλο για αποστολή καθώς και σε ορισμένες περιπτώσεις που το μέγεθος των μηνυμάτων που μπορούν να αποσταλούν είναι περιορισμένο. Η τμηματοποίηση γίνεται μετά από όλες τις άλλες επεξεργασίες

Το PGP επιτρέπει στο χρήστη να καθορίζει πόση εμπιστοσύνη δίνει σε κάθε άλλον χρήστη. Υπάρχουν τρία επίπεδα εμπιστοσύνης: καθόλου, μερική, και πλήρης εμπιστοσύνη.

2.4.13.2 PEM (Private – Enhanced Mail)

Το PEM είναι ένα πρότυπο του Διαδικτύου που παρέχει υπηρεσίες ασφάλειας για εφαρμογές ηλεκτρονικού ταχυδρομείου (e-mail). Έχει τα ακόλουθα χαρακτηριστικά:

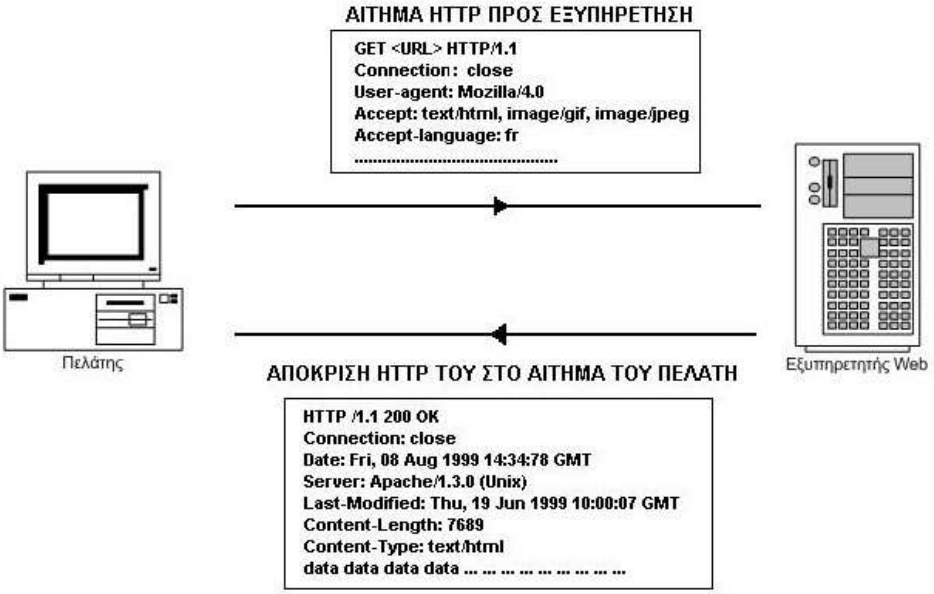
- Έχει υλοποιηθεί στο επίπεδο εφαρμογής και είναι ανεξάρτητο από τα άλλα επίπεδα και το λειτουργικό σύστημα.
- Είναι διάφανο σε ενδιάμεσα στοιχεία προώθησης mail και είναι συμβατό με όλα τα περιβάλλοντα μεταφοράς mail.
- Είναι συμβατό με διάφορα περιβάλλοντα χρήστη.
- Υποστηρίζει ταχυδρομικές λίστες (mailing lists).
- Είναι συμβατό με διάφορους τρόπους για τη διαχείριση των κλειδιών.

Η επεξεργασία ενός μηνύματος προς μετάδοση στο PEM περιλαμβάνει τέσσερα στάδια:

- Μετατροπή του μηνύματος σε κανονική μορφή.
- Ακεραιότητα μηνύματος και αυθεντικοποίηση.
- Κρυπτογράφηση του μηνύματος (προαιρετικό)
- Μετατροπή σε εκτυπώσιμη μορφή (προαιρετικό)

2.5. HTTP (HYPERTEXT TRANSFER PROTOCOL: ΠΡΩΤΟΚΟΛΛΟ ΜΕΤΑΦΟΡΑΣ ΥΠΕΡΚΕΙΜΕΝΟΥ)

Πρόκειται για το πρωτόκολλο που επιτρέπει την πρόσβαση στα δεδομένα του Παγκοσμίου Ιστού (WWW). Οφείλει το όνομά του στο ότι επιτρέπει την χρήση ενός περιβάλλοντος υπερκειμένων όπου ο χρήστης μπορεί να περνάει με γρήγορο τρόπο από τη μία σελίδα στην άλλη. Η λειτουργία του πρωτοκόλλου αυτού μοιάζει με αυτή των SMTP και FTP. Το HTTP μεταφέρει αρχεία, αλλά χρησιμοποιεί μόνο μια σύνδεση σε αντίθεση με το FTP που χρησιμοποιεί 2 συνδέσεις TCP. Η μεταφορά αυτή από τον εξυπηρετητή στο πελάτη μοιάζει με τη μεταφορά μηνυμάτων, αλλά τα μηνύματα του HTTP απαιτούν ειδικό λογισμικό ώστε να μεταφραστούν (Web Browsers). Επιπλέον, τα μηνύματα HTTP μεταφέρονται αμέσως στον πελάτη, ενώ τα SMTP έχουν χαμηλότερη προτεραιότητα.



Εικόνα 2.5.1. *Λειτουργία του Πρωτοκόλλου Μεταφοράς Υπερκειμένου (HTTP)*

2.5.1. Πρόσθετες πληροφορίες για το πρωτόκολλο HTTP

Το πρωτόκολλο μεταφοράς υπερκειμένου (HyperText Transfer Protocol, HTTP) είναι ένα πρωτόκολλο επικοινωνίας. Αποτελεί το κύριο πρωτόκολλο που χρησιμοποιείται στους φυλλομετρητές του Παγκόσμιου Ιστού για να μεταφέρει δεδομένα ανάμεσα σε ένα διακομιστή (server) και ένα πελάτη (client).

Ο όρος υπερκείμενο (hypertext), που περιέχεται στην ονομασία του πρωτοκόλλου, χρησιμοποιήθηκε αρχικά από τον Ted Nelson το 1965. Η γενική ιδέα του πρωτοκόλλου προτάθηκε, μαζί με την δημιουργία της γλώσσας HTML, από τον Tim Berners-Lee και την ομάδα του, ώστε σε συνδυασμό με το ήδη υπάρχον Διαδίκτυο και το πρωτόκολλο TCP, να γίνει εφικτή η δημιουργία του Παγκόσμιου Ιστού (WWW).

Η πρώτη τεκμηριωμένη έκδοση ήταν η 0.9.

Αρχικά το πρωτόκολλο δεν μετέφερε καμιά πληροφορία σχετικά με το πρόγραμμα-πελάτης και η μόνη επιλογή που υπήρχε ήταν η ζήτηση από τον εξυπηρετητή μιας σελίδας κειμένου το οποίο περιείχε μόνο χαρακτήρες ASCII και πιθανόν χαρακτήρες τερματισμού γραμμής.

Σήμερα το πρωτόκολλο αυτό είναι πλέον καθιερωμένο και διαδεδομένο σε σημείο που σχεδόν όλοι οι φυλλομετρητές να το θεωρούν δεδομένο και να το

χρησιμοποιούν σε περίπτωση που ο χρήστης δεν καθορίσει ποιο πρωτόκολλο θέλει να χρησιμοποιήσει. Αν δηλαδή ο χρήστης δεν γράψει:

http://my.url

αλλά γράψει σκέτο το:

my.url

σχεδόν όλοι οι φυλλομετρητές θεωρούν σαν δεδομένο το πρωτόκολλο http και όχι κάποιο άλλο (https, ftp, mail, gopher κλπ).

Η διαδικασία που ακολουθούσε το αρχικό πρωτόκολλο ήταν η εξής:

1. Σύνδεση στον εξυπηρετητή.
2. Ερώτηση προς τον εξυπηρετητή.
3. Απάντηση από τον εξυπηρετητή.
4. Αποσύνδεση.

Σήμερα χρησιμοποιεί πολλά περισσότερα χαρακτηριστικά τα οποία παρέχουν ακόμα και την δυνατότητα στο πρόγραμμα-πελάτης να στέλνει δεδομένα στον εξυπηρετητή.

Η ανάπτυξη του HTTP έγινε υπό την εποπτεία του World Wide Web Consortium και του Internet Engineering Task Force (IETF). Το απλό πρωτόκολλο http δεν εγγυάται καμία ασφάλεια. Από τα RFCs (Requests for Comments) που έχουν κατά καιρούς δημοσιευτεί για το HTTP αξίζει να εστιάσουμε στα εξής:

- RFC 2616 (Ιούνιος 1999) που όριζε το HTTP/1.1, την έκδοση που χρησιμοποιείται κυρίως σήμερα.
- Τον Ιούνιο 2014, το RFC 2616 αποσύρθηκε και το HTTP/1.1 ορίστηκε εκ νέου από τα RFCs 7230, 7231, 7232, 7233, 7234 και 7235.

Η έκδοση HTTP/2 βρίσκεται ακόμα σε προπαρασκευαστικό στάδιο.

2.5.2. Επισκόπηση πρωτοκόλλου

Το HTTP λειτουργεί σαν ένα πρωτόκολλο του τύπου «αίτημα-απόκριση» (request-response) στο πληροφοριακό μοντέλο πελάτη-εξυπηρετητή. Ένας φυλλομετρητής ιστού, για παράδειγμα, μπορεί να είναι ο πελάτης και μια εφαρμογή που τρέχει σε ένα υπολογιστή που φιλοξενεί μια ιστοσελίδα στο Διαδίκτυο μπορεί να είναι ο εξυπηρετητής. Ο πελάτης υποβάλλει ένα μήνυμα αιτήματος HTTP στον διακομιστή. Ο διακομιστής, που παρέχει πόρους όπως για παράδειγμα αρχεία HTML και άλλο περιεχόμενο ή επιτελεί άλλες λειτουργίες εκ μέρους του πελάτη, επιστρέφει ένα μήνυμα απόκρισης στον πελάτη. Η απόκριση περιέχει

ολοκληρωμένες πληροφορίες κατάστασης για το αίτημα που στάλθηκε στον διακομιστή και μπορεί επίσης να περιέχει και συναφές με το αίτημα περιεχόμενο στο κυρίως σώμα του μηνύματος.

Ένας φυλλομετρητής ιστού είναι ένα παράδειγμα ενός user agent (UA). Άλλοι τύποι UA περιλαμβάνουν το λογισμικό ανεύρεσης (indexing software) που χρησιμοποιείται από τους παρόχους αναζήτησης (web crawlers), voice browsers, mobile apps και άλλο λογισμικό που προσπελαύνει, «καταναλώνει» ή αναπαράγει περιεχόμενο του Παγκόσμιου Ιστού.

Το HTTP έχει σχεδιαστεί ώστε να επιτρέπει στα ενδιάμεσα δομικά συστατικά του Διαδικτύου να βελτιώσουν ή να επιτρέψουν τις επικοινωνίες μεταξύ πελάτη και εξυπηρετητή. Οι ιστοσελίδες μεγάλης επισκεψιμότητας συνήθως επωφελούνται από τους λεγόμενους web cache servers που διακινούν περιεχόμενο εκ μέρους άλλων εξυπηρετητών (upstream servers) για να βελτιώσουν τον χρόνο απόκρισης. Οι φυλλομετρητές ιστού αποθηκεύουν στην κρυφή μνήμη πόρους του Διαδικτύου που προσπελάστηκαν σε κάποια προηγούμενη χρονική στιγμή και τους ξαναχρησιμοποιούν, όποτε αυτό καταστεί δυνατό, για να μειώσουν την κίνηση στο δίκτυο. Οι proxy servers του HTTP σε όρια ιδιωτικών δικτύων μπορούν να διευκολύνουν την επικοινωνία για τους πελάτες χωρίς να είναι αναγκαία κάποια παγκόσμια διακινούμενη διεύθυνση, απλά αναμεταδίδοντας μηνύματα με εξωτερικούς δρομολογητές.

Το HTTP είναι ένα πρωτόκολλο του επιπέδου εφαρμογής (application layer) που έχει σχεδιαστεί εντός του πλαισίου του Internet Protocol Suite. Ο ορισμός του υπονοεί ένα κρυφό και αξιόπιστο πρωτόκολλο του επιπέδου μεταφοράς (transport layer) και για αυτό τον λόγο χρησιμοποιείται συνήθως το πρωτόκολλο TCP (Transmission Control Protocol). Παρόλα αυτά όμως το HTTP μπορεί να χρησιμοποιήσει μη αξιόπιστα πρωτόκολλα, όπως το UDP (User Datagram Protocol), για παράδειγμα στο SSDP (Simple Service Discovery Protocol).

Οι πόροι του HTTP αναγνωρίζονται και εντοπίζονται στο δίκτυο μέσω των URIs (Uniform Resource Identifiers)-ή πιο συγκεκριμένα μέσω των URLs (Uniform Resource Locators)- χρησιμοποιώντας τα σχήματα http ή https. Τα URIs και οι υπερσύνδεσμοι στα έγγραφα HTML (Hypertext Markup Language) δημιουργούν σελίδες (ή ακόμα και ολόκληρα webs!) από διασυνδεδεμένα έγγραφα υπερκειμένου.

Το HTTP/1.1 είναι μια αναθεώρηση του αρχικού HTTP (HTTP/1.0). Στο HTTP/1.0 μια μεμονωμένη σύνδεση στον ίδιο διακομιστή δημιουργείται για κάθε ξεχωριστό αίτημα που του αποστέλλεται. Το HTTP/1.1 μπορεί να ξαναχρησιμοποιήσει μια σύνδεση πολλές φορές για να κατεβάσει εικόνες, scripts, stylesheets κλπ. αφότου η σελίδα έχει παραληφθεί. Οι επικοινωνίες στο HTTP/1.1 συνεπώς εμφανίζουν μικρότερο latency καθώς η εγκατάσταση των TCP συνδέσεων παρουσιάζει ένα σημαντικό overhead.

2.5.3 Ειδικές λεπτομέρειες του πρωτοκόλλου

Μια σύνοδος HTTP (HTTP session) είναι μια ακολουθία μεταδόσεων «αίτημα-απόκριση» εντός του δικτύου. Ένας πελάτης HTTP αρχίζει την μετάδοση ενός αιτήματος εγκαθιστώντας μια σύνδεση TCP σε μια συγκεκριμένη θύρα του διακομιστή (συνήθως την θύρα 80, περιστασιακά και την θύρα 8080). Ένας διακομιστής HTTP που ακούει σε αυτή την θύρα περιμένει μέχρι να λάβει το αίτημα του πελάτη. Μόλις το λάβει, ο διακομιστής επιστρέφει πίσω μια γραμμή κατάστασης, όπως «HTTP/1.1 200 OK» καθώς και ένα μήνυμα απόκρισης. Το κυρίως σώμα του μηνύματος τυπικά είναι ο πόρος (ή οι πόροι) του συστήματος που ζήτησε ο πελάτης, παρόλο που ένα μήνυμα σφάλματος ή κάποια άλλη πληροφορία μπορεί να επιστραφεί.

2.5.4 Μέθοδοι

Το HTTP ορίζει μεθόδους (που μερικές φορές αναφέρονται και ως ρήματα-verbs) για να δηλώσει την επιθυμητή ενέργεια που θα πρέπει να εκτελεστεί πάνω στον προς αναζήτηση πόρο. Το τι αναπαριστά αυτός ο πόρος εξαρτάται από την υλοποίηση του διακομιστή. Συνήθως αντιστοιχεί σε κάποιο αρχείο ή σε κάποια έξοδο από την εκτέλεση συγκεκριμένης ενέργειας στον διακομιστή. Το HTTP/1.0 όριζε τις μεθόδους GET, POST και HEAD και το HTTP/1.1 πρόσθεσε άλλες 5: OPTIONS, PUT, DELETE, TRACE και CONNECT. Κάθε πελάτης μπορεί να χρησιμοποιήσει οποιαδήποτε μέθοδο και ο διακομιστής μπορεί να ρυθμιστεί για να υποστηρίζει οποιαδήποτε συνδυασμό μεθόδων. Αν μια μέθοδος είναι άγνωστη θα αντιμετωπιστεί ως μη προκαθορισμένη και μη ασφαλής. Δεν υπάρχει όριο στον αριθμό μεθόδων που μπορούν να οριστούν και αυτό επιτρέπει και μελλοντικές προτάσεις χωρίς να καταρρεύσει η υπάρχουσα υποδομή. Για παράδειγμα το WebDAV (Web Distributed Authoring and Versioning, επέκταση του HTTP, ορίζεται στο RFC 4918) όρισε 7 νέες μεθόδους και το RFC 5789 όρισε την μέθοδο PACH.

GET. Αναπαριστά ουσιαστικά το αίτημα για τον προς αναζήτηση πόρο. Τα αιτήματα που χρησιμοποιούν την μέθοδο GET θα πρέπει μόνο να ανακαλούν δεδομένα και δεν θα πρέπει να προβαίνουν σε άλλη ενέργεια. (Αυτό ισχύει και για ορισμένες άλλες μεθόδους). Προς αυτή την κατεύθυνση το W3C έχει καθορίσει συγκεκριμένες οδηγίες, λέγοντας «Η σχεδίαση διαδικτυακών εφαρμογών θα πρέπει να ενημερώνεται από τους παραπάνω κανόνες αλλά επίσης και από τους σχετικούς περιορισμούς».

HEAD. Ρωτά για την απόκριση που θα πρέπει να είναι ίδια με εκείνη που αντιστοιχεί σε ένα αίτημα GET, αλλά χωρίς το κυρίως σώμα της απόκρισης. Αυτό

είναι χρήσιμο κατά την ανάκληση μετα-δεδομένων που εμπεριέχονται στις επικεφαλίδες των αποκρίσεων, χωρίς να χρειάζεται να αποστείλουμε ολόκληρο το περιεχόμενο.

POST. Δηλώνει ότι ο διακομιστής αποδέχεται τα δεδομένα που περικλείονται στο κυρίως σώμα του μηνύματος της απόκρισης για λόγους αποθήκευσης. Χρησιμοποιείται συνήθως όταν μεταφορτώνουμε ένα αρχείο ή όταν υποβάλλουμε μια ολοκληρωμένη web form.

PUT. Δηλώνει ότι τα δεδομένα μας μπορούν να αποθηκευτούν με βάση το παρεχόμενο URI. Αν το URI αναφέρεται σε ήδη υπάρχοντα πόρο, τροποποιείται- αν όχι, τότε ο διακομιστής μπορεί να δημιουργήσει τον πόρο με βάση το συγκεκριμένο URI.

DELETE. Διαγράφει τον πόρο.

TRACE. Εντοπίζει και ανασύρει την απόκριση στο αίτημα του πελάτη έτσι ώστε ο τελευταίος να μπορέσει να δει (αν υπάρχουν) τι αλλαγές ή προσθήκες έγιναν από ενδιάμεσους διακομιστές.

