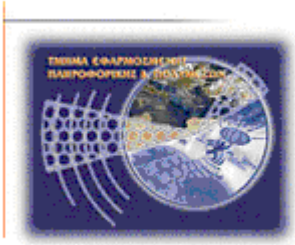
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων



Πτυχιακή εργασία

Ασφάλεια σε διομότιμα δίκτυα

Γιακουμιδάκης Ανδρέας (ΑΜ: 1985)
E-mail: Ks4d3rfos@hotmail.com

Ηράκλειο – 12/7/2010

Επόπτης Καθηγητής: Δρ. Μανιφάβας Χαράλαμπος

Γιακουμιδάκης Ανδρέας

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

Ιστορικό εκδόσεων

Ημερομηνία	**Έκδοση**	**Συγγραφέας**	**Λεπτομέρειες**
12/01/2010	Version.1	Γιακουμιδάκης Ανδρέας	2ο Κεφάλαιο
31/01/2010	Version.2	Γιακουμιδάκης Ανδρέας	3ο Κεφάλαιο
07/02/2010	Version.3	Γιακουμιδάκης Ανδρέας	2ο & 3ο Κεφάλαιο
17/02/2010	Version.4	Γιακουμιδάκης Ανδρέας	2ο & 3ο Κεφάλαιο
01/03/2010	Version.5	Γιακουμιδάκης Ανδρέας	2ο & 3ο & 4ο Κεφάλαιο
1/06/2010	Version.6	Γιακουμιδάκης Ανδρέας	2ο & 3ο & 4ο & 5ο Κεφάλαιο
28/06/2010	Version.7	Γιακουμιδάκης Ανδρέας	1ο &2ο & 3ο & 4ο & 5ο Κεφάλαιο
12/07/2010	Version.8	Γιακουμιδάκης Ανδρέας	1ο &2ο & 3ο & 4ο & 5ο Κεφάλαιο
12/07/2010	Version.9	Γιακουμιδάκης Ανδρέας	1ο &2ο & 3ο & 4ο & 5ο Κεφάλαιο

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή της πτυχιακής εργασίας μου, Δρ. Μανιφάβα Χαράλαμπο. Οι οδηγίες του, οι υποδείξεις του και η κατανόηση που έδειξε κατά τη συγγραφή της εργασίας αποτέλεσαν καθοριστικά στοιχεία για την εκπόνησή της. Ήταν μεγάλη τιμή για εμένα να συνεργαστώ μαζί του.

Θα ήθελα επίσης να εκφράσω την ευγνωμοσύνη μου στην οικογένεια μου και στους ανθρώπους που είχα δίπλα μου όλη αυτήν την περίοδο.

Περίληψη

Με αφορμή την έξαρση των εφαρμογών peer to peer την πρώτη δεκαετία του 2010, γίνεται σε αυτή την πτυχιακή μια παρουσίαση της κατάστασης σε παγκόσμια κλίμακα των εν λόγω εφαρμογών. Γίνεται μια ιστορική αναδρομή σε περιόδους ακμής αλλά και παρακμής των peer to peer εφαρμογών και της χρησιμότητας τους στον παγκόσμια διαδικτυακή κοινότητα. Παράλληλα τονίζονται θέματα και προβλήματα άξια προσοχής από μελλοντικούς developers.Επίσης η πτυχιακή αυτή ασχολείται με μια από τις δημοφιλέστερες peer to peer εφαρμογές και αναλυτικά παρουσιάζει δυνατά σημεία αλλά και αδυναμίες της .Κατόπιν ως επαλήθευση των ήδη αναφερθέντων γίνεται μια επισκόπηση στατιστικών στοιχείων τα οποία καλύπτουν ένα πολύ ευρύ φάσμα της διομότιμης δραστηριότητας, παρουσιάζοντας ως επί το πλείστον κενά ασφαλείας και άλλα προβλήματα. Τέλος μια σχετικά πρόσφατη μόδα , η JXTA τεχνολογία , αναλύεται ,αναφέρονται τα κύρια πλεονεκτήματά της και η δομή της ενώ σε πρακτική εφαρμογή βλέπουμε και κατανοούμε πως αναπτύσσονται βασικά στοιχεία της με τη χρήση Java.

Abstract

In light of the rise of peer to peer applications in the first decade of the 21st century, this is a graduate of the situation worldwide in such applications. A review to times of prosperity and decline of peer to peer applications and the usefulness to the global Internet community is being done, while highlighting issues and problems worthy of attention from prospective developers. In Addition, the thesis deals with one of the most popular peer to peer applications and presents it's strengths and weaknesses. Afterwards a verification of those already mentioned is given through an overview of statistics which cover a very wide range of world-peer2peer activity showing mostly security flaws and other problems. Finally, a relatively recent fashion, JXTA technology is analyzed, and it indicates the main strengths and structure and in practice we shall see and understand how key elements of this technology are being developed through the use of Java.

Περιεχόμενα

Εικόνες

Πίνακες

Κεφάλαιο 1

1.1 Φορέας

Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology [NIST]) ανέπτυξε αυτό το έγγραφο ως προαγωγή των θεσπισμένων ευθυνών του κάτω από την Ομοσπονδιακή Πράξη Διαχείρισης Ασφάλειας της Πληροφορίας (Federal Information Security Management Act [FISMA]) του 2002, Δημόσιος Νόμος (Ηνωμένων Πολιτειών της Αμερικής) 107-347.

Το NIST είναι υπεύθυνο για την ανάπτυξη προτύπων και οδηγιών, συμπεριλαμβανομένου των ελαχίστων απαιτήσεων για την παροχή επαρκών πληροφοριών ασφάλειας για όλες τις συντελεστικές λειτουργίες και στοιχεία, αλλά τέτοια πρότυπα και οδηγίες δεν απευθύνονται σε συστήματα εθνικής ασφάλειας. Αυτές οι οδηγίες είναι σύμφωνες με τις απαιτήσεις της εγκυκλίου Α-130 του Υπουργείου Οικονομίας και Διοίκησης (Office of Management and Budget [OMB]) των Ηνωμένων Πολιτειών της Αμερικής, ενότητα 8b(3), "*Securing Agency Information Systems*", όπως αναλύεται στην ενότητα Α-130, Παράρτημα IV: *Analysis of Key Sections*.

Αυτές οι οδηγίες είναι προετοιμασμένες για χρήση από Ομοσπονδιακούς παράγοντες. Μπορούν να χρησιμοποιηθούν από μη-κυβερνητικούς οργανισμούς σε εθελούσια βάση και δεν αποτελούν αντικείμενο κατοχύρωσης πνευματικών δικαιωμάτων (copyright), αν και η συμβολή στο συνολικό έργο είναι επιθυμητή.

Σε καμία περίπτωση αυτό το έγγραφο δεν αναιρεί τα πρότυπα και τις οδηγίες που έχουν δημιουργηθεί αποκλειστικά και υποχρεωτικά πάνω σε Ομοσπονδιακούς παράγοντες από τη Γραμματεία Εμπορίου υπό θεσπισμένης αρχής, ούτε και θα πρέπει αυτές οι οδηγίες να ερμηνευτούν ως εναλλακτική ή αντικατάσταση των υπαρχόντων αρχών της Γραμματείας Εμπορίου, του Συμβουλίου του OMB, ή οποιασδήποτε άλλης ομοσπονδιακής αρχής.

1.2 Αντικείμενο και Σκοπός

Ο οδηγός αυτός σκοπό έχει να προσφέρει στον αναγνώστη ,εξειδικευμένο ή μη ,την δυνατότητα να μπορεί να κρίνει και να αξιολογεί ένα μεγάλο μέρος των peer to peer εφαρμογών .Το συνολικό σχεδόν κομμάτι αυτής της δημοσίευσης ασχολείται με τις εν λόγω εφαρμογές και τονίζει τα κυριότερα αδύνατα σημεία τους, χωρίς όμως να περιορίζεται μόνο σε αυτά καθώς έχουμε και προτάσεις για βελτιώσεις σε τομείς νευραλγικούς όπως η ασφάλεια και η βελτιστοποίηση της παροχής υπηρεσιών.

Δίδεται μια προσπάθεια να προσφερθεί στον εκάστοτε αναγνώστη μια σφαιρική άποψη της παλαιότερης ,παρούσας ,αλλά και ενδεχόμενης μελλοντικής κατάστασης .Ο οδηγός αυτός προσπαθεί να ξεχωρίσει κάποιες δημοφιλείς εφαρμογές ώστε να παρέχει πληροφορίες για την καλύτερη και ασφαλέστερη χρήση τους με σεβασμό στους άλλους peers του διαδικτύου .Επιπλέον δεν παραλείπεται η αναφορά στο παρελθόν και η συνολική πορεία αυτών των εφαρμογών μέχρι και σήμερα. Αυτά προβάλλονται και με την παρουσίαση διαφόρων σχετικών και πρόσφατων

στατιστικών στοιχείων Η παρουσίαση ασχολείται και με πρωτοποριακές εφαρμογές οι οποίες σκοπό έχουν να εισαγάγουν νέα μοντέλα peer to peer δικτύωσης απαλλαγμένα από μειονεκτήματα του παρελθόντος. Για την εγκατάσταση αυτών των μοντέλων αλλά και την πρακτική δοκιμή τους δεν υπάρχει κάποια ιδιαίτερη απαίτηση σε πλατφόρμα καθώς είναι διαλειτουργικά στο σύνολό τους και το μόνο που ίσως απαιτηθεί είναι επεξεργαστική ισχύς λόγω χρήσης της Java.

1.3 Απευθυνόμενο Κοινό

Το απευθυνόμενο κοινό όπως ήδη αναφέρθηκε μπορεί να είναι και εξειδικευμένο σε θέματα υπολογιστών αλλά και απλοί ενδιαφερόμενοι καθώς οι εκάστοτε υπολογιστικοί όροι προσδιορίζονται με σαφήνεια και με οργανωτική σειρά κατά την ανάπτυξη του κάθε κεφαλαίου. Έτσι δίνεται η ευκαιρία καλύτερης κατανόησης των θεμάτων της παρουσίασης αλλά η ευκαιρία κριτικής σκέψης από πλευράς αναγνωστών.

1.4 Δομή Εγχειριδίου

Το υπόλοιπο του εγχειριδίου είναι οργανωμένο σε 5 κύριες ενότητες, και βιβλιογραφία:

- Η Ενότητα 2 παρέχει μία ιστορική αναδρομή στις εφαρμογές peer to peer αλλά και στις κύριες αιτίες προβλημάτων που προκλήθηκαν ανά καιρούς προτείνοντας λύσεις.

- Η Ενότητα 3 παρουσιάζει έναν από τους σημαντικότερους BitTorrent clients, τον μTorrent που πρωταγωνιστεί στον τομέα των file-sharing εφαρμογών.

- Η Ενότητα 4 παρουσιάζει ένα πλήθος στατιστικών στοιχείων, αριθμών αλλά και διαγραμμάτων σχετικά με τις peer to peer εφαρμογές όπως προκύπτουν από την χρήση τους την τελευταία δεκαετία κυρίως.

- Η Ενότητα 5 εισαγάγει την τεχνολογία JXTA ως μια λύση προβλημάτων συμβατότητας και εισαγωγής πολλών άλλων συσκευών εκτός από PC στην JXTA peer to peer δικτύωση.

- Η βιβλιογραφία αναφέρεται στην έντυπη αλλά και ηλεκτρονική βιβλιογραφία η οποία χρησιμοποιήθηκε για την εκπόνηση αυτής της πτυχιακής εργασίας.

Κεφάλαιο 2

2.1 Εισαγωγή

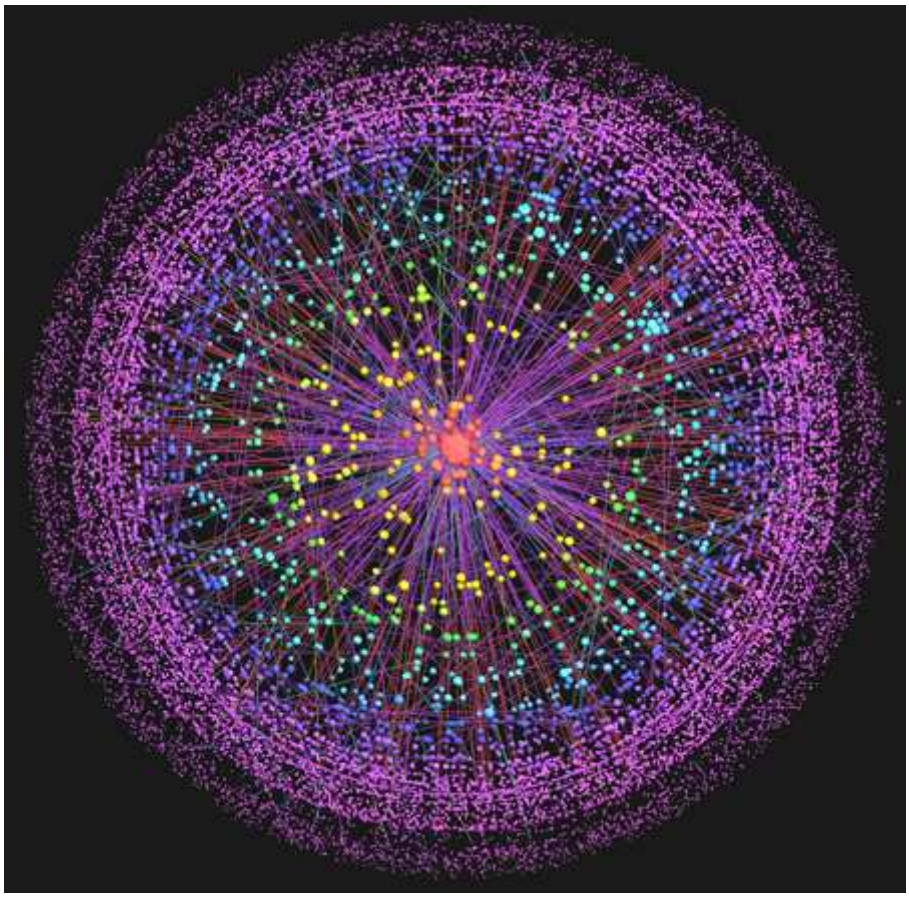
Το Internet είναι ένα κοινό αγαθό, ένα δίκτυο συνεργασίας που αποτελείται από εκατομμύρια hosts από όλο τον κόσμο. Σήμερα υπάρχουν περισσότερες εφαρμογές από ποτέ οι οποίες θέλουν να χρησιμοποιήσουν το διαδίκτυο, να καταναλώσουν εύρος ζώνης, και να στείλουν πακέτα οπουδήποτε. Από το 1994, το ευρύ κοινό αγωνίζεται να ενταχθεί στην κοινότητα των κόμβων του Internet, και να εκμεταλλευτεί το πιο βασικό αγαθό αυτού, το εύρος ζώνης. Επίσης η αυξανόμενη εξάρτηση από το Διαδίκτυο για κρίσιμες εφαρμογές έφερε μαζί της νέες απαιτήσεις ασφαλείας, με αποτέλεσμα τείχη προστασίας(Firewalls) που διαχωρίζουν το δίκτυο σε κομμάτια και δεν επιτρέπουν την άμεση χωρίς έλεγχο σύνδεση μεταξύ των υπολογιστών. Έτσι με την πάροδο των χρόνων και φυσικά με την βοήθεια των αμέτρητων Network Access Providers(NAPs) ,το διαδίκτυο τελικά έχει ξεφύγει κατά πολύ από τον αρχικό του σχεδιασμό.

Το έτος 2000, όμως, κάτι άλλαξε - ή, ίσως, επανήλθε. Το μοντέλο του δικτύου που επέζησε της τεράστιας διαδικτυακής αύξησης των προηγούμενων πέντε ετών, έχει κατά κάποιο τρόπο ανατραπεί. Μέσα από μια εφαρμογή ανταλλαγής μουσικών αρχείων που ονομάζεται Napster[1], και το μεγαλύτερο κίνημα επονομαζόμενο "peer to peer," τα εκατομμύρια χρήστες που συνδέονται στο Διαδίκτυο έχουν αρχίσει να χρησιμοποιούν τους όλο και πιο αναπτυσσόμενους υπολογιστές τους για κάτι περισσότερο από το να «surfάρουν» στο διαδίκτυο και να ανταλλάσουν e-mail. Αντί αυτού, οι προσωπικοί υπολογιστές συνδέονται απευθείας μεταξύ τους σχηματίζοντας ομάδες συνεργασίας δημιουργώντας μηχανές αναζήτησης χρηστών και συστήματα κοινή χρήσης αρχείων.

Πάντως δεν είχε άμεσα ευρεία αποδοχή. Ορισμένες αντιρρήσεις κυρίως αναφέρονται σε νομικές ή ηθικές ανησυχίες. Άλλα προβλήματα είναι τεχνικά Πολλοί providers δικτύου, έχουν στήσει τα συστήματά τους με την ιδέα ότι οι χρήστες θα ξόδευαν τον περισσότερο χρόνο τους ανακτώντας δεδομένα από κεντρικούς εξυπηρετητές, κάπου εκεί εκπίπτουν και οι οικονομικές αντιρρήσεις για τα peer to peer μοντέλα. Μερικοί έχουν αρχίσει να διακόπτουν την πρόσβαση σε peer to peer υπηρεσίες με την αιτιολογία ότι παραβιάζουν την συμφωνία χρήστη και καταναλώνουν πάρα πολύ εύρος ζώνης. Όπως αναφέρθηκε από το online site News.com[2], το ένα τρίτο των ερωτηθέντων κολεγίων των ΗΠΑ είχαν απαγορεύσει το Napster, διότι μέσω της χρήσης του, οι μαθητές προκαλούσαν πολλές φορές κορεσμό του πανεπιστημιακού δικτύου.

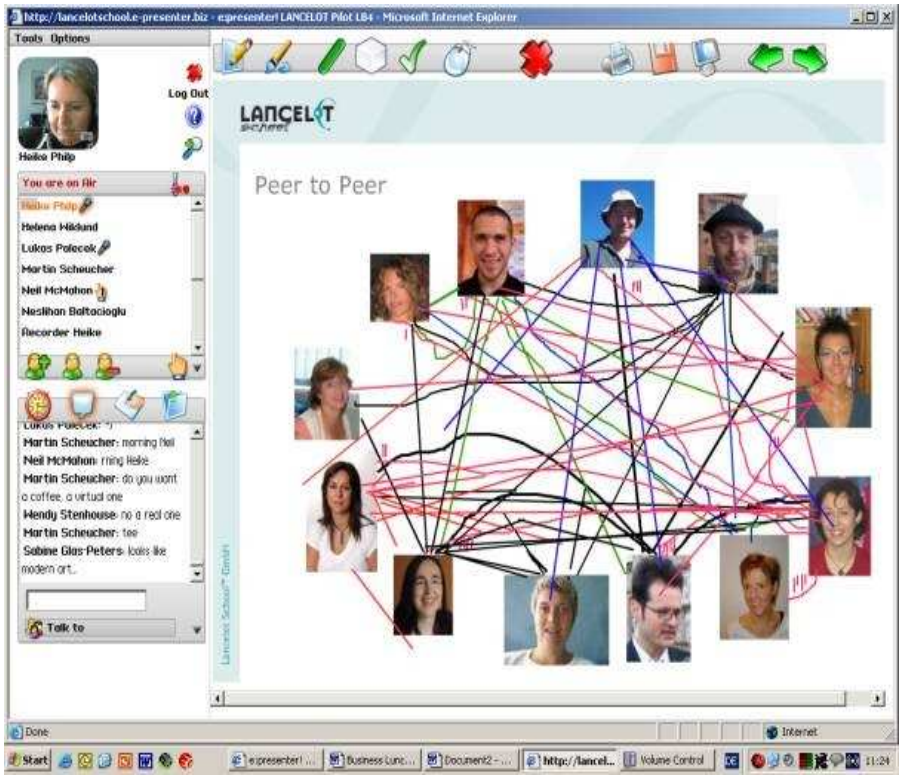
[1] Napster:http://en.wikipedia.org/wiki/Napster
[2]News.com : http://www.news.com.au/story/0,668,24833960-1702,00.html

Αρχικά το Internet είχε σχεδιαστεί ως ένα peer to peer σύστημα , με την πάροδο του χρόνου όμως γινόταν ολοένα και πιο client/server[3] σαν μοντέλο δηλαδή η ιδέα του εξυπηρετητή και του πελάτη, με τα εκατομμύρια των πελατών- καταναλωτών να διεκδικούν επικοινωνία με μια σχετικά προνομιακή σειρά server πληρώνοντας κάποιες φορές αδρά για μεγάλες ταχύτητες download κυρίως. Η σημερινή σειρά των peer to peer [4]εφαρμογών χρησιμοποιεί το Διαδίκτυο όπως είχε σχεδιαστεί αρχικά: ως μέσο επικοινωνίας για μηχανές όπου οι πόροι του δικτύου θα μοιράζονταν μεταξύ τους ισόποσα. Πάντως οι σημερινοί σχεδιαστές peer to peer εφαρμογών θα πρέπει να λάβουν ,αν όχι ως πρότυπο, τουλάχιστον ως βοηθό ,τις εφαρμογές εκείνης της εποχής που είναι ουκ ολίγες.



Εικόνα 1. Μια αφηρημένη αναπαράσταση του internet.

[3]Client-server Model http://www.it.uom.gr/project/client_server/theoria1.htm
[4] Peer to peer: http://en.wikipedia.org/wiki/Peer-to-peer

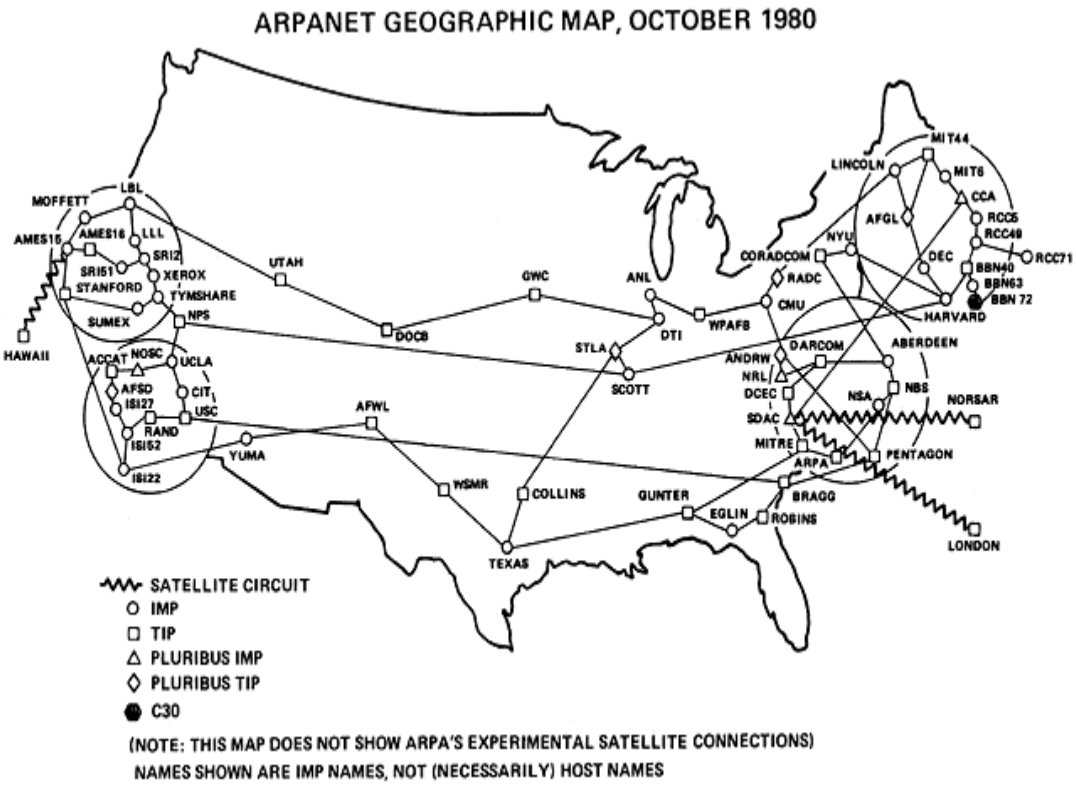


Εικόνα 2. Απλοϊκή αναπαράσταση της ιδέας του peer to peer

2.1.1 Μια συνοπτική ιστορία των συστημάτων peer to peer (1969-1995)

Το Διαδίκτυο, όπως είχε αρχικά σχεδιαστεί στα τέλη της δεκαετίας του 1960 ήταν ένα peer to peer σύστημα. Ο στόχος του αρχικού ARPANET[5] ήταν να μοιράζονται υπολογιστικοί πόροι σε όλες τις ΗΠΑ. Η πρόκληση για αυτήν την προσπάθεια ήταν να ενοποιηθούν οι διάφορες μορφές των υφισταμένων δικτύων, καθώς και τεχνολογίες του μέλλοντος με μια κοινή αρχιτεκτονική δικτύου που θα επιτρέπει σε κάθε host να είναι ισάξιος παίκτης. Το ARPANET αποτελούσε την σύνδεση μεταξύ αυτών των host ,δεν δημιουργούσε συνδέσεις master-slave ούτε client-server,αντιθέτως αντιμετωπίζονταν ως ισάξιες υπολογιστικές μονάδες.

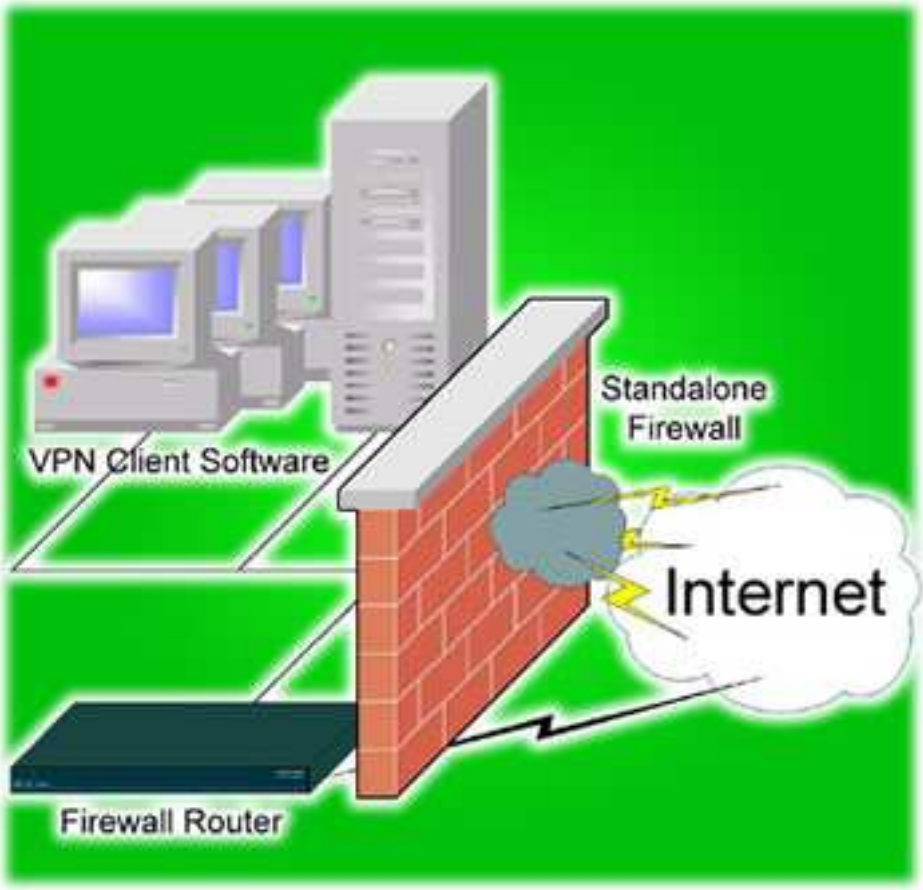
[5]Arpanet: http://pacific.jour.auth.gr/internet/page%201.2.htm



Εικόνα 3 Το ARPANET στις ΗΠΑ παραστατικά(Οκτώβριος 1980)

Αρχικά το Internet ήταν επίσης πολύ πιο ανοιχτό και ελεύθερο από την σημερινή του μορφή. Το Firewall[6] ήταν άγνωστο μέχρι τα τέλη της δεκαετίας του 1980. Σε γενικές γραμμές, οποιεσδήποτε μηχανές του Διαδικτύου μπορούσαν να στείλουν πακέτα η μια στην άλλη. Το διαδίκτυο ήταν ο χώρος συνεταιρισμένων ερευνητών, οι οποίοι κατά κανόνα δεν χρειάζονταν προστασία ο ένας από τον άλλο. Τα πρωτόκολλα μεταφοράς αποστολής και συνόδου, αν μιλήσουμε με σημερινά δεδομένα, ήταν ασαφή και εξειδικευμένα αρκετά συνεπώς οι επιθέσεις ήταν σπάνιες και συνήθως αβλαβείς. Όπως θα δούμε αργότερα, το σύγχρονο Διαδικτύου είναι πολύ πιο στεγανό.

[6]Firewall: http://en.wikipedia.org/wiki/Firewall



Εικόνα 4. Η Τυπική χρησιμότητα ενός Firewall σε απλή παρουσίαση

Το FTP[7] και το Telnet[8], είναι client/server εφαρμογές. Ένας πελάτης Telnet συνδέεται σε έναν server, και ένας πελάτης FTP αποστέλλει και λαμβάνει αρχεία από έναν server.Πάντως το pattern ήταν ότι εκείνη την εποχή ο οποιοσδήποτε host μπορούσε να χρησιμοποιήσει υπηρεσίες FTP και Telnet από και προς οποιοδήποτε άλλο host(Οι servers είχαν μια client συμπεριφορά).

Αυτή η θεμελιώδης συμμετρία, είναι που έκανε το Internet τόσο ριζοσπαστικό. Με τη σειρά της, επέτρεψε μια ποικιλία πιο πολύπλοκων συστημάτων, όπως Usenet και DNS που χρησιμοποιούν peer to peer μορφές επικοινωνίας με έναν ενδιαφέροντα τρόπο. Κατά τα επόμενα έτη, το Διαδίκτυο τείνει όλο και περισσότερο σε client/server εφαρμογές.

[7]Ftp: http://el.wikipedia.org/wiki/File_Transfer_Protocol
[8] Telnet:http://www.telnet.org/

2.2 USENET

Το Usenet εφαρμόζει ένα αποκεντρωμένο μοντέλο ελέγχου που κατά κάποιο τρόπο είναι ο παππούς των σημερινών peer to peer εφαρμογών, όπως η Gnutella[9] και το Freenet. Ουσιαστικά, το Usenet είναι ένα σύστημα που, χωρίς την χρήση κεντρικού ελέγχου, αντιγράφει αρχεία μεταξύ υπολογιστών. Από τότε που το Usenet ήταν στην πιάτσα ,περίπου το 1979, προσφέρει μια σειρά από μαθήματα και είναι σώφρον να εξετάζεται και για τις σύγχρονες file-sharing εφαρμογές.

Το σύστημα Usenet βασίστηκε αρχικά σε μια εγκατάσταση που ονομάζεται Unix to Unix πρωτόκολλο αντιγραφής, ή UUCP[10]. Το UUCP ήταν ένας μηχανισμός με τον οποίο ένα Unix μηχάνημα θα καλούσε αυτόματα ένα άλλο με σκοπό την ανταλλαγή αρχείων με αυτό, και ακολούθως αποσύνδεση. Ο μηχανισμός αυτός επέτρεψε στις διαδικτυακές Unix τοποθεσίες την ανταλλαγή e-mail, αρχείων,patches του συστήματος, ή άλλα μηνύματα. Το Usenet, χρησιμοποιούσε UUCP για την ανταλλαγή μηνυμάτων σε μια σειρά θεμάτων, έτσι ώστε οι σπουδαστές στο Πανεπιστήμιο της Βόρειας Καρολίνας και του Duke University να μπορούν ο καθένας να κάνει "post" μηνύματα σε ένα θέμα, να διαβάζει τα μηνύματα από τους άλλους για το ίδιο θέμα, και να γίνονται συναλλαγές μηνυμάτων μεταξύ των 2 ιδρυμάτων. Το Usenet αυξήθηκε από αυτούς τους αρχικούς δύο οικοδεσπότες ,σε εκατοντάδες χιλιάδες sites. Καθώς το διαδίκτυο μεγάλωσε, το ίδιο συνέβη με τον αριθμό και τη δομή των θεμάτων στα οποία θα μπορούσε ένα μήνυμα να δημοσιευτεί. Το Usenet σήμερα χρησιμοποιεί πρωτόκολλο με βάση TCP / IP που είναι γνωστό ως Network News Transport Protocol (NNTP)[11], το οποία επιτρέπει σε δύο υπολογιστές στο δίκτυο Usenet να ανακαλύψουν νέες ομάδες συζήτησης με αποτελεσματικότητα και να προβούν σε ανταλλαγή μηνυμάτων μεταξύ τους.

Το βασικό μοντέλο του Usenet παρέχει τοπικό έλεγχο και σχετικά απλή διαχείριση. Ένα site Usenet ενώνεται με τον υπόλοιπο κόσμο, με τη δημιουργία μιας σύνδεσης ανταλλαγής ειδήσεων με ένα τουλάχιστον άλλο sever στο δίκτυο Usenet. Σήμερα, η ανταλλαγή παρέχεται συνήθως από την εταιρία ISP(Internet Service Provider).

Ο διαχειριστής της εταιρείας μπορεί να ελέγχει το μέγεθος των μεταφερόμενων δεδομένων, προσδιορίζοντας ποιος server θα τα μεταφέρει. Επιπλέον, ο διαχειριστής μπορεί να καθορίσει μια στιγμή λήξης αναλόγως την ομάδα ή την ιεραρχία, έτσι ώστε τα άρθρα σε μια ομάδα συζήτησης να ανακτώνται για ένα ορισμένο χρονικό διάστημα. Οι έλεγχοι αυτοί επιτρέπουν σε κάθε οργανισμό να συμμετάσχει εθελοντικά στο δίκτυο με τους δικούς του όρους. Πολλοί οργανισμοί αποφασίζουν να μην μεταφέρονται για παράδειγμα newsgroups που μεταδίδουν σεξουαλικό περιεχόμενο ή παράνομο υλικό. Αυτή είναι μια ειδοποιός διαφορά από το Freenet , το οποίο (ως επιλογή του σχεδιασμού) δεν επιτρέπει σε έναν χρήστη να ξέρει τι υλικό έχει λάβει.

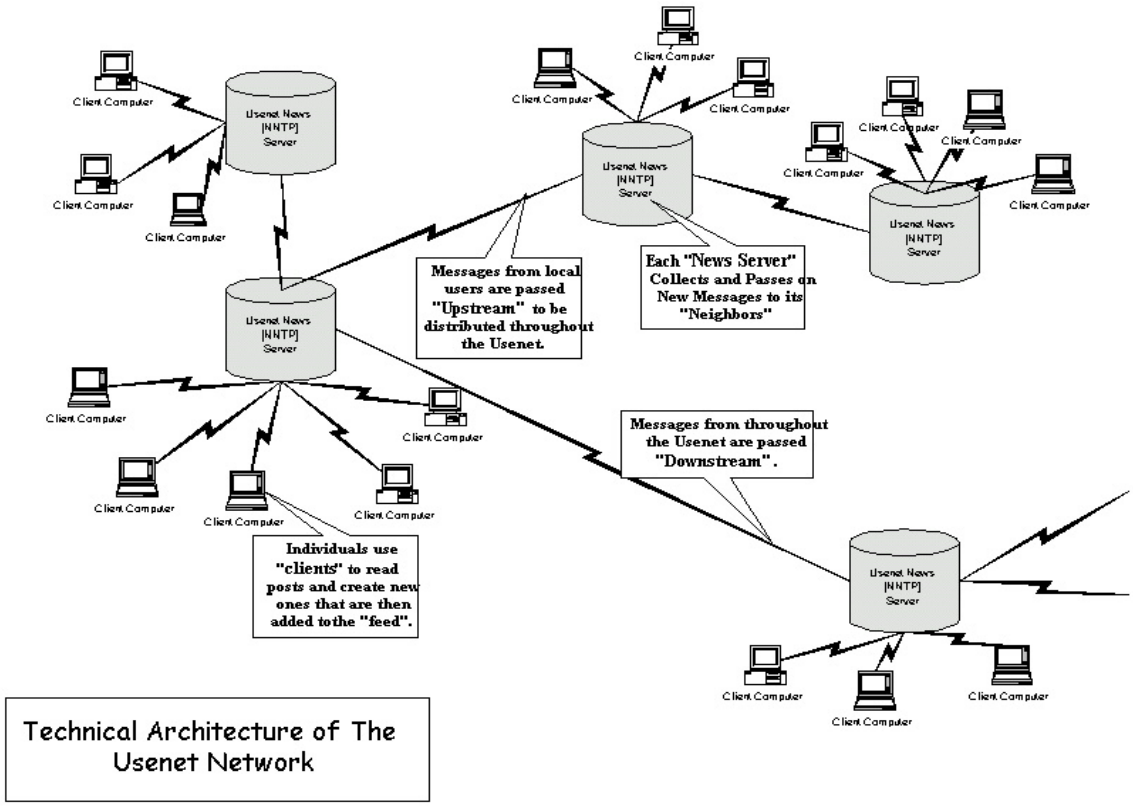
---

[9] Gnutellahttp://en.wikipedia.org/wiki/Gnutella
[10] UUCP:http://en.wikipedia.org/wiki/UUCP
[11] NNTP:http://www.academ.com/academ/nntp/

Το Usenet έχει εξελιχθεί σε ένα από τα καλύτερα παραδείγματα των αποκεντρωμένων δομών ελέγχου στο Διαδίκτυο. Δεν υπάρχει κεντρική αρχή που ελέγχει το σύστημα ειδήσεων. Η προσθήκη νέων ομάδων συζήτησης στο κύριο θέμα ελέγχεται από μια αυστηρή διαδικασία εκδημοκρατισμένη, με την news admin ομάδα Usenet να προτείνει και να συζητά τη δημιουργία νέων ομάδων. Αφότου μια νέα ομάδα προτείνεται και συζητιέται για ένα ορισμένο χρονικό διάστημα, ο οποιοσδήποτε με διεύθυνση ηλεκτρονικού ταχυδρομείου μπορεί να υποβάλει ένα email ώστε να ψηφίσει υπέρ ή κατά της πρότασης. Εάν μια ομάδα συζήτησης τελικά εκλεχθεί, ένα νέο μήνυμα ομάδας στέλνεται και αναπαράγεται μέσω του δικτύου Usenet.

Η ανοικτή, αποκεντρωμένη φύση του Usenet μπορεί να είναι επιβλαβής, καθώς και επωφελής. Το Usenet έχει τεράστια επιτυχία ως ένα σύστημα με την έννοια ότι έχει επιβιώσει από το 1979 και εξακολουθεί να φιλοξενεί ακμάζουσες κοινότητες εμπειρογνωμόνων. Έχει διογκωθεί κατά πολύ σε σχέση με το μέτριο ξεκίνημά του. Όμως, εν πολλοίς, η έμπιστη, αποκεντρωμένη φύση του πρωτοκόλλου μείωσε τη χρησιμότητά του και το κατέστησε ως ένα εξαιρετικά θορυβώδη δίαυλο επικοινωνίας.

Ιδιαίτερα, όπως θα αναφερθεί αργότερα, το Usenet έπεσε θύμα spamming[12] νωρίς κατά την αύξηση των διαφημιστικών δραστηριοτήτων στο Internet. Πάντως, το σύστημα Usenet με τον αποκεντρωμένο του έλεγχο και τις τεχνικές αποφυγής πλημμύρας αποτελεί ένα εξαιρετικό αντικείμενο μελέτης στα χέρια των σχεδιαστών συστημάτων peer to peer.



Εικόνα 5. Η αρχιτεκτονική του Usenet

[12]Spamming: http://en.wikipedia.org/wiki/Spam_(electronic)

2.3 DNS

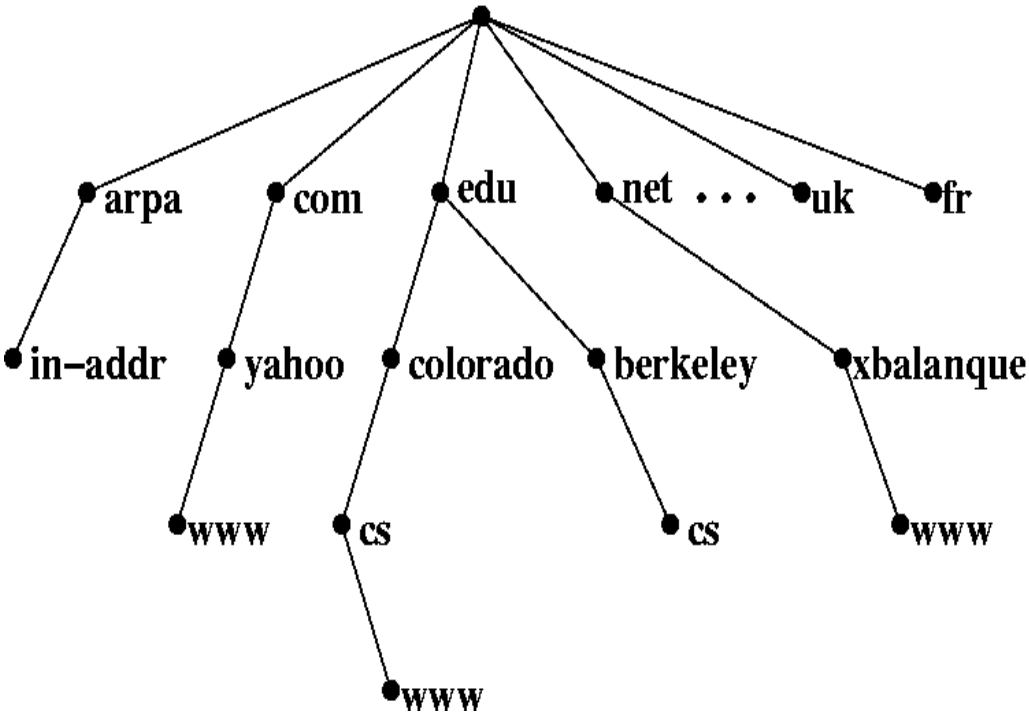
Το Domain Name System (DNS) είναι ένα παράδειγμα ενός συστήματος που συνδυάζει peer to peer δικτύωση με ένα ιεραρχικό μοντέλο κυριότητας πληροφοριών. Το αξιοσημείωτο με το DNS είναι το πόσο καλά έχει αντέξει στο χρόνο, από τους λίγους χιλιάδες hosts που είχε σχεδιαστεί αρχικά για να στηρίξει το 1983 στους εκατοντάδες εκατομμύρια που φιλοξενεί σήμερα στο διαδίκτυο. Τα διδάγματα από το DNS εφαρμόζονται άμεσα στις σύγχρονες peer to peer file sharing εφαρμογές.

Το DNS ιδρύθηκε ως λύση σε ένα πρόβλημα επιμερισμού αρχείων. Κατά τις πρώτες ημέρες του Internet, ο τρόπος να χαρτογραφήσεις ένα πιο ανθρώπινα φιλικό όνομα όπως BBN σε μια διεύθυνση IP όπως 4.2.49.2 ήταν μέσω ενός και μόνο απλού αρχείου, hosts.txt το οποίο διανεμόταν παντού. Δεδομένου ότι το δίκτυο αυξήθηκε σε χιλιάδες hosts και η διαχείριση αυτού του αρχείου κατέστη αδύνατη, το DNS εξελίχθηκε ως ένας τρόπος για να διανέμονται τα δεδομένα σε ολόκληρο το τότε peer to peer Internet.

Τα λεγόμενα namespace του DNS είναι φυσικά ιεραρχικά. Για παράδειγμα, η O'Reilly & associates , Inc κατέχει το namespace oreilly.com: και είναι η μόνη αρμόδια εταιρία για όλα τα ονόματα στον τομέα , όπως www.oreilly.com. Αυτό το ενσωματωμένο σύστημα αποδόσεως ιεραρχίας έχει έναν απλό, φυσικό τρόπο για να μεταβιβάσει την ευθύνη σε ένα μέρος της βάσης δεδομένων DNS. Κάθε τομέας έχει μια αρχή, τον name server που κρατά όλες τις εγγραφές των host αυτού του τομέα. Όταν ένας host στο Διαδίκτυο θέλει να ξέρει τη διεύθυνση για ένα συγκεκριμένο όνομα, θέτει ένα ερώτημα στον πλησιέστερο name server του για να ζητήσει τη διεύθυνση. Αν δεν γνωρίζει το όνομα, μεταβιβάζει το ερώτημα στην αρχή για εκείνη την περιοχή. Αυτό το ερώτημα, με τη σειρά του, μπορεί να ανατεθεί σε μια ανώτερη αρχή, φτάνοντας ακόμα και στους root name servers του internet. Δεδομένου ότι η απάντηση στέλνεται πίσω στον αιτούντα, η πορεία ανάμεσα στους name server αποθηκεύεται, ώστε η επόμενη αναζήτηση να είναι πιο αποτελεσματική. Οι name servers λειτουργούν τόσο ως πελάτες όσο και ως servers..

Το DNS στο σύνολό του λειτουργεί εκπληκτικά καλά, έχοντας κλίμακα έως 10.000 φορές το αρχικό του μέγεθος. Υπάρχουν πολλά βασικά στοιχεία σχεδιασμού του DNS που έχουν αναπαραχθεί σε πολλά κατανεμημένα συστήματα σήμερα. Ένα στοιχείο είναι ότι οι hosts μπορούν να λειτουργήσουν τόσο ως πελάτες όσο και ως servers, διανέμοντας αιτήσεις όταν χρειαστεί. Το δεύτερο στοιχείο είναι η φυσική μέθοδος διανομής requests σε όλο το δίκτυο. Κάθε DNS server μπορεί να θέσει ερωτήματα σε οποιοδήποτε άλλο, αλλά σε κανονική λειτουργία υπάρχει ένα πρότυπο μονοπάτι μέσω της αλυσίδας ιεραρχίας. Το φορτίο κατανέμεται φυσικά σε όλο το δίκτυο DNS, έτσι ώστε κάθε name server να εξυπηρετεί μόνο τις ανάγκες των πελατών του και του namespace που διαχειρίζεται ατομικά.

Έτσι, από πρώτα στάδια του, το Internet χτίστηκε βασισμένο σε peer to peer μορφές επικοινωνίας. Ένα πλεονέκτημα αυτής της ιστορίας είναι ότι έχουμε την εμπειρία να αντλήσουμε για το σχεδιασμό νέων peer to peer συστημάτων. Τα προβλήματα που αντιμετωπίζουν σήμερα οι νέες peer to peer εφαρμογές, όπως η κοινή χρήση αρχείων ,είναι αρκετά παρόμοια με τα προβλήματα που το Usenet και το DNS αντιμετώπιζαν 20 ή 25 χρόνια πριν.