OPTIONS. Επιστρέφει τις μεθόδους που ο διακομιστής υποστηρίζει για το συγκεκριμένο URL. Με αυτό μπορούμε να ελέγξουμε την λειτουργικότητα ενός web server δηλώνοντας σαν αίτημα το σύμβολο «*» αντί για κάποιο συγκεκριμένο πόρο.

CONNECT. Μετατρέπει την αρχική σύνδεση σε ένα διαφανές κανάλι TCP/IP, συνήθως για να διευκολύνει περιπτώσεις που έχουμε κρυπτογραφημένη (με βάση το SSL) επικοινωνία (HTTPS) μέσω ενός μη κρυπτογραφημένου proxy server.

PATCH. Εφαρμόζει μερικές τροποποιήσεις σε ένα πόρο.

Οι διακομιστές HTTP απαιτούμε να υλοποιούν τουλάχιστον τις μεθόδους GET και HEAD και όποτε παραστεί ανάγκη και την μέθοδο OPTIONS.

2.5.5 Μορφή αιτήματος

Ένα αίτημα στο HTTP αποτελείται από τα ακόλουθα:

1. Μια γραμμή αιτήματος, για παράδειγμα GET /images/logo.png HTTP/1.1, με την οποία αναζητούμε ένα πόρο από τον διακομιστή, τον πόρο /images/logo.png.
2. Πεδία επικεφαλίδας, όπως Accept-Language: en
3. Μια κενή γραμμή.
4. Ένα προαιρετικό κυρίως σώμα του μηνύματος.

Η γραμμή αιτήματος και τυχόν πεδία επικεφαλίδας πρέπει να τελειώνουν το καθένα με <CR><LF>. Η κενή γραμμή πρέπει να αποτελείται μόνο από <CR><LF> και κανένα άλλο κενό χώρο. Στο πρωτόκολλο HTTP/1.1 όλα τα πεδία επικεφαλίδας εκτός από το Host είναι προαιρετικά.

Μια γραμμή αιτήματος που περιέχει μόνο το όνομα του μονοπατιού γίνεται αποδεκτή από τους διακομιστές για να διατηρήσουν την συμβατότητα με τους πελάτες HTTP πριν ακόμα τυποποιηθεί το HTTP/1.0 στο RFC 1945.

2.5.6 Μορφή απόκρισης

Μια απόκριση στο HTTP αποτελείται από τα ακόλουθα:

1. Μια γραμμή κατάστασης, που περιλαμβάνει τον κώδικα κατάστασης και ένα μήνυμα (π.χ. HTTP/1.1 200 OK, που δηλώνει ότι το αίτημα του πελάτη απαντήθηκε επιτυχώς).
2. Πεδία επικεφαλίδας, π.χ. Content-Type: text/html
3. Μια κενή γραμμή.
4. Ένα προαιρετικό κυρίως σώμα του μηνύματος.

Η γραμμή κατάστασης και τυχόν πεδία επικεφαλίδας πρέπει να τελειώνουν το καθένα με <CR><LF>. Η κενή γραμμή πρέπει να αποτελείται μόνο από <CR><LF> και κανένα άλλο κενό χώρο.

2.5.7 Παράδειγμα συνόδου

Ακολουθεί ένα δείγμα συνομιλίας μεταξύ πελάτη και εξυπηρετητή και τρέχει στο www.example.com, θύρα 80.

Αίτημα πελάτη

GET /index.html HTTP/1.1

Host: www.example.com

Απόκριση διακομιστή

HTTP/1.1 200 OK

Date: Mon, 23 May 2005 22:38:34 GMT

Server: Apache/1.3.3.7 (Unix) (Red-Hat/Linux)

Last-Modified: Wed, 08 Jan 2003 23:11:55 GMT

ETag: “ef80f-1b6-3e1cb03b”

```
Content-Type: text/html;  charset=UTF-8
Content-Length: 131
Accept-Ranges: bytes
Connection: close
<html>
<head>
<title>An Example Page </title>
</head>
<body>
Hello World, this is a very simple HTML document.
</body>
</html>
```

Η ετικέτα ETag (entity tag) που χρησιμοποιείται εδώ ως πεδίο επικεφαλίδας χρησιμοποιείται για να προσδιορίσουμε ένα μια αποθηκευμένη έκδοση του προς αναζήτηση πόρου είναι ίδια με την παρούσα έκδοση του πόρου στον διακομιστή. Το πεδίο Content-Type συγκεκριμενοποιεί τον τύπο των δεδομένων του Διαδικτύου που μεταδίδονται μέσω του HTTP μηνύματος, ενώ το Content-Length δηλώνει το μέγεθος του μηνύματος σε bytes. Ο web server στο HTTP/1.1 δημοσιεύει την ικανότητά του να αποκρίνεται σε αιτήματα για συγκεκριμένα σύνολα από bytes αυτού του εγγράφου και σε αυτό χρησιμεύει το πεδίο Accept-Ranges: bytes. Αυτό είναι χρήσιμο εάν ο πελάτης χρειάζεται να έχει μόνο συγκεκριμένες ποσότητες του πόρου που αποστέλλεται από τον διακομιστή, κάτι που δηλώνεται με τον όρο byte serving. Όταν αποστέλλεται το πεδίο Connection: close, σημαίνει ότι ο διακομιστής θα τερματίσει την σύνδεση TCP αμέσως μόλις ολοκληρωθεί η μεταφορά του πόρου στον πελάτη.

Οι περισσότερες από τις γραμμές της επικεφαλίδας είναι προαιρετικές. Όταν απουσιάζει το Content-Length, το μέγεθος καθορίζεται με άλλους τρόπους. Μπορούμε επίσης να εφαρμόσουμε συμπίεση και στα προς αποστολή δεδομένα μέσω του Content-Encoding (π.χ. gzip). Βέβαια υπάρχουν και άλλα πεδία επικεφαλίδας που μπορούμε να χρησιμοποιήσουμε αλλά δεν θα επεκταθούμε περαιτέρω.

Καταλήγοντας και για ιστορικούς λόγους αξίζει να αναφερθούμε στο πρωτόκολλο Gopher που ήταν ένα πρωτόκολλο μεταφοράς περιεχομένου και αντικαταστάθηκε από το HTTP στις αρχές του 1990. Επίσης έχει εμφανιστεί και ένα νέο πρωτόκολλο το SPDY (διαβάζεται speedy) που είναι παρόμοιο με το HTTP και το

οποίο τροποποιεί την αλληλεπίδραση μεταξύ πελάτη και εξυπηρετητή που στηρίζεται στο μοντέλο request-response.

2.5.8. HTTPS (HYPERTEXT TRANSFER PROTOCOL SECURE: ΑΣΦΑΛΕΣ ΠΡΩΤΟΚΟΛΛΟ ΜΕΤΑΦΟΡΑΣ ΥΠΕΡΚΕΙΜΕΝΟΥ)

Το HTTPS (Hypertext Transfer Protocol Secure) είναι ένα πρωτόκολλο το οποίο χρησιμοποιείται για να δηλώσει μία ασφαλή δικτυακή σύνδεση http. Όταν ένας σύνδεσμος (URL) αρχίζει με το πρόθεμα https, υποδηλώνει ότι θα χρησιμοποιηθεί το πρωτόκολλο HTTP, σε διαφορετική πόρτα (443 αντί 80) και τα δεδομένα που θα ανταλλάσσονται θα είναι κρυπτογραφημένα. Το πρωτόκολλο αυτό σχεδιάστηκε αρχικά από την εταιρία Netscape Communications Corporation για να χρησιμοποιηθεί σε ιστοτόπους όπου απαιτούνταν αυθεντικοποίηση χρηστών και κρυπτογραφημένη επικοινωνία. Πλέον, χρησιμοποιείται ευρέως στο διαδίκτυο όπου χρειάζεται αυξημένη ασφάλεια διότι διακινούνται ευαίσθητες πληροφορίες, όπως αριθμοί πιστωτικών καρτών, κωδικοί, κ.ο.κ..

Εικόνα 2.5.2. *Διαφορά του Πρωτοκόλλου Μεταφοράς Υπερκειμένου (HTTP) με το Ασφαλές Πρωτόκολλο Μεταφοράς Υπερκειμένου (HTTPS)*

2.5.8.1. Τρόπος λειτουργίας

Το HTTPS δεν είναι ένα διαφορετικό πρωτόκολλο, όπως κάποιοι νομίζουν, αλλά είναι ο συνδυασμός χρήσης του απλού HTTP πρωτοκόλλου και με τις δυνατότητες

κρυπτογράφησης που παρέχονται από το πρωτόκολλο Secure Sockets Layer (SSL). Η κρυπτογράφηση που χρησιμοποιείται διασφαλίζει ότι τα κρυπτογραφημένα δεδομένα δεν θα μπορούν να υποκλαπούν από άλλους κακόβουλους χρήστες ή από επιθέσεις man-in-the-middle.

Για να μπορεί να χρησιμοποιηθεί το πρωτόκολλο HTTPS σε έναν εξυπηρετητή, θα πρέπει ο διαχειριστής του να εκδώσει ένα πιστοποιητικό δημοσίου κλειδιού. Ανάλογα με το λειτουργικό σύστημα των εξυπηρετητών, εκδίδονται τα πιστοποιητικά δημοσίου κλειδιού από τα ανάλογα προγράμματα. Για παράδειγμα, στους εξυπηρετητές που χρησιμοποιούν το λειτουργικό σύστημα UNIX αυτό γίνεται μέσω του προγράμματος OpenSSL. Στην συνέχεια το πιστοποιητικό αυτό θα πρέπει να υπογραφεί από μία Τρίτη Έμπιστη Οντότητα, η οποία είναι αρχή πιστοποίησης (certificate authority) και πιστοποιεί ότι ο εκδότης του πιστοποιητικού είναι νομότυπος και ότι το πιστοποιητικό είναι έγκυρο. Με τον τρόπο αυτό οι χρήστες μπορούν να δουν την υπογραφή της αρχής πιστοποίησης και να ταυτοποιήσουν ότι το πιστοποιητικό είναι έγκυρο και ότι δεν χρησιμοποιείται από κάποιον κακόβουλο χρήστη που το έχει πλαστογραφήσει.

2.5.8.2. Πρωτόκολλο TLS (Transfer Layer Security: Ασφάλεια σε Επίπεδο Μεταφοράς)

Το πρωτόκολλο **Transport Layer Security (TLS)** και ο προκάτοχός του **Secure Sockets Layer (SSL)**, που συχνά αναφέρονται με τη κοινή ονομασία «SSL», είναι κρυπτογραφικά πρωτόκολλα τα οποία παρέχουν ασφαλείς επικοινωνίες σε ένα δίκτυο υπολογιστών. Αρκετές εκδόσεις των πρωτοκόλλων μπορεί να συναντήσει κάποιος ευρέως σε διάφορες εφαρμογές, όπως στη περιήγηση στο διαδίκτυο, στο ηλεκτρονικό ταχυδρομείο, στην ανταλλαγή άμεσων μηνυμάτων, στις τηλεδιασκέψεις (VoIP), κ.α.. Αρκετοί ιστότοποι χρησιμοποιούν το πρωτόκολλο TLS για την ασφαλή επικοινωνία μεταξύ των εξυπηρετητών και των φυλλομετρητών.

Το πρωτόκολλο TLS στοχεύει πρωτίστως να παρέχει ιδιωτικότητα και ακεραιότητα δεδομένων μεταξύ της επικοινωνίας δύο εφαρμογών υπολογιστών. Με την ασφάλεια του TLS, οι συνδέσεις μεταξύ πελάτη και εξυπηρετητή έχουν μία ή περισσότερες από τις ακόλουθες ιδιότητες:

- Η σύνδεση είναι ιδιωτική (ή ασφαλής) επειδή χρησιμοποιείται συμμετρική κρυπτογράφηση για τα μεταδιδόμενα δεδομένα. Τα κλειδιά για αυτή την συμμετρική κρυπτογράφηση δημιουργούνται μοναδικά για κάθε σύνδεση βασιζόμενα σε μία κοινή μυστική διαπραγμάτευση στην έναρξη της συνεδρίας. Ο εξυπηρετητής και ο πελάτης διαπραγματεύονται τις λεπτομέρειες για ποιον κρυπτογραφικό αλγόριθμο και κρυπτογραφικά κλειδιά θα χρησιμοποιηθούν πριν το πρώτο byte δεδομένων μεταδοθεί. Η διαπραγμάτευση ενός κοινού

μυστικού είναι και ασφαλής (το διαπραγματευόμενο μυστικό δεν είναι διαθέσιμο στους κακόβουλους χρήστες και δεν μπορούν να το αποκτήσουν, ακόμα και αν ένας επιτιθέμενος τοποθετηθεί στο μέσον της επικοινωνίας τους) και αξιόπιστη (κανένας επιτιθέμενος δεν μπορεί να τροποποιήσει τις επικοινωνίες κατά τη διάρκεια της διαπραγμάτευσης χωρίς να ανιχνευθεί).

- Η ταυτότητα των επικοινωνούντων μερών μπορεί να αυθεντικοποιηθεί με τη χρήση της κρυπτογράφησης δημοσίου κλειδιού. Η αυθεντικοποίηση μπορεί να είναι προαιρετική, αλλά γενικά απαιτείται για τουλάχιστον ένα από τα συμμετέχοντα μέρη (συνήθως για τον εξυπηρετητή).
- Η σύνδεση εγγυάται την ακεραιότητα γιατί κάθε μεταδιδόμενο μήνυμα εμπεριέχει μήνυμα ελέγχου ακεραιότητας χρησιμοποιώντας κώδικα μηνύματος αυθεντικοποίησης για να αποτρέψει μη ανιχνεύσιμη απώλεια ή τροποποίηση δεδομένων κατά τη διάρκεια της μετάδοσης.

Πέρα των ανωτέρω ιδιοτήτων, η προσεκτική παραμετροποίηση του πρωτοκόλλου TLS παρέχει επιπρόσθετες ιδιότητες ιδιωτικότητας, όπως η προς τα εμπρός ασφάλεια (forward secrecy), η οποία εγγυάται ότι η οποιαδήποτε μελλοντική αποκάλυψη των κρυπτογραφημένων κλειδιών δεν μπορεί να οδηγήσει στην αποκρυπτογράφηση των καταγεγραμμένων επικοινωνιών που έγιναν με τη χρήση του TLS.

Το πρωτόκολλο TLS υποστηρίζει ποικίλες μεθόδους ανταλλαγής κλειδιών, κρυπτογράφησης δεδομένων, και ακεραιότητας αυθεντικοποιημένων μηνυμάτων. Σαν αποτέλεσμα αυτού, η ασφαλής παραμετροποίηση του πρωτοκόλλου TLS εμπεριέχει πολλές διαμορφώσιμες παραμέτρους, πέρα των ανωτέρω που περιγράφονται, και παρέχουν ιδιότητες ιδιωτικότητας

Έχουν πραγματοποιηθεί πολλές προσπάθειες για να ανατρέπουν τα χαρακτηριστικά της ασφάλειας επικοινωνιών που το πρωτόκολλο TLS επιζητά να παρέχει, και για αυτό το πρωτόκολλο έχει αναθεωρηθεί αρκετές φορές ώστε να αντιμετωπίσει αυτές τις απειλές ασφαλείας. Οι προγραμματιστές των φυλλομετρητών έχουν επίσης αναθεωρήσει τα προϊόντα τους για να αντιμετωπίσουν τις όποιες πιθανές αδυναμίες μετά την ανακάλυψη αυτών.

Το πρωτόκολλο TLS περιλαμβάνει δύο επίπεδα, το πρωτόκολλο TLS καταγραφής (TLS record protocol) και το πρωτόκολλο TLS ανταλλαγής μηνυμάτων (TLS handshake protocol).

Το πρωτόκολλο TLS προτάθηκε από τον διεθνή οργανισμό πιστοποίησης Internet Engineering Task Force (IETF), για πρώτη φορά το 1999 και αναθεωρήθηκε από τα RFC 5246 (Αύγουστος 2008) και RFC 6176 (Μάρτιος 2011). Είναι βασισμένο στις προηγούμενες προδιαγραφές που τέθηκαν από το πρωτόκολλο SSL (1994, 1995, 1996) και αναπτύχθηκαν από την Netscape Communications, η οποία προσέθεσε το πρωτόκολλο HTTPS στους δικούς τους φυλλομετρητές.

2.5.8.2.1. Περιγραφή

Οι εφαρμογές πελάτη – εξυπηρετητή χρησιμοποιούν το πρωτόκολλο TLS για να επικοινωνούν μέσα σε ένα δίκτυο με τέτοιο τρόπο σχεδιασμένο ώστε να αποτρέπεται η παρακολούθηση και η παραποίηση.

Από τη στιγμή που τα πρωτόκολλα μπορούν να λειτουργήσουν είτε με είτε χωρίς τη χρήση του TLS (ή του SSL), είναι απαραίτητο για τον πελάτη να υποδείξει στον εξυπηρετητή τη ρύθμιση μίας σύνδεσης με TLS. Υπάρχουν δύο τρόποι να επιτευχθεί αυτό, η μία επιλογή είναι η χρήση διαφορετικής πόρτας για τις συνδέσεις με TLS (π.χ. την 443 για το HTTPS), και η άλλη είναι ο πελάτης να χρησιμοποιήσει συγκεκριμένο μηχανισμό πρωτοκόλλου (π.χ. το STARTTLS για τα ηλεκτρονικά μηνύματα και τα νέα πρωτόκολλα) για να ζητήσει από τον εξυπηρετητή να ανοίξει μία σύνδεση σε TLS.

Μετά τη συμφωνία πελάτη – εξυπηρετητή για τη χρήση του πρωτοκόλλου TLS, διαπραγματεύονται μία σταθερή σύνδεση μέσω μιας διαδικασίας ανταλλαγής μηνυμάτων. Κατά την ανταλλαγή αυτή, συμφωνούν μεταξύ τους για διάφορες παραμέτρους για να εδραιωθεί η ασφάλεια της σύνδεσής τους (βλέπε Εικόνα 2.5.3).

Η ανταλλαγή ξεκινά όταν πελάτης συνδεθεί σε έναν εξυπηρετητή που έχει ενεργοποιημένο το TLS απαιτώντας μία ασφαλή σύνδεση και παρουσιάζει μία λίστα από υποστηριζόμενες κρυπτογραφικές σουίτες (αλγόριθμοι κρυπτογράφησης και συναρτήσεις κατακερματισμού). Από τη λίστα αυτή, ο εξυπηρετητής επιλέγει έναν αλγόριθμο κρυπτογράφησης και μία συνάρτηση κατακερματισμού που υποστηρίζει αυτός και ειδοποιεί τον πελάτη για την απόφαση αυτή. Ο εξυπηρετητής συνήθως αποστέλλει την ταυτότητά του σε μορφή ψηφιακού πιστοποιητικού. Το πιστοποιητικό περιέχει το όνομα του εξυπηρετητή και την έμπιστη αρχή έκδοσης του πιστοποιητικού, καθώς και το δημόσιο κλειδί κρυπτογράφησης του. Ο πελάτης επιβεβαιώνει την εγκυρότητα του πιστοποιητικού πριν προχωρήσει η διαδικασία.