Εικόνα 6. Ιεραρχία DNS namespaces από πάνω προς τα κάτω.

2.4 Το διαδικτυακό μοντέλο κατά την έκρηξη του Internet (1995-1999)

Η έκρηξη του Διαδικτύου το 1994 άλλαξε ριζικά τη μορφή του Internet, μετατρέποντάς το από μια ήσυχη επαγγελματική ουτοπία σε ένα πολυσύχναστο μέσο μαζικής ενημέρωσης. Εκατομμύρια νέα άτομα προσήλθαν μαζικά στις θυρίδες του Διαδικτύου. Αυτό το κύμα αντιπροσώπευε ένα νέο είδος ανθρώπων – συνηθισμένα άτομα που ενδιαφέρονται για το Διαδίκτυο ως έναν τρόπο να στείλουν e-mail, να δουν ιστοσελίδες και να κάνουν αγορές και όχι επιστήμονες πληροφορικής που ενδιαφέρονται για τις λεπτομέρειες των πολύπλοκων δικτύων των ηλεκτρονικών υπολογιστών. Η αλλαγή του Διαδικτύου σε ένα μαζικό πολιτιστικό φαινόμενο είχε εκτεταμένες συνέπειες στην αρχιτεκτονική του δικτύου, ένα αντίκτυπο που επηρεάζει άμεσα την ικανότητά μας να δημιουργήσουμε peer to peer εφαρμογές στο σημερινό Διαδίκτυο. Αυτές οι αλλαγές παρατηρούνται στον τρόπο χρήσης του δικτύου, στην διακοπή της αγαστής συνεργασίας στο Διαδίκτυο, στην αύξηση της εγκατάστασης τειχών προστασίας στο Διαδίκτυο, καθώς και στην αύξηση των ασύμμετρων συνδέσεων δικτύου όπως το ADSL[13] και τα καλωδιακά μόντεμ.

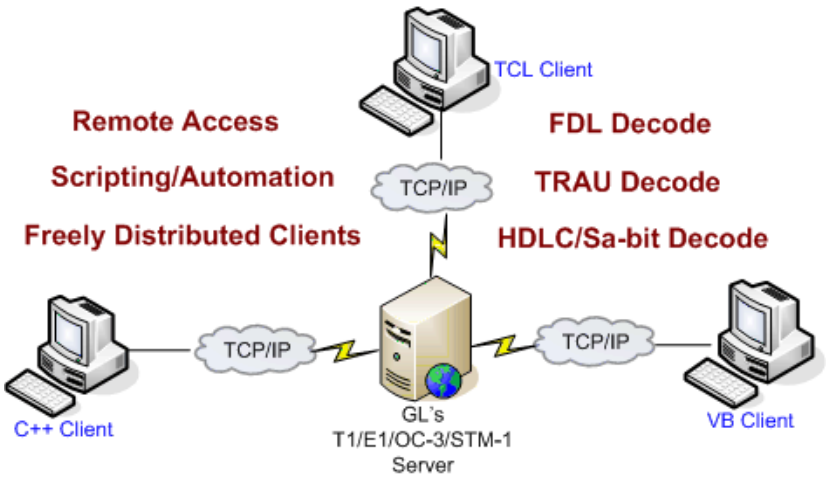
[13] ADSL:http://www.adslgr.com/

2.4.1 Η μετάβαση στο μοντέλο Client/Server

Το διαδικτυακό μοντέλο των εφαρμογών χρήστη – όχι μόνο από την άποψη της κατανάλωσης εύρους ζώνης, αλλά και των μεθόδων τους για την απονομή διευθύνσεων και την επικοινωνία με άλλες μηχανές -άλλαξε σημαντικά με την αύξηση των εμπορικών δραστηριοτήτων στο Διαδίκτυο και την έλευση των εκατομμυρίων απλών χρηστών όπως αναφέρθηκε παραπάνω, στη δεκαετία του 1990. Τα μοντέρνα πρωτόκολλα σύνδεσης , όπως SLIP και PPP έγιναν συχνές, τυπικές εφαρμογές στοχευόμενες στα αργά σε ταχύτητα αναλογικά modem, επιπλέον οι εταιρείες άρχισαν να διαχειρίζονται τα δίκτυά τους με τείχη προστασίας και με την χρήση Network Address Translation (NAT)[14], στο οποίο θα αναφερθούμε εκτενέστερα παρακάτω.

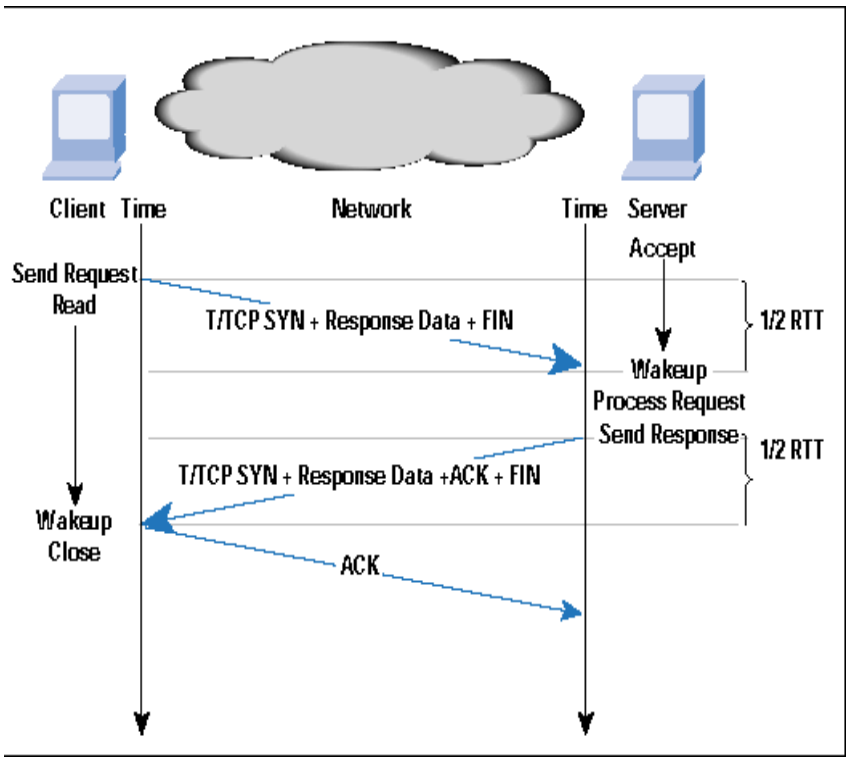
Τα πρόγραμμα περιήγησης στο διαδίκτυο(browsers), και πολλές από τις εφαρμογές που δημιουργήθηκαν κατά τη διάρκεια της εμπορευματοποίησης του Διαδικτύου, είχαν ως βάση ένα απλό client/server πρωτόκολλο: ο πελάτης ξεκινά μια σύνδεση με ένα γνωστό server, κατεβάζει ορισμένα δεδομένα και αποσυνδέεται. Όταν ο χρήστης έχει τελειώσει με την ανάκτηση δεδομένων, η διαδικασία επαναλαμβάνεται. Το μοντέλο είναι απλό και εύκολο. Δουλεύει για τα πάντα, από την απλή περιήγηση , για την παρακολούθηση streaming video[15], interactive παιχνίδια, και ένα σωρό άλλα πράγματα. Ο client δεν χρειάζεται να έχει μια μόνιμη ή γνωστή διεύθυνση IP, δεν χρειάζεται συνεχή σύνδεση με το Internet και τέλος δεν χρειάζεται να φιλοξενήσει πολλαπλούς χρήστες. Πρέπει μόνο να γνωρίζει πως θα θέσει ένα ερώτημα και πώς θα λάβει την απάντηση.

Αν και ορισμένοι επικρότησαν αυτό το μοντέλο αρχικά και οι αρχιτέκτονες των συστημάτων που επέτρεψαν την εμπορική επέκταση του δικτύου υπέθεσαν ότι αυτό το μοντέλο ήρθε για να μείνει, είναι πιθανόν οι σύγχρονες peer to peer εφαρμογές να το εκτοπίσουν λόγω των τεραστίων διαφορών φιλοσοφίας και πρωτοκόλλου.



Εικόνα 7. Απεικόνιση του μοντέλου client-server και της λειτουργίας του

[14] NAT:http://en.wikipedia.org/wiki/Network_address_translation
[15] Streaming Media:http://en.wikipedia.org/wiki/Streaming_media



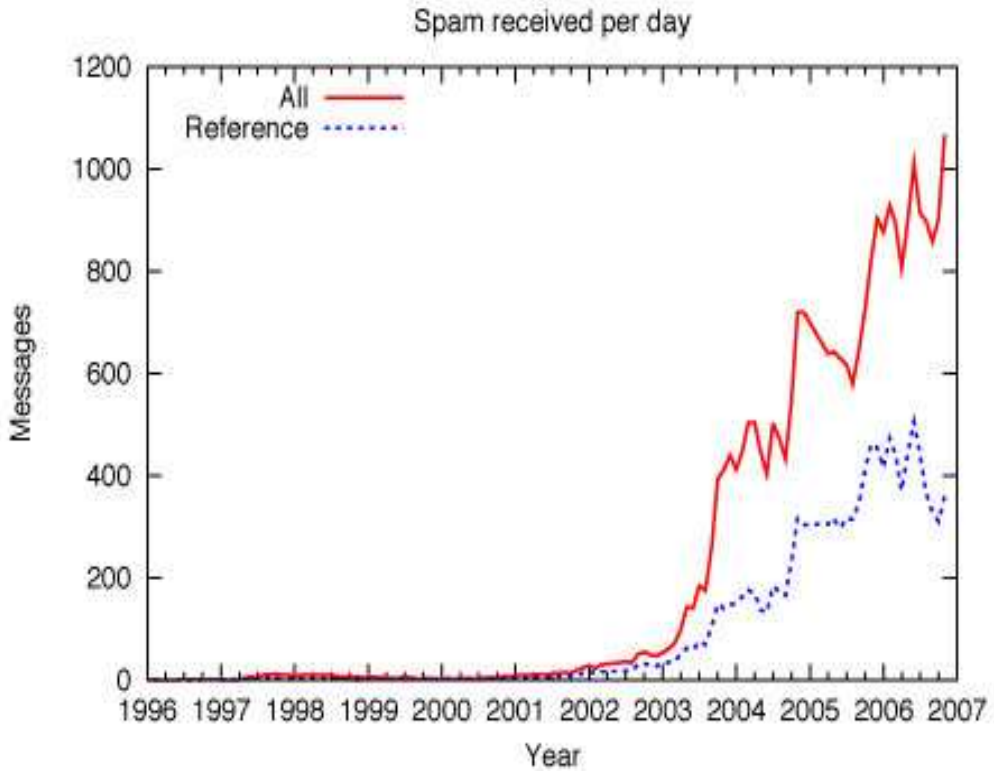
Εικόνα 8. Η λειτουργικότητα της διαδικασίας requests και responses μεταξύ client-server

Αρχικά το Internet έχει σχεδιαστεί για τις αρχές της συνεργασίας και της καλής μηχανικής. Όλοι όσοι εργάζονταν για το σχεδιασμό του Διαδικτύου είχαν τον ίδιο στόχο: την οικοδόμηση ενός αξιόπιστου, αποτελεσματικού, ισχυρού δικτύου. Καθώς το Διαδίκτυο εισήλθε στην τρέχουσα εμπορική φάση του, οι δομές του άλλαξαν, με αποτέλεσμα μια σειρά προβλημάτων. Το φαινόμενο αυτό έχει αποδειχθεί με πολλούς τρόπους, κυρίως με την αύξηση του spam στο Διαδίκτυο και τις προκλήσεις της οικοδόμησης αποδοτικών πρωτοκόλλων δικτύου που να διαχειρίζονται σωστά τους κοινούς υπολογιστικούς πόρους.

2.4.2 Spam: μη συνεργάσιμα άτομα

Το Spam, ή αυτόκλητα εμπορικά μηνύματα, είναι πλέον καθημερινό φαινόμενο στο διαδίκτυο. Πίσω στο προ-εμπορικό δίκτυο ωστόσο, οι αυτόκλητες διαφημίσεις αντιμετωπίζονταν με έκπληξη και οργή. Το τέλος της αθωότητας συνέβη στις 12 Απριλίου 1994.Τη ημέρα αυτή, η άσημοι Canter και Seigel που διαφήμιζαν τις υπηρεσίες τους για την απόκτηση πράσινης κάρτας εμφανίστηκαν στο Usenet. Η επιθετική πράξη τους ήταν μία διαφήμιση που δημοσιεύτηκε ατομικά σε κάθε ομάδα συζήτησης του Usenet, στέλνοντας σε όλο τον κόσμο ένα μήνυμα που διαφήμιζε τις υπηρεσίες τους. Εκείνη την εποχή, αυτό το είδος της δράσης ήταν άνευ προηγουμένου και προκάλεσε έντονη αποδοκιμασία. Όχι μόνο οι περισσότεροι άνθρωποι δεν ενδιαφέρθηκαν για την υπηρεσία, αλλά πολλοί θεώρησαν ότι οι Canter και Seigel είχαν καταχραστεί τους πόρους του Usenet.
Οι διαφημιστές δεν πλήρωναν για τη μετάδοση της διαφήμισης Αντιθέτως το κόστος πληρωνόταν από το Usenet στο σύνολό του.

Σήμερα στο Internet, το spam δεν φαίνεται παράξενο. Το Usenet σε μεγάλο βαθμό έχει δοθεί πάνω σε αυτό και τώρα οι ISP's παρέχουν φιλτράρισμα ανεπιθύμητων μηνυμάτων για τις e-mail υπηρεσίες των χρηστών τους, τόσο για να βοηθήσουν τους χρήστες τους όσο και για αυτοάμυνα. Η συνεργασία αυτή παρόλα αυτά σήμερα δεν υπάρχει. Το σύγχρονο Internet στερείται εν γένει αποτελεσματική τεχνολογία για την πρόληψη spam.



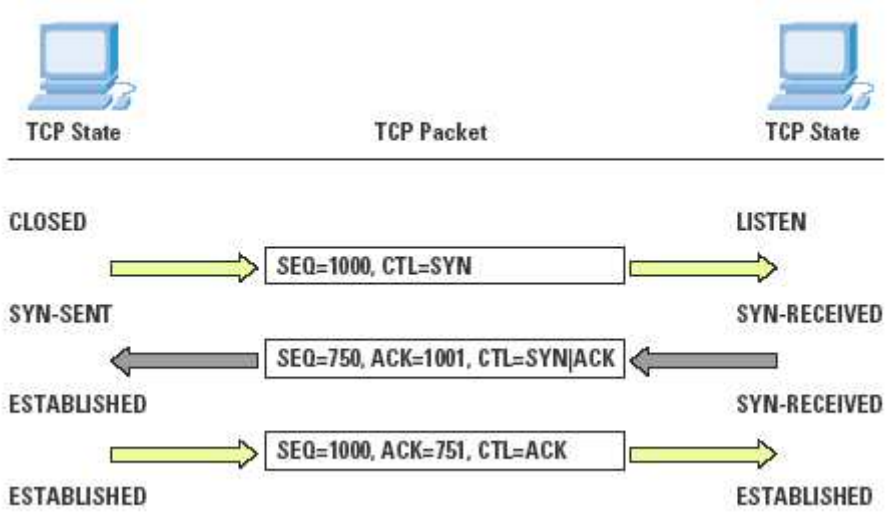
Εικόνα 9. Γραφική αναπαράσταση της έκρηξης του spam το διάστημα 1996-2007

Το πρόβλημα είναι η αδυναμία στην αρχιτεκτονική του Διαδικτύου. Επειδή κάθε host μπορεί να συνδεθεί με οποιοδήποτε άλλο host, και επειδή οι συνδέσεις είναι σχεδόν ανώνυμες, οι άνθρωποι μπορούν να εισαγάγουν spam στο δίκτυο σε οποιοδήποτε σημείο. Υπήρξε μία κούρσα προσπαθειών που περιελάμβανε κλείσιμο των ανοικτών send-mail κέντρων, παρακολούθηση πηγών του spam στο Usenet, αντίποινα κατά των αποστολέων - αλλά η μάχη έχει χαθεί, και σήμερα όλοι μας έχουμε μάθει να ζούμε με το spam.

Το μάθημα για τους σχεδιαστές peer to peer είναι ότι χωρίς την ανάλογη πρόληψη σε ένα δίκτυο, είναι δύσκολο να επιβληθούν κανόνες κοινωνικής ευθύνης. Ακριβώς όπως με το Usenet και το e-mail, σήμερα οι peer to peer εφαρμογές διατρέχουν τον κίνδυνο spamming διαφόρων μηνυμάτων. Είναι δύσκολο να σχεδιαστεί ένα σύστημα όπου η κοινωνικά μη αποδεκτή χρήση να εμποδίζεται. Τεχνολογίες για την υπευθυνότητα, όπως κρυπτογραφικές αναγνωρίσεις, μπορούν να αποτελέσουν πολύτιμα εργαλεία για να βοηθήσουν τη διαχείριση ενός peer to peer δικτύου. Υπήρξαν προτάσεις για την εκ των υστέρων τοποθέτηση ανάλογων δυνατοτήτων σε Usenet και e-mail, αλλά καμία δεν είναι ευρέως διαδεδομένη σήμερα.

2.4.3Η εξίσωση μέσω TCP: Συνεργάσιμα πρωτόκολλα

Μια βασική αρχή σχεδιασμού του Διαδικτύου είναι η βέλτιστη παράδοση πακέτων. "Βέλτιστη προσπάθεια" στην συγκεκριμένη περίπτωση σημαίνει ότι το Διαδίκτυο δεν εγγυάται ότι ένα πακέτο θα περάσει, απλά ότι το Δίκτυο θα καταβάλει κάθε δυνατή προσπάθεια για να φτάσει το πακέτο στον εκάστοτε προορισμό. Υψηλότερου επιπέδου πρωτόκολλα όπως το TCP δημιουργηθούν αξιόπιστες συνδέσεις παρέχοντας ανίχνευση, όταν ένα πακέτο χάνεται και ξαναστέλνεται. Μια σημαντική ποσότητα πακέτων δεν παραδίδονται λόγο συμφόρησης π.χ. αν ένα router έχει υποστεί κορεσμό, θα ξεκινήσει να αποθέτει πακέτα τυχαία. Το TCP φροντίζει για αυτό ρυθμίζοντας την ταχύτητα με την οποία στέλνονται τα δεδομένα. Όταν το δίκτυο είναι κορεσμένο, κάθε σύνδεση TCP επιβραδύνει ανεξάρτητα την ροή προσπαθώντας να βρει το βέλτιστο σημείο ενώ δεν χάνει πάρα πολλά πακέτα. Επιπλέον όχι μόνο οι ατομικές συνδέσεις TCP βελτιστοποιούν την χρήση του εύρους ζώνης, το TCP έχει σχεδιαστεί επίσης για να καταστεί το Διαδίκτυο ως σύνολο λειτουργικότερο. Η συλλογική συμπεριφορά πολλών μεμονωμένων συνδέσεων TCP οδηγεί σε μείωση της συμφόρησης στο δρομολογητή, κατά τρόπο που να είναι προσαρμοσμένος στην αποτελεσματική χρήση του. Στην ουσία, ο αλγόριθμος αυτός, ο επονομαζόμενος back off TCP ,είναι ένας τρόπος για τους peers να διαχειριστούν τους πόρους χωρίς κάποιον κεντρικό συντονιστή.



Εικόνα 10. Αναπαράσταση της επικοινωνίας με TCP πρωτόκολλο

Το πρόβλημα είναι ότι η απόδοση του TCP[16] στην κλίμακα του Διαδικτύου απαιτεί ριζική συνεργασία: κάθε χρήστης του δικτύου πρέπει να παίζει με τους ίδιους κανόνες. Οι επιδόσεις μίας TCP σύνδεσης είναι αντιστρόφως ανάλογη προς την τετραγωνική ρίζα του ποσοστού απώλειας πακέτων.. Πρωτόκολλα που ακολουθούν αυτόν τον νόμο είναι γνωστά ως "TCP-friendly πρωτόκολλα." Είναι δυνατόν να σχεδιάσουν άλλα πρωτόκολλα που δεν ακολουθούν την εξίσωση του παραπάνω ποσοστού TCP, και που προσπαθούν να καταναλώνουν περισσότερο εύρος ζώνης από ό, τι τους αναλογεί. Τα πρωτόκολλα αυτά μπορούν να χαλάσουν την δίκαιη

[16] TCP:http://el.wikipedia.org/wiki/Transmission_Control_Protocol

μοιρασιά πόρων για όλους. Αυτό το αφηρημένο πρόβλημα δικτύωσης είναι ένα κλασικό παράδειγμα της σημερινής κατάστασης που διαδέχτηκε την peer to peer κοινότητα και το Διαδίκτυο σήμερα είναι αρκετά ευάλωτο σε αυτό.

Το πρόβλημα δεν είναι μόνο θεωρητικό, είναι επίσης αρκετά πρακτικό. Διάφορα πρωτόκολλα έχουν αναπτυχθεί τα τελευταία χρόνια από τις εταιρείες με εμπορικές απαιτήσεις, και υπάρχει αυξανόμενη ανησυχία ότι τα μη-φιλικά αυτά πρωτόκολλα θα αρχίσουν να βλάπτουν το Internet.

Πρώιμο παράδειγμα ήταν ένα χαρακτηριστικό που προστέθηκε από την Netscape στον browser[17] της και έδινε τη δυνατότητα να ληφθούν πολλά αρχεία ταυτόχρονα. Οι μηχανικοί της Netscape ανακάλυψαν ότι εάν γινόταν λήψη εικόνων, παράλληλα, και όχι μια κάθε φορά, όλη τη σελίδα θα φορτώνονταν ταχύτερα και οι χρήστες θα ήταν πιο ευχαριστημένοι. Αλλά υπήρχε ένα ερώτημα: ήταν αυτή η χρήση του εύρους ζώνης δίκαιη; Με το να πρέπει να σταλούν περισσότερες εικόνες συγχρόνως, δημιουργούνται περισσότερα κανάλια και παραμερίζονται οι TCP αλγόριθμοι συμφόρησης .. Σήμερα η τεχνική αυτή είναι στάνταρ σε τους browsers. Το πρόβλημα που αναδύθηκε πλέον είναι οι "επιταχυντές κατεβάσματος", προγράμματα που κατεβάζουν διάφορα κομμάτια του ίδιου αρχείου ταυτόχρονα, και πάλι απειλούν να διαταράξουν την ευαίσθητη διαχείριση της κυκλοφοριακής συμφόρησης στο Διαδίκτυο.

Μια πιο μεγάλη ανησυχία σχετικά με τη διαχείριση της συμφόρησης είναι η αύξηση των υπερκαταναλωτικών Broadband streaming media. Τυπικές εφαρμογές streaming media δεν χρησιμοποιούν το πρωτόκολλο TCP, αντιθέτως χρησιμοποιούν UDP βασισμένα πρωτόκολλα με το δικό τους έλεγχο της κυκλοφοριακής συμφόρησης και των δικών τους στρατηγικών διαχείρισης αποτυχίας μετάδοσης πακέτων. Πολλά από αυτά τα πρωτόκολλα είναι ιδιόκτητα. Μηχανικοί δικτύων δεν έχουν καν πρόσβαση στις εφαρμογές τους ώστε να εξετάσουν εάν είναι TCP-friendly. Μέχρι στιγμής δεν έχει υπάρξει μεγάλο πρόβλημα. Οι πωλητές streaming media φαίνεται να παίζουν με τους κανόνες, και όλα είναι καλά. Αλλά ριζικά το σύστημα είναι εύθραυστο.

Τελικά τι είναι κοινό μεταξύ των TCP αλγορίθμων και του spam?Και τα δύο δείχνουν ότι η σωστή λειτουργία του Internet είναι εύθραυστη και απαιτεί τη συνεργασία όλων των εμπλεκομένων. Στην περίπτωση του TCP, το σύστημα έχει λειτουργήσει ως επί το πλείστον και το δίκτυο έχει διατηρηθεί. Στην περίπτωση του spam, ωστόσο, η μάχη έχει χαθεί και η άπληστη συμπεριφορά θα είναι μαζί μας για πάντα. Το μάθημα για τους peer to peer σχεδιαστές του συστήματος είναι να εξετάσει το ζήτημα της αλληλεγγύης . Είτε θα πρέπει να σχεδιαστούν συστήματα που δεν απαιτούν τη συνεργασία για να λειτουργούν σωστά, ή θα πρέπει να δημιουργήσουμε κίνητρα για τη συνεργασία, ανταμείβοντας την ορθή συμπεριφορά, έτσι ώστε η κακή συμπεριφορά να τιμωρείται..Ένα τέτοιο παράδειγμα είναι η centralized file-sharing peer to peer εφαρμογή IPTORRETS όπου όχι μόνο το spam αλλά και το δυσανάλογο download σε σχέση με τα uploaded δεδομένα τιμωρείται με ban.Η είσοδος επίσης σε αυτή την κοινότητα γίνεται κατόπιν invitation στον χρήστη και δημοκρατικής συζήτησης, κάτι που θυμίζει λίγο Usenet.

[17]Browser: http://el.wikipedia.org/wiki/Web_browser

Εικόνα 11. Το λογότυπο της IPTORRENTS στην κεντρική σελίδα

2.4.4 Firewalls, δυναμική IP, NAT: Το τέλος του ανοικτού δικτύου

Την ίδια στιγμή που η συνεταιριστική φύση του Διαδικτύου απειλούνταν, οι διαχειριστές του δικτύου έθεσαν σε εφαρμογή διάφορα μέτρα διαχείρισης που είχαν ως αποτέλεσμα το διαδίκτυο να μετατραπεί σε ένα πολύ λιγότερο ανοικτό δίκτυο. Κατά τις πρώτες ημέρες του Διαδικτύου, όλοι οι hosts ήταν ίσα συμμετέχοντες. Το δίκτυο ήταν συμμετρικό - εάν ένας host ήταν δυνατό να επικοινωνήσει στο διαδίκτυο, ο καθένας στο Διαδίκτυο μπορεί να επικοινωνήσει με αυτόν τον host. Κάθε υπολογιστής μπορούσε εξίσου να είναι πελάτης και server. Αυτή η δυνατότητα άρχισε να διαβρώνεται στα μέσα της δεκαετίας του 1990 με την ανάπτυξη του τείχους προστασίας, την χρήση δυναμικών διευθύνσεων IP, και την δημοτικότητα του Network Address Translation (NAT).

Καθώς το Διαδίκτυο ωρίμασε ήρθε η ανάγκη για την εξασφάλιση του δικτύου, για την προστασία των hosts από την απεριόριστη πρόσβαση . Από προεπιλογή, κάθε host που μπορεί να έχει πρόσβαση στο Διαδίκτυο μπορεί επίσης να αποτελεί πρόσβαση από κάποιους άλλους μέσω του διαδικτύου. Αφότου ο μέσος όρος των χρηστών δεν θα μπορούσε να χειριστεί τους κινδύνους ασφάλειας που προέκυψαν από μια συμμετρική σχεδίαση, οι διαχειριστές του δικτύου στράφηκαν προς τα τείχη προστασίας ως ένα εργαλείο για τον έλεγχο της πρόσβασης στις μηχανές τους.

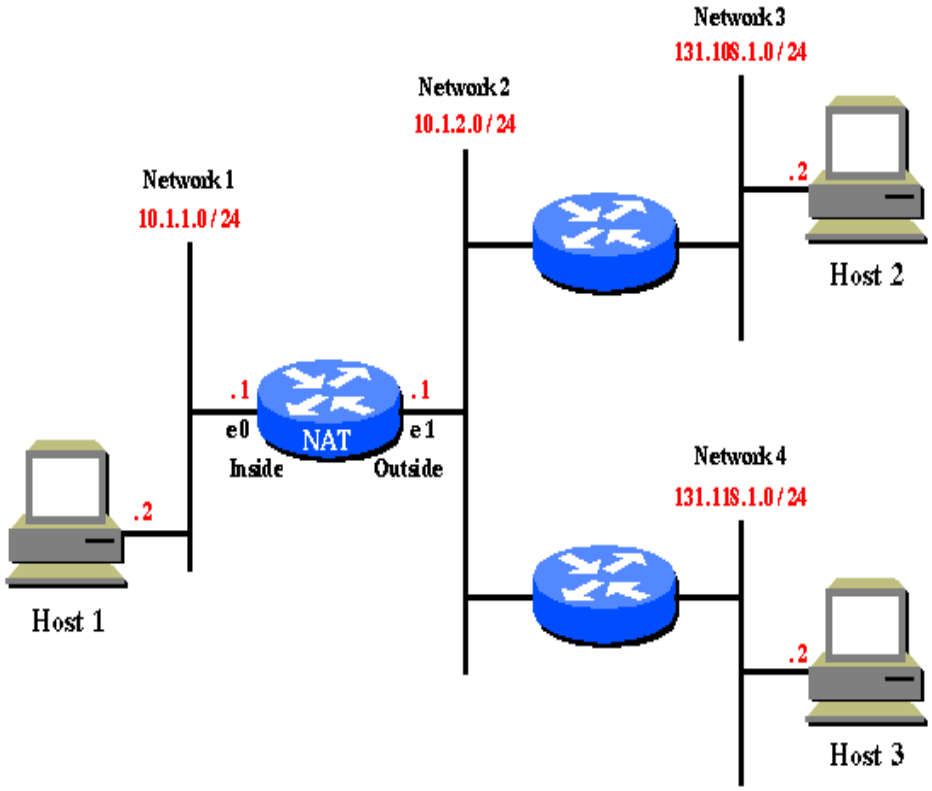
Τα Firewall στέκονται σαν μια πύλη μεταξύ του εσωτερικού δικτύου και του Internet. Τα πακέτα φιλτράρονται, και επιλέγεται ποια κυκλοφορία πακέτων θα περάσει και ποια θα κοπεί. Ένα τείχος προστασίας αποτελεί θεμελιώδη αλλαγή στο μοντέλο του Διαδικτύου: ορισμένα μέρη του δικτύου δεν δύνανται να επικοινωνήσουν με άλλα μέρη. Τα Firewalls είναι πολύ χρήσιμα εργαλεία για την ασφάλεια, αλλά αποτελούν σοβαρό εμπόδιο για peer to peer μοντέλα επικοινωνίας.

Ένα τυπικό τείχος προστασίας επιτρέπει σε οποιονδήποτε μέσα στο εσωτερικό δίκτυο να ξεκινήσει μια σύνδεση προς οποιονδήποτε στο Διαδίκτυο, αλλά εμποδίζει άλλους άγνωστους hosts του διαδικτύου από την έναρξη συνδέσεων με hosts στο εσωτερικό δίκτυο. Αυτό το είδος του τείχους προστασίας είναι σαν μία πύλη μονής κατεύθυνσης: μπορείς να βγεις έξω, αλλά δεν μπορείς να μπείτε μέσα Ένας host που προστατεύεται με τον τρόπο αυτό δεν μπορεί εύκολα να λειτουργήσει ως server. Το μόνο που μπορεί να είναι , είναι πελάτης. Επιπλέον, οι εξερχόμενες συνδέσεις μπορούν να περιορίζονται σε ορισμένες εφαρμογές όπως το FTP και το Web με το φράξιμο της κυκλοφορίας για ορισμένες θύρες από το τείχος προστασίας.

Το ότι επιτρέπεται σε έναν host να είναι μόνο πελάτης και όχι server , είναι ένα θέμα που προήλθε από τις αλλαγές στο Internet μετά την καταναλωτική έκρηξη. Με την αύξηση των χρηστών που συνδέονταν με μόντεμ στο Διαδίκτυο, η παλαιά πρακτική του να δίνεται σε κάθε host μια σταθερή διεύθυνση IP κατέστη ανέφικτη, επειδή δεν υπήρχαν αρκετές διευθύνσεις IP. Οι Δυναμικές διευθύνσεις IP είναι πλέον ο κανόνας για πολλούς κεντρικούς υπολογιστές στο Internet, όπου ένας συγκεκριμένος υπολογιστής μπορεί να αλλάζει κάθε μέρα. Οι Broadband Providers υπηρεσιών έχουν επίσης κάνει την διαπίστωση ότι οι δυναμικές IP είναι χρήσιμες για τις υπηρεσίες τους, δηλαδή της συνεχούς σύνδεσης στο διαδίκτυο . Το τελικό αποτέλεσμα είναι ότι πολλοί host στο Διαδίκτυο δεν είναι εύκολοι στην πρόσβαση, επειδή οι διευθύνσεις τους αλλάζουν διαρκώς. Οι Peer to peer εφαρμογές, όπως είναι το instant messaging και το file-sharing πρέπει να εξελιχθούν για να παρακάμψουν το πρόβλημα αυτό, δημιουργώντας δυναμικά directories για τους hosts.. Στις αρχές του Διαδικτύου, όπου οι hosts ήταν στατικοί, ήταν πολύ απλούστερα τα πράγματα.

Μια πρόσφατη τάση είναι όχι μόνο να μην δίνεται σε ένα host μια έγκυρη public διεύθυνση, αλλά αντί αυτού να χρησιμοποιείται το NAT για να αποκρυφτεί η διεύθυνση αυτή πίσω από ένα τείχος προστασίας. Το NAT συνδυάζει τα προβλήματα των firewalls και των δυναμικών διευθύνσεων IP: δεν είναι μόνο ασταθής η διεύθυνση κάποιου host, δεν είναι καν εφικτό να γίνει γνωστή! Κάθε επικοινωνία πρέπει να περάσει από ένα μοτίβο που ο δρομολογητής NAT να μπορεί να κατανοήσει, με αποτέλεσμα την μεγάλη απώλεια της ευελιξίας σε εφαρμογές επικοινωνίας. Για παράδειγμα, πολλά παιχνίδια στο Διαδίκτυο έχουν πρόβλημα με το NAT: κάθε παίκτης στο παιχνίδι θέλει να είναι σε θέση να επικοινωνήσει με κάθε άλλο παίκτη, αλλά τα πακέτα δεν μπορούν να περάσουν μέσω του δρομολογητή NAT. Το αποτέλεσμα είναι ότι ένας κεντρικός server στο Internet πρέπει να ενεργεί ως ένας δρομολογητής μηνυμάτων επιπέδου εφαρμογής, μιμούμενος τη λειτουργία που κάνει το πρωτόκολλο TCP / IP .

Τα Firewalls, η δυναμική IP, και το NAT γεννήθηκαν μέσα από μια σαφή ανάγκη στον τομέα της αρχιτεκτονικής του Διαδικτύου που επεκτάθηκε, για ασφαλή συστήματα. Έλυσαν μεν το πρόβλημα του να φέρουν εκατομμύρια υπολογιστές-πελάτες στο Διαδίκτυο γρήγορα και εύχρηστα, αλλά αυτές οι ίδιες τεχνολογίες έχουν μειώσει την υποδομή του Διαδικτύου στο σύνολό του, υποβιβάζοντας την πλειοψηφία των υπολογιστών στο να είναι μόνο πελάτες.



Εικόνα 12. Το Network Address Translation μέσω των αντίστοιχων δρομολογητών.

2.4.5 Ασύμμετρό Εύρος ζώνης

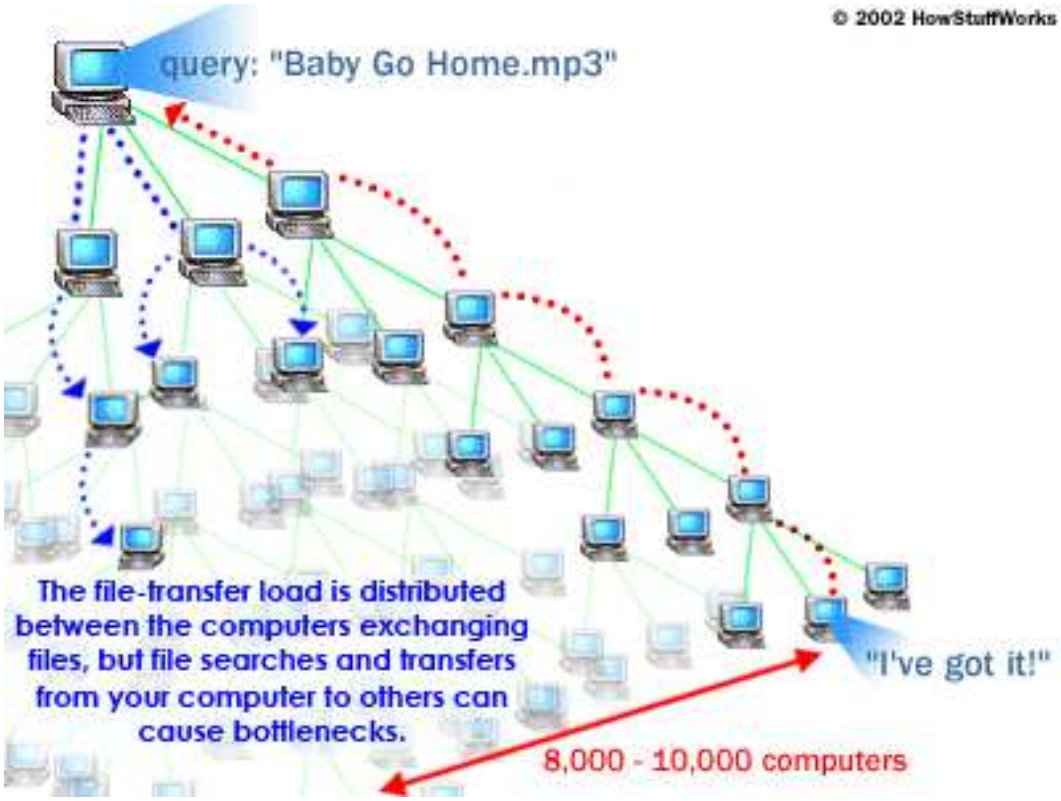
Μία τάση του Διαδικτύου στα τέλη της δεκαετίας του 1990 που αποτελεί πρόκληση για τις peer to peer εφαρμογές είναι η αύξηση των ασύμμετρων συνδέσεων δικτύου, όπως η ADSL και τα καλωδιακά μόντεμ. Προκειμένου να επωφεληθούν το μέγιστο από την αποτελεσματικότητα των διαθέσιμων καλωδίων, οι σημερινοί Broadband Providers επιλέγουν την παροχή ασύμμετρου εύρους ζώνης. Μια τυπική ADSL ή καλωδιακή εγκατάσταση με μόντεμ προσφέρει τρεις έως οκτώ φορές μεγαλύτερο εύρος ζώνης όταν παίρνει δεδομένα από το Διαδίκτυο(download) από ό, τι κατά την αποστολή δεδομένων σε αυτό(upload), ευνοώντας την χρήση ως client έναντι αυτής του server.

Το πρόβλημα σήμερα είναι ότι οι peer to peer εφαρμογές αλλάζουν την υπόθεση ότι οι τελικοί χρήστες μόνο θα κατεβάζουν από το Internet, και ποτέ δεν θα φορτώνουν σε αυτό.File-Sharing[18] εφαρμογές, όπως το Napster ή το Gnutella μπορούσαν(στην περίπτωση του πρώτου) να αντιστρέψουν το εύρος ζώνης, κάνοντας ένα μηχάνημα να στέλνει πιο πολλά αρχεία από ότι κατεβάζει. Αυτό όμως δεν μπορεί να εφαρμοστεί πλήρως. Ακόμη χειρότερα, τα στοιχεία του ελέγχου του TCP για τον ρυθμό μετάδοσης υπαγορεύουν πως εάν η διαδρομή προς τα πάνω έχει βουλώσει, το ίδιο συμβαίνει και στην διαδρομή του download. Έτσι, εάν ένας υπολογιστής που

[18]File sharing: http://en.wikipedia.org/wiki/File_sharing

ανεβάζει τα αρχεία με σχετικά αργό ρυθμό, δεν μπορεί εύκολα να κατεβάσει ταυτόχρονα με πιο γρήγορο ρυθμό.

Το ADSL και τα καλωδιακά μόντεμ χρησιμοποιούν ασύμμετρο εύρος ζώνης για κάθε μεμονωμένο χρήστη. Αυτή η χρήση παρατηρείται ακόμη πιο έντονα στα εσωτερικά δίκτυα των ISP , τα οποία έχουν σχεδιαστεί για ροή δεδομένων προς τους χρήστες και όχι από αυτούς. Το τελικό αποτέλεσμα είναι μια δικτυακή υποδομή που έχει βελτιστοποιηθεί για υπολογιστές που είναι μόνο πελάτες, όχι servers. Αλλά η peer to peer τεχνολογία γενικά κάνει κάθε host να λειτουργεί τόσο ως πελάτης όσο και server. Η παραπάνω ασύμμετρη υπόθεση θεωρείται εσφαλμένη. Δεν υπάρχει peer to peer εφαρμογή που να μπορεί να λειτουργεί σε ασύμμετρο εύρος ζώνης. Όσο οι peer to peer εφαρμογές γίνονται πιο διαδεδομένες, η αρχιτεκτονική του δικτύου θα πρέπει να αλλάξει για να χειριστεί καλύτερα τα νέα μοντέλα κυκλοφορίας δεδομένων.



Εικόνα 13.Το GNUTELLA απλοϊκά.

2.5 Παρατηρήσεις στις πρόσφατες σειρές των peer to peer εφαρμογών (2000)

Ενώ η νέα σειρά των peer to peer εφαρμογών μπορεί να πάρει μαθήματα από τα προηγούμενα μοντέλα, τις εφαρμογές αυτές εισάγουν επίσης νέα χαρακτηριστικά ή λειτουργίες .Οι εφαρμογές peer to peer μας επιτρέπουν να διαχωρίζουμε τις έννοιες της συγγραφής και δημοσίευσης πληροφοριών. Επίσης επιτρέπουν την αποκεντρωμένη εφαρμογή του σχεδιασμού, κάτι που είναι ταυτόχρονα μια ευκαιρία και μια πρόκληση.

2.5.1 Διαχωρισμός συγγραφής-δημοσίευσης

Μία από τις υποσχέσεις του Διαδικτύου είναι ότι οι άνθρωποι είναι σε θέση να είναι εκδότες του εαυτού τους, για παράδειγμα, χρησιμοποιώντας προσωπικές ιστοσελίδες για να γνωστοποιήσουν τις απόψεις και τα ενδιαφέροντά τους. Αυτό το λεγόμενο Self-publishing σίγουρα έχει γίνει πιο κοινό φαινόμενο με την εμπορευματοποίηση του Διαδικτύου. Πιο συχνά, ωστόσο, οι χρήστες ξοδεύουν τον περισσότερο χρόνο τους στην ανάγνωση (downloading) των πληροφοριών και λιγότερο χρόνο στην δημοσίευση(upload), και όπως αναφέρθηκε προηγουμένως, οι εμπορικές εταιρείες παροχής πρόσβασης στο Διαδίκτυο έχουν δομήσει την προσφορά τους γύρω από αυτή την ασυμμετρία.

Το παράδειγμα του Napster δημιουργεί μια ενδιαφέρουσα μέση οδό μεταξύ της ιδέας του ότι "ο καθένας δημοσιεύει" και τη φαινομενική πραγματικότητα του "όλοι καταναλώνουν". Το Napster ιδιαίτερα καθιστά πολύ εύκολο να δημοσιεύονται στοιχεία από κάποιον που δεν τα έχει συγγράψει. Στην πραγματικότητα, χρησιμοποιείται ως repeater ώστε να αναμεταδίδει τα δεδομένα τη στιγμή που αυτά φτάνουν σε διάφορους host. Αυτός είναι ο λόγος που πολλά δίκτυα, όπως campus κολλεγίων είχαν απαγορεύσει να χρησιμοποιείται το Napster.

Εικόνα 14.Το λογότυπο του NAPSTER.

Οι χρήστες δεν χρειάζεται να δημιουργούν περιεχόμενο, ώστε να μπορούν να το δημοσιεύσουν.

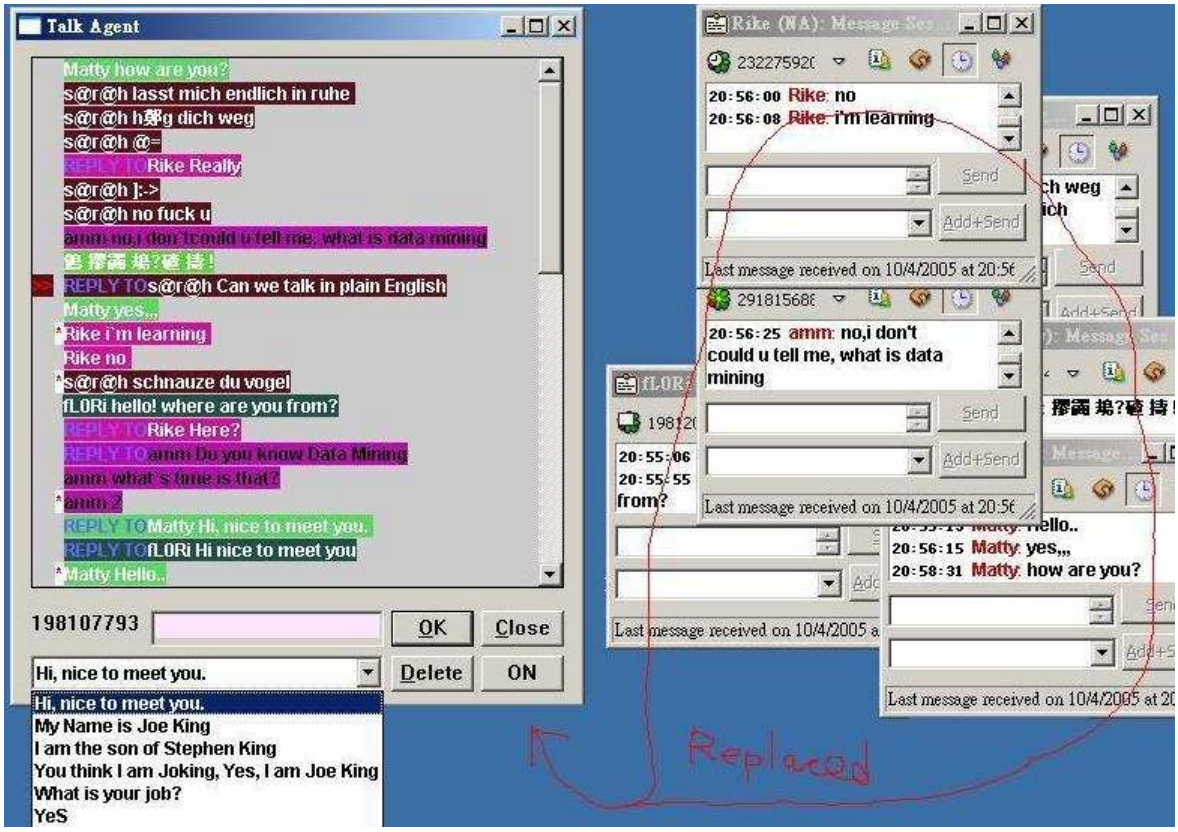
2.5.2 Αποκέντρωση

Τα peer to peer συστήματα φαίνεται να πηγαίνουν χέρι-χέρι με τα αποκεντρωμένα συστήματα. Σε ένα πλήρως αποκεντρωμένο σύστημα, δεν είναι μόνο κάθε host ισάξια συμμετέχοντας, αλλά δεν υπάρχουν hosts με ειδικές ικανότητες ή διοικητικούς ρόλους. Στην πράξη, να δημιουργηθεί ένα πλήρως αποκεντρωμένο σύστημα μπορεί να είναι δύσκολο, και πολλές peer to peer εφαρμογές χρησιμοποιούν υβριδικές προσεγγίσεις για την επίλυση των προβλημάτων. Όπως έχουμε ήδη δει, το DNS είναι peer to peer στο σχεδιασμό πρωτοκόλλου, αλλά με μια ενσωματωμένη έννοια της ιεραρχίας. Υπάρχουν πολλά άλλα παραδείγματα συστημάτων που είναι peer to peer εν γένει και όμως έχουν κάποια κεντρική οργάνωση πρακτικά, όπως το Usenet, το instant messaging, και το Napster.