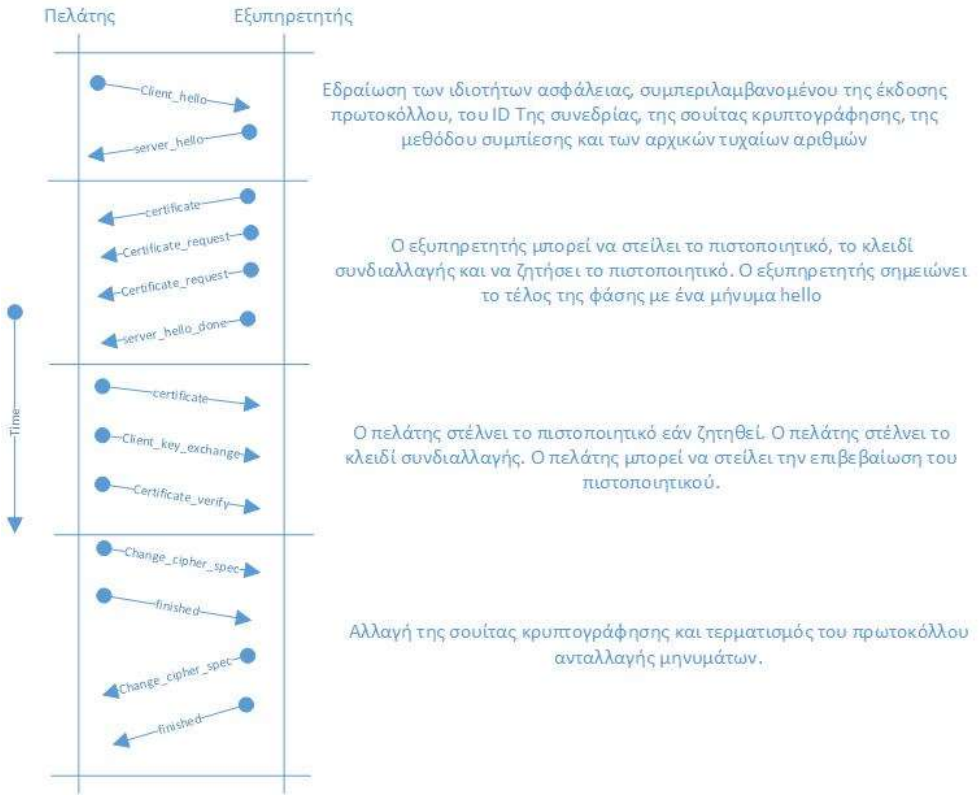
Για τη δημιουργία των κλειδιών της συνεδρίας που θα χρησιμοποιηθούν, ο πελάτης είτε:

- κρυπτογραφεί ένα τυχαίο αριθμό με το δημόσιο κλειδί του εξυπηρετητή και στέλνει το αποτέλεσμα σε αυτόν (το οποίο μόνο ο εξυπηρετητής μπορεί να αποκρυπτογραφήσει με το ιδιωτικό του κλειδί), και μετά και τα δύο συνδιαλλέγεντα μέρη χρησιμοποιούν αυτόν τον τυχαίο αριθμό για να δημιουργήσουν ένα μοναδικό κλειδί συνεδρίας για τις επόμενες κρυπτογραφήσεις και αποκρυπτογραφήσεις δεδομένων κατά τη διάρκεια της συνεδρίας.

ή

- χρησιμοποιεί την ανταλλαγή κλειδιού του Diffie-Hellman για να δημιουργηθεί με ασφάλεια ένα μοναδικό κλειδί συνεδρίας για την κρυπτογράφηση και την αποκρυπτογράφηση, η οποία έχει την επιπρόσθετη ιδιότητα της forward secrecy: εάν το ιδιωτικό κλειδί του εξυπηρετητή αποκαλυφθεί στο μέλλον, δεν θα μπορεί να χρησιμοποιηθεί για να αποκρυπτογραφηθεί η παρούσα συνεδρία, ακόμα και αν η συνεδρία παρακολουθείται και καταγράφεται από έναν τρίτο.

Έτσι, ολοκληρώνεται η ανταλλαγή μηνυμάτων και ξεκινά η ασφαλής σύνδεση, η οποία κρυπτογραφείται και αποκρυπτογραφείται με το κλειδί της συνεδρίας μέχρι το τερματισμό αυτής. Εάν κάποιο από τα στάδια της ανωτέρω διαδικασίας αποτύχει, τότε και η ανταλλαγή μηνυμάτων για το TLS αποτυγχάνει και δεν εδραιώνεται η σύνδεση.



Εικόνα 2.5.3. *Λειτουργία του Ασφαλούς Πρωτοκόλλου Μεταφοράς Υπερκειμένου (HTTPS)*

Τα πρωτόκολλα TLS και SSL ορίζονται ότι λειτουργούν πάνω από ένα αξιόπιστα επίπεδο μεταφοράς, το οποίο τα τοποθετεί ως πρωτόκολλα επιπέδου εφαρμογών

στο σχήμα των επιπέδων του TCP/IP και ως πρωτόκολλα επιπέδου παρουσίασης στο σχήμα OSI. Τα πρωτόκολλα χρησιμοποιούν ανταλλαγή μηνυμάτων με ασύμμετρη κρυπτογράφηση για να θέσουν τις ρυθμίσεις κρυπτογράφησης και ένα διαμοιραζόμενα κλειδί για τη συνεδρία. Τα υπόλοιπα στοιχεία της επικοινωνίας κρυπτογραφούνται με συμμετρική κρυπτογράφηση και με το κλειδί της συνεδρίας.

2.5.8.2.2. Ιστορική αναδρομή και εξέλιξηHistory and development

Ασφαλής Προγραμματισμός Δικτύου

Οι πρώιμες ερευνητικές προσπάθειες για την ασφάλεια επιπέδου μεταφοράς περιλάμβαναν το περιβάλλον Ασφαλούς Προγραμματισμού Δικτύων (SNP) και προγραμματισμού εφαρμογών (API), οι οποίες το 1993 διερεύνησαν την προσέγγιση της ύπαρξης μίας ασφαλούς εφαρμογής στο επίπεδο μεταφοράς και να έχει ομοιότητες με τις υποδοχές Berkeley, ώστε να διευκολυνθεί η αναθεώρηση των προϋπάρχουσων εφαρμογών δικτύου σύμφωνα με τα μέτρα ασφαλείας.

SSL 1.0, 2.0 και 3.0

Η Netscape ανέπτυξε τα πρωτότυπα SSL πρωτόκολλα. Η έκδοση 1.0 ποτέ δεν δημοσιεύθηκε λόγω σοβαρών αδυναμιών ασφαλείας, η έκδοση 2.0 δημοσιεύθηκε το Φεβρουάριο του 1995, όπου πάλι υπήρχαν σοβαρές αδυναμίες οι οποίες οδήγησαν στην αναθεώρησή του και στο σχεδιασμό της έκδοσης της 3.0. Το SSL 3.0 δημοσιεύθηκε το 1996 αντιπροσωπεύοντας ενός καθολικού ανασχεδιασμού του πρωτοκόλλου από τον Paul Kocher σε συνεργασία με τους σχεδιαστές της Netscape Phil Karlton και Alan Freier και με υλοποίηση από τους Christopher Allen και Tim Dierks της Consensus Development. Οι νεότερες εκδόσεις των SSL/TLS βασίζονται στο SSL 3.0. Το προσχέδιο του SSL 3.0 δημοσιεύθηκε από τον IETF ως ιστορικό κείμενο με τον κωδικό RFC 6101. Ο Dr. Taher Elgamal, επικεφαλής των ερευνητών της Netscape Communications από το 1995 έως το 1998, θεωρείται ως ο πατέρας του SSL.

Από τη στιγμή που από το 2014 η έκδοση 3.0 θεωρείται μη ασφαλής, καθώς είναι ευπαθής στην επίθεση POODLE, η οποία επηρεάζει όλους τους κρυπτοαλγορίθμους του SSL, ο RC4, που είναι ο μόνος μη - κρυπτοαλγόριθμος που υποστηρίζει το SSL 3.0, είναι πιθανό να σπάσει. Το SSL 2.0 καταργήθηκε το 2011 από το RFC 6176 και το SSL 3.0 τον Ιούνιο του 2015 από το RFC 7568.

TLS 1.0

Το πρωτόκολλο TLS έκδοση 1.0 πρώτα ορίστηκε στο RFC 2246 τον Ιανουάριο του 1999 ως αναβάθμιση του πρωτοκόλλου SSL έκδοσης 3.0, και σχεδιάστηκε από

τους Christopher Allen και Tim Dierks της Consensus Development. Όπως αναφέρεται στο RFC, "οι διαφορές μεταξύ αυτού του πρωτοκόλλου και του SSL 3.0 δεν είναι δραματικές, αλλά είναι αξιοσημείωτες ώστε να απαγορεύσουν τη διαλειτουργικότητα μεταξύ του TLS 1.0 και SSL 3.0". Το πρωτόκολλο TLS 1.0 δεν περιλαμβάνει ένα μέσο με το οποίο η υλοποίηση του TLS μπορεί να υποβαθμίσει τη σύνδεση σε SSL 3.0, αποδυναμώνοντας έτσι την ασφάλεια.

TLS 1.1

Το πρωτόκολλο TLS έκδοση 1.1 ορίσθηκε με το RFC 4346 τον Απρίλιο του 2006. Είναι μία ενημερωμένη έκδοση του 1.0 και περιλαμβάνει σημαντικές αλλαγές, όπως οι ακόλουθες:

- Πρόσθετη προστασία ενάντια στις επιθέσεις των αλυσιδωτών κρυπτοαλγορίθμων (Cipher-block chaining (CBC) attacks).
- Το αόριστο διάνυσμα αρχικοποίησης αντικαταστάθηκε με ένα ορισμένο.
- Αλλαγή στον χειρισμό λαθών padding.
- Υποστήριξη της καταγραφής IANA με παραμέτρους.

TLS 1.2

Το πρωτόκολλο TLS έκδοση 1.2 ορίσθηκε με το RFC 5246 τον Αύγουστο του 2008. Είναι βασισμένο στη προηγούμενη έκδοση 1.1. Οι κυριότερες διαφορές είναι:

- Ο συνδυασμός MD5-SHA-1 στην ψευδοτυχαία συνάρτηση (PRF) αντικαταστάθηκε από την SHA-256, με την επιλογή να χρησιμοποιεί κρυπτογραφική σουίτα οριζόμενη από τις PRFs.
- Ο συνδυασμός MD5-SHA-1 στο τελευταίο μήνυμα κατακερματισμού αντικαταστάθηκε από τη SHA-256, με την επιλογή να χρησιμοποιεί κρυπτογραφική σουίτα με συγκεκριμένους αλγορίθμους κατακερματισμού. Παρ' όλ' αυτά, το μέγεθος του κατακερματισμού στο τελευταίο μήνυμα πρέπει να είναι τουλάχιστον 96 bits.
- Ο συνδυασμός MD5-SHA-1 στο ψηφιακά υπογεγραμμένο στοιχείο αντικαταστάθηκε με μία μονοσήμαντη διαπραγμάτευση κατά τη διάρκεια ανταλλαγής μηνυμάτων, που προεπιλεγμένη είναι η SHA-1.
- Ενίσχυση της ικανότητας των πελατών και των εξυπηρετητών για να καθορίσουν ποιον κατακερματισμό και ποιους αλγορίθμους υπογραφής δέχονται.

- Επέκταση της υποστήριξης για πιστοποιημένους αλγορίθμους κρυπτογράφησης, χρησιμοποιούμενοι κυρίως για Galois/Counter Mode (GCM) και CCM mode από την κρυπτογράφηση της Advanced Encryption Standard.
- Ορισμοί των επεκτάσεων του TLS και κρυπτογραφικές σουίτες της Advanced Encryption Standard προστέθηκαν.

Όλες οι εκδόσεις του TLS αναθεωρήθηκαν περαιτέρω στο RC 6176 τον Μάρτιο του 2011, αφαιρώντας την παλαιότερη συμβατότητά τους με το SSL, έτσι ώστε οι συνεδρίες του TLS να μην διαπραγματεύονται ποτέ την έκδοση 2.0 του Secure Sockets Layer (SSL).

TLS 1.3

Από τον Ιούλιο του 2016, το πρωτόκολλο TLS έκδοση 1.3 δημοσιεύθηκε σε προσχέδιο για να υπεισέλθουν βελτιώσεις, και οι λεπτομέρειες είναι προσωρινές και ημιτελείς. Είναι βασισμένο στην έκδοση 1.2 και οι κυριότερες διαφορές είναι οι ακόλουθες:

- Αφαίρεση υποστήριξης των αδύναμων και λιγότερο χρησιμοποιούμενων ελλειπτικών καμπύλων
- Αφαίρεση υποστήριξης των κρυπτογραφικών συναρτήσεων κατακερματισμού MD5 and SHA-224
- Απαίτηση χρήσης ψηφιακών υπογραφών ακόμα και εάν χρησιμοποιείται προηγούμενη έκδοση παραμετροποιήσεων.
- Ενσωμάτωση του HKDF και της ημι-εφήμερης πρότασης DH.
- Αντικατάσταση της επανάληψης με PSK και ετικέτες
- Υποστήριξη της ανταλλαγής μηνυμάτων 1-RTT και αρχική υποστήριξη για το 0-RTT
- Παύση υποστήριξης για πολλά ανασφαλή ή παρωχημένα χαρακτηριστικά συμπεριλαμβανομένου της συμπίεσης, της επαναδιαπραγμάτευσης, των κρυπτογραφικών αλγορίθμων non-AEAD, της ανταλλαγής κλειδιών με στατικό RSA και DH, των προσαρμοζόμενων ομάδων DHE, του σημείου μορφής διαπραγμάτευσης, του πρωτοκόλλου αλλαγής χαρακτηριστικών κρυπτογραφικών αλγορίθμων, της ώρας UNIX του μηνύματος Hello και του μήκους πεδίου της εισόδου AD στους κρυπτογραφικούς αλγορίθμους AEAD.
- Απαγόρευση της διαπραγμάτευσης του SSL ή RC4 για παλαιότερη συμβατότητα

- Ενσωμάτωση της χρήσης συνεδρίας κατακερματισμού
- Αποφυγή χρήσης του αριθμού έκδοσης για το επίπεδο καταγραφής και «πάγωμα» του αριθμού για βελτιωμένη παλαιότερη συμβατότητα.
- Μεταφορά κάποιων λεπτομερειών των σχετικών αλγορίθμων ασφαλείας από το παράρτημα στην παραμετροποίηση και υποβιβάζοντας το ClientKeyShare σε παράρτημα.
- Προσθήκη του ChaCha20 stream cipher με τον κώδικα αυθεντικοποίησης μηνύματος Poly1305.
- Προσθήκη των αλγορίθμων ψηφιακής υπογραφής Ed25519 και Ed448.
- Προσθήκη των πρωτοκόλλων ανταλλαγής κλειδιών x25519 και x448.

2.5.8.2.3. Πρόσθετες Πληροφορίες για το πρωτόκολλο HTTPS

Το πρωτόκολλο TLS ανταλλάσσει *αρχεία*, τα οποία ενθυλακώνουν δεδομένα που θα ανταλλαχθούν με μία συγκεκριμένη μορφή. Κάθε αρχείο μπορεί να συμπιεστεί, να παραγεμιστεί, να επεκταθεί με κώδικα αυθεντικοποίησης μηνύματος (message authentication code – MAC), ή να κρυπτογραφηθεί, και όλα είναι εξαρτώμενα από τη σύνδεση. Κάθε αρχείο έχει ένα πεδίο *τύπου περιεχομένου* που δηλώνει τον τύπο δεδομένων που ενθυλακώνει, το μήκος πεδίου, και το πεδίο με την έκδοση του TLS. Τα ενθυλακώμενα δεδομένα μπορεί να είναι ελέγχου ή μηνύματα διαδικασίας του TLS, ή απλά τα στοιχεία της αίτησης που απαιτούνται για να μεταφερθούν από το TLS. Οι προδιαγραφές (σουίτα κρυπτογράφησης, κλειδιά κ.λπ.) που απαιτούνται για την ανταλλαγή δεδομένων εφαρμογής από το TLS, έχουν συμφωνηθεί στο στην ανταλλαγή μηνυμάτων του TLS μεταξύ του πελάτη ζητώντας τα στοιχεία και του εξυπηρετητή να ανταποκρίνεται στα αιτήματα. Ως εκ τούτου, το πρωτόκολλο καθορίζει τόσο τη δομή των ωφέλιμων φορτίων που μεταφέρονται με το TLS και τη διαδικασία για τη δημιουργία και την παρακολούθηση της μεταφοράς.

Ανταλλαγή μηνυμάτων με το πρωτόκολλο TLS

Όταν η σύνδεση εκκινεί, το αρχείο ενθυλακώνει ένα πρωτόκολλο ελέγχου, το πρωτόκολλο ανταλλαγής μηνυμάτων (τύπος περιεχομένου 22). Αυτό το πρωτόκολλο χρησιμοποιείται για την ανταλλαγή των πραγματικών δεδομένων της εφαρμογής από το TLS. Ορίζει την μορφή των μηνυμάτων ή περιέχει την απαιτούμενη πληροφορία και τη σειρά των ανταλλαγών τους. Αυτά μπορεί να ποικίλουν ανάλογα με τις απαιτήσεις του πελάτη και του εξυπηρετητή, π.χ. υπάρχουν πολλές πιθανές διαδικασίες εγκαθίδρυσης μίας σύνδεσης. Αυτό αρχικά

ανταλλάσσει τα αποτελέσματα μιας επιτυχούς σύνδεσης TLS ή ενός προειδοποιητικού μηνύματος.

Ανταλλαγή μηνυμάτων με το πρωτόκολλο Basic TLS

Ένα παράδειγμα μιας τυπικής σύνδεσης ακολουθεί, αποτυπώνοντας την ανταλλαγή μηνυμάτων όπου ο εξυπηρετητής (και όχι ο πελάτης) αυθεντικοποιείται από το πιστοποιητικό του:

1. Φάση διαπραγμάτευσης:
   - Ο πελάτης στέλνει ένα μήνυμα ClientHello προσδιορίζοντας την έκδοση πρωτοκόλλου TLS που υποστηρίζει, τον τυχαίο αριθμό, μία λίστα σουιτών κρυπτογράφησης και τις προτεινόμενες μεθόδους συμπίεσης. Εάν ο πελάτης προσπαθήσει να εκτελέσει μία σύνοψη ανταλλαγής μηνυμάτων, τότε μπορεί να στείλει το ID της συνεδρίας. Εάν ο πελάτης μπορεί να χρησιμοποιήσει μία διαπραγμάτευση πρωτοκόλλου σε επίπεδο εφαρμογής, μπορεί να περιλαμβάνει μία λίστα από υποστηριζόμενα πρωτόκολλα εφαρμογής, όπως το HTTP/2.
   - Ο εξυπηρετητής απαντά με ένα μήνυμα ServerHello, το οποίο περιέχει το επιλεγμένο πρωτόκολλο, τον τυχαίο αριθμό, τη κρυπτογραφική σουίτα και τη μέθοδο συμπίεσης από τις επιλογές που προσφέρονται από τον πελάτη. Για να επικυρωθεί ή να επιτραπεί μία σύνοψη ανταλλαγής μηνυμάτων, ο εξυπηρετητής μπορεί να στείλει το ID της συνεδρίας. Η επιλεγμένη έκδοση πρωτοκόλλου θα πρέπει να είναι η πιο πρόσφατη που υποστηρίζουν και οι δύο. Για παράδειγμα, εάν ο πελάτης υποστηρίζει το TLS 1.1 και ο εξυπηρετητής την έκδοση 1.2, τότε θα επιλεγεί η έκδοση 1.1 και όχι η 1.0.
   - Ο εξυπηρετητής στέλνει το μήνυμα Certificate (εξαρτώμενο από την επιλεγμένη κρυπτογραφική σουίτα, αν και μπορεί να παραλειφθεί από τον εξυπηρετητή).
   - Ο εξυπηρετητής στέλνει το μήνυμα ServerKeyExchange (εξαρτώμενο από την επιλεγμένη κρυπτογραφική σουίτα, αν και μπορεί να παραλειφθεί από τον εξυπηρετητή). Αυτό το μήνυμα αποστέλλεται σε όλες τις κρυπτογραφικές σουίτες DHE και DH_anon.
   - Ο εξυπηρετητής αποστέλλει ένα μήνυμα ServerHelloDone, υποδεικνύοντας ότι γίνεται με διαπραγμάτευση κάνοντας ανταλλαγή μηνυμάτων.
   - Ο πελάτης απαντά με ένα μήνυμα ClientKeyExchange, το οποίο μπορεί να περιέχει το PreMasterSecret, το δημόσιο κλειδί, ή τίποτα. (Αυτό εξαρτάται από την επιλεγμένη κρυπτογραφική σουίτα) Το PreMasterSecret είναι

κρυπτογραφημένο με το δημόσιο κλειδί του πιστοποιητικού του εξυπηρετητή.

- Ο πελάτης και ο εξυπηρετητής μετά χρησιμοποιούν τους τυχαίους αριθμούς και το PreMasterSecret για να υπολογιστεί το κοινό μυστικό, που ονομάζεται «κύριο μυστικό». Όλα τα άλλα δεδομένα κλειδιού για τη σύνδεση αυτή προέρχονται από το «κύριο μυστικό», το οποίο περνά από μία προσεκτικά σχεδιασμένη ψευδοτυχαία συνάρτηση.

2. Ο πελάτης στέλνει το αρχείο **ChangeCipherSpec**, λέγοντας ουσιαστικά στον εξυπηρετητή, " Ότι σου πω από εδώ και πέρα θα είναι αυθεντικοποιημένο (και κρυπτογραφημένο, εάν οι παράμετροι κρυπτογράφησης έχουν δηλωθεί στο πιστοποιητικό του εξυπηρετητή)." Το αρχείο ChangeCipherSpec είναι ένα πρωτόκολλο επιπέδου αρχείου με τύπο περιεχομένου 20.
   - Τέλος, ο πελάτης στέλνει ένα αυθεντικοποιημένο και κρυπτογραφημένο μήνυμα Finished, που περιέχει τον κατακερματισμό και MAC σύμφωνα με τα προηγούμενα μηνύματα που ανταλλάχθηκαν.
   - Ο εξυπηρετητής θα προσπαθήσει να αποκρυπτογραφήσει το μήνυμα Finished του πελάτη και να επιβεβαιώσει τον κατακερματισμό και MAC. Εάν η αποκρυπτογράφηση ή η επιβεβαίωση αποτύχει, η ανταλλαγή μηνυμάτων θεωρείται αποτυχημένη η σύνδεση κλείνει.

3. Τέλος, ο εξυπηρετητής στέλνει το **ChangeCipherSpec**, λέγοντας στον πελάτη, "Ότι σου πω από εδώ και πέρα θα είναι αυθεντικοποιημένο (και κρυπτογραφημένο, εάν έχει διαπραγματευτεί κρυπτογράφηση)."
   - Ο εξυπηρετητής αποστέλλει το αυθεντικοποιημένο και κρυπτογραφημένο μήνυμά του Finished.
   - Ο πελάτης χρησιμοποιεί την ίδια αποκρυπτογράφηση και επιβεβαίωση.

4. Φάση εφαρμογής:

   Σε αυτό το σημείο, ανταλλαγή μηνυμάτων ολοκληρώνεται και το πρωτόκολλο εφαρμογής είναι ενεργοποιημένο, με τύπο περιεχομένου 23. Τα μηνύματα της εφαρμογής που ανταλλάχθηκαν μεταξύ του πελάτη και του εξυπηρετητή επίσης θα αυθεντικοποιηθούν και προαιρετικά κρυπτογραφηθούν ακριβώς σαν τον μήνυμα *Finished*. Αλλιώς, ο τύπος περιεχομένου θα επιστρέψει το 25 και ο πελάτης δεν θα αυθεντικοποιηθεί.

2.6. Ο ΠΑΓΚΟΣΜΙΟΣ ΙΣΤΟΣ – WORLD WIDE WEB

Μέχρι και τις αρχές της δεκαετίας του 1990, τον πληθυσμό του Internet αποτελούσαν κυρίως ακαδημαϊκοί, κυβερνητικοί και βιομηχανικοί ερευνητές. Αυτό άλλαξε όταν το 1989 στο **CERN**, το Ευρωπαϊκό Κέντρο Πυρηνικών

Ερευνών (European Laboratory for Particle Physics ή Conseil Europene pour la Recherche Nucleire) επινοήθηκε μια καινούργια εφαρμογή από τον φυσικό **Tim Berners-Lee**. Η εφαρμογή αυτή ονομάστηκε **Παγκόσμιος Ιστός WWW (World Wide Web)** και έφερε εκατομμύρια νέους, μη ακαδημαϊκούς χρήστες στο δίκτυο. Ο Tim Berners-Lee δεν άλλαξε τίποτα από τις υποκείμενες υπηρεσίες αλλά τις κατέστησε περισσότερο εύχρηστες. Το WWW μαζί με την πρώτη διεπαφή που δημιουργήθηκε για τον χρήστη, το Mosaic (Φεβρουάριος 1993) κατέστησε δυνατή τη δημιουργία, σε κάποιο μέρος, σελίδων πληροφορίας που περιέχουν κείμενο, εικόνες, ήχο ακόμη και βίντεο, με **παραπομπές (embedded links)** σ' άλλες σελίδες. Με ένα κλικ του ποντικιού πάνω στην παραπομπή, ο χρήστης μεταφέρεται ξαφνικά στη σελίδα που δείχνει η παραπομπή. Η ομάδα, λοιπόν, του CERN δημιούργησε ένα πρωτόκολλο βασισμένο σε **υπερ-κείμενο (hypertext)** που καθιστά δυνατή τη σύνδεση περιεχομένων στον ιστό χρησιμοποιώντας **υπερ-ζεύξεις (hyperlinks)**.

Η τεράστια δημοτικότητά του έγκειται στο γεγονός ότι έχει μία έγχρωμη γραφική διεπαφή, εύχρηστη από αρχάριους και παρέχει τεράστιο πλούτο πληροφοριών για κάθε πιθανό θέμα.

Σύμφωνα με τον ιδρυτή του ιστού, Tim Berners-Lee, "Το όνειρο που κρύβεται πίσω από τον παγκόσμιο ιστό είναι ένας κοινός χώρος / ένα κοινό διάστημα πληροφορίας, μες στον οποίο επικοινωνούμε μοιράζοντας πληροφορίες. Η παγκοσμιότητα του είναι ουσιώδης: ένα, **παραπομπή ή σύνδεσμος υπερκειμένου (hypertext link)** μπορεί να οδηγήσει, να δείξει σε οτιδήποτε, προσωπικό, τοπικό, σφαιρικό, πρόχειρο ή πολύ τελειοποιημένο."

2.6.1. Ποιος Ελέγχει τον Παγκόσμιο Ιστό;

Κανείς δεν ελέγχει τον Παγκόσμιο Ιστό (World Wide Web). Τα σημερινά συγγραφικά εργαλεία ιστοσελίδων (Web site authoring tools) επιτρέπουν ουσιαστικά σε καθέναν που έχει πρόσβαση σε κάποιον υπολογιστή και στο Internet να δημιουργήσουν μια ιστοσελίδα και να συμβάλλουν στον καθορισμό του τι είναι και τι κάνει. Υπάρχει όμως μια διεθνής οργάνωση, το λεγόμενο "**World Wide Web Consortium**" ή εν συντομία **W3C** που είναι αφιερωμένη στην περαιτέρω ανάπτυξη του Ιστού, την τυποποίηση των πρωτοκόλλων και την ενθάρρυνση της συνεργασίας μεταξύ των θέσεων Internet.

Πρόκειται για μια διεθνή ομάδα από εμπορικούς και ακαδημαϊκούς αντιπροσώπους που ελέγχει και επιβλέπει την ανάπτυξη των τεχνολογιών γύρω από τον Ιστό (web technology). Το 1994, το CERN και το M.I.T. (Massachusetts Institute of Technology's Laboratory for Computer Science) υπέγραψαν την συμφωνία για την ίδρυση του World Wide Web Consortium και διευθυντής της έγινε ο πατέρας του παγκόσμιου ιστού, Tim Berners-Lee.

Η οργάνωση δίνει πληροφορίες, κώδικα αναφοράς, πρωτότυπα και δείγματα εφαρμογών σε ερευνητές και χρήστες. Το M.I.T. διευθύνει το αμερικάνικο τμήμα του οργανισμού, το γαλλικό ερευνητικό κέντρο Institut National de Recherche en Informatique et en Automatique διευθύνει το ευρωπαϊκό τμήμα, και το Keio University Shonan Fujisawa Campus το Ιαπωνικό.

2.6.1.1 URI (Uniform Resource Identifier)

Κάθε πόρος που βρίσκεται στον Ιστό έχει ένα URI, δηλαδή Uniform Resource Identifier. Ένα URI μπορεί να είναι και URL (Uniform Resource Locator, or Web Address) ή κάποιο άλλο είδος ξεχωριστής αναγνώρισης. Σε αυτό το σημείο πρέπει να αναφερθεί ότι ένας αναγνωριστής δεν χρειάζεται κατ'ανάγκην να επιτρέπει την πρόσβαση σε έναν πόρο. Τα URI συστήματα έχουν οριστεί όχι μόνο ως Web Locations αλλά ακόμα για ποικίλα αντικείμενα όπως αριθμούς τηλεφώνου, αριθμούς ISBN και γεωγραφικές τοποθεσίες. Υπάρχει μια μεγάλη συζήτηση για την φύση του URI, ακόμα και αγγίζοντας φιλοσοφικά ερωτήματα, όπως για παράδειγμα τι είναι κατάλληλο μοναδικό αναγνωριστικό για ένα άτομο ή κάποιο άλλο αντικείμενο. Γενικά, υποθέτουμε ότι το URI είναι ένα αναγνωριστικό για διαδικτυακούς πόρους.

2.6.1.2 URN (Uniform Resource Identifier)

Ένα uniform resource name (URN) παρέχει λειτουργίες όπως το όνομα ενός ατόμου, καθώς και το uniform resource locator (URL) παρομοιάζεται με τη διεύθυνση ενός ατόμου. Με άλλα λόγια το URN ορίζει την ταυτότητα ενός αντικειμένου, ενώ το URL παρέχει μια μέθοδο για την εύρεση αυτού. Ένα URN είναι ένα URI που αναγνωρίζει έναν πόρο με βάση το όνομα σε ένα συγκεκριμένο namespace. Ένα URN μπορεί να χρησιμοποιηθεί για να επεξηγήσει έναν πόρο χωρίς να υπονοεί τη θέση του ή το πώς να αποκτήσει πρόσβαση.

Το International Standard Book Number (ISBN) αποτελεί ένα σύστημα μοναδικής αναγνώρισης βιβλίων παρέχει ένα τυπικό παράδειγμα για την χρήση των URN. Για παράδειγμα το ISBN 0-486-27557-4 καθορίζει απερίφραστα μια συγκεκριμένη έκδοση του έργου του Shakespeare για τον Ρομέο και την Ιουλιέτα. Το URN για αυτήν την έκδοση θα είναι urn:isbn:0-486-27557-4. Για να αποκτηθεί πρόσβαση σε αυτό και για να διαβαστεί το βιβλίο χρειάζεται η τοποθεσία για την οποία το URL θα πρέπει να έχει προσδιοριστεί.

2.6.1.3 URL (Uniform Resource Locator)

Κάθε πηγή πληροφορίας διαθέσιμη στον Ιστό – κάποιο έγγραφο HTML, εικόνα, βίντεο, πρόγραμμα κλπ. – έχει μία διεύθυνση που μπορεί να κωδικοποιηθεί από έναν Παγκόσμιο Αναγνωριστή Πόρων URI (***Universal Resource Identifier).***

Τα URIs ουσιαστικά αποτελούνται από τρία μέρη:

- Το ονομαστικό σχήμα του μηχανισμού που χρησιμοποιείται για την πρόσβαση στην πηγή πληροφοριών.
- Το όνομα της μηχανής που φιλοξενεί την πηγή.
- Το όνομα της ίδιας της πηγής, δοσμένη ως μονοπάτι.

Για παράδειγμα το URI που ορίζει την σελίδα του τμήματος της Πληροφορικής του Πανεπιστημίου: http://www.unipi.gr/cs. Αυτό το URI διαβάζεται ώς εξής: Υπάρχει ένα έγγραφο διαθέσιμο μέσω του πρωτοκόλλου HTTP, που βρίσκεται στη μηχανή www.unipi.gr και είναι προσβάσιμο μέσω του μονοπατιού "/cs". Άλλα σχήματα που μπορεί να συναντήσετε σε έγγραφα HTML είναι τα "mailto" για email και "ftp" για FTP.

Το παρακάτω είναι ένα ακόμα παράδειγμα ενός URI, που παραπέμπει στην ταχυδρομική θυρίδα ενός χρήστη:

> *...κείμενο...*
>
> For all comments, please send email to
>
> <A href="mailto:joe@someplace.com">Joe Cool</A>.

Ο όρος *"URL" είναι ένα υποσύνολο του γενικού ονομαστικού σχήματος URI.* Ο ομοιόμορφος εντοπιστής πόρων URL (Uniform Resource Locator) λειτουργεί περισσότερο σαν μία ταχυδρομική διεύθυνση ή διεύθυνση ηλεκτρονικού ταχυδρομείου. Όπως ακριβώς οι προαναφερθείσες διευθύνσεις περιέχουν ένα όνομα και μία τοποθεσία έτσι και το URL ή η διεύθυνση Web δείχνει το σημείο στο οποίο είναι τοποθετημένος ο υπολογιστής υποδοχής, τη θέση του δικτυακού τόπου στον host, το όνομα της ιστοσελίδας και τον τύπο του αρχείου κάθε εγγράφου. Ένα τυπικό URL έχει την παρακάτω μορφή:

> http://www.unipi.gr/cs/index.htm

Μεταφράζοντας τις εντολές του εν λόγω URL από αριστερά προς τα δεξιά θα μπορούσαμε να ακολουθήσουμε τα παρακάτω βήματα: "πήγαινε στον υπολογιστή υποδοχής που ονομάζεται unipi, στον φάκελο που ονομάζεται cs και ανάκτησε το έγγραφο με όνομα index.htm". Το URL δηλώνει στον browser το έγγραφο που πρέπει να φέρει και που ακριβώς θα το βρει σε κάποιον καθορισμένο host υπολογιστή που βρίσκεται κάπου στο Internet.

Το πρώτο τμήμα του URL δείχνει τον τύπο του πρωτοκόλλου μεταφοράς που χρησιμοποιείται για την ανάκληση του καθορισμένου εγγράφου. Το πλέον συνηθισμένο πρωτόκολλο για έγγραφα υπερκειμένου είναι το HTTP (Hypertext Transfer Protocol).

Το δεύτερο τμήμα του URL αναφέρεται σε έναν καθορισμένο host υπολογιστή στον οποίο βρίσκεται το έγγραφο που θα αναζητήσει ο browser. Το συγκεκριμένο τμήμα της διεύθυνσης ονομάζεται domain name.

Το τρίτο τμήμα του URL αντιστοιχεί στο directory του host υπολογιστή που περιέχει ένα καθορισμένο Web site ή πολλαπλά Web sites. Αυτό τοποθετείται αμέσως μετά την πρώτη μονή κάθετη γραμμή του URL και είναι ουσιαστικά ο υποκατάλογος του σκληρού δίσκου που φιλοξενεί το Web site. Στο σημείο αυτό της διεύθυνσης μπορεί να εμφανίζονται και υποκατάλογοι.

Το τελευταίο τμήμα του URL είναι το όνομα του αρχείου. Αν μια διεύθυνση δεν έχει filename εννοείται ότι το όνομα index.html περιλαμβάνει την σελίδα που έχει ζητηθεί. Το κείμενο που παραδίδει εξ' ορισμού ο Web server στον client όταν δεν παρουσιάζεται άλλο όνομα αρχείου είναι το index.html.

Ένα URL για ένα πρόγραμμα όπως ένα CGI Script, που είναι γραμμένο σε γλώσσα Perl θα έχει την ακόλουθη μορφή:

http://whatis.com/cgi-bin/comments.pl

Ένα URL για ένα αρχείο που θέλουμε να κατεβάσουμε στο δίσκο του υπολογιστή μας, απαιτεί το πρωτόκολλο "ftp" :

ftp://www.somecompany.com/whitepapers/widgets.ps

Μια γενική σύνταξη για τα URL είναι:

σχήμα://μηχανή φιλοξενίας. ονομασία χώρου [:πύλη]/*μονοπάτι/ όνομα αρχείου*

όπου σχήμα είναι ένα από τα:

file: ένα αρχείο στο τοπικό σύστημα.

ftp: ένα αρχείο σε κάποιον ανώνυμο εξυπηρετητή FTP.

http: ένα αρχείο στον Παγκόσμιο Ιστό.

gopher: ένα αρχείο σε έναν εξυπηρετητή Gopher.

WAIS: ένα αρχείο σε έναν εξυπηρετητή WAIS.

news: μια ομάδα ειδήσεων στο Usenet.

telnet: μια σύνδεση σε ένα απομακρυσμένο τερματικό.

Ο αριθμός της πύλης δεν είναι απαραίτητος συχνά. Αν δεν δοθεί, απλά παραλείπεται.