Το Usenet είναι ένα διαφωτιστικό παράδειγμα της εξέλιξης ενός αποκεντρωμένου συστήματος. Το Usenet λειτουργεί συμμετρικά: Όλοι οι hosts μοιράζονται την κυκλοφορία . Όμως, λόγω του υψηλού κόστους της διατήρησης ενός πλήρους τροφοδότη , στην πράξη υπάρχει μια ραχοκοκαλιά(backbone) όπου οι εβρισκόμενοι πάνω σε αυτήν hosts φέρουν όλη την κυκλοφορία και εξυπηρετούν ένα μεγάλο αριθμό branch hosts ο ρόλος των οποίων είναι κυρίως να λαμβάνουν τα άρθρα. Εντός Usenet, υπήρχε μια φυσική τάση κυκλοφορικής ιεραρχίας, ακόμη και αν το υποκείμενο πρωτόκολλο δεν το απαιτούσε . Αυτή η μορφή της ήπιας κεντρικότητας μπορεί να αποδειχθεί οικονομική για πολλά peer to peer συστήματα με υψηλό κόστος μετάδοσης δεδομένων.

Πολλές άλλες τρέχουσες peer to peer εφαρμογές παρουσιάζουν ένα αποκεντρωμένο πρόσωπο αν και στηρίζονται σε ένα κεντρικό υπεύθυνο για τον συντονισμό των ενεργειών. Σε ένα χρήστη ενός συστήματος άμεσων μηνυμάτων, η εφαρμογή φαίνεται peer to peer, καθώς η αποστολή δεδομένων γίνεται άμεσα με τον άλλο συμμετέχοντα στην συζήτηση Αλλά όλα τα μεγάλα συστήματα instant messaging [19]έχουν κάποιου είδους server στο παρασκήνιο που διευκολύνει τους κόμβους να επικοινωνούν ο ένας με τον άλλο. Ο server δημιουργεί μια συσχέτιση μεταξύ του ονόματος του χρήστη και της τρέχουσας διεύθυνσης IP , αποστέλλει ενημερωτικά μηνύματα σε περίπτωση που ο χρήστης δεν είναι συνδεδεμένος και περνάει τα μηνύματα προς τους χρήστες μέσα από τα τείχη προστασίας. Ορισμένα συστήματα (όπως το ICQ)[20] επιτρέπουν την άμεση επικοινωνία όταν αυτό είναι δυνατόν, αλλά έχουν έναν κεντρικό υπολογιστή, ως εναλλακτική. Μια πλήρως αποκεντρωμένη προσέγγιση στο instant messaging δεν θα λειτουργούσε στο διαδίκτυο σήμερα.

[19] http://noc.auth.gr/services/voice-video/instantMessaging/index.html
[20] http://www.icq.com/download/



Εικόνα 15.Το GUI της εφαρμογής ICQ

Το Napster είναι άλλο ένα παράδειγμα ενός υβριδικού συστήματος. Η κοινή χρήση αρχείων στο Napster είναι αποκεντρωμένη: ένας client κατεβάζει ένα αρχείο απευθείας από την μηχανή άλλου client του Napster. Αλλά ο κατάλογος των αρχείων είναι κεντρικός, με τους servers του Napster να απαντούν σε ερωτήματα αναζήτησης να δημιουργούν συνδέσεις μεταξύ των πελατών. Αυτή η υβριδική προσέγγιση φαίνεται είναι καλή και οικονομική στην χρήση εύρους ζώνης, και η ανταλλαγή αρχείων μπορεί να συμβεί ακόμα και στα άκρα του δικτύου.

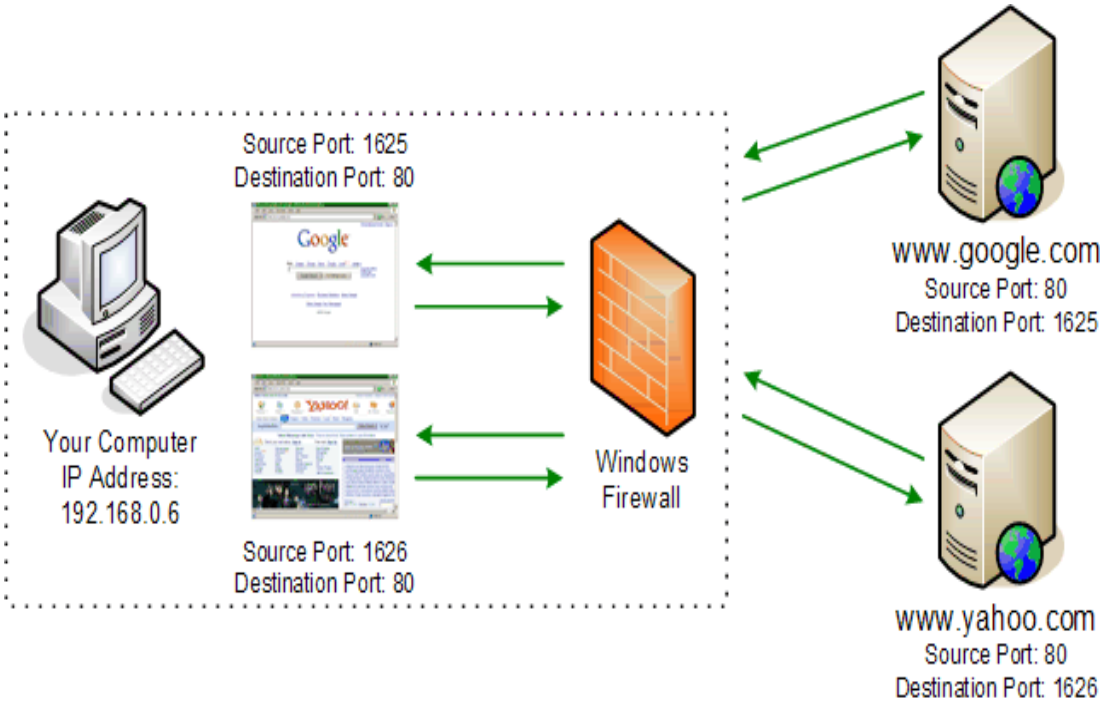
Στην πράξη, ορισμένες εφαρμογές μπορεί να λειτουργούν καλύτερα με ένα απόλυτα κεντρικό σχεδιασμό, και να μην χρησιμοποιούν καμία peer to peer τεχνολογία. Ένα παράδειγμα είναι μια αναζήτηση σε μια μεγάλη, σχετικά στατική βάση δεδομένων. Τρέχουσες μηχανές αναζήτησης στο διαδίκτυο είναι σε θέση να εξυπηρετήσουν έως και ένα δισεκατομμύριο σελίδες όλες από ένα μόνο σημείο.

Επίσης, εφαρμογές που απαιτούν συγκεντρωτική ανταλλαγή πληροφοριών είναι δύσκολο να εξαπλωθούν σε ένα αποκεντρωμένο δίκτυο. Για παράδειγμα, μια τοποθεσία δημοπρασιών πρέπει να εγγυηθεί ότι η καλύτερη τιμή κερδίζει. Αυτό μπορεί να είναι δύσκολο εάν η διαδικασία υποβολής προσφορών έχει εξαπλωθεί σε πολλές τοποθεσίες. Η αποκέντρωση δημιουργεί ένα εντελώς νέο κεφάλαιο στο διαδίκτυο με βλάβες: αναξιοπιστία, ανακριβή συγχρονισμό δεδομένων, κλπ. Οι σχεδιαστές peer to peer συστημάτων χρειάζονται να εξισορροπήσουν την δύναμη των peer to peer μοντέλων κατά των επιπλοκών και των περιορισμών των αποκεντρωμένων συστημάτων.

2.5.3 Κατάχρηση της port 80

Ένα από τα πιο περίεργα φαινόμενα στο σημερινό Διαδίκτυο είναι η κατάχρηση της θύρας 80[21], τη θύρα που χρησιμοποιεί για την κίνηση το πρωτόκολλο HTTP[22] όταν οι άνθρωποι surfάρουν στο διαδίκτυο .Τα Firewalls συνήθως φιλτράρουν την κυκλοφορία με βάση την κατεύθυνση της κίνησης (εισερχόμενη ή εξερχόμενη) και τον προορισμό της κυκλοφορίας. Επειδή το internet είναι μια κύρια εφαρμογή πολλών χρηστών του Διαδικτύου, σχεδόν όλα τα firewalls επιτρέπουν εξερχόμενες συνδέσεις στη θύρα 80, ακόμη και αν οι ρυθμίσεις του τείχους προστασίας είναι πολύ σφιχτές.

Κατά τις πρώτες ημέρες του Διαδικτύου, ο αριθμός της θύρας συνήθως αναφερόταν στο ποια εφαρμογή χρησιμοποιούσε το διαδίκτυο. Αλλά ακριβώς επειδή πολλά firewalls επιτρέπουν συνδέσεις στη θύρα 80, άρχισε δειλά μια ποικιλία εφαρμογών να την χρησιμοποιεί ως δίοδο. Streaming multimedia, άμεσα μηνύματα, ακόμη και κινητή τηλεφωνία εξυπηρετούνται μέσω της θύρας 80. Πιο πρόσφατες peer to peer εφαρμογές έχουν κάποιο τρόπο να χρησιμοποιούν τη θύρα 80, προκειμένου να παρακάμψουν τις πολιτικές ασφάλειας του δικτύου. Οπότε η αποτυχία των firewall συνίσταται στο ότι περνάει πολλές φορές κίνηση που πιθανόν να έπρεπε να γίνει block.



Εικόνα 16.Ενδεικτικά η απεικόνιση χρήσεως της port 80

[21] Port80:http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212808,00.html
[22] HTTP Protocol:http://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol

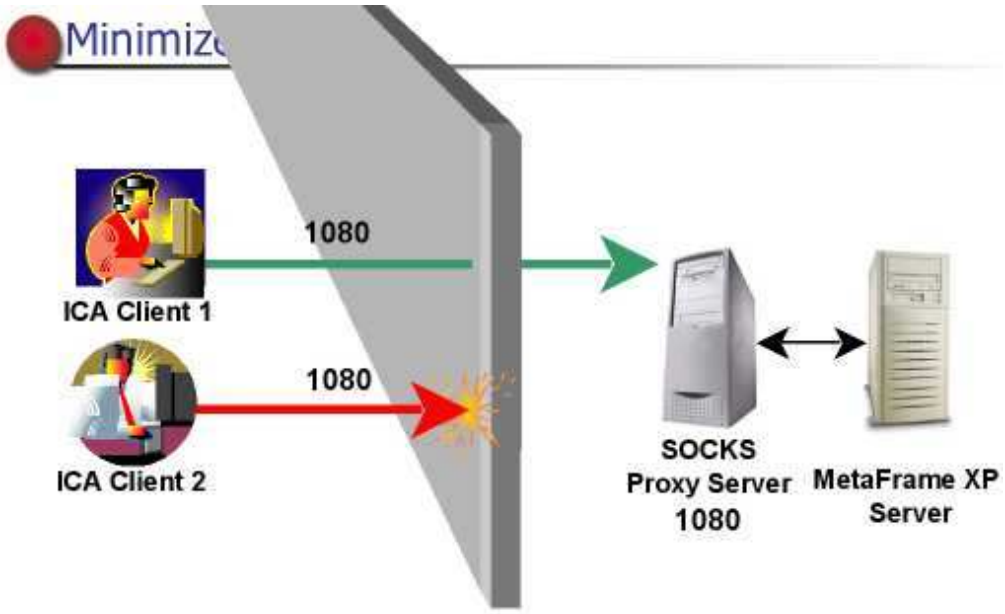
2.6 Συνταγές peer to peer για την σύγχρονη εποχή(2001-…)

Τελικά επιστροφή στα παλιά?

Όπως είδαμε η έκρηξη του internet στο καταναλωτικό πλαίσιο έφερε μαζί της αλλαγές που δυσκολεύουν την peer to peer δικτύωση. Τα firewall κάνουν δύσκολη την επικοινωνία με άλλους hosts και το NAT σε συνεργασία με τις δυναμικές IP την κάνουν αδύνατη. Οι τρέχουσες peer to peer εφαρμογές γενικά μπορούν να κερδίσουν πολλά από ένα δίκτυο που να μοιάζει με το αυθεντικό παλιό όπου δεν υπήρχαν τέτοιοι περιορισμοί. Πώς τελικά μπορούμε να κάνουμε τις σημερινές εφαρμογές peer to peer να είναι άκρως λειτουργικές με τα σημερινά τεχνολογικά δεδομένα?

Τα Firewall εξυπηρετούν μια σημαντική ανάγκη, επιτρέπουν στους διαχειριστές να εφαρμόζουν τις πολιτικές που θέλουν για την χρήση του δικτύου τους. Αυτό δεν θα αλλάξει με τις peer to peer εφαρμογές. Η λύση είναι να δημιουργηθούν firewall πιο έξυπνα ώστε να μπορούν να συνεργαστούν με τις peer to peer εφαρμογές συνεπώς να επιτρέπουν να περάσει η κίνηση που επιθυμεί ο διαχειριστής. Πρέπει να επιτρέπεται σε συστήματα πέραν αυτών να ζητούν άδεια να τρέξουν peer to peer εφαρμογές. Οι σχεδιαστές λοιπόν πρέπει να συνεισφέρουν σε αυτήν την προοπτική και να ενεργοποιήσουν τις εφαρμογές τους να χρησιμοποιούν αυτούς τους μηχανισμούς.

Μία καλή αρχή είναι το πρωτόκολλο SOCKS[23] με την χρήση ενός ενδιάμεσου proxy server,όμως πρέπει να διευρυνθεί ώστε να είναι πιο ευέλικτο σε εφαρμογές αντί σε απλούς αριθμούς συγκεκριμένων ports.



Εικόνα 17.Λειτουργία SOCKS Protocol με χρήση Proxy server

[23]SOCKS: http://en.wikipedia.org/wiki/SOCKS

Τα προβλήματα που δημιουργήθηκαν από τις τεχνολογίες δυναμικής IP και NAT ήδη έχουν τεχνική λύση, το IPV6[24].Αυτή η καινούργια έκδοση είναι η εξέλιξη της αρχιτεκτονικής πρωτοκόλλου Internet.To address space πλέον είναι 128 bit,αρκετά για κάθε host στο internet να έχει μια μόνιμη IP διεύθυνση ακριβώς όπως παλιά. Χωρίς αυτό οι peer to peer εφαρμογές είναι αναγκασμένες να συνεχίσουν να αντιμετωπίζουν αμαρτίες του παρελθόντος. Έτσι το μόνο που απομένει είναι να αναμείνουμε και να δούμε αν τελικά θα γίνει κοινά αποδεκτό αυτό το νέο πρωτόκολλο.

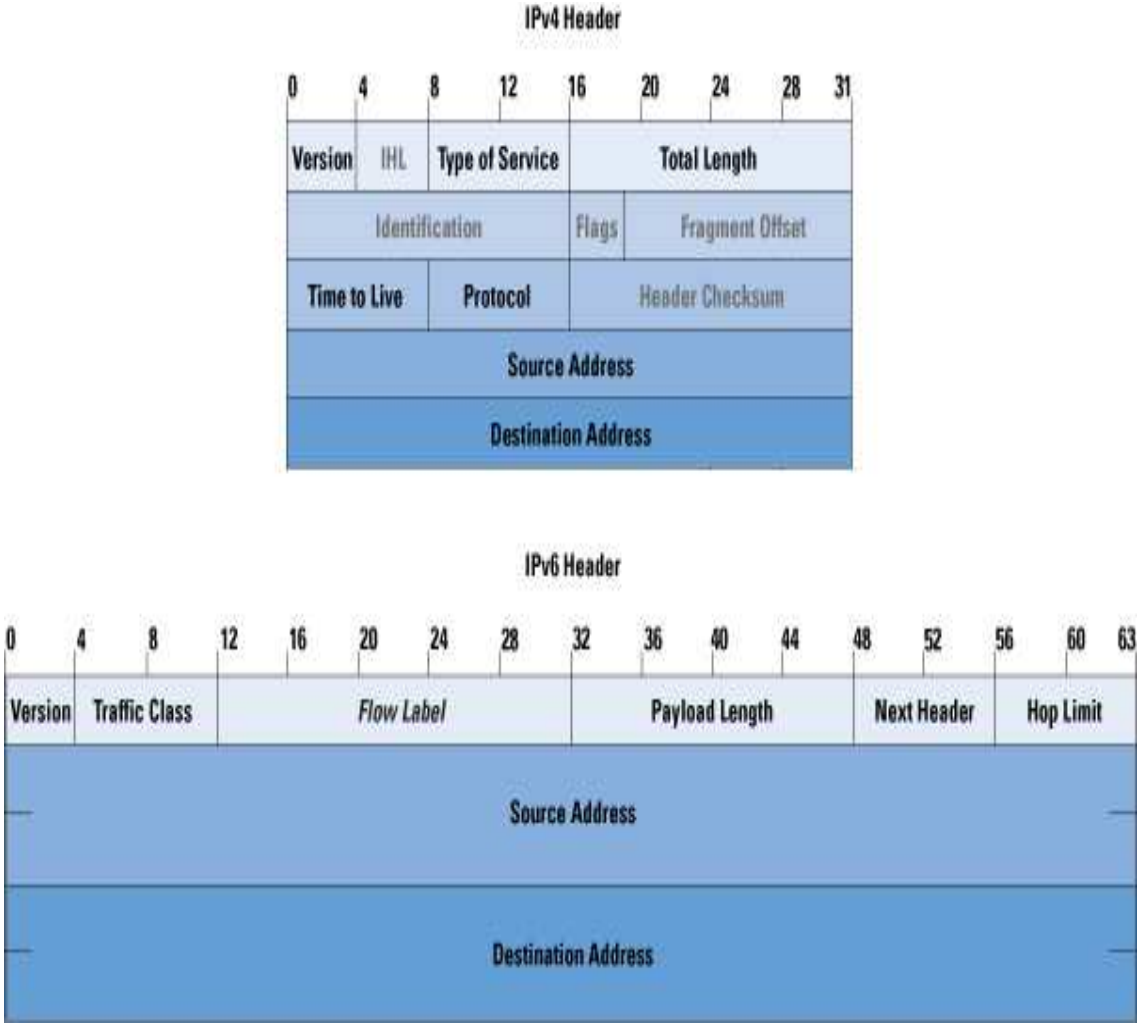
Οι peer to peer εφαρμογές τονώνουν τη χρήση του εύρους ζώνης του σημερινού Internet. Πρώτον, αμφισβητούν την υπόθεση της ασυμμετρίας την οποία το ADSL και το καλωδιακό μόντεμ υιοθετούν. Δεν υπάρχει απλός τρόπος που οι peer to peer εφαρμογές να μπορούν να επιλύσουν αυτό το πρόβλημα.

Ωστόσο, οι peer to peer εφαρμογές μπορούν να κάνουν πολλά πράγματα για να χρησιμοποιήσουν το υπάρχον εύρος ζώνης πιο αποτελεσματικά.

1) Η προσωρινή αποθήκευση των δεδομένων είναι μια φυσική επιλογή για κάθε peer to peer εφαρμογή που εκπέμπει στοιχεία. Θα ήταν μια σημαντική πρόοδος αν βεβαιωνόμασταν ότι ένα πρόγραμμα δεν στέλνει ξανά ή αναμεταδίδει δεδομένα σε άλλο host.

2) Μια peer to peer εφαρμογή πρέπει να διαθέτει αποτελεσματικά μέσα για να επιτρέπει στους χρήστες να ελέγχουν το εύρος ζώνης που χρησιμοποιεί η εκάστοτε υπηρεσία. Αν μπορώ να εκτελέσω μια εφαρμογή του Gnutella στο σπίτι, θα ήθελα να διευκρινιστεί ότι μπορεί να χρησιμοποιήσει μόνο το 50% του εύρους ζώνης μου. Τρέχοντα λειτουργικά συστήματα και βιβλιοθήκες δεν παρέχουν καλά εργαλεία για αυτού του είδους τον περιορισμό, αλλά όσο οι peer to peer εφαρμογές θα απαιτούν περισσότερους πόρους δικτύου από υπολογιστές, οι χρήστες θα πρέπει να χρησιμοποιήσουν τέτοια εργαλεία για τον έλεγχο πιθανής υπερβολικής χρήσης των πόρων.

[24] IPV6:http://www.ipv6.org/



Εικόνα 18.Οι headers μίας διεύθυνσης IPV6

2.7 Επίλογος

Το Internet ξεκίνησε ως ένα εντελώς συμμετρικό, peer to peer δίκτυο που περιελάμβανε συνεργαζόμενους χρήστες. Όσο το διαδίκτυο μεγάλωνε με σκοπό να φιλοξενήσει τους εκατομμύρια προσερχόμενους σε αυτό χρήστες, οι διάφορες τεχνολογίες πρωτοκόλλων διαμορφώθηκαν έτσι ώστε τελικά κατακερμάτισαν το Internet σε συστήματα με σχετικά λίγους server και πάρα πολλούς clients την ίδια στιγμή που διάφορες τεχνολογίες για να αποφευχθούν αντικοινωνικές συμπεριφορές αποξενώνουν έως εσχάτων τους υπάρχοντες hosts.

Αυτά τα φαινόμενα στέκονται ως προκλήσεις στις εφαρμογές peer to peer. Τόσο το διαδίκτυο όσο και οι εφαρμογές αυτές εν γένει σχεδιάστηκαν για να λειτουργούν σε αλληλουχία. Πρέπει να γίνει κατανοητό ότι το peer to peer σήμερα αποτελεί την online δημοκρατία, μια πηγή ελεύθερων αρχείων μακριά από την σημερινή εμπορευματοποίηση, μια πηγή μαζικής διανομής ελεύθερου κώδικα και προϊόντων ψυχαγωγίας. Τι και αν το Napster υπέκυψε στις δικαστικές διαμάχες πνευματικών δικαιωμάτων υπάρχουν τόσες άλλες εφαρμογές που αντέχουν στις αντίξοες από πλευράς αρχιτεκτονικής και όχι μόνο συνθήκες και μπορούν τελικά σταδιακά να επαναφέρουν τον original χαρακτήρα του Internet, τον peer to peer.