2.6.2. Η Πλευρά του Πελάτη

Για τους χρήστες, ο Ιστός αποτελεί μια παγκόσμια συλλογή εγγράφων με τη μορφή **σελίδων (pages)**. Κάθε τέτοια σελίδα μπορεί να περιέχει παραπομπές / δείκτες προς άλλες σελίδες, σχετικές με αυτές στον Ιστό. Οι χρήστες μπορεί να ακολουθήσουν μια παραπομπή, κάνοντας ένα απλό κλικ πάνω σε αυτή. Αυτή η διαδικασία μπορεί να συνεχιστεί, διασχίζοντας στην πορεία αυτή ενδεχομένως εκατοντάδες συνδεδεμένων σελίδων. Λέμε ότι οι σελίδες που παραπέμπουν σε άλλες σελίδες χρησιμοποιούν **υπέρ-κείμενο (hypertext).**

Οι συρμοί του κειμένου που αποτελούν παραπομπές προς άλλες σελίδες αποκαλούνται **υπερ-ζεύξεις (hyperlinks)** και απεικονίζονται με έντονο τρόπο, είτε με υπογράμμιση είτε με συγκεκριμένο χρώμα είτε και με τα δύο.

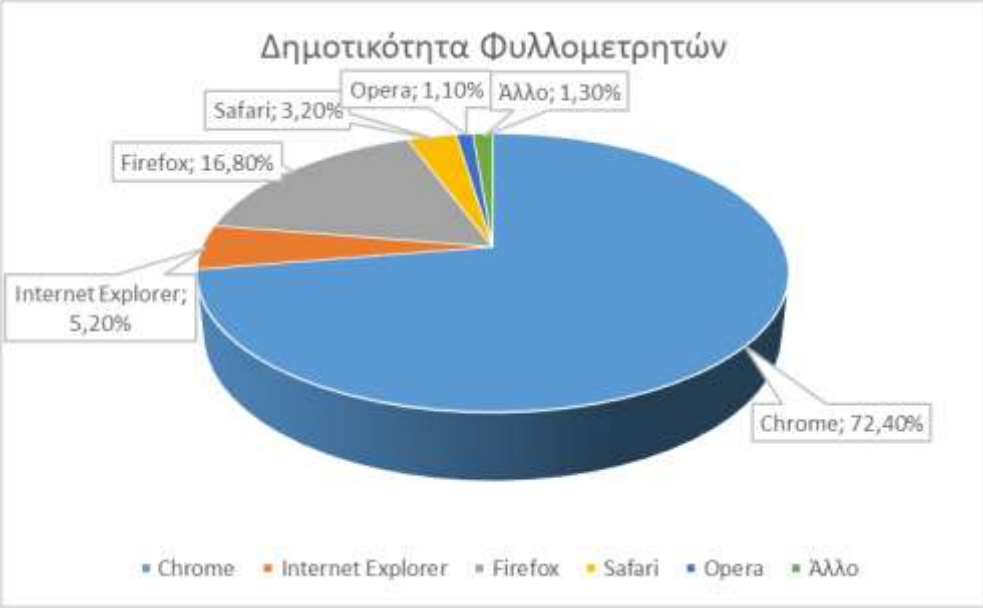
Τις σελίδες τις βλέπουμε με τη βοήθεια ενός προγράμματος που ονομάζεται **φυλλομετρητής (browser).** Το **Mosaic** ήταν η πρώτη διεπαφή με γραφικά και αναπτύχθηκε τον Φεβρουάριο του 1993 από τον Marc Andreessen στο National Center for Supercomputing Applications (Διεθνές Κέντρο Εφαρμογών για Υπερ-υπολογιστές). Το Mosaic ήταν τόσο δημοφιλές, ώστε ένα χρόνο αργότερα ο ίδιος ο Marc Andreessen, έφυγε από το National Center for Supercomputing Applications, για να ιδρύσει μια εταιρία, την Netscape Communications Corp., της οποίας στόχος ήταν η ανάπτυξη λογισμικού πελατών, εξυπηρετητών και εφαρμογών για τον Ιστό. Το **Netscape** ήταν το δεύτερο πιο δημοφιλές πρόγραμμα που αναπτύχθηκε.

2.6.2.1 Φυλλομετρητές (Browsers)

Στην αγορά πλέον υπάρχουν αρκετοί φυλλομετρητές που διεκδικούν ένα ισάξιο μερίδιο από την πίτα. Κάποιο από τους πιο δημοφιλείς φυλλομετρητές είναι ο Internet Explorer, ο Mozilla Firefox, Google Crome και Safari. Μαζί αυτοί αποτελούν το 90% (ή και περισσότερο) της χρήσης των φυλλομετρητών σήμερα.

Ο χώρος των φυλλομετρητών έχει στιγματιστεί από τους τρείς αυτούς ανταγωνιστές και τη μάχη τους για επικράτηση στην αγορά. Η προσπάθειά τους αυτή να είναι συνεχώς πιο καλοί από τον αντίπαλο είχε σαν αποτέλεσμα τη

δημιουργία μιας σειράς ιδιόκτητων στοιχείων της HTML (HTML tags), DHTML (Dynamic HTML) και πλεόν και HTML5, αλλά και η JavaScript και τα Cascading Style Sheets που χρησιμοποιούνται για τη μορφοποίηση των σελίδων. Βέβαια, αυτή η διαμάχη για την επικράτηση των φυλλομετρητών είχε και τη θετική πλευρά: οδήγησε σε ταχεία πρόοδο του μέσου γενικά.



Εικόνα 2.6.1. *Δημοτικότητα των φυλλομετρητών (Αύγουστος 2016)*

2.6.2.1.1 Internet Explorer

Ο Windows Internet Explorer (προηγουμένως γνωστός ως Microsoft Internet Explorer και με συντομογραφία MSIE), με συντομογραφία IE, είναι μια σειρά γραφικών προγραμμάτων περιήγησης στο διαδίκτυο, που αναπτύχθηκε από τη Microsoft και είναι μέρος του λειτουργικού συστήματος Microsoft Windows, με αφετηρία το 1995. Είναι το πιο ευρέως χρησιμοποιούμενο πρόγραμμα περιήγησης στο διαδίκτυο από το 1999, σε ποσοστό 95% του μεριδίου χρήσης μέσα στο 2002 και το 2003 με τον IE5 και τον IE6, αλλά με σταδιακή πτώση της χρήσης του από την κυκλοφορία του IE7.

Ο Internet Explorer πρωτοκυκλοφόρησε σαν πρόσθετο του Plus! for Windows 95. Οι επόμενες εκδόσεις διατίθενται ως δωρεάν στοιχεία λήψης και περιλαμβάνονται στις επισκευαστικές εκδόσεις OEM των Windows 95 και επόμενων εκδόσεων των

Windows. Μία ακόμα έκδοση του προγράμματος είναι η 10.0, η οποία διατίθεται ως δωρεάν ενημέρωση για τα Windows 7 με Service Pack 1 και τον Windows Server 2008 R2 με Service Pack 1 και περιλαμβάνεται στα Windows 8 σε metro ui και desktop. Μια ενσωματωμένη έκδοση OEM με την ονομασία Internet Explorer for Windows CE (IE CE) είναι επίσης διαθέσιμη για πλατφόρμες WinCE και βασίζεται προσωρινά στον IE6. Ένα άλλο πρόγραμμα περιήγησης για Windows CE/ Windows Mobile, γνωστό ως Internet Explorer Mobile, προέρχεται από διαφορετική βάση κώδικα και δεν πρέπει να συγχέεται με τις επιτραπέζιες εκδόσεις του προγράμματος. Ακόμη, στα Windows 10 παρουσιάστηκε μία εξελιγμένη έκδοση του Internet Explorer με την ονομασία Microsoft Edge, στην οποία έκδοση έχουν ενσωματωθεί επεκτάσεις που χρησιμοποιούνται σε άλλους φυλλομετρητές. Η καινοτομία σε αυτόν τον φυλλομετρητή έγκειται στο ότι έχει ενσωματωθεί το χαρακτηριστικό Cortana, το οποίο επιτρέπει την αναζήτηση στο διαδίκτυο με φωνητικές εντολές και ότι είναι συμβατή η χρήση του σε όλες τις συσκευές (υπολογιστές και κινητές συσκευές).

Εικόνα 2.6.2. *Παράθυρο πλοήγησης Internet Explorer*

2.6.2.1.2 Opera

Ο Opera Desktop είναι η βασική έκδοση του φυλλομετρητή βασίζεται πλέον στο πακέτο ανοιχτού κώδικά της Google, γνωστό ως Chromium της Google, το ίδιο πακέτο βασίζεται και ο Google Chrome. Λειτουργεί σε περιβάλλον Microsoft Windows, Mac OS X καθώς και η παλιά έκδοση 12 σε διανομές GNU/Linux, Unix, FreeBSD και παλιότερα Solaris.

Επίσης έχει λειτουργίες ad blocking, search plugins, δέχεται widget, έχει προστασία από phishing και malware, bookmark manager και έχει ορθογραφικό έλεγχο στα ελληνικά και σε πολλές άλλες γλώσσες. Λειτουργεί χωρίς πρόβλημα με τα plugins της Macromedia , Real Player, Microsoft Media Player, QuickTime, Acrobat Reader, Sun JAVA κλπ.

Είναι ο πρώτος browser που απέκτησε καρτέλες (tabs) ενώ αρκετές άλλες λειτουργίες του δεν υπάρχουν σε άλλους browsers ή υπάρχουν μόνο ως επεκτάσεις (add-ons). Η παλιά έκδοση του Opera παρείχε λειτουργίες ανάγνωσης e-mail μέσω POP3, ανάγνωση RSS Feed και κατέβασμα αρχείου μέσω του ενσωματωμένου BitTorrent, καθώς και πρόγραμμα επεξεργασίας ιστοσελίδων (Opera Drangonfly).

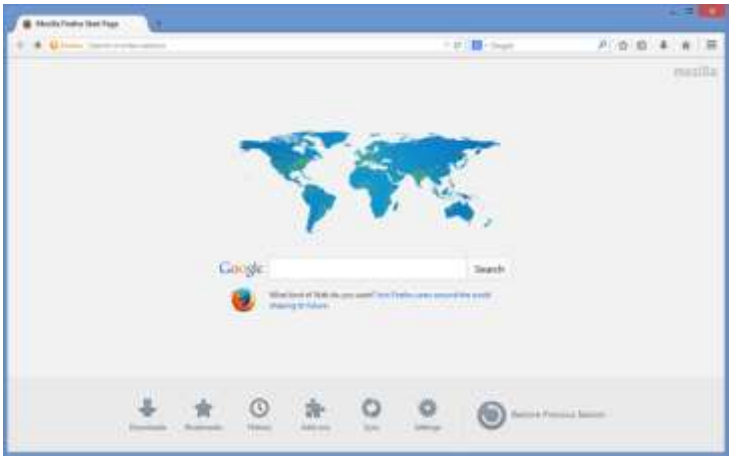
Εικόνα 2.6.3. *Παράθυρο πλοήγησης Opera*

2.6.2.1.3 Firefox

Ο Mozilla Firefox είναι ελεύθερος και ανοικτού κώδικα φυλλομετρητής (browser) του παγκόσμιου ιστού. Προήλθε από το Application Suite της Mozilla και η ανάπτυξή του εξακολουθεί να γίνεται κατά μεγάλο ποσοστό από την Mozilla Corporation, ενώ συνεισφέρουν και μεμονωμένοι χρήστες σε μικρότερο βαθμό. Ο Firefox κατείχε το 25% της καταγεγραμμένης χρήσης φυλλομετρητών Ιστού για τον Νοέμβριο του 2009, κατατάσσοντας τον στη δεύτερη θέση των πιο δημοφιλών φυλλομετρητών παγκοσμίως, μετά τον Internet Explorer.

Στις λειτουργίες του Firefox περιλαμβάνονται φραγή αυτόκλητα αναδυόμενων παραθύρων, περιήγηση με καρτέλες, ορθογραφικός έλεγχος, επιμέρους εύρεση, ενεργοί σελιδοδείκτες, διαχείριση των μεταφορτώσεων, ιδιωτική περιήγηση και ένα ενσωματωμένο πεδίο αναζήτησης με δυνατότητα επιλογής της επιθυμητής μηχανής αναζήτησης. Περαιτέρω λειτουργίες ενεργοποιούνται μέσω πρόσθετων που αναπτύχθηκαν από τρίτους. Τα πιο δημοφιλή από τα πρόσθετα είναι το NoScript που απενεργοποιεί τα σενάρια JavaScript, ο ενσωματωμένος στη γραμμή κατάστασης αναπαραγωγέας πολυμέσων FoxyTunes, το Adblock Plus που κάνει φραγή διαφημίσεων, το StumbleUpon, το DownThemAll! και η γραμμή εργαλείων Web Developer.

Για την απεικόνιση των ιστοσελίδων, ο Firefox χρησιμοποιεί τη μηχανή διάταξης Gecko, η οποία εφαρμόζει τα περισσότερα από τα σημερινά πρότυπα του Παγκόσμιου Ιστού αλλά και επιπλέον πρότυπα που θα ισχύουν στον μέλλον. Ο Firefox λειτουργεί σε αρκετές εκδόσεις των Microsoft Windows, στο Mac OS X, στο GNU/Linux, Android και σε πολλά λειτουργικά συστήματα που προήλθαν από το λειτουργικό Unix.



Εικόνα 2.6.4. *Παράθυρο πλοήγησης Mozilla Firefox*

2.6.2.1.4 Safari

Ο Safari είναι ένας φυλλομετρητής Web (Web browser) που παρέχεται με τους υπολογιστές Macintosh. Αρχικά εκδόθηκε στις 7 Ιανουαρίου του 2003 ως συνοδευτικό λογισμικό μαζί με το λειτουργικό σύστημα της εταιρίας Mac OS X, έγινε εντέλει ο προκαθορισμένος φυλλομετρητής στο Mac OS X v10.3. Είναι επιπλέον ο σύγχρονος φυλλομετρητής του Apple iPhone, του iPad και του iPod touch.

Εικόνα 2.6.5. *Παράθυρο πλοήγησης Safari*

2.6.2.1.5 Google Chrome

Το Google Chrome είναι πρόγραμμα περιήγησης στο Διαδίκτυο που αναπτύσσεται από την Google και χρησιμοποιεί τη μηχανή απεικόνισης WebKit. Κυκλοφόρησε στην έκδοση beta για Windows στις 2 Σεπτεμβρίου του 2008, ενώ η επίσημη σταθερή έκδοση κυκλοφόρησε στις 11 Δεκεμβρίου του 2008. Το όνομα προέρχεται από το πλαίσιο γραφικού περιβάλλοντος χρήστη, ή «χρώμιο», των φυλλομετρητών, κυκλοφορεί σε 3 εκδόσεις, Chrome (Browser), Chrome (Android), ChromeBox (OS), Chromebook (OS).

Ο Google Chrome είναι ο πρώτος περιηγητής που χρησιμοποιούν οι χρήστες παγκοσμίως, ξεπερνώντας κατά πολύ τον περιηγητή των Windows που για αρκετά χρόνια ήταν στην κορυφή. Χαρακτηριστικό είναι ότι η Google διαφημίζει τον περιηγητή στην αρχική σελίδα αναζήτησης κάθε φορά που δεν ανιχνεύεται.

Εικόνα 2.6.6. *Παράθυρο πλοήγησης Google Chrome*

2.6.2.2 Φυλλομετρητές & Ανάπτυξη Ιστοσελίδων

Οι περισσότεροι συγγραφείς ιστοσελίδων συμφωνούν, στο ότι η μεγαλύτερη πρόκληση (αλλά και ο πονοκέφαλος) όλων, κατά την σχεδίαση και ανάπτυξη μίας ιστοσελίδας ή μίας εφαρμογής Διαδικτύου, είναι η διαχείριση των ιδιαιτεροτήτων του κάθε φυλλομετρητή και της κάθε πλατφόρμας. Και αυτό γιατί καθένα υποστηρίζει και υλοποιεί με τον δικό του τρόπο τις εντολές HTML και τα διάφορα σενάρια.

Τα χαρακτηριστικά και οι δυνατότητες πληθαίνουν με κάθε νέα έκδοση φυλλομετρητών, κάτι που δε σημαίνει απαραίτητα ότι οι παλιότερες εκδόσεις θα εκλείψουν. Οι περισσότεροι σχεδιαστές τείνουν στο να μην δουλεύουν με τις πιο νέες εκδόσεις και τους καλύτερους φυλλομετρητές – πολλοί είναι απλά ενημερωμένοι για τις νέες εκδόσεις φυλλομετρητών και τις επιπρόσθετες δυνατότητες τους και κάποιοι άλλοι εργάζονται σε κάποια εταιρεία ή οργανισμό και χρησιμοποιούν τους υπολογιστές μαζί με τους φυλλομετρητές, που τους παρέχει η ίδια η εταιρεία.

Γνωρίζοντας ποιοι φυλλομετρητές χρησιμοποιούνται περισσότερο μας βοηθάει στο να αποφασίσουμε ποιες από τις τεχνολογίες να υιοθετήσουμε και που να τραβήξουμε τη γραμμή στο θέμα της συμβατότητας με προηγούμενες εκδόσεις.

Οι πιο σημαντικές στατιστικές είναι εκείνες που παίρνει κανείς από τη δική του σελίδα. Το λογισμικό παρακολούθησης του εξυπηρετητή τυπικά αναλύει και ταξινομεί της επισκέψεις της σελίδας σύμφωνα με τον φυλλομετρητή που κάνει την αίτηση. Έτσι, αν βρεθεί ότι μόνο το 20% των επισκεπτών χρησιμοποιεί την έκδοση 5.0 των φυλλομετρητών, τότε δεν θα ήταν καλό να χρησιμοποιηθεί κάποιο είδος σχεδίασης ή κάποια τεχνολογία που υποστηρίζεται μόνο στις νέες εκδόσεις.

2.6.2.3. Λειτουργία Φυλλομετρητών

Ένας φυλλομετρητής περιλαμβάνει το βασικό λογισμικό που χρειαζόμαστε προκειμένου να βρούμε, να λάβουμε, να δούμε και να αποστείλουμε πληροφορίες μέσω του Διαδικτύου. Περιέχει λογισμικό που μας επιτρέπει να:

- Στείλουμε και να λάβουμε μηνύματα ηλεκτρονικού ταχυδρομείου παγκόσμια σχεδόν ακαριαία.
- Διαβάσουμε μηνύματα από ομάδες ειδήσεων ή από μέρη διακίνησης ιδεών (newsgroups ή forums) για χίλια – πολλά θέματα που οι χρήστες του μοιράζονται και πληροφορίες και γνώμες / ιδέες.
- Ξεφυλλίσουμε τον παγκόσμιο ιστό, όπου βρίσκει κανείς μια πλούσια συλλογή πληροφοριών κειμένου, γραφικών και αλληλεπιδραστικής πληροφορίας.

Ο φυλλομετρητής προσκομίζει τη ζητούμενη σελίδα, ερμηνεύει το κείμενο και τις εντολές μορφοποίησης που περιέχονται σ' αυτό και απεικονίζει κατάλληλα τη σελίδα στην οθόνη.

Εκτός από το συνηθισμένο κείμενο (όχι υπογραμμισμένο) και το υπερ-κείμενο (υπογραμμισμένο), οι ιστοσελίδες μπορούν να περιέχουν εικονίδια, σχέδια, χάρτες και φωτογραφίες. Καθένα απ' αυτά μπορεί να συνδεθεί με μία άλλη σελίδα. Η επιλογή κάποιων απ' αυτά τα στοιχεία υποχρεώνει τον φυλλομετρητή να προσκομίσει την σελίδα στην οποία γίνεται η παραπομπή και την απεικονίσει, όπως ακριβώς και η επιλογή ενός κείμενο.

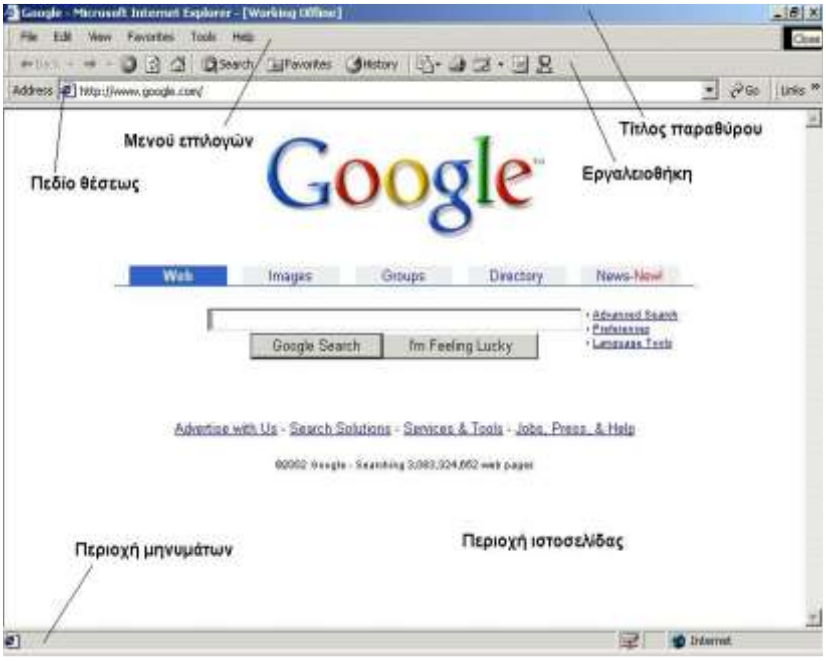
Δεν είναι δυνατό να δει κανείς όλες τις σελίδες με τον καθιερωμένο τρόπο. Κάποιες σελίδες περιέχουν κομμάτια ήχου, βιντεοκλίπ ή και τα δύο. Όταν συνυπάρχουν σελίδες υπερ-κειμένου με άλλα μέσα, τότε λέμε ότι έχουμε **υπερ-μέσα (hypermedia)**. Κάποιοι φυλλομετρητές μπορούν να απεικονίσουν όλα τα είδη υπερ-μέσων, κάποιοι άλλοι κοιτούν στο αρχείο διάρθρωσης για να δουν με ποιόν τρόπο θα χειρισθούν τα λαμβανόμενα δεδομένα. Συνήθως, το αρχείο διάρθρωσης δίνει το όνομα ενός προγράμματος που ονομάζεται **εξωτερικός απεικονιστής (external viewer)** ή **βοηθητική εφαρμογή (helper application),** που πρόκειται να τρέξει με την αφιχθείσα σελίδα ως είσοδο. Αν δεν έχει οριστεί κανένας απεικονιστής, ο φυλλομετρητής ζητά από τον χρήστη να διαλέξει έναν. Αν πάλι δεν υπάρχει απεικονιστής, ο χρήστης έχει τη δυνατότητα να πει στον φυλλομετρητή να σώσει την αφιχθείσα σελίδα σε κάποιο αρχείο στο δίσκο ή να την απορρίψει.

Για να λειτουργήσει ο φυλλομετρητής, η μηχανή πρέπει να είναι συνδεδεμένη με κάποιο τρόπο στο Διαδίκτυο. Αυτό είναι αναγκαίο, επειδή ο τρόπος με τον οποίο ο φυλλομετρητής προσκομίζει τη σελίδα είναι να εγκαταστήσει μια σύνδεση TCP με τη μηχανή όπου βρίσκεται η σελίδα και μετά να στείλει μήνυμα μέσω της σύνδεσης που να ζητά τη σελίδα.

2.6.2.4. Παρουσίαση ενός Φυλλομετρητή

Οι περισσότεροι φυλλομετρητές έχουν πολυάριθμα κουμπιά και δυνατότητες που κάνουν την πλοήγηση στον Ιστό ευκολότερη. Αρκετοί έχουν ένα κουμπί επιστροφής στην προηγούμενη σελίδα, ένα για προώθηση στην επόμενη σελίδα, που είναι σε λειτουργία μόνο όταν ο χρήστης έχει επιστρέψει απ' αυτήν, και ένα κουμπί για την απ' ευθείας μετάβαση στην **οικεία σελίδα (homepage)** του χρήστη. Οι περισσότεροι φυλλομετρητές έχουν ένα κουμπί ή κάποια επιλογή στο μενού (menu) για την τοποθέτηση **σελιδοδείκτη (bookmark)** σε μια δοθείσα σελίδα. Πολλές επιλογές και κουμπιά είναι διαθέσιμες για τον έλεγχο και τη ρύθμιση και ποικίλλουν ανάλογα με τον φυλλομετρητή.

Ο Φυλλομετρητής που χρησιμοποιείται πιο συχνά στο Internet είναι ο Internet Explorer της Microsoft. Παρέχει στον χρήστη ένα απλό γραφικό περιβάλλον της ακόλουθης μορφής.



Εικόνα 2.6.7. *Παρουσίαση του φυλλομετρητή «Microsoft Internet Explorer»*

Στις περισσότερες περιπτώσεις η κύρια οθόνη των πιο γνωστών φυλλομετρητών περιλαμβάνει τα παρακάτω τμήματα:

1. **Μπάρα τίτλου του παραθύρου (window title bar)**: Εμφανίζει τον τίτλο ή το URL του τρέχοντος υπερκειμένου.

2. **Κύριο μενού επιλογών (main menu)**: Επιτρέπει την ενεργοποίηση των επιλογών του φυλλομετρητή.
3. **Εργαλειοθήκη (toolbar)**: Έχει πλήκτρα για την ενεργοποίηση των σημαντικότερων λειτουργιών ενός φυλλομετρητή. Για τους δύο δημοφιλέστερους φυλλομετρητές του περιβάλλοντος των Windows, οι κυριότερες λειτουργίες της μπάρας εργαλείων αναλύονται στον πίνακα 2.6.1.

Πίνακας 2.6.1. *Λειτουργίες της μπάρας εργαλείων των φυλλομετρητών*

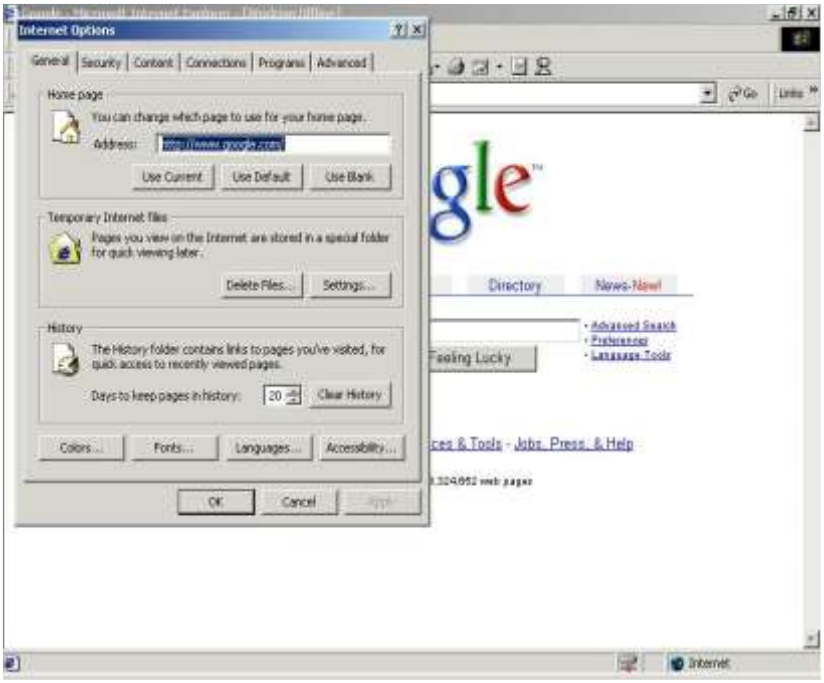
Πλήκτρο	**Λειτουργία**
Πίσω (Back)	Επιστροφή στην προηγούμενη ιστοσελίδα που επισκέφτηκε ο χρήστης.
Εμπρός (Forward)	Ανάκτηση της επόμενης ιστοσελίδας (είναι ενεργό μόνο όταν υπάρχει επόμενη σελίδα).
Αρχική (Home)	Ανάκτηση της ιστοσελίδας που ορίστηκε ως αρχική στον υπολογιστή του χρήστη.
Επαναφόρτωση	Επανάκτηση της τρέχουσας σελίδας από τον εξυπηρετητή ιστού.
Εκτύπωση (Print)	Εκτύπωση της τρέχουσας ιστοσελίδας.
Διακοπή (Stop)	Διακοπή φόρτωσης της ιστοσελίδας, από τον απομακρυσμένο εξυπηρετητή στον τοπικό υπολογιστή.
Αναζήτηση (Search)	Ενεργοποιεί τη διαδικασία αναζήτησης στον Ιστό.
Σελιδοδείκτες	Ενεργοποιεί τη διαδικασία της οργάνωσης και χρήσης των διαδικτυακών διευθύνσεων (URL) που ενδιαφέρουν τον χρήστη.

1. **Πεδίο θέσης**: Στο πεδίο αυτό (Address) εμφανίζεται το URL της τρέχουσας σελίδας. Επίσης, μπορεί σε αυτό το πεδίο να οριστεί και η διεύθυνση URL της σελίδας στην οποία θέλει να μεταβεί κανείς.
2. **Περιοχή ιστοσελίδας**: Στην περιοχή αυτή εμφανίζεται η τρέχουσα ιστοσελίδα.
3. **Περιοχή μηνυμάτων κατάστασης**: Στην περιοχή αυτή εμφανίζεται κείμενο που περιγράφει την τρέχουσα ιστοσελίδα ή δείχνει την κατάσταση

μεταφοράς της ιστοσελίδας από τον εξυπηρετητή στον τοπικό υπολογιστή. Όταν ο δείκτης του ποντικιού βρίσκεται πάνω σε έναν σύνδεσμο ή πάνω σε μια εικόνα που αποτελεί σύνδεσμο, τότε στην περιοχή αυτή εμφανίζεται το URL του αντίστοιχου συνδέσμου.

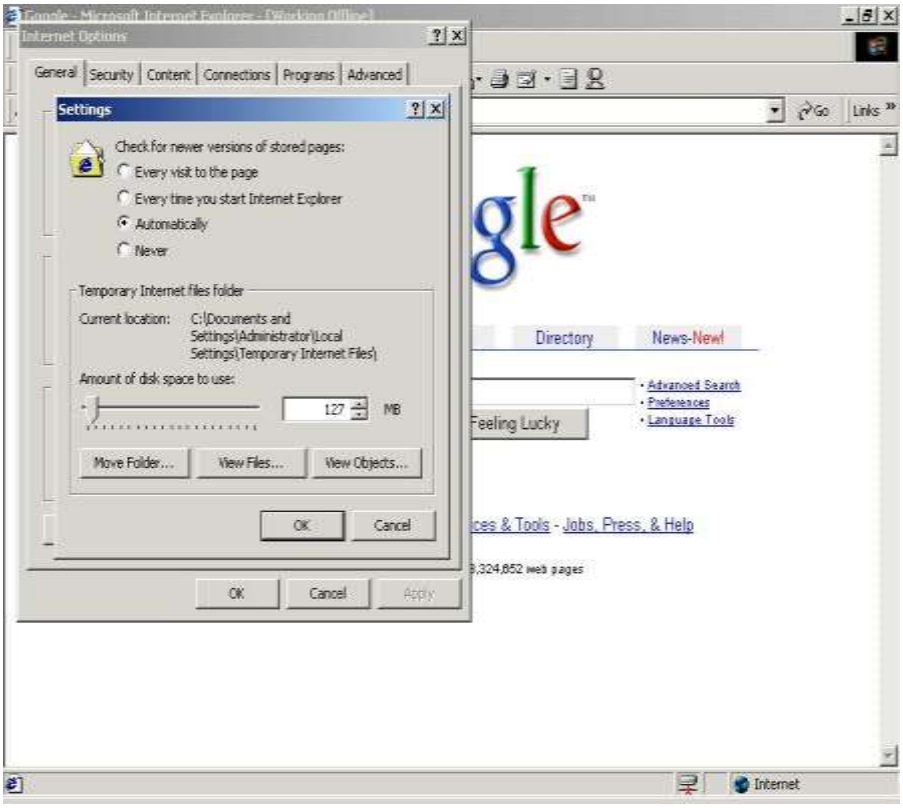
2.6.2.5. Ρύθμιση Φυλλομετρητή

Μπορεί να γίνουν κάποιες ρυθμίσεις σε ένα φυλλομετρητή, πηγαίνοντας στο μενού επιλογών στα **Εργαλεία (Tools) → Επιλογές Internet (Internet Options).** Στο παράθυρο που θα εμφανιστεί υπάρχουν διάφορες καρτέλες. Στην **Καρτέλα Γενικά (General tab)** συμπληρώνοντας το πεδίο **Διεύθυνση (Address)** μπορούμε να ορίσουμε την αρχική σελίδα του φυλλομετρητή, δηλαδή μπορεί να οριστεί η ιστοσελίδα που θα εμφανιστεί πρώτη όταν ενεργοποιηθεί ο φυλλομετρητής.



Εικόνα 2.6.8. *Το παράθυρο των ρυθμίσεων του «Microsoft Internet Explorer»*

Στη συνέχεια πατώντας στο κουμπί **Ρυθμίσεις (Settings)** μπορούμε να ορίσουμε την τοποθεσία αποθήκευσης του περιεχομένου των ιστοσελίδων που επισκεπτόμαστε, αλλά και το χώρο που θα καταλαμβάνει ο φάκελος αυτός στον υπολογιστή μας.



Εικόνα 2.6.9. *Επιπλέον ρυθμίσεις για τον «Microsoft Internet Explorer»*

Μπορούμε ακόμα να προσδιορίσουμε τον αριθμό των ημερών που θέλουμε να διατηρούνται στον υπολογιστή μας οι Διαδικτυακές διευθύνσεις (URL) των ιστοσελίδων που επισκεπτόμαστε, συμπληρώνοντας το πεδίο **Αριθμός ημερών για διατήρηση των σελίδων στο ιστορικό (Days to keep pages in history).**

Στο τέλος της καρτέλας **Γενικά** υπάρχουν κουμπιά με τα οποία έχουμε τη δυνατότητα να ορίσουμε το χρώμα που θα έχει το κείμενο, το φόντο, οι σύνδεσμοι που έχουμε αλλά και αυτοί που δεν έχουμε επισκεφτεί και να αλλάξουμε τη γραμματοσειρά, η οποία χρησιμοποιείται σε ιστοσελίδες που δεν έχουν ενσωματώσει συγκεκριμένη γραμματοσειρά.

2.6.3. Η Πλευρά του Εξυπηρετητή

Ένας **εξυπηρετητής** είναι κάποιος υπολογιστής που τρέχει ένα λογισμικό που του δίνει τη δυνατότητα να απαντά σε αιτήσεις για έγγραφα και άλλα δεδομένα. Τα προγράμματα που ζητούν και αναπαριστάνουν τα έγγραφα (όπως οι είναι

φυλλομετρητές) ονομάζονται **πελάτες**. Οι όροι όπως, "**στην πλευρά του πελάτη**" και "**στην πλευρά του εξυπηρετητή**", σε σχέση με ειδικές λειτουργίες / συναρτήσεις, αναφέρονται στο ποια μηχανή κάνει την επεξεργασία. Οι λειτουργίες / συναρτήσεις στην πλευρά του πελάτη συμβαίνουν στη μηχανή του χρήστη, ενώ οι λειτουργίες / συναρτήσεις στην πλευρά του εξυπηρετητή λαμβάνουν χώρα σε απομακρυσμένη μηχανή. Οι εξυπηρετητές Ιστού (Web servers) απαντούν σε αιτήματα φυλλομετρητών (πρόγραμμα πελάτη), ανακτούν το συγκεκριμένο αρχείο (ή εκτελούν ένα σενάριο όπως θα δούμε παρακάτω) και επιστρέφουν το έγγραφο ή τα αποτελέσματα του σεναρίου. Οι φυλλομετρητές και οι εξυπηρετητές επικοινωνούν διαμέσου του **HTTP**.

Θεμελιώδης αρχή στη λειτουργία του HTTP είναι η ιδέα πως αρχεία μπορούν να περιέχουν αναφορές σε άλλα αρχεία, η επιλογή των οποίων θα συμπεράνει επιπλέον αιτήσεις μεταφοράς. Κάθε εξυπηρετητής του Ιστού περιέχει, εκτός από τα αρχεία τύπου HTML και διάφορα άλλα αρχεία, όπως ένα δαίμονα HTTP, που είναι ένα πρόγραμμα σχεδιασμένο να περιμένει αιτήσεις HTTP και να τις επεξεργάζεται. Ο φυλλομετρητής είναι ένας πελάτης HTTP, που στέλνει αιτήσεις σε μηχανές εξυπηρετητές. Όταν ένας χρήστης του φυλλομετρητή εισάγει αιτήσεις αρχείων είτε ανοίγοντας ένα αρχείο (γράφοντας στο URL) είτε επιλέγοντας σε κάποιο σύνδεσμο υπερκειμένου, ο φυλλομετρητής θα σχηματίσει μια αίτηση HTTP και θα την αποστείλει στη διεύθυνση IP που υποδηλώνεται στο URL. Ο δαίμονας HTTP στη μηχανή προορισμού λαμβάνει το αίτημα και μετά από την απαραίτητη επεξεργασία, επιστρέφεται το ζητούμενο αρχείο.

2.6.3.1. Βασικές Λειτουργίες Εξυπηρετητών

2.6.3.1.1 Root directory

Όταν ένας φυλλομετρητής απαιτεί ένα έγγραφο, ο εξυπηρετητής το αναζητά, ξεκινώντας από τον αρχικό του κατάλογο εγγράφων (document root directory). Αυτός είναι ένας κατάλογος που έχει δημιουργηθεί και οριστεί ώστε να περιέχει όλα τα έγγραφα που πρόκειται να μοιραστεί διαμέσου του Ιστού. Ο αρχικός κατάλογος δεν εμφανίζεται απαραίτητα στο URL που δείχνει στο έγγραφο, έτσι είναι απαραίτητο να γνωρίζει κανείς ποιος είναι ο αρχικός κατάλογος όταν ανεβάζει τα αρχεία του στον εξυπηρετητή.