Κεφάλαιο 3

Bιt-Torrent και ο μTorrent client

3.1 Εισαγωγή στο Bit-Torrent software

Ένα peer to peer σύστημα όπως είδαμε και παραπάνω είναι ο διαμοιρασμός υπολογιστικών πόρων και υπηρεσιών με άμεση ανταλλαγή μεταξύ των συστημάτων.Το Bit-Torrent[25] είναι ένα peer-to-peer software που αναπτύχθηκε από τον Bram Cohen και την Bit-Torrent, Inc που χρησιμοποιείται για την αποστολή και λήψη αρχείων μέσω του Bit-Torrent πρωτοκόλλου.Το Bit-Torrent ήταν ο πρώτος client που γράφτηκε για το πρωτόκολλο αυτό. Το παρατσούκλι του είναι Mainline από τους προγραμματιστές το οποίο δηλώνει επισήμως την προέλευσή του. Από την έκδοση 6.0 και μετά, ο Bit-Torrent client είναι μια επανέκδοση του μTorrent. Ως εκ τούτου, δεν παρέχει πλέον πηγαίο κώδικα , και είναι προς το παρόν διαθέσιμο μόνο για Windows και Mac OS X 10.5.x.

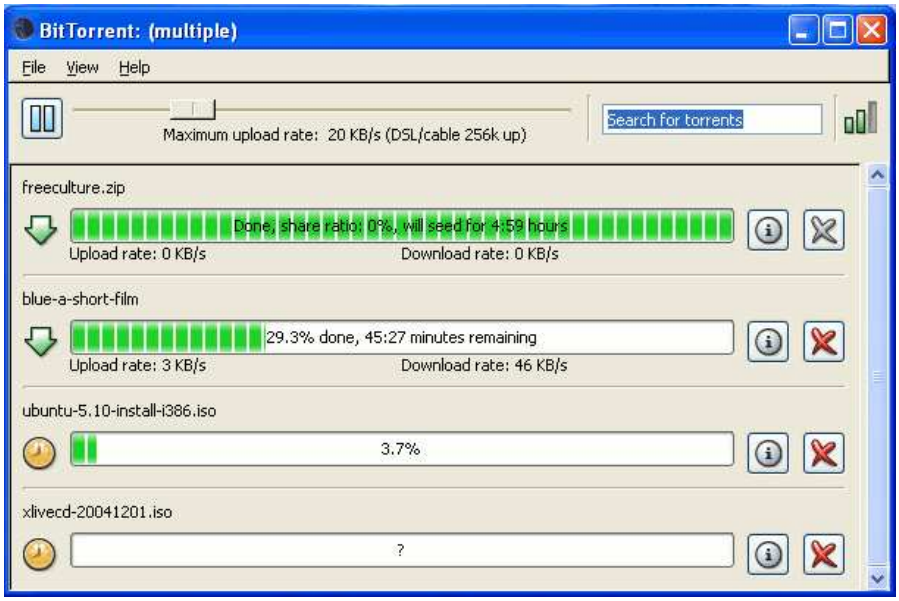
Η έκδοση 4.20 του client ονομάστηκε Allegro από την Bit-Torrent Inc και αναπτύχθηκε από την εν λόγο εταιρεία για την επιτάχυνση της λήψης καθώς και για την καλύτερη διαχείρηση του ληφθέντος υλικού.

Πριν από την έκδοση 6.0,το Bit-Torrent ήταν γραμμένο σε Python, και ήταν ελεύθερο λογισμικό. Ο πηγαίος κώδικας για τις εκδόσεις 4.x και 5.x έχει τεθεί στο πλαίσιο του Bit-Torrent Open Source License, μια τροποποιημένη έκδοση της Άδειας Jabber Open Source. Εκδόσεις μέχρι και την 3.4.2 διανεμήθηκαν υπό την άδεια του MIT.Η έκδοση 5.3 και η έκδοση 4.0 ήταν relicensed υπό την GPL. (General Public License)

Το Bit-Torrent software επιτρέπει σε ένα χρήστη να αναζητήσει και να κάνει download torrent αρχεία χρησιμοποιώντας ένα ενσωματωμένο πλαίσιο αναζήτησης («αναζήτηση για torrents»), στο κύριο παράθυρο, το οποίο ανοίγει την σελίδα αναζήτησης του Torrent search engine με τα αποτελέσματα αναζήτησης να δίνονται στον browser του χρήστη .

[25]BitTorrent: http://www.bittorrent.com/btusers/download/?

Ο τρέχων client δίνει μια σειρά από χαρακτηριστικά, συμπεριλαμβανομένων των πολλαπλών παράλληλων λήψεων. Το Bit-Torrent έχει αρκετές στατιστικές, πίνακες και γραφικές απόψεις που επιτρέπουν σε ένα χρήστη να δει τι γεγονότα συμβαίνουν στο παρασκήνιο. Μια σειρά από παραστάσεις προσφέρουν πληροφορίες σχετικά με τον αριθμό των peers και των seeds που είναι παρόντες, από τον όγκο των δεδομένων των οποίων γίνεται λήψη μέχρι τον όγκο των δεδομένων που έχει γίνει upload. Διαθέτει σύστημα αυτόματης επαναφοράς το οποίο ελέγχει όλα τα στοιχεία που έχουν χρησιμοποιηθεί, μετά από έναν αναπάντεχο τερματισμό, όπως μια διακοπή ρεύματος. Είναι επίσης ένας ενδιάμεσος σταθμός ανταλλαγής πακέτων μεταξύ του εαυτού του, http servers[26] και άλλων πελατών, αποφέροντας έτσι μεγάλη βελτίωση της αποτελεσματικότητας της διανομής. Ο client αυτός δίνει επίσης τη δυνατότητα στους χρήστες να δημιουργούν και να μοιράζονται αρχεία torrent.



Εικόνα 19 BitTorrent: Ένα δείγμα πολλαπλού download

3.2 Το Bit-Torrent Protocol

3.2.1 Γενικά για το πρωτόκολλο

Το Bit-Torrent protocol[27] είναι ένα πρωτόκολλο για peer to peer ανταλλαγή αρχείων που χρησιμοποιείται για τη διανομή μεγάλων ποσοτήτων δεδομένων. Το Bit-Torrent είναι ένα από τα πιο κοινά πρωτόκολλα για τη μεταφορά μεγάλων αρχείων, και εκτιμάται ότι αντιπροσωπεύει περίπου το 27-55% της συνολικής κίνησης του Internet (ανάλογα με τη γεωγραφική θέση) σύμφωνα με πηγή από την επίσημη σελίδα www.utorrent.com το Φεβρουάριο του 2009.

[26] File Server: http://en.wikipedia.org/wiki/File_server
[27] BitTorrent protocol: http://en.wikipedia.org/wiki/BitTorrent_(protocol)

Το πρωτόκολλο αυτό επιτρέπει στους χρήστες να διανέμουν μεγάλο όγκο δεδομένων. Το πρωτόκολλο επίσης λειτουργεί ως μια εναλλακτική μέθοδος διανομής των δεδομένων που κάνει ακόμη και μικρές υπολογιστικές συσκευές (π.χ. κινητά τηλέφωνα) με χαμηλό εύρος ζώνης να μπορούν να συμμετέχουν σε μεγάλες μεταφορές δεδομένων. Η διαδικασία έχει ως εξής:

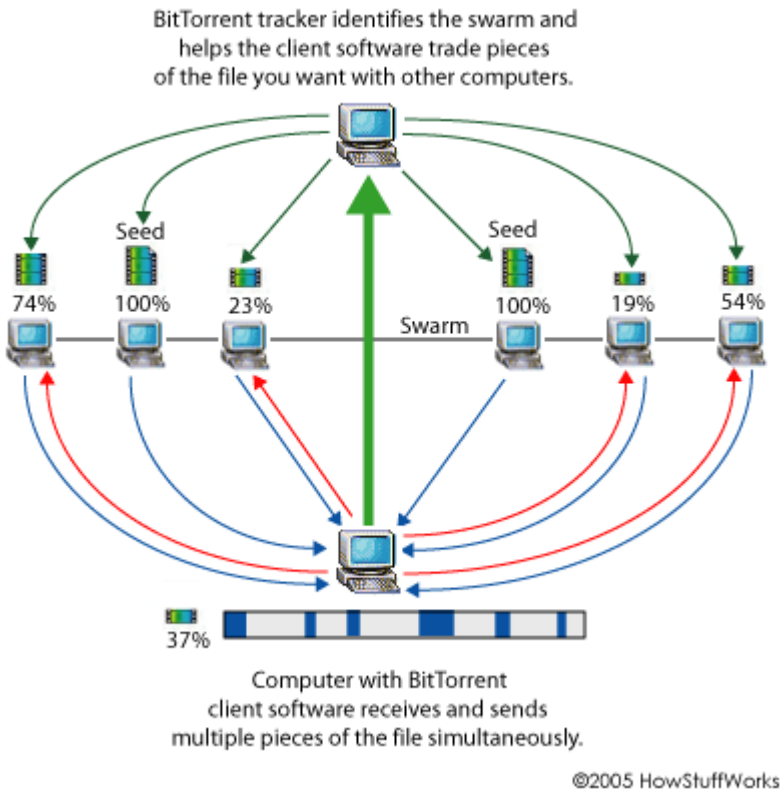
Πρώτον, ο χρήστης παίζοντας το ρόλο του αρχείου-πηγή, θέτει ένα αρχείο στη διάθεση του δικτύου. Το αρχικό αρχείο χρήστη που γίνεται upload ονομάζεται seed και παρουσιάζει τη διαθεσιμότητα του για το δίκτυο και παράλληλα επιτρέπει προς άλλους χρήστες, που αποκαλούνται peers, να συνδεθούν και να αρχίσουν να κατεβάζουν το seed.

Δεύτερον,όταν νέοι peers συνδεθούν στο δίκτυο και ζητήσουν download από το αρχείο, ο υπολογιστής τους λαμβάνει ένα διαφορετικό κομμάτι των δεδομένων από το seed. Μόλις πολλαπλοί peers έχουν πολλαπλά κομμάτια του seed,το Bit-Torrent επιτρέπει σε καθένα από αυτούς να γίνεις up loader για το τμήμα εκείνο του αρχείου μετά την πλήρη ανάκτηση του από τον κάθε peer. Το αποτέλεσμα αυτού είναι να αναλάβουν ένα μικρό μέρος των καθηκόντων προς ανακούφιση του αρχικού χρήστη, διανέμοντας το αρχείο λήψης μεταξύ των seeders και πολλών peers. Με το Bit-Torrent, κανείς υπολογιστής δεν χρειάζεται για να παρέχει δεδομένα σε ποσότητες που θα μπορούσαν να θέσουν σε κίνδυνο την καλή διανομή των πόρων.Να σημειψθεί ότι οι παραπάνω χρήστες οι οποίοι συνδέονται και μοιράζονται ταυτόχρονα κομμάτια του ίδιου αρχείου ονομάζονται Swarm.

Τρίτον, αφότου το αρχείο έχει ανακτηθεί με επιτυχία από ένα συγκεκριμένο peer, ο peer είναι σε θέση να αντιστρέψει τους ρόλους και να γίνει ένας πρόσθετος seeder, βοηθώντας τους υπόλοιπους peers να λάβουν το σύνολο του φακέλου. Αυτή η ενδεχόμενη εναλλαγή από peer σε seeder καθορίζει τη συνολική «υγεία» του αρχείου (όπως καθορίζεται από τον αριθμό των φορών που ένα αρχείο είναι διαθέσιμο στην ολοκληρωμένη μορφή του).

Αυτή η κατανεμημένη φύση του Bit-Torrent οδηγεί σε μια πλημμύρα σαν εξάπλωση ενός αρχείου σε όλους τους peers. Καθώς όλο και περισσότεροι peers έρχονται να ενταχθούν στην ομάδα, η πιθανότητα μιας επιτυχούς λήψης αυξάνεται. Γενικά επιτυγχάνεται μια σημαντική μείωση αναγκαίων πόρων hardware και bandwidth για τον αρχικό διανομέα. Παρέχει, επίσης, μείωση των προβλημάτων του συστήματος, μειώνει την εξάρτηση από το αρχικό διανομέα και παρέχει μια πηγή για το αρχείο ,πολλαπλή από ένα σημείο και μετά και επομένως το καθιστά πιο εύκολο στον εντοπισμό του από ότι προβλέπεται με τις πρότυπες τεχνικές διανομής αρχείων από συγκεκριμένη πηγή.

Ο προγραμματιστής Bram Cohen σχεδίασε το πρωτόκολλο τον Απρίλιο του 2001 και κυκλοφόρησε σε πρώτη έκδοση στις 2 Ιουλίου 2001.Πλέον διατηρείται από την εταιρεία Cohen Bit-Torrent, Inc .Υπάρχουν πολυάριθμοι Bit-Torrent clients που διατίθενται για διάφορες πλατφόρμες. Σε αυτούς θα αναφερθούμε εκτενέστερα αργότερα.



Εικόνα 20.BitTorrent:Ένα παράδειγμα της λειτουργίας του πρωτοκόλλου του

3.2.2 Λειτουργία του πρωτοκόλλου

Ένας Bit-Torrent client είναι κάθε πρόγραμμα που υλοποιεί το πρωτόκολλο Bit-Torrent. Κάθε client είναι σε θέση να προετοιμάζει, να ζητά, και να διαβιβάζει οποιοδήποτε τύπο αρχείου υπολογιστή μέσω δικτύου, χρησιμοποιώντας το πρωτόκολλο. Ένας peer είναι κάθε υπολογιστής που εκτελεί έναν οποιοδήποτε Bit-Torrent client και όχι μόνο.

Για να διαμοιραστεί ένα αρχείο ή μια ομάδα αρχείων, ο κάθε peer δημιουργεί ένα μικρό αρχείο που ονομάζεται "torrent" (π.χ.File.Torrent). Αυτό το αρχείο περιέχει metadata (χαρακτηρίζονται και ως data των data καθώς περιέχουν τεχνικές λεπτομέρειες) σχετικά με τα αρχεία που διαμοιράζονται και σχετικά με τον tracker, τον υπολογιστή δηλαδή που συντονίζει τη διανομή αρχείων. Οι peers που θέλουν να κατεβάσουν το αρχείο πρέπει πρώτα να αποκτήσουν ένα torrent αρχείο για αυτό, και να συνδεθούν με το συγκεκριμένο tracker, που τους λέει, από ποιούς άλλους peers να κατεβάσουν τα κομμάτια του αρχείου.

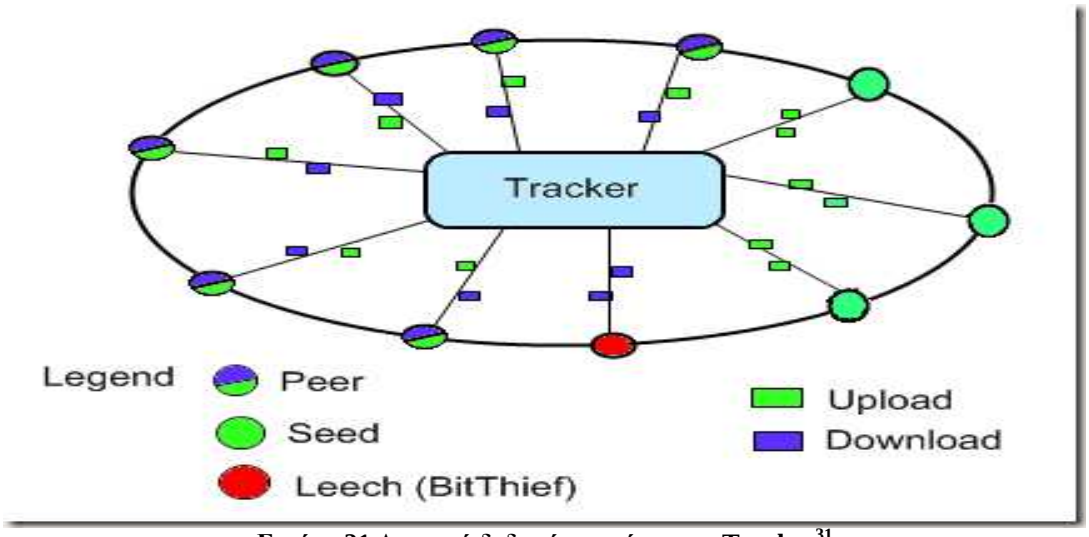
Αν και οι δύο τρόποι έχουν ως αποτέλεσμα τη μεταφορά αρχείων μέσω δικτύου, ένα Bit-Torrent download διαφέρει από μια κλασική λήψη (όπως HTTP ή FTP[28] αίτηση, για παράδειγμα) σε ένα κυρίως σημείο:

[28] FTP: http://el.wikipedia.org/wiki/File_Transfer_Protocol

Το Bit-Torrent κάνει πολλές μικρές αιτήσεις δεδομένων μέσω διαφορετικών συνδέσεων TCP σε διαφορετικές μηχανές, ενώ το κλασσικό download γίνεται συνήθως μέσω μίας σύνδεσης TCP σε μία μόνο μηχανή.

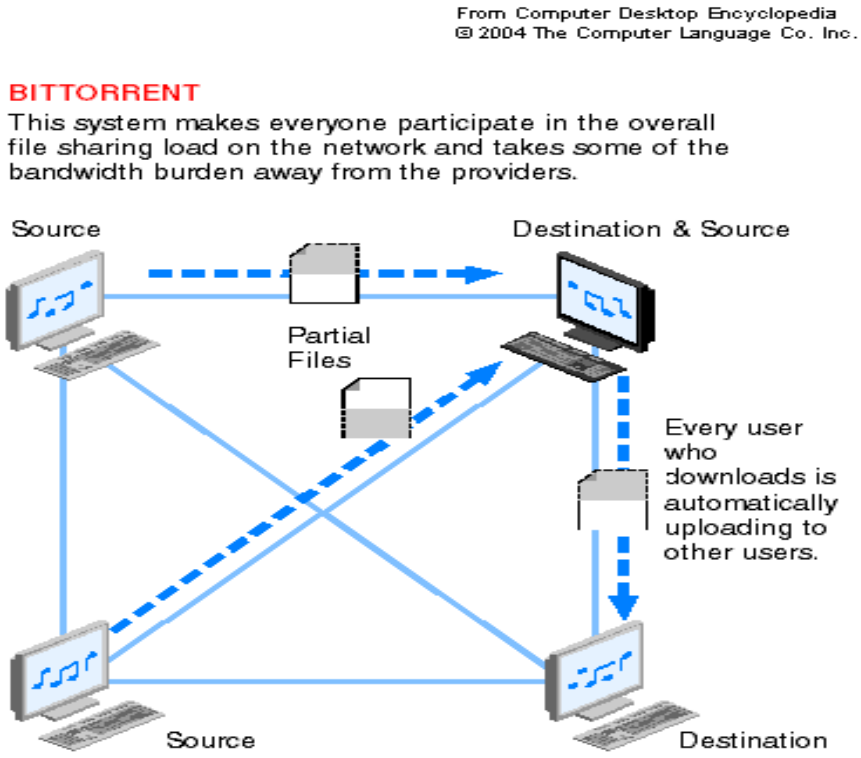
Στο σύνολό τους, οι όποιες διαφορές υπάρχουν, επιτρέπουν στο Bit-Torrent την επίτευξη πολύ χαμηλότερου κόστους για τον provider του περιεχομένου, πολύ υψηλότερο πλεονασμό, και πολύ μεγαλύτερη αντοχή σε κατάχρηση από ότι το κλασσικό λογισμικό Server. Ωστόσο, η προστασία αυτή, θεωρητικά, έρχεται με ένα κόστος: Τα downloads μπορεί να πάρουν χρόνο για την επίτευξη μέγιστης ταχύτητας ,διότι μπορεί να χρειαστεί αρκετός χρόνος για να δημιουργηθούν οι διάφορες TCP συνδέσεις με τους εκάστοτε peers, και μπορεί να χρειαστεί πολύς χρόνος για έναν κόμβο να λάβει επαρκή στοιχεία για να γίνει ένας αποτελεσματικός up loader. Αυτό έρχεται σε αντίθεση με τις κλασσικές τακτικές λήψης (όπως από ένα Server HTTP, για παράδειγμα) , ενώ είναι πιο ευάλωτες στην υπερφόρτωση και κατάχρηση, φτάνουν στην μέγιστη ταχύτητα πολύ γρήγορα και την διατηρούν σε όλη την διάρκεια της διαδικασίας. Επιπλέον υπάρχει το πρόβλημα του Leech που θα παρουσιαστεί παρακάτω και αναφέρεται στην αποφυγή upload μετά την ολοκλήρωση της λήψης.

Σε γενικές γραμμές, η φύση του Bit-Torrent απέναντι σε μεθόδους μη συνεχόμενου download, το εμπόδισαν να υποστηρίζει τα λεγόμενα «προοδευτικά downloads" ή τις "streaming αναπαραγωγές πολυμέσων". Ωστόσο, παρατηρήσεις που διατυπώθηκαν από τον Bram Cohen τον Ιανουάριο του 2007[29] δείχνουν ότι τα streaming[30] torrent downloads σύντομα θα είναι καθημερινότητα.



Εικόνα 21.Διανομή δεδομένων μέσω του Tracker[31]

[29] Cohen Interview 2007 http://torrentfreak.com/interview-with-bram-cohen-the-inventor-of-bittorrent/
[30] Streaming Media: http://en.wikipedia.org/wiki/Streaming_media
[31] Tracker: http://en.wikipedia.org/wiki/BitTorrent_tracker



Εικόνα 22. Διανομή δεδομένων σε ένα file sharing σύστημα

3.2.3 Δημιουργία και δημοσίευση των torrent files

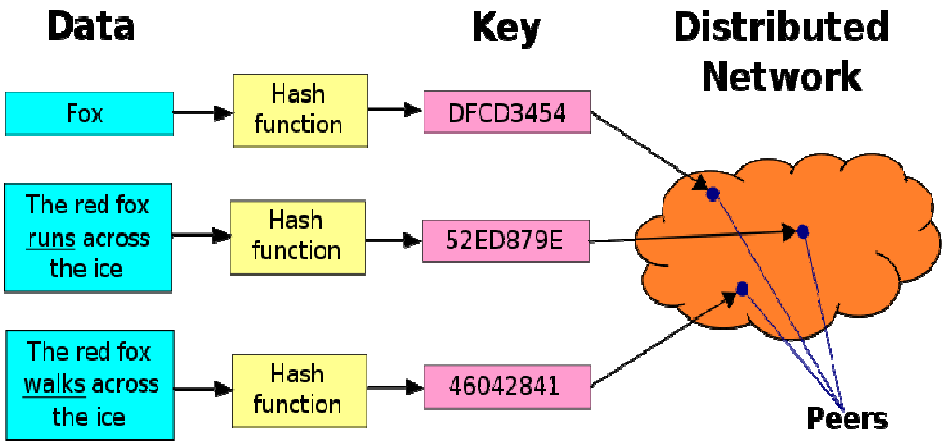
Ο peer που διανέμει ένα αρχείο δεδομένων θεωρεί το αρχείο ως μια σειρά πανομοιότυπων κομματιών μεγέθους, συνήθως μεταξύ 32 KB και 4 MB το καθένα. Ο peer δημιουργεί ένα checksum δηλαδή ένα κωδικοποιημένο κομμάτι για κάθε ένα αντίστοιχο κομμάτι της εισόδου, χρησιμοποιώντας το SHA1[32] hash αλγόριθμο , και τα καταγράφει όλα αυτά στο αρχείο torrent. Τεμάχια μεγέθους άνω των 512 KB θα μειώσουν το μέγεθος ενός αρχείου torrent που απαιτείται για ένα πολύ μεγάλο φορτίο, αλλά υποστηρίζεται ότι προκαλεί μείωση στην αποτελεσματικότητα του πρωτοκόλλου . Όταν κάποιος άλλος peer λάβει αργότερα ένα συγκεκριμένο κομμάτι, το checksum[33] του κομματιού συγκρίνεται με το πιο πρόσφατα καταγεγραμμένο checksum για να εξακριβωθεί ότι το κομμάτι δεν είναι λάθος. Οι peers που παρέχουν ένα πλήρες αρχείο ονομάζονται seeders, και οι peers που παρέχουν το αρχικό αντίτυπο αποκαλούνται initial seeders.Πολλές φορές οι peers που μια δεδομένη χρονική στιγμή κατεβάζουν ένα αρχείο και προφανώς δεν είναι ακόμα up loaders ή δεν γίνονται ποτέ ,χαρακτηρίζονται ως Leechers .