Για παράδειγμα, αν ο αρχικός κατάλογος στον εξυπηρετητή littlechair.com είναι /users/httpd/www/ και ο φυλλομετρητής ζητά το http://www.littlechair.com/super/cool.html, τότε ο εξυπηρετητής στην ουσία ανακτά /users/httpd/www/super/cool.html. Αυτό φυσικά είναι αόρατο στον χρήστη.

2.6.3.1.2 Index files

Το σύμβολο (/) στο τέλος ενός URL συμβολίζει ότι το URL δείχνει σε έναν κατάλογο και όχι σε κάποιο αρχείο. Γενικά, οι εξυπηρετητές εμφανίζουν το περιεχόμενο του καταλόγου που καθορίζει ένα URL. Οι περισσότεροι εξυπηρετητές είναι έτσι ορισμένοι ώστε να εμφανίζουν ένα συγκεκριμένο αρχείο, που καλείται **αρχείο δείκτη (index file)**, αντί να εμφανίζουν μια λίστα καταλόγου. Το αρχείο δείκτη ονομάζεται γενικά index.html, αλλά σε μερικούς εξυπηρετητές μπορεί να λέγεται και welcome.html ή default.html.

2.6.3.1.3 HTTP response header

Μόλις ο εξυπηρετητής βρει το αρχείο, στέλνει, πίσω στον φυλλομετρητή, κάποιες **HTTP επικεφαλίδες απόκρισης (HTTP response headers)** και τα περιεχόμενα του αρχείου. Οι επικεφαλίδες παρέχουν στον φυλλομετρητή πληροφορία για το αρχείο που λαμβάνει, συμπεριλαμβανομένου του **τύπου του μέσου (media type ή "content type" ή "MIME type")**. Συνήθως, ο εξυπηρετητής καθορίζει τη μορφή των αρχείων από την κατάληξη του αρχείου. Για παράδειγμα, το αρχείο με κατάληξη .gif θα αναγνωριστεί ως αρχείο εικόνας.

Ο φυλλομετρητής διαβάζει την πληροφορία στην επικεφαλίδα και αποφασίζει πώς θα χειριστεί το αρχείο, είτε παρουσιάζοντας / προβάλλοντας το στο παράθυρο είτε ανοίγοντας την κατάλληλη εφαρμογή.

2.6.3.1.4 Σενάρια CGI

Ένα URL μπορεί να ζητήσει να τρέξει ένα πρόγραμμα CGI, αντί να δείξει προς ένα αρχείο HTML. CGI σημαίνει **Συνηθισμένη Διεπαφή Πύλης (Common Gateway Interface)** και είναι αυτό που επιτρέπει στον εξυπηρετητή να επικοινωνήσει με άλλα προγράμματα (CGI scripts), που τρέχουν στον εξυπηρετητή. Τα σενάρια CGI μπορεί να είναι γραμμένα σε Perl, C, or C++ .

Τα σενάρια CGI μπορεί να χρησιμοποιηθούν για να εκτελεστούν μια σειρά από λειτουργίες / συναρτήσεις, όπως είναι η αναζήτηση, χειρισμός εικόνων-χαρτών (image maps) στην πλευρά του εξυπηρετητή. Οι περισσότεροι διαχειριστές εξυπηρετητών έχουν τη συνήθεια να αποθηκεύουν τα σενάρια CGI σε έναν κοινό κατάλογο με το όνομα cgi-bin (CGI-binaries), γεγονός που διευκολύνει τη διαχείριση και την ασφάλεια του εξυπηρετητή. Όταν ένας φυλλομετρητής ζητήσει κάποιο σενάριο CGI, ο εξυπηρετητής εκτελεί τη λειτουργία και επιστρέφει το δυναμικό περιεχόμενο στο φυλλομετρητή.

2.6.4. Τύποι Αρχείων στον Παγκόσμιο Ιστό

Από τη συζήτηση στα προηγούμενα κεφάλαια καθίσταται φανερό ότι η αναζήτηση από την πλευρά του πελάτη πληροφορίας από ένα εξυπηρετητή μπορεί να φέρει

πληροφορία η οποία είναι ήδη έτοιμη και προ-επεξεργασμένη στον επεξεργαστή ή πολλές φορές πληροφορία για την οποία ο επεξεργαστής πρέπει να τρέξει κάποιο πρόγραμμα. Μπορούμε να διακρίνουμε τρεις διαφορετικές τεχνολογίες στον τρόπο ανάκτησης και πρόσβασης σε πληροφορία στον παγκόσμιο ιστό.

α) **Στατικές σελίδες (static documents):** Είναι αρχεία στον εξυπηρετητή τα οποία δεν αλλάζουν μετά από τη συγγραφή τους. Τα αρχεία αυτά αποστέλλονται όπως είναι στον πελάτη.

β) **Δυναμικές σελίδες (dynamic documents):** Οι δυναμικές σελίδες ή δυναμικά αρχεία δεν υπάρχουν έτοιμα στην πλευρά του εξυπηρετητή, αλλά δημιουργούνται κάθε φορά που ένα φυλλομετρητής τα ζητάει. Όταν φτάσει η αίτηση ο εξυπηρετητής τρέχει ένα πρόγραμμα, την έξοδο του οποίου στέλνει στον πελάτη. Καθώς κάθε φορά τρέχει ένα πρόγραμμα κάθε αίτηση δεν λαμβάνει πάντα την ίδια απάντηση.

γ) **Ενεργά αρχεία (active documents):** Στην περίπτωση αυτή ο εξυπηρετητής δεν στέλνει κάποια απάντηση στον πελάτη για την αίτηση που έχει κάνει, αλλά του στέλνει το αντίγραφο ενός προγράμματος το οποίο πρέπει να τρέξει ο χρήστης τοπικά στον δικό του υπολογιστή. Το ενεργό αυτό πρόγραμμα μπορεί να αλληλεπιδρά με τον χρήστη και αλλάζει το τι εμφανίζεται συνεχώς.

Οι στατικές σελίδες είναι απλές, αξιόπιστες και γρήγορες στο φόρτωμα. Μπορεί να δημιουργηθούν χωρίς μεγάλη εμπειρία και άμα έχουν ελεγχθεί πλήρως κατά τη στιγμή της δημιουργίας τους ισχύουν για όσο καιρό υπάρχουν. Δεν μπορούν όμως να ανανεωθούν κάθε φορά που αλλάζει η πληροφορία. Για να γίνει αλλαγή πρέπει κάποιος να αλλάξει το αρχείο.

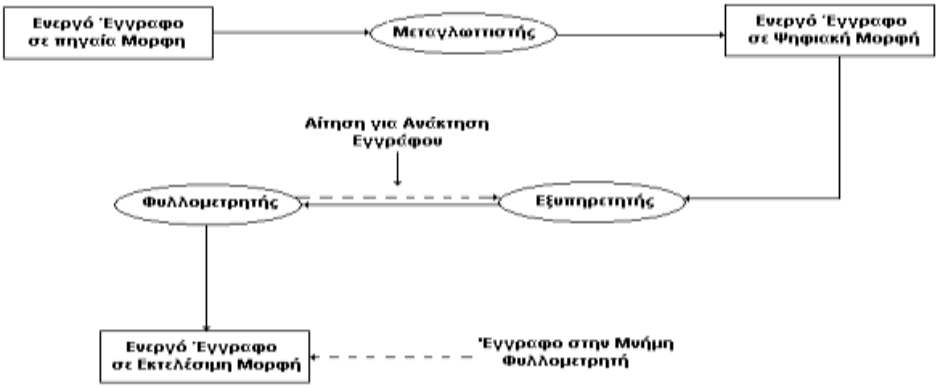
Για εφαρμογές που αλλάζουν τακτικά οι δυναμικές σελίδες παρέχουν μια αποτελεσματική λύση. Οι δυναμικές σελίδες μπορούν να μας ενημερώνουν π.χ. για τη θερμοκρασία ή την κίνηση σε μία δεδομένη χρονική στιγμή ή να μας μεταφέρουν τις πιο πρόσφατες τιμές του χρηματιστηριακού δείκτη. Για το σκοπό αυτό μόλις ζητηθεί η πληροφορία τρέχει ένα ειδικό πρόγραμμα. Ο πελάτης δεν καταλαβαίνει τη διαφορά στη σελίδα που λαμβάνει, λαμβάνει δηλαδή μια σελίδα HTML. Για να γραφούν τα προγράμματα αυτά στην πλευρά του εξυπηρετητή απαιτείται μεγαλύτερη εμπειρία από ότι στην περίπτωση των στατικών σελίδων. Επίσης απαιτείται ο εξυπηρετητής να είναι πιο γρήγορος και συνάμα ο πελάτης διαπιστώνει μια μεγαλύτερη καθυστέρηση.

Επειδή πολλές φορές η πληροφορία αλλάζει πολύ γρήγορα, σχεδιάστηκαν οι δυναμικές σελίδες όπου το πρόγραμμα τρέχει στην πλευρά του πελάτη. Έτσι ο πελάτης μπορεί να βλέπει πληροφορία που αλλάζει γρήγορα ή ακόμη και κινούμενη εικόνα, χωρίς να χρειάζεται να κάνει συνεχείς αιτήσεις στον εξυπηρετητή. Η δημιουργία και η χρήση των ενεργών σελίδων είναι πιο ακριβή

από τις άλλες δύο περιπτώσεις. Επίσης υπάρχει ένα πρόβλημα ασφάλειας καθώς το πρόγραμμα που έρχεται στον πελάτη εισάγει και εξάγει πληροφορία.

Για τη λειτουργία των δυναμικών σελίδων χρησιμοποιείται η τεχνολογία των CGI που αναφέρθηκε παραπάνω. Ο εξυπηρετητής πρέπει να μπορεί να χειρίζεται στατικές και δυναμικές σελίδες και να γνωρίζει ποιες σελίδες αντιστοιχούν σε δυναμικές ώστε να μπορεί να καλεί τα αντίστοιχα προγράμματα.

Για τα ενεργά αρχεία χρησιμοποιείται η τεχνολογία των Java applets. Για να λειτουργήσουν επιτυχώς πρέπει να τα έχουμε σε τρεις μορφές: την πηγαία μορφή, τη δυαδική και την εκτελέσιμη, όπως φαίνεται στην εικόνα 2.6.10. Οι τρεις αυτές τεχνικές – δηλαδή οι στατικές σελίδες, οι δυναμικές σελίδες και τα ενεργά αρχεία – θα παρουσιαστούν αναλυτικά στα επόμενα κεφάλαια του βιβλίου.



Εικόνα 2.6.10. *Οι τρεις μορφές των ενεργών αρχείων*

2.6.4.1. Στατικές έναντι Δυναμικών ιστοσελίδων

Συνοψίζοντας όσα έχουν αναφερθεί έως τώρα, διαπιστώνουμε ότι μια ιστοσελίδα δεν είναι τίποτα παραπάνω από ένα μέρος το οποίο παρέχει πληροφορίες για πολλούς χρήστες/ επισκέπτες που συνδέονται με αυτήν. Αυτό το μέρος ονομάζεται εξυπηρετητής Διαδικτύου και αποτελεί έναν μοναδικό τομέα (domain) όπου βρίσκονται αποθηκευμένα τα δεδομένα. Ο χρήστης στέλνει ένα αίτημα για πρόσβαση στα δεδομένα μέσω του πρωτοκόλλου HTTP. Ο εξυπηρετητής Διαδικτύου στέλνει την απάντηση στον χρήστη. Η απάντηση αυτή περιέχει τα δεδομένα με τη μορφή σήμανσης (markup). Αυτή η απόκριση ονομάζεται ιστοσελίδα. Αυτή η ιστοσελίδα μπορεί να έχει δημιουργηθεί από οποιαδήποτε γλώσσα σήμανσης όπως η HTML, η οποία παρουσιάζει περιεχόμενο, όπως κείμενο, εικόνες, κινούμενα σχέδια, συνδέσεις, ήχου, βίντεο κτλ.

Σημείωση: *«Ένας ιστότοπος είναι μια συλλογή από ιστοσελίδες που παρέχουν πληροφορίες για τον πελάτη/επισκέπτη ενός εξυπηρετητή μέσω του Διαδικτύου».*

Υπάρχουν στατικές και δυναμικές ιστοσελίδες που παρουσιάζουν η καθεμιά τους πλεονεκτήματα και μειονεκτήματα.

Στατικές ιστοσελίδες: - Οι στατικές ιστοσελίδες περιέχουν ορισμένο αριθμό σελίδων, η μορφοποίηση των οποίων είναι καθορισμένη. Το περιεχόμενο των σελίδων αυτών δεν μπορεί να αλλαχθεί χωρίς να γίνει απευθείας επεξεργασία του πηγαίου «κώδικα». Οπότε χρειάζεται στοιχειώδη γνώση της γλώσσας σήμανσης δηλαδή της HTML. Η δημιουργία τους μπορεί να πραγματοποιηθεί με τη χρήση ενός απλού κειμενογράφου.

Δυναμικές ιστοσελίδες: - Στις δυναμικές ιστοσελίδες το περιεχόμενό μπορεί να αλλαχθεί δυναμικά ενώ η ιστοσελίδα βρίσκεται στο φυλλομετρητή του επισκέπτη. Αυτού του είδους οι ιστότοποι χρησιμοποιούν τεχνικές προγραμματισμού στη πλευρά του εξυπηρετητή, όπως τη γλώσσα PHP, ώστε να τροποποιηθεί το περιεχόμενο δυναμικά. Οι δυναμικές ιστοσελίδες χρησιμοποιούν προγραμματισμό στη πλευρά του επισκέπτη για την μορφοποίηση/ παρουσίαση δυναμικού περιεχομένου και προγραμματισμό στη πλευρά του εξυπηρετητή για τη διαχείριση γεγονότων, συνδέσεων (session) και (cookies), καθώς και την αποθήκευση και την ανάκτηση δεδομένων από μια βάση δεδομένων.

Ο πίνακας 2.6.2. παρουσιάζει συνοπτικά τις διαφορές ανάμεσα σε στατικές και δυναμικές ιστοσελίδες.

Πίνακας 2.6.2. *Διαφορές στατικών και δυναμικών ιστοσελίδων*

Στατικές Ιστοσελίδες	*Δυναμικές Ιστοσελίδες*
Περιέχουν ορισμένο αριθμό σελίδων.	Ο αριθμός των σελίδων μπορεί να αυξηθεί κατά βούληση.
Ο σχεδιασμός των σελίδων είναι καθορισμένος.	Ο σχεδιασμός των σελίδων μπορεί να αλλάζει κατά βούληση.
Έχουν ταχύτερη εμφάνιση στον φυλλομετρητή του χρήστη, επειδή περιέχουν συνήθως απλό κείμενο.	Έχουν μεγαλύτερο χρόνο εμφάνισης καθώς απαιτείται επεξεργασία στη πλευρά του εξυπηρετητή και δημιουργία δυναμικού περιεχομένου.
Δε χρησιμοποιούν κάποια βάση δεδομένων.	Δημιουργούν δυναμικό περιεχόμενο με τη χρήση ερωταποκρίσεων στη βάση δεδομένων.

Είναι γενικά ασφαλείς καθώς η επικοινωνία είναι μονόδρομη από τον εξυπηρετητή στον χρήστη.	Οι δυναμικές ιστοσελίδες παρουσιάζουν θέματα ασφάλειας καθώς ο χρήστης μπορεί να αλλάζει δεδομένα στον εξυπηρετητή.
Χρησιμοποιούνται ώστε να παρέχουν πληροφορίες, όπως για π.χ. οργανισμούς και ιδρύματα.	Χρησιμοποιούνται σε περιπτώσεις που το περιεχόμενο αλλάζει συχνά, όπως π.χ. σε ηλεκτρονικά καταστήματα.
Για τη δημιουργία τους δεν απαιτείται η χρήση γλωσσών προγραμματισμού, μόνο σήμανσης και μορφοποίησης (HTML και CSS).	Για τη δημιουργία τους αλλά και τη λειτουργία τους απαιτούν τη χρήση πολυπλοκότερων μηχανισμών προγραμματισμού. Αυτοί οι μηχανισμοί μπορεί να εκτελούνται στην πλευρά του εξυπηρετητή, όπως π.χ. PHP, perl κτλ ή στην πλευρά του πελάτη, όπως javascript, κτλ.
Η δημιουργία τους είναι σχετικά εύκολη, καθώς από πλευράς ανάπτυξης απαιτείται γνώση της HTML και CSS.	Η ανάπτυξή, η διαχείρισή και η συντήρηση τους απαιτούν ικανότητες από πολλά γνωστικά αντικείμενα, όπως γλώσσες προγραμματισμού, βάσεις δεδομένων κτλ.
Η αλλαγή του περιεχομένου απαιτεί τη διαγραφή και φόρτωση της νέας σελίδας στον εξυπηρετητή. Απαιτούνται εξειδικευμένες γνώσεις.	Το περιεχόμενο μπορεί να τροποποιηθεί σχετικά εύκολα, καθώς υπάρχουν αυτοματοποιημένες διαδικασίες. Δεν απαιτούνται εξειδικευμένες γνώσεις.

2.7. ΕΠΑΝΑΛΗΠΤΙΚΕΣ ΑΣΚΗΣΕΙΣ - ΕΡΩΤΗΣΕΙΣ

2.7.1. ΕΡΩΤΗΣΕΙΣ

Υπάρχουν και άλλα διαδίκτυα εκτός από το Διαδίκτυο (Internet)	Σωστό
	Λάθος
Πριν την έλευση του WWW δεν υπήρχε τρόπος αναζήτησης στο Διαδίκτυο	Σωστό
	Λάθος
Πριν την έλευση του WWW δεν υπήρχε η δυνατότητα ηλεκτρονικού ταχυδρομείου στο Διαδίκτυο	Σωστό
	Λάθος
Το μοντέλο πελάτη εξυπηρετητή είναι αποκλειστικό χαρακτηριστικό του Διαδικτύου	Σωστό
	Λάθος
Τα δίκτυα ISDN διατίθενται σε ταχύτητες	128 kbps
	1,55 Mbps
	2,0 Mbps
	196 Kbps
Στο μοντέλο πελάτη – εξυπηρετητή	Ο εξυπηρετητής αναφέρεται σε συγκεκριμένο υπολογιστή με μεγάλη υπολογιστική ισχύ
	Ο εξυπηρετητής αναφέρεται σε ένα λογισμικό
	Ο υπολογιστής του πελάτη και του εξυπηρετητή είναι διαφορετικοί
	Ο πελάτης χρεώνεται για τις υπηρεσίες που του προσφέρονται
Το πρωτόκολλο IP υπάρχει πάντα σε μία σύνδεση με αρχιτεκτονική TCP/IP	Σωστό
	Λάθος
Το πρωτόκολλο TCP/IP υπάρχει πάντα σε μία σύνδεση με αρχιτεκτονική TCP/IP	Σωστό
	Λάθος

Οι διευθύνσεις στο Διαδίκτυο	Έχουν σταθερό μήκος
	Το μήκος τους εξαρτάται από το μέγεθος του δικτύου
	Έχουν μόνο τοπική σημασία
	Αντιστοιχούν απόλυτα στις αντίστοιχες τηλεφωνικές ενός οργανισμού
Οι πίνακες δρομολόγησης παραμένουν σταθεροί κατά τη διάρκεια μιας συνδιάλεξης (κλήσης)	Σωστό
	Λάθος
Το ανώνυμο ftp επιτρέπει	Την πρόσβαση σε οποιαδήποτε πληροφορία υπάρχει στον απομακρυσμένο υπολογιστή
	Την πρόσβαση μόνο σε ορισμένες πληροφορίες στον απομακρυσμένο υπολογιστή
	Την πρόσβαση μόνο σε εξουσιοδοτημένους χρήστες
Για να στείλουμε μήνυμα με ηλεκτρονικό ταχυδρομείο	Πρέπει να έχουμε πρόσβαση στον υπολογιστή του παραλήπτη
	Πρέπει ο υπολογιστής του παραλήπτη να είναι ανοικτός
	Αρκεί ο παραλήπτης να υπάρχει
	Να έχουμε πρόσβαση σε ένα πρόγραμμα αποστολής ηλεκτρονικού ταχυδρομείου
Ένα μήνυμα ηλεκτρονικού ταχυδρομείου	Μπορεί να μην έχει θέμα και κείμενο
	Μπορεί να μην έχει αποστολέα
	Μπορεί να μην έχει παραλήπτη
	Μπορεί να μην έχει ημερομηνία
Ένα μήνυμα ηλεκτρονικού ταχυδρομείου	Μπορεί να σταλεί σε περισσότερους από ένα παραλήπτες
	Μπορεί να σταλεί σε περισσότερους από ένα παραλήπτες χωρίς να το

	γνωρίζουν οι παραλήπτες
	Μπορεί να σταλεί σε περισσότερους από ένα παραλήπτες χωρίς να το γνωρίζουν όλοι οι παραλήπτες
Αν στείλετε ένα μήνυμα με ηλεκτρονικό ταχυδρομείο	Το μήνυμα που θα παραληφθεί θα έχει το ίδιο μέγεθος
	Το μήνυμα που θα παραληφθεί θα έχει μεγαλύτερο μέγεθος
	Το μήνυμα που θα παραληφθεί θα έχει μικρότερο μέγεθος
Το Διαδίκτυο δεν υφίσταται χωρίς το WWW	Σωστό
	Λάθος
Δεν μπορούμε να μπούμε στο Διαδίκτυο αν δεν έχουμε ένα φυλλομετρητή	Σωστό
	Λάθος
Οι στατικές σελίδες δημιουργούνται στην πλευρά του πελάτη	Σωστό
	Λάθος
Οι δυναμικές σελίδες δημιουργούνται στην πλευρά του εξυπηρετητή	Σωστό
	Λάθος
Οι δυναμικές σελίδες εμφανίζονται στην πλευρά του εξυπηρετητή	Σωστό
	Λάθος
Τα ενεργά αρχεία εκτελούνται στην πλευρά του πελάτη	Σωστό
	Λάθος

2.7.2. ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ

1. Επισκεφτείτε τους δικτυακούς τόπους εφημερίδων και τηλεοπτικών σταθμών και συζητήστε τις καινούριες δυνατότητες που προσφέρει το Διαδίκτυο.

2. Βρείτε την ιστορική εξέλιξη της τοπολογίας του Διαδικτύου. Παρουσιάστε το δίκτυο κορμού και τα διασυνδεδεμένα σε αυτό δίκτυα.

3. Βρείτε τη διαδικασία έγκρισης προτύπων από το IETF.

4. Αναφέρατε τα κυριότερα χαρακτηριστικά των μηχανών Archie και WAIS. Να τα συγκρίνετε με τα αντίστοιχα χαρακτηριστικά του παγκόσμιου ιστού.

5. Επισκεφτείτε την ιστοσελίδα του IETF και της IANA και αναφέρατε ποια είναι τα προβλήματα που αντιμετωπίζουν τη σημερινή εποχή.

6. Δημιουργείστε ένα πίνακα με τους παροχείς υπηρεσιών Διαδικτύου στην Ελλάδα, τις υπηρεσίες που προσφέρουν και τις τιμολογιακές τους πολιτικές.

7. Δώστε σύνθετες εξαρτήσεις σε περιβάλλοντα πελάτη εξυπηρετητή που οδηγούν σε προβληματικές επικοινωνίες.

8. Δώστε σε σχεδιαγράμματα το ρυθμό ανάπτυξης του Διαδικτύου και του παγκοσμίου ιστού (αριθμός χρηστών, αριθμός υπολογιστών υποδοχής, αριθμός ιστοσελίδων κ.λπ.)

9. Αναπτύξτε τα χαρακτηριστικά των εξυπηρετητών που αναφέρονται στο κεφάλαιο αυτό. Δώστε παραδείγματα προϊόντων που προσφέρουν τις υπηρεσίες αυτές.

10. Ποια είναι τα τελευταία πρότυπα για του IETF για το επίπεδο μεταφοράς;

11. Δώστε διαφορές της διευθυνσιοδότησης στο τηλεφωνικό σύστημα με τη διευθυνσιοδότηση στο Διαδίκτυο.

12. Βρείτε τη λίστα με όλες τις επιτρεπόμενες καταλήξεις στις διευθύνσεις στο Διαδίκτυο.

13. Δώστε παραδείγματα χρήσης των εντολών του ftp.

14. Βρείτε τρία προγράμματα ftp με εύχρηστες διεπαφές και συγκρίνετέ τα.

15. Βρείτε τρία προγράμματα ηλεκτρονικού ταχυδρομείου με εύχρηστες διεπαφές και συγκρίνετέ τα.

16. Βρείτε το πρότυπο του http και αναφέρατε τις κυριότερες λειτουργίες και εντολές του.

17. Συγκρίνετε τους φυλλομετρητές που αναφέρονται στο κεφάλαιο αυτό. Ποια χαρακτηριστικά επηρεάζουν την επιλογή ενός από αυτούς;

18. Να αναφέρετε εφαρμογές όπου είναι απαραίτητη η χρήση δυναμικών σελίδων και εφαρμογές όπου απαιτείται η χρήση ενεργών αρχείων.

19. Βρείτε τα RFCs που αφορούν τις κυριότερες υπηρεσίες του Διαδικτύου.

2.7.3. ΠΡΟΒΛΗΜΑΤΑ

1. Περιγράψτε τα βήματα που ακολουθεί η αποστολή ενός μηνύματος με ηλεκτρονικό ταχυδρομείο. Δείξτε το ρόλο των διαφόρων διευθύνσεων. Συγκρίνετε τη διαδικασία με αυτή της αποστολής ενός φακέλου μέσω του κλασικού ταχυδρομείου και με την αποστολή ενός μηνύματος μέσω του κινητού τηλεφώνου. Οι διαδικασίες αυτές είναι με σύνδεση ή χωρίς σύνδεση (προσοχή στη χρήση των όρων αυτών στην κινητή τηλεφωνία);

2. Να συγκρίνετε το DNS με τη χρήση του καταλόγου για την εύρεση τηλεφωνικών αριθμών.

3. Ένα μηχάνημα είναι συνδεδεμένο σε δύο δίκτυα. Γιατί χρειάζεται διαφορετική διεύθυνση IP για κάθε σύνδεση.

4. Υποθέστε ότι χρησιμοποιείται κάποιον φυλλομετρητή και επισκέπτεστε κάποιον δικτυακό τόπο (Site). Στη συνέχεια, επιλέγεται με το 'ποντίκι' μία παραπομπή (Hyperlink) προς κάποια ιστοσελίδα. Περιγράψτε τη διαδικασία που ακολουθεί μέχρι να φορτωθεί η ιστοσελίδα στον φυλλομετρητή σας. Τι γίνεται στην περίπτωση όπου η ιστοσελίδα περιέχει κάποιες εικόνες ή κάποια Java Applets;

5. Φανταστείτε ότι δουλεύετε σε μια εταιρεία που παράγει και τυποποιεί πολυμεσικές εφαρμογές. Να εξηγήσετε, λαμβάνοντας υπόψη τη λειτουργία των πρωτοκόλλων TCP και UDP, ποιο από τα δύο πρωτόκολλα μεταφοράς θα επιλέγατε για την υποστήριξη των πολυμεσικών εφαρμογών (π.χ. μεταφορά αρχείων βίντεο, διαμέσου του Διαδικτύου) και για ποιο λόγο.

6. Να εντοπιστούν τα κυριότερα μειονεκτήματα του πρωτοκόλλου IP, όσο αφορά την χρήση του σε εφαρμογές πραγματικού χρόνου.

7. Να συμπληρώσετε τα κενά στον παρακάτω πίνακα:

Διεύθυνση IP σε δυαδικό σύστημα	**Διεύθυνση IP σε δεκαδικό σύστημα**	**Κλάση διεύθυνσης IP**
	133.88.4.66	
11100011 11100110 01000100 00000111		
01000001 10001000 00011001 00011101		
	231.17.22.3	
10000100 00001100 11100010 00100111		
01100110 00111001 00011001 10010111		
	34.89.245.30	
11001100 00111000 10101101 11001010		
	128.17.222.72	

8. Να μετατρέψετε σε δυαδική μορφή τις ακόλουθες διευθύνσεις:

197.228.72.0, 195.251.230.15, 127.34.140.1, 161.0.10.32, 178.18.23.255,

10.232.0.0, 10.2.0.37

- Ποιες από τις παραπάνω διευθύνσεις είναι διευθύνσεις εκπομπής, ποιες διευθύνσεις δικτύου και ποιες διευθύνσεις υπολογιστών;
- Μπορεί η διεύθυνση 255.255.184.0 να είναι μία μάσκα δικτύου; Δικαιολογήστε

9. Ένα δίκτυο κλάσης Β έχει μάσκα υποδικτύου 255.255.224.0. Πόσα διαφορετικά υποδίκτυα και πόσους δυνατούς hosts μπορούμε να έχουμε.

10. Έστω ότι έχουμε ένα δίκτυο κλάσης Β με διεύθυνση 170.228.0.0 και θέλουμε να δημιουργήσουμε 8 υποδίκτυα.
    - Πόσα επιπλέον bits πρέπει να χρησιμοποιήσουμε, από την υπάρχουσα μάσκα δικτύου, για τη δημιουργία αυτών των υποδικτύων;
    - Ποια θα είναι η μάσκα των υποδικτύων και ποια τα υποδίκτυα αυτά;
    - Βρείτε σε ποια υποδίκτυα ανήκουν οι υπολογιστές με διευθύνσεις 170.228.40.10 και 170.228.200.4;

11. Σε ένα δίκτυο κλάσης Γ με διεύθυνση 195.230.251.0 ορίζουμε 4 υποδίκτυα. Πόσους υπολογιστές μπορούμε να έχουμε σε κάθε υποδίκτυο. Για κάθε υποδίκτυο γράψτε 2 παραδείγματα IP διευθύνσεων υπολογιστών που ανήκουν σ' αυτό.

12. Ανατρέξτε στο Διαδίκτυο που εμφανίζεται στην εικόνα 2.4.6. Φανταστείτε και σχεδιάστε τον πίνακα δρομολόγησης των δύο δρομολογητών της εικόνας.

13. Γράψτε ένα πρόγραμμα που να διαβάζει μια διεύθυνση IP σε δεκαδική μορφή και να δίνει το ισοδύναμό της σε δυαδική μορφή, να αποφασίζει την κλάση, το υποδίκτυο και τον υπολογιστή υποδοχής.

14. Γιατί κάθε δρομολογητής πρέπει να έχει τη δική του διεύθυνση; Γιατί έχει περισσότερες από μία διευθύνσεις; Θα μπορούσε κάθε υπολογιστής και όχι κάθε δικτυακή σύνδεση να έχει τη δική της διεύθυνση;

15. Αν ένα αυτοδύναμο πακέτο για να φτάσει στον προορισμό του περνάει μέσα από Ν δρομολογητές πόσες φορές θα κομματιαστεί στην χειρότερη περίπτωση;

16. Εξηγήστε πώς μπορεί μια εφαρμογή πελάτη να αιτείται υπηρεσίες από περισσότερους από έναν εξυπηρετητές.

17. Δώστε ένα παράδειγμα όπου ένας εξυπηρετητής για να ολοκληρώσει μια εργασία γίνεται πελάτης ενός άλλου εξυπηρετητή.

18. Σε κάποιον δρομολογητή, φθάνει ένα αυτοδύναμο πακέτο IP το οποίο φέρει διεύθυνση προορισμού 135.43.56.218.
    i. Σε ποια κλάση ανήκει η παραπάνω διεύθυνση;
    ii. Να γράψετε ποια θα είναι η διεύθυνση του δικτύου η του υποδικτύου που θα προκύψει, αν ο δρομολογητής φιλτράρει το πακέτο με βάση τις εξής μάσκες: α) 255.255.0.0, β) 255.255.255.0, γ) 255.255.134.0, δ) 255.236.0.0 και ε) 255.124.54.0.
    iii. Ποιες από τις παραπάνω περιπτώσεις μασκών αφορούν υποδίκτυα και ποιες αφορούν υποδίκτυα.
    iv. Φτιάξτε ένα σχεδιάγραμμα της επιλογής σας, το οποίο να αντιστοιχεί στην περίπτωση της μάσκας 255.255.134.0. Προφανώς, στο σχεδιάγραμμα θα απεικονίζονται κάποια δίκτυα ή υποδίκτυα με τις διευθύνσεις τους. Θα πρέπει επίσης να φαίνεται το δίκτυο ή υποδίκτυο στο οποίο τελικά θα παραδοθεί το αυτοδύναμο πακέτο IP.

19. Σε έναν δρομολογητή καταφθάνουν αυτοδύναμα πακέτα IP με διευθύνσεις προορισμού που ανήκουν στη δεύτερη κλάση. Ο δρομολογητής τα φιλτράρει κάνοντας χρήση της μάσκας 255.255.107.0.
    i. Υποστηρίζει η μάσκα αυτή υποδίκτυα;
    ii. Αν η μάσκα, υποστηρίζει υποδίκτυα, ποιος είναι ο μέγιστος αριθμός υποδικτύων που μπορεί να εξυπηρετεί ο δρομολογητής χρησιμοποιώντας αυτή τη μάσκα;
    iii. Πόσα, το πολύ, τελικά συστήματα μπορούν να είναι συνδεδεμένα στο κάθε υποδίκτυο;

2.8. Παράρτημα Α

Ακολουθεί τμήμα ανταλλαγής πακέτων μεταξύ υπολογιστή πελάτη και διακομιστή (client/server)

```
//----- Ether Header -----
ETHER:
ETHER:  Packet 414 arrived at 16:39:17.41
ETHER:  Packet size = 62 bytes
ETHER:  Destination = 8:0:20:8f:18:b1, Sun
ETHER:  Source      = 0:10:a6:6e:50:82,
ETHER:  Ethertype = 0800 (IP)
ETHER:
//----- IP Header -----
IP:
IP:   Version = 4
IP:   Header length = 20 bytes
IP:   Type of service = 0x00
IP:         xxx. .... = 0 (precedence)
IP:         ...0 .... = normal delay
IP:         .... 0... = normal throughput
IP:         .... .0.. = normal reliability
IP:   Total length = 48 bytes
IP:   Identification = 49085
IP:   Flags = 0x4
IP:         .1.. .... = do not fragment
IP:         ..0. .... = last fragment
IP:   Fragment offset = 0 bytes
IP:   Time to live = 62 seconds/hops
IP:   Protocol = 6 (TCP)
IP:   Header checksum = 1cbf
IP:   Source address = 195.251.95.100, 195.251.95.100
IP:   Destination address = 143.233.173.2, phaethon
IP:   No options
IP:
// ----- TCP Header -----
TCP:
TCP:  Source port = 1081
TCP:  Destination port = 21 (FTP)
TCP:  Sequence number = 2727492842
```

```
TCP:  Acknowledgement number = 0
TCP:  Data offset = 28 bytes
TCP:  Flags = 0x02
TCP:        ..0. .... = No urgent pointer
TCP:        ...0 .... = No acknowledgement
TCP:        .... 0... = No push
TCP:        .... .0.. = No reset
TCP:        .... ..1. = Syn
TCP:        .... ...0 = No Fin
TCP:  Window = 8760
TCP:  Checksum = 0x1cd1
TCP:  Urgent pointer = 0
TCP:  Options: (8 bytes)
TCP:    - Maximum segment size = 1460 bytes
TCP:    - No operation
TCP:    - No operation
TCP:    - Option 4 (unknown - 0 bytes)
TCP:
// ----- FTP:   -----
FTP:
FTP:  ""
FTP:

// ----- Ether Header -----
ETHER:
ETHER:  Packet 415 arrived at 16:39:17.41
ETHER:  Packet size = 58 bytes
ETHER:  Destination = 0:10:a6:6e:50:82,
ETHER:  Source      = 8:0:20:8f:18:b1, Sun
ETHER:  Ethertype = 0800 (IP)
ETHER:
// ----- IP Header -----
IP:
IP:   Version = 4
IP:   Header length = 20 bytes
IP:   Type of service = 0x00
IP:         xxx. .... = 0 (precedence)
IP:         ...0 .... = normal delay
IP:         .... 0... = normal throughput
```

```
IP:       .... .0.. = normal reliability
IP:   Total length = 44 bytes
IP:   Identification = 35845
IP:   Flags = 0x4
IP:       .1.. .... = do not fragment
IP:       ..0. .... = last fragment
IP:   Fragment offset = 0 bytes
IP:   Time to live = 255 seconds/hops
IP:   Protocol = 6 (TCP)
IP:   Header checksum = 8f7a
IP:   Source address = 143.233.173.2, phaethon
IP:   Destination address = 195.251.95.100, 195.251.95.100
IP:   No options
IP:
// ----- TCP Header -----
TCP:
TCP:  Source port = 21
TCP:  Destination port = 1081
TCP:  Sequence number = 3909527894
TCP:  Acknowledgement number = 2727492843
TCP:  Data offset = 24 bytes
TCP:  Flags = 0x12
TCP:       ..0. .... = No urgent pointer
TCP:       ...1 .... = Acknowledgement
TCP:       .... 0... = No push
TCP:       .... .0.. = No reset
TCP:       .... ..1. = Syn
TCP:       .... ...0 = No Fin
TCP:  Window = 8760
TCP:  Checksum = 0x9f69
TCP:  Urgent pointer = 0
TCP:  Options: (4 bytes)
TCP:    - Maximum segment size = 1460 bytes
TCP:
// ----- FTP:   -----
FTP:
FTP:  ""
FTP:
```