Οι ακριβείς πληροφορίες που περιέχονται στο αρχείο torrent εξαρτώνται από την έκδοση του πρωτοκόλλου Bit-Torrent. Κατά σύμβαση, το όνομα ενός αρχείου torrent έχει την κατάληξη. Torrent.Τα αρχεία torrent έχουν ένα τμήμα, το οποίο προσδιορίζει το URL του tracker(announce section), και ένα info section , που περιέχει ονόματα για τα αρχεία, το μήκος τους, το μήκος του κομματιού που χρησιμοποιείται, καθώς

[32] SHA1:http://en.wikipedia.org/wiki/SHA_hash_functions
[33] Checksum:http://www.online-tech-tips.com/cool-websites/what-is-checksum/el/

και SHA-1 hash κώδικα για κάθε κομμάτι αφού όλα αυτά τα κομμάτια είναι checksums, τα οποία χρησιμοποιούνται από τους πελάτες για την επαλήθευση της ακεραιότητας των δεδομένων που λαμβάνουν.

Τα αρχεία Torrent συνήθως δημοσιεύονται σε ιστοσελίδες ή αλλού, και έχουν καταγεγραμμένο τουλάχιστον ένα tracker. Ο tracker διατηρεί καταλόγους των clients που συμμετέχουν στο Torrent. Εναλλακτικά, σε ένα σύστημα χωρίς tracker κάθε peer ενεργεί ως tracker.Το Azureus ήταν ο πρώτος Bit-Torrent client ο οποίος εφάρμοσε την ιδέα ενός τέτοιου συστήματος, μέσω Distributed hash tables (DHT).Μ[34]ε την συγκεκριμένη μέθοδο τα κομμάτια των αρχείων κωδικοποιούνταν με τέτοιο τρόπο ώστε να μπορούν να είναι πιο εύκολα στον εντοπισμό μέσα σε ένα αποκεντρωμένο σύστημα. Μια εναλλακτική στο DHT σύστημα, γνωστή ως Mainline DHT(Kademlia)[35], αναπτύχθηκε αργότερα και έγινε αποδεκτή από μια σειρά Bit-Torrent clients μεταξύ αυτών και το μTorrent.



Εικόνα 23.Μια αναπαράσταση της διαδικασίας του DHT

Μετά που το DHT υιοθετήθηκε, μια "private flag"[36](δηλαδή ειδικά αναγνωριστικά bits ανάλογα με αυτά που χρησιμοποιούνται στο Broadcasting[37]) εισήχθη ανεπίσημα, λέγοντας στους πελάτες να περιορίσουν τη χρήση του αποκεντρωμένου tracking, ανεξάρτητα από τις επιθυμίες του χρήστη. Ο σκοπός του flag είναι η πρόληψη ώστε να μην μοιράζονται torrents μεταξύ πελατών που δεν έχουν πρόσβαση στον tracker. Βεβαίως δεν έγινε δεκτή αυτή η αλλαγή με χαρά, πάντως οι πελάτες που την αγνόησαν έχουν υποστεί ban από τους εκάστοτε trackers ώστε να απαξιωθούν τέτοιες ενέργειες.

Οι χρήστες περιηγούνται στο διαδίκτυο με κάποιον browser για να βρουν ένα torrent αρχείο που τους προκαλεί το ενδιαφέρον, να το κατεβάσουν και να το ανοίξουν με έναν Bit-Torrent client. Ο πελάτης συνδέεται με τον tracker (pirate bay etc) που καθορίζεται μέσα στο αρχείο torrent.Μέσω του flag, από το οποίο λαμβάνει μια λίστα

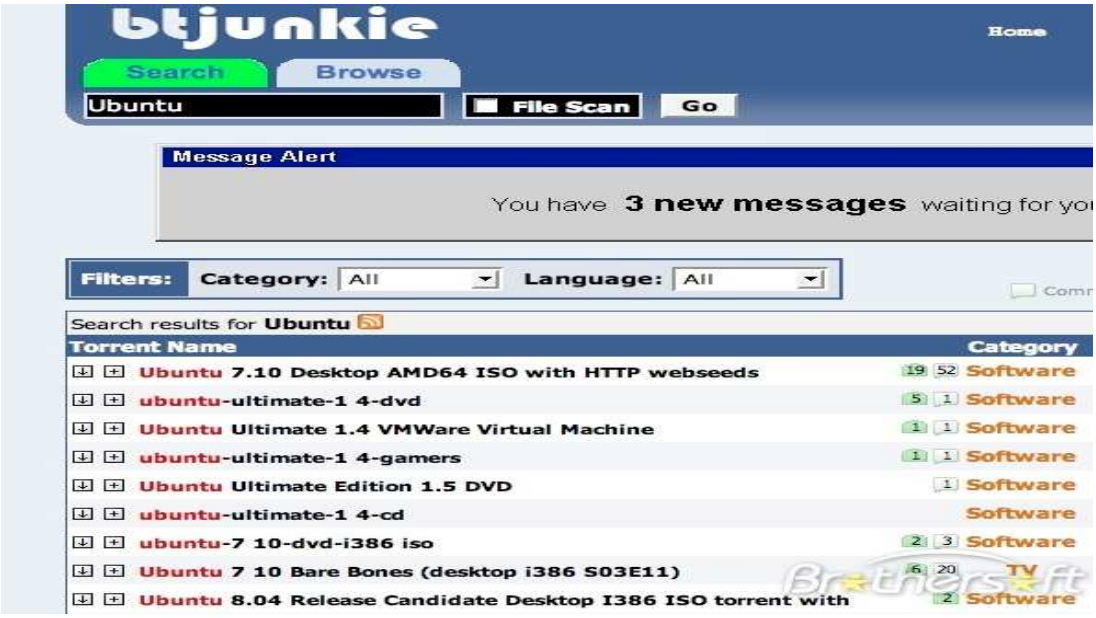
[34]DHT: http://en.wikipedia.org/wiki/Distributed_hash_table
[35] Kademlia: http://en.wikipedia.org/wiki/Kademlia
[36]Private Flag: http://forum.utorrent.com/viewtopic.php?id=7463
[37] Broadcasting: http://en.wikipedia.org/wiki/Broadcasting

των peers που εκείνη την στιγμή μεταφέρουν κομμάτια του αρχείου/ων που καθορίζονται στο Torrent, ο πελάτης συνδέεται με τους peers αυτούς για να αποκτήσει αυτά τα κομμάτια του αρχείου. Αν περιέχεται μόνο ο αρχικός seeder, ο πελάτης συνδέεται άμεσα με αυτόν και αρχίζει να ζητάει τα κομμάτια.

Οι πελάτες χρησιμοποιούν μηχανισμούς για τη βελτιστοποίηση του download και του upload rate τους. Για παράδειγμα με το να κατεβάζουν κομμάτια με τυχαία σειρά αυξάνεται η ευκαιρία για την ανταλλαγή δεδομένων, η οποία είναι δυνατή μόνο εάν δύο peers έχουν διαφορετικά κομμάτια του αρχείου.

Η αποτελεσματικότητα αυτής της ανταλλαγής δεδομένων εξαρτάται σε μεγάλο βαθμό από τις πολιτικές που χρησιμοποιούν οι πελάτες στο να καθορίσουν σε ποιον πρέπει να στέλνονται δεδομένα. Κάποιοι μπορεί να προτιμούν να στέλνουν δεδομένα στους peers που στέλνουν δεδομένα πίσω σε αυτούς , κάτι το οποίο ενθαρρύνει την δίκαιη εμπορική συναλλαγή. Αλλά οι αυστηρές πολιτικές συχνά οδηγούν σε ανεπιθύμητες καταστάσεις, όπως όταν πρόσφατα ενταγμένοι peers δεν είναι σε θέση να λαμβάνουν όλα τα δεδομένα, διότι δεν έχουν ακόμη κομμάτια για αυτό το σκοπό ή όταν δύο peers με μια καλή σύνδεση μεταξύ τους δεν ανταλλάσσουν στοιχεία απλώς και μόνον επειδή δεν αναλαμβάνει κάποιος από αυτούς την πρωτοβουλία.

Η κοινότητα των Bit-Torrent χρηστών απαξιώνει την πρακτική της αποσύνδεσης από το δίκτυο αμέσως μετά την επιτυχή λήψη ενός αρχείου, και ενθαρρύνει να παραμένουν online ώστε να έχουν το ρόλο του seeder[38] για αυτό που έχουν κατεβάσει .Αυτό μπορεί να πάρει και μέρες ανάλογα την σύνδεση βέβαια.



Εικόνα 24.Η παράθεση των torrent files και των λεπτομερειών τους από γνωστό tracker

[38]BitTorrent Vocabulary: http://en.wikipedia.org/wiki/BitTorrent_vocabulary

3.2.4 Bit-Torrent clients

Ένας Bit-Torrent client λοιπόν είναι ένα πρόγραμμα υπολογιστή που διαχειρίζεται downloads και uploads χρησιμοποιώντας το πρωτόκολλο Bit-Torrent. Ο πρώτος client, γνωστός ως Bit-Torrent, ιδρύθηκε από τον Bram Cohen[39], τον Οκτώβριο του 2002.

Εικόνα 25.Ο Bram Cohen

Πολλοί clients που εμφανίστηκαν μετέπειτα έχουν βασιστεί έστω και εν μέρει σε αυτόν. Όλοι οι clients πάντως δεν είχαν κατασκευαστεί για το Bit-Torrent αρχικά, αλλά είχαν προσθέσει την υποστήριξη για το πρωτόκολλο αυτό αργότερα. Έχουν γίνει επίσης προσπάθειες και για την διανομή κακόβουλου λογισμικού πιθανόν λόγω της ύπαρξης πολλών μη νομιμοφρόνων πελατών και της προθυμίας των χρηστών να θέλουν να δοκιμάσουν καινούργια πράγματα.

Παρατίθενται παρακάτω οι Bit-Torrent clients[40] έως και σήμερα(15/2/2010) καθώς και κάποια χαρακτηριστικά τους:

[39] Cohen Site: http://bramcohen.com/
[40] BitTorrent Clients :http://en.wikipedia.org/wiki/Comparison_of_BitTorrent_clients

Πίνακας 1

BitTorrent client	GUI	web	CLI	other	Programming language	Based on	IPv6[54]
ABC	Yes	Yes	No	No	Python	BitTornado	buggy[55]
Acquisition	Yes	No	No	No	Objective-C and Cocoa	Limewire	?
Anatomic P2P	Yes	No	old	No	Python	BitTornado	No
Arctic Torrent	Yes	No	No	No	C++	libtorrent (Rasterbar)	No
Aria	obsolete[56]	No	Partial	Daemon	C++	-	?
BitComet	Yes	Yes	Partial[57]	No	C++	-	No
Bitflu	No	Yes	Yes	Telnet	Perl	-	Yes
BitLet	No	Yes	No	No	Java and JavaScript	-	?
BitLord	Yes	No	No	No	C++	BitComet	No
BitThief	Yes	No	No	No	Java	?	?
BitTornado	Yes	No	Partial	No	Python	BitTorrent	Yes
BitTorrent 5 / Mainline	Yes	No	Partial	No	Python	-	No
BitTorrent 6	Yes	Yes	Partial	No	C++	µTorrent	Yes
Bits on Wheels	Yes	No	No	No	Objective-C and Cocoa	-	Yes
BitTyrant	Yes	Yes	Partial	Telnet, XML over HTTP remote control API	Java and SWT	Azureus	Yes
Blog Torrent	Yes	No	No	No	?	?	?
BTG	Yes	Yes	Partial	No	C++	libtorrent (Rasterbar)	Partial
Burst!	Yes	No	No	No	Python	?	?
CTorrent	No	No	Partial	No	C++	?	No
Deluge	Yes	Yes	Partial	Daemon	Python and C++	libtorrent (Rasterbar)	Yes [58]
FlashGet	Yes	No	No	No	?	?	No
Folx	Yes	No	No	No	?	?	No
Free Download Manager	Yes	Yes	Partial	No	C++	libtorrent (Rasterbar)	?

G3 Torrent	Yes	Yes	No	No	Python	BitTorrent	*?*
Gnome BitTorrent	Yes	No	No	No	Python	*?*	*?*
Halite	Yes	No	No	No	C++	libtorrent (Rasterbar)	*?*
KGet	Yes	Yes	Partial[59]	Web Interface	C++	-	Yes
KTorrent	Yes	Yes	Partial	Web Interface	C++	-	Yes
LimeWire	Yes	No	No	No	Java	libtorrent (Rasterbar)	No
Miro	Yes	No	No	No	C++	libtorrent (Rasterbar)	*?*
MP3 Rocket	Yes	No	No	No	Java	-	No
MLDonkey	Network GUI	Yes	Partial	Telnet	Ocaml	-	No
OneSwarm	Yes	Yes	*?*	Classic Ui and Web Interface	Java	Azureus	Yes
Opera	Yes	No	No	No	C++	-	Yes
QTorrent	Qt (toolkit)	No	No	No	C++/PyQt	BitTornado	*?*
qBittorrent	Qt (toolkit)	Yes	Partial	No	C++	libtorrent (Rasterbar)	Yes
rTorrent	No	No	Yes	SCGI	C++	libtorrent (Rakshasa)	No[60]
Shareaza	Yes	Yes	Partial	No	C++	-	No
SymTorrent	Yes	No	No	No	*?*	*?*	*?*
Tixati	Yes	No	No	No	C++	-	Yes
Tomato Torrent	Yes	No	No	No	Cocoa	BitTorrent	No
Torium	gtkmm	No	No	directory monitoring (ssh,sftp)	C++	libtorrent (Rasterbar)	Partial
Torrent Swapper	Yes	Yes	No	No	Python	BitTorrent	buggy[55]
TorrentFlux	No	Yes	No	No	PHP	BitTornado	Yes
TorrentVolve	No	Yes	No	No	PHP	Azureus	Partial [61]
Transmission	Yes	Yes	Yes	Daemon	C and Cocoa	-	Yes
Tribler	Yes	No	Partial	No	Python	ABC	Yes
µTorrent	Yes	Yes	No[62]	No	C++[63]	-	Yes[64]
Vuze (formerly Azureus)	Yes	Yes	Partial	Telnet, XML over HTTP remote control API	Java and SWT	-	Yes

ZipTorrent	Yes	No	No	No	C++	libtorrent (Rasterbar)	?
BitTorrent client	**GUI**	web	**CLI**	other	**Programming language**	Based on	**IPv6**[54]

Πίνακας 2:BitTorrent Clients και χαρακτηριστικά τους.

Μετά από αυτήν την εισαγωγή στο πρωταρχικό πρωτόκολλο Bit-Torrent και σε κάποιες βασικές αρχές λειτουργίας του, ήρθε η ώρα να ασχοληθούμε με έναν σχετικά μικρό σε μέγεθος , ευέλικτο client που αναπτύχθηκε σχετικά πρόσφατα και χρησιμοποιεί το Bit-Torrent πρωτόκολλο , ο λόγος για το μTorrent.

Εικόνα 26.Το λογότυπο του client μTorrent

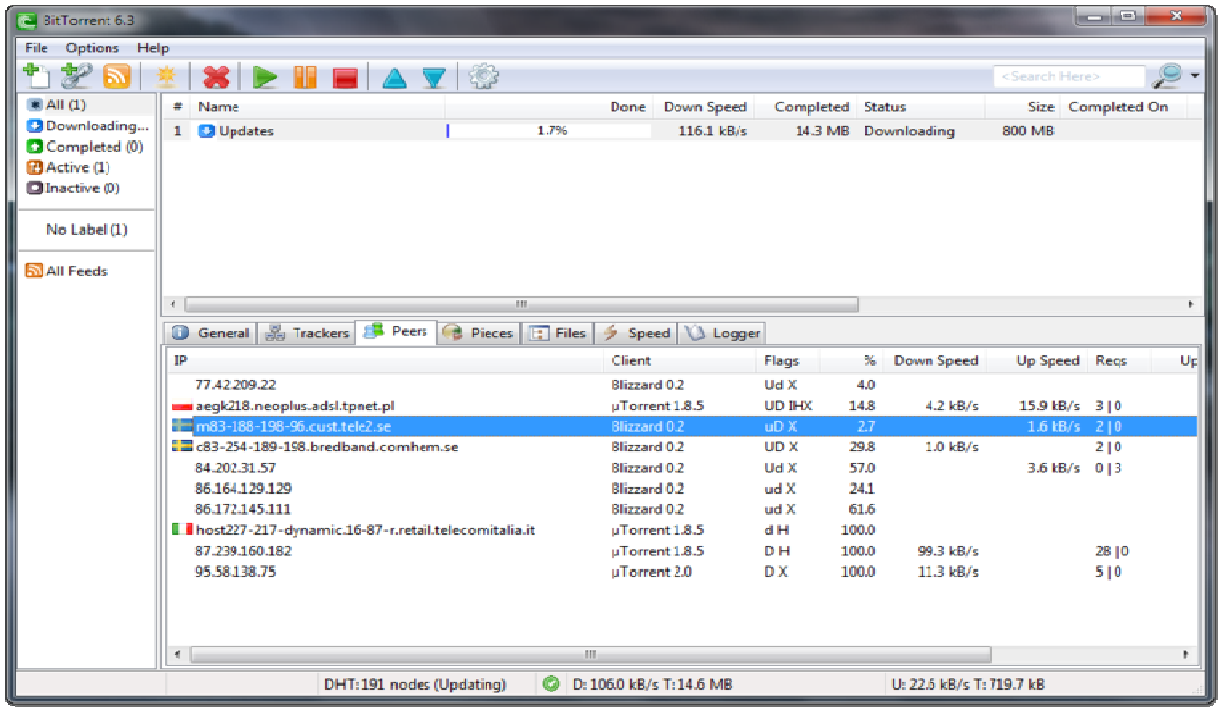
3.3 Γενική επισκόπηση του μTorrent client

Το μTorrent είναι ένα δωρεάν λογισμικό, κλειστού κώδικα δυστυχώς, από την Bit-Torrent, Inc και είναι διαθέσιμο για τα Microsoft Windows και τα Mac OS X. Και οι δύο εκδόσεις είναι γραμμένες σε C + +. Παίρνει το "μ" στο όνομά του από το SI πρόθεμα “micro” που σημαίνει ένα εκατομμυριοστό και αναφέρεται στο μικρό footprint του προγράμματος δηλαδή του ποσοστού της κύριας μνήμης που χρησιμοποιεί(14 MB) όταν το τρέχουμε. Το πρόγραμμα έχει σχεδιαστεί για να χρησιμοποιεί ελάχιστους πόρους του υπολογιστή ενώ η λειτουργικότητα που προσφέρει είναι πολύ άνετα συγκρίσιμη με μεγαλύτερους Bit-Torrent clients, όπως το Vuze[41] και το BitComet[42].

Το πρόγραμμα έχει λάβει σταθερά καλές κριτικές για το σύνολο των λειτουργιών του, τις επιδόσεις του, τη σταθερότητα, και την υποστήριξη των παλαιότερων hardware

[41]Vuze: http://en.wikipedia.org/wiki/Vuze
[42]BitComet: http://www.bitcomet.com/

και εκδόσεων των Windows. Μια έκθεση[43] έδειξε ότι το μTorrent είναι το δεύτερο πιο δημοφιλές Bit-Torrent client (μετά το κινέζικο Xunlei)[44].
Το πρόγραμμα έχει αναπτυχθεί με ταχείς ρυθμούς από την πρώτη έκδοση του το 2005. Παρόλο που αρχικά αναπτύχθηκε από τον Ludvig Strigeus[45], από τις 7 Δεκεμβρίου του 2006 ο κώδικας ανήκει και διατηρείται από την Bit-Torrent, Inc . Ο κώδικας αυτός έχει επίσης αποτελέσει την βάση για την έκδοση 6.3 του Bit-Torrent client, στην ουσία κάτι σαν επανέκδοση του μTorrent.



Εικόνα 27.Το Interface του Bit-Torrent 6.3

3.3.1 Τεχνικά χαρακτηριστικά

- Το μTorrent χρησιμοποιεί ούτε λίγο ούτε πολύ 14MB RAM απαιτώντας επεξεργαστή 486 MHZ σε πλατφόρμα windows 95.
- Υποστήριξη IPV6.
- Από την έκδοση 2.0 και μετά υποστηρίζει UDP Torrent Protocol.

[43] Research about Utorrent ::http://webcache.googleusercontent.com/search?q=cache:oeAcwVHWdWIJ:www.ehow.com/utorrent/+utorrent+the+second+most+used+client+after+xunlei&cd=3&hl=el&ct=clnk&gl=gr

[44] Xunlei : http://en.wikipedia.org/wiki/Xunlei
[45] Strigeus Biography: http://en.wikipedia.org/wiki/Ludvig_Strigeus

- Κρυπτογράφηση πρωτοκόλλου που παρέχει παράκαμψη κυκλοφορίας ορισμένων Internet Service Providers με διάφορες τεχνικές κλειδώματος του εύρους ζώνης.Δεν παρέχεται πάντως προστασία προσωπικών δεδομένων.

- Ανταλλαγή δεδομένων με peers που χρησιμοποιούν άλλους Bit-Torrent clients.

- Υποστήριξη ύπαρξης proxy server[46] δηλαδή ενδιάμεσου server μεταξύ των peers

- Υποστηρίζει 52 διαφορετικές γλώσσες

- Υποστηρίζει HTTPS(HTTP SECURE) Trackers

- Διαθέτει έξυπνο σύστημα προσωρινής αποθήκευσης δεδομένων στο δίσκο το οποίο είναι εύκολο στην διαχείριση από τον χρήστη.

- Εξατομικευμένη search bar και λειτουργικό, απλό GUI[47](Graphical User Interface) με αρκετά skins για όλες τις προτιμήσεις.

- Οι διάφορες αλλαγές στα settings και οι προσωρινοί φάκελοι αποθηκεύονται σε μια συγκεκριμένη τοποθεσία έτσι είναι εύκολη η φορητή χρήση τους.

- Παρέχει την δυνατότητα να ρυθμίσεις το μέγιστο bandwidth που θέλεις να αφιερώσεις ώστε να γίνεται καλύτερη διανομή πόρων μέσα σε ένα δίκτυο.

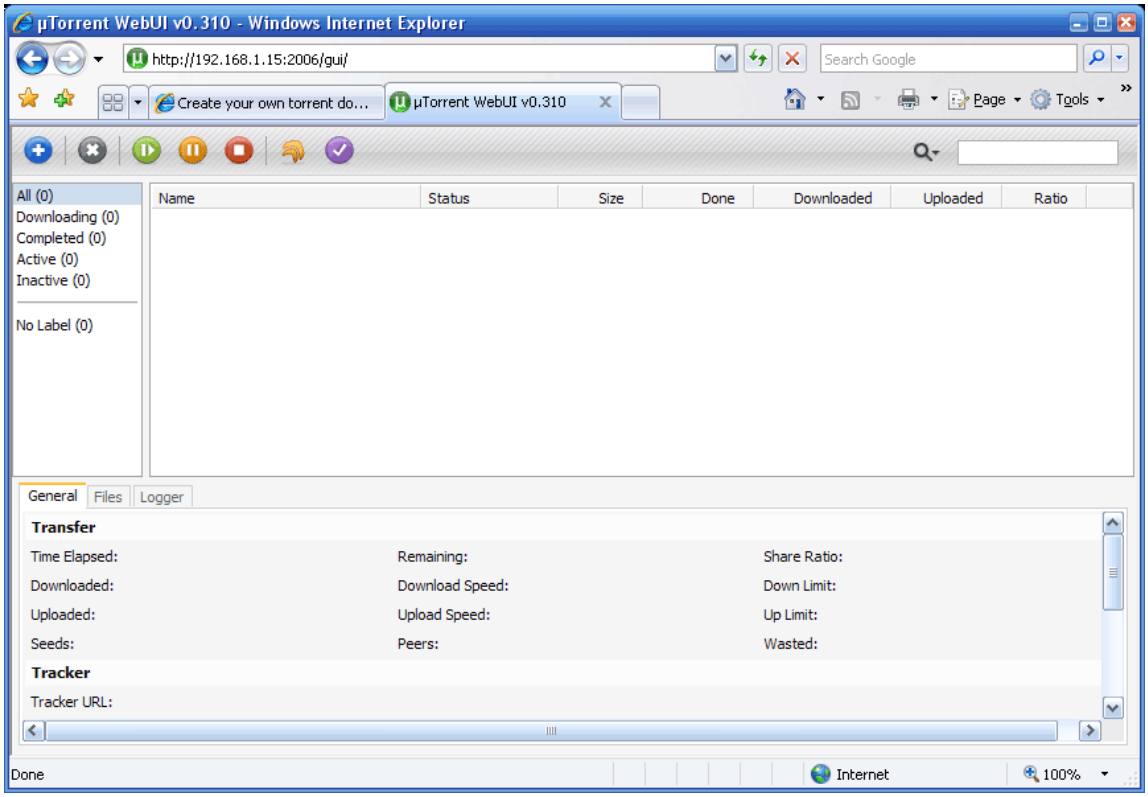
- Initial seeding, δηλαδή την δυνατότητα να ελαχιστοποιούνται τα δεδομένα που απαιτούνται από ένα client να κάνει upload για να ολοκληρώθεί ένα download ,αρκετά χρήσιμο όταν υπάρχει μόνο ένας seeder στην αρχή.

- Υποστήριξη Distributed Hash Table (DHT)

- Download Bar

- Υποστήριξη IP Block-list

[46] Proxy Server: http://en.wikipedia.org/wiki/Proxy_server
[47]GUI: http://en.wikipedia.org/wiki/Graphical_user_interface



Εικόνα 28.Το Interface του µTorrent

Σε ότι αφορά το μέγεθος του, το µTorrent είναι και διατίθεται ως ένα ενιαίο αυτόνομο συμπιεσμένο εκτελέσιμο αρχείο, και απαιτεί εγκατάσταση μέσω ενός installer, το οποίο είναι διαθέσιμο για πολλαπλές εγκαταστάσεις. Οι πρόσφατες εκδόσεις έχουν συμπεριλάβει τη δυνατότητα να εγκατασταθούν σε πρώτη εκτέλεση. Μικρό μέγεθος εκτελέσιμου αρχείου επιτυγχάνεται με την αποφυγή της χρήσης πολλών βιβλιοθηκών, κυρίως της C + + πρότυπης βιβλιοθήκης. Το εκτελέσιμο συμπιέζεται στο μισό περίπου μέγεθος από το μέγεθος που είχε μετά το compile με την χρήση της τεχνικής συμπίεσης εκτελέσιμων αρχείων UPX[48](Ultimate Packer for Executables).

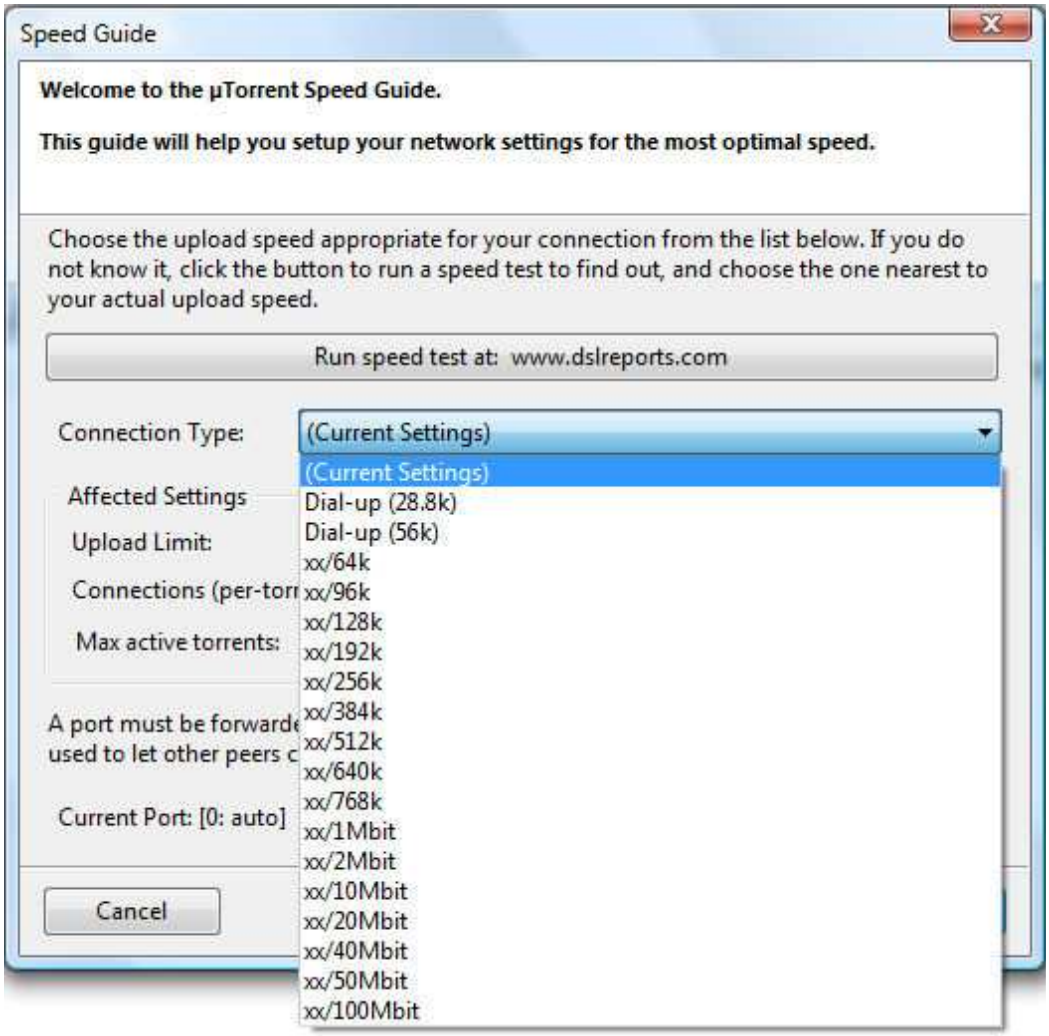
3.4 Οδηγός για το Setup

Το επίκεντρο σε αυτό εδώ το κομμάτι είναι να δοθούν οδηγίες για να διαμορφωθεί το µTorrent ώστε να είναι σε θέση να επιτύχει την βέλτιστη ταχύτητα για την σύνδεσή στο Internet. Αν και σωστές ρυθμίσεις δεν εγγυώνται πάντα ότι θα χτυπήσει μέγιστο upload και download speed, τουλάχιστον όμως η προσπάθεια θα τείνει προς εκεί. Αυτό που έχουμε λοιπόν να κάνουμε είναι πρώτα να πάμε στην κεντρική σελίδα http://www.utorrent.com/ και να κατεβάσουμε το μόλις 282kb συμπιεσμένο εκτελέσιμο αρχείο του µTorrent και έπειτα να το τρέξουμε και να το εγκαταστήσουμε στον υπολογιστή μας

[48] UPX: http://upx.sourceforge.net/

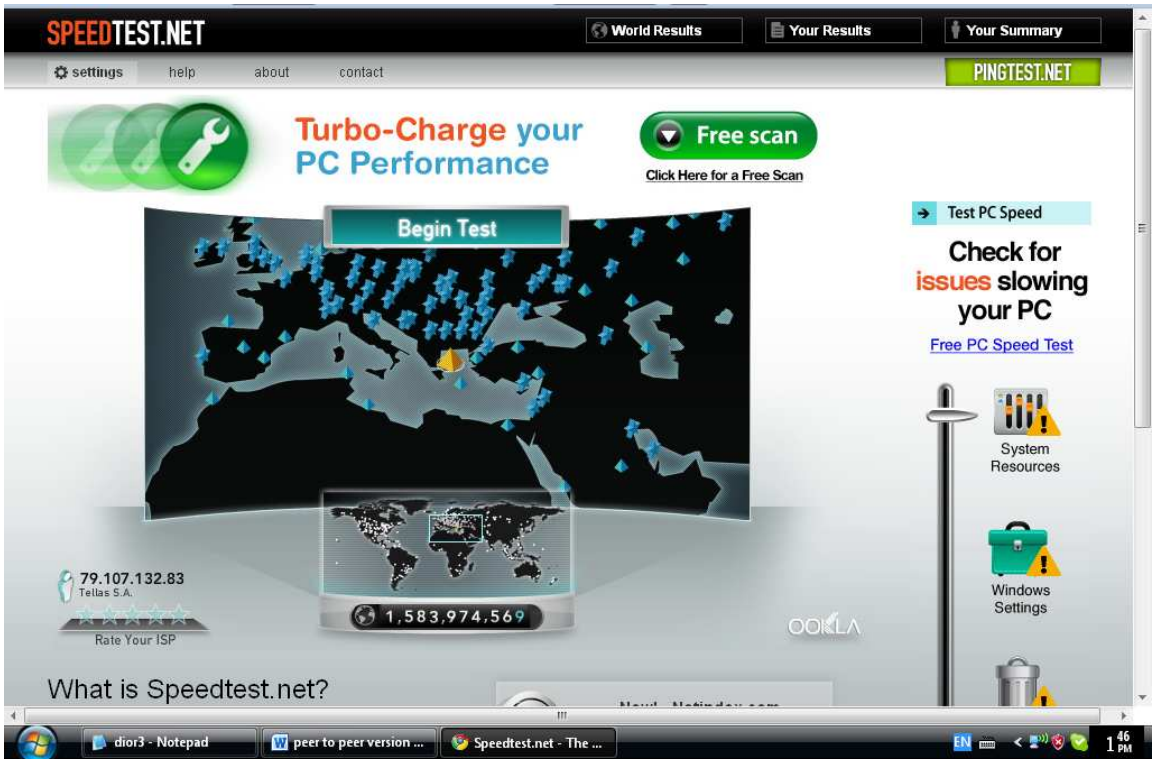
Οδηγός Ταχύτητας

Όταν ανοίγει το μTorrent για πρώτη φορά, παρουσιάζεται το μTorrent Speed Guide. Στο πρώτο μέρος, θα ζητηθεί να επιλέξετε την ταχύτητα upload σας από το dropdown μενού. Εάν δεν γνωρίζετε την συγκεκριμένη πληροφορία , μπορείτε να δοκιμάσετε τη σύνδεσή στο Internet με αριστερό κλικ στο αντίστοιχο κουμπί για test(run speed test).



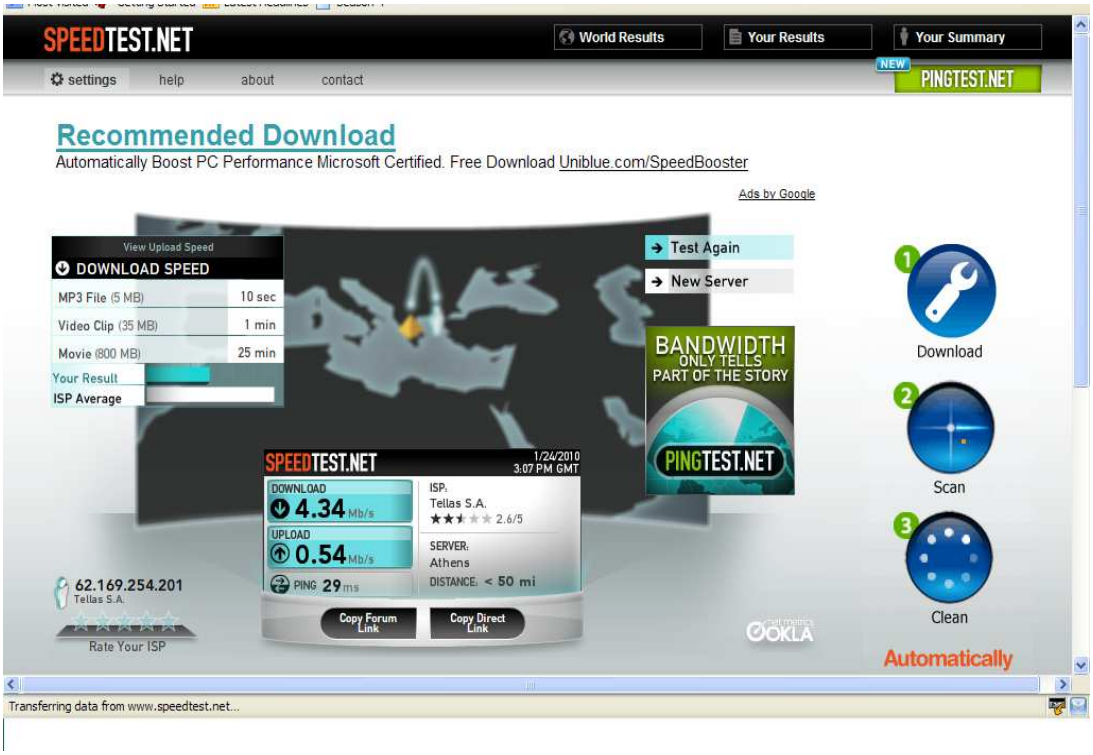
Εικόνα 29.Το speed guide του μTorrent

Στη σελίδα αυτή θα εμφανιστούν πολλά Mirrors μπροστά σας και το καλύτερο που μπορείτε να κάνετε είναι να επιλέξετε αυτόν που βρίσκεται πλησιέστερα προς τον τόπο κατοικίας σας ,επειδή όμως η σελίδα είναι αμερικάνικη έχει μόνο τους αμερικανικούς mirror servers οπότε μεταφερόμαστε στην σελίδα www.speedtest.net και διαλέγουμε την πυραμίδα για τον mirror της Αθήνας.



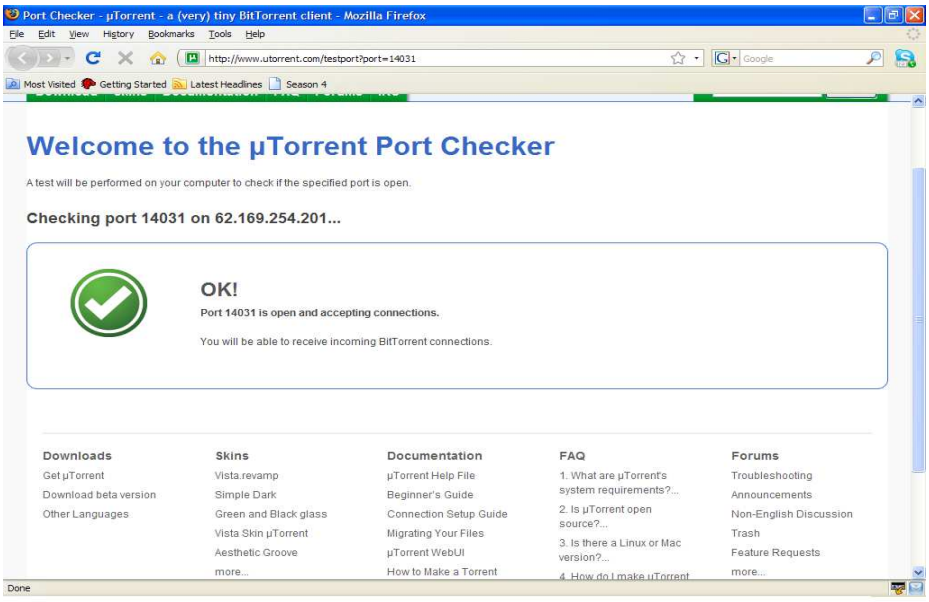
Εικόνα 30.Η σελίδα του speed test

Όταν εκτελείται το speed test, πρέπει να είμαστε βέβαιοι ότι δεν χρησιμοποιείται η σύνδεσή στο Internet για οτιδήποτε άλλο εκτός από τη δοκιμή. Εκτελέστε τη δοκιμή αρκετές φορές, και υπολογίστε τον μέσο όρο των ταχυτήτων upload που θα σας δοθεί στις δοκιμές. Από το "Connection Type" dropdown menu, επιλέξτε την επιλογή που βρίσκεται πλησιέστερα προς μέση ταχύτητα upload. Σημειώστε ότι υπάρχει διάκριση μεταξύ των bits και bytes, και τα αποτελέσματα της ταχύτητας δίνονται συνήθως σε kbps (kilobit ανά δευτερόλεπτο), η οποία δεν πρέπει να συγχέεται με KB / s (kiloBytes ανά δευτερόλεπτο, απλά το αναφέρουμε!). Μην μπείτε στον πειρασμό να επιλέξετε μια επιλογή πολύ υψηλότερη από την ταχύτητα που προέβλεψε το speed test με την ελπίδα ότι αυτό θα σας βοηθήσει να κατεβάσετε γρηγορότερα, καθώς δεν είναι έτσι τα πράγματα και αντιθέτως μπορεί να είναι επιζήμιο για την ταχύτητα. Σύμφωνα με τα αποτελέσματα του upload στο παράδειγμα, πρέπει να επιλεγεί το xx/640k από το dropdown Menu.



Εικόνα 31.Τα αποτελέσματα για την συγκεκριμένη σύνδεση

Στο δεύτερο μέρος, μια θύρα επιλέγεται τυχαία την πρώτη φορά που το Speed Guide εμφανίζεται, αν και είναι δυνατό να αλλάξετε τη θύρα που χρησιμοποιείται. Εναλλακτικά, μπορείτε να επιλέξετε την 0 ώστε να επιλεγεί τυχαία ποιά θα είναι η Port που θα δέχεται τις peer συνδέσεις. Αφού την επιλέξετε, τότε κάνουμε αριστερό κλικ "Έλεγχος λειτουργίας θύρας" για να είναι βέβαιο ότι η θύρα είναι ανοικτή. Είναι σημαντικό η θύρα να είναι ανοικτή ώστε να μπορεί το μTorrent να «ακούει» εισερχόμενες συνδέσεις. Χρήση επιλεγμένων ρυθμίσεων λοιπόν και τέλος.



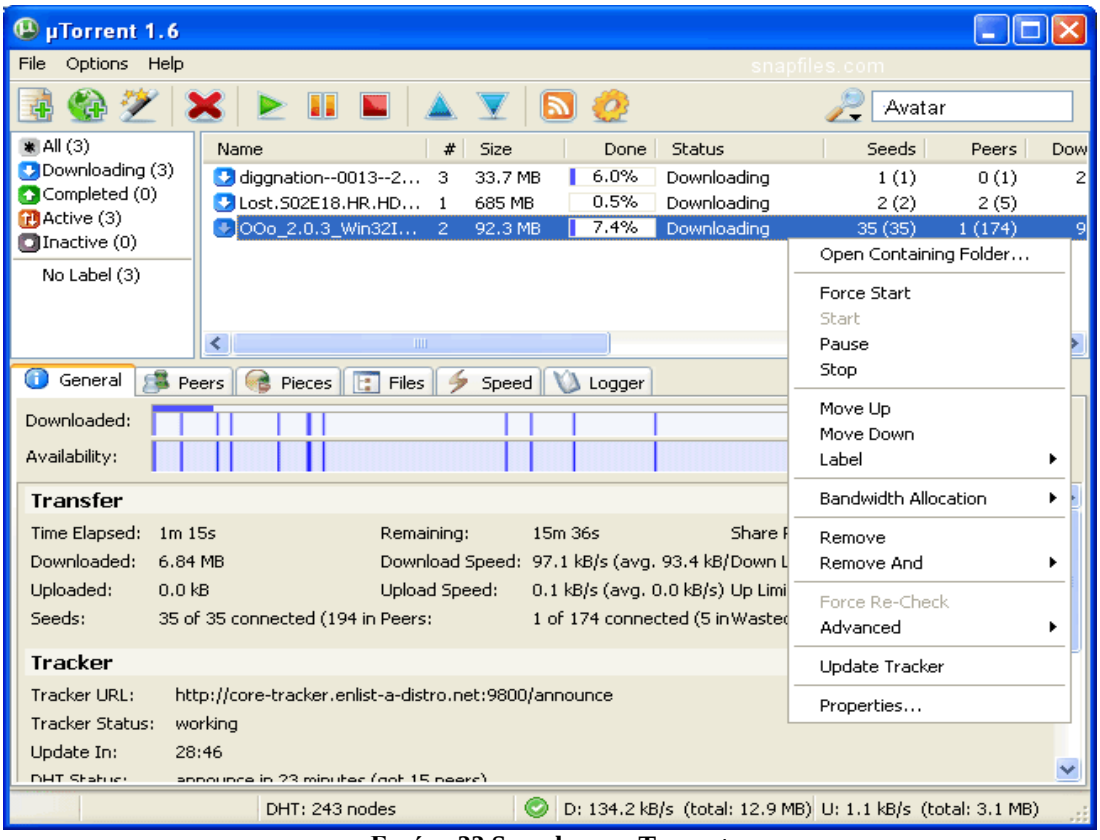
Εικόνα 32.Ο έλεγχος της port

3.5 Downloading με το μTorrent

Παρόμοια με το ότι χρειάζεται ένα URL, όπως http://www.utorrent.com, για να μας πάει σε μια ιστοσελίδα και να γίνει λήψη περιεχομένου, ένα αρχείο .Torrent απαιτείται για τη λήψη περιεχομένου το οποίο διατίθεται μέσω του Bit-Torrent. Τις περισσότερες φορές, μπορείτε να κάνετε λήψη αυτού του αρχείου από μια ιστοσελίδα, αν και μπορείτε να το πάρετε και από έναν τρίτο(φυσικό πρόσωπο) ή με κάποια άλλη μορφή μεταβίβασης. Πολλές ιστοσελίδες προσφέρουν. πάντως αρχεία torrent ως μία μέθοδο λήψης αρχείων που διατίθενται μέσω του δικτυακού τόπου τους(Torrent Root,Demonoid). . Αυτές οι περιοχές είναι οι λεγόμενοι trackers όπως αναφέρθηκαν σε προηγούμενο κεφάλαιο.

Τι γίνεται λοιπόν όταν κάποια μηχανή αναζήτησης πρέπει να χρησιμοποιηθεί για αυτά τα .Torrent αρχεία. Κάλλιστα μπορεί να γίνει αναζήτηση με μία επιθυμητή μηχανή αναζήτησης,με μόνο επιπλέον να τοποθετηθεί στο τέλος του query[49] το .Torrent και τα αποτελέσματα είναι αρκετά αξιοπρεπή. Το μTorrent περιλαμβάνει επίσης μια ενσωματωμένη μπάρα αναζήτησης σε ορισμένες από τις πιο δημοφιλείς μηχανές αναζήτησης Torrent αρχείων στον κόσμο.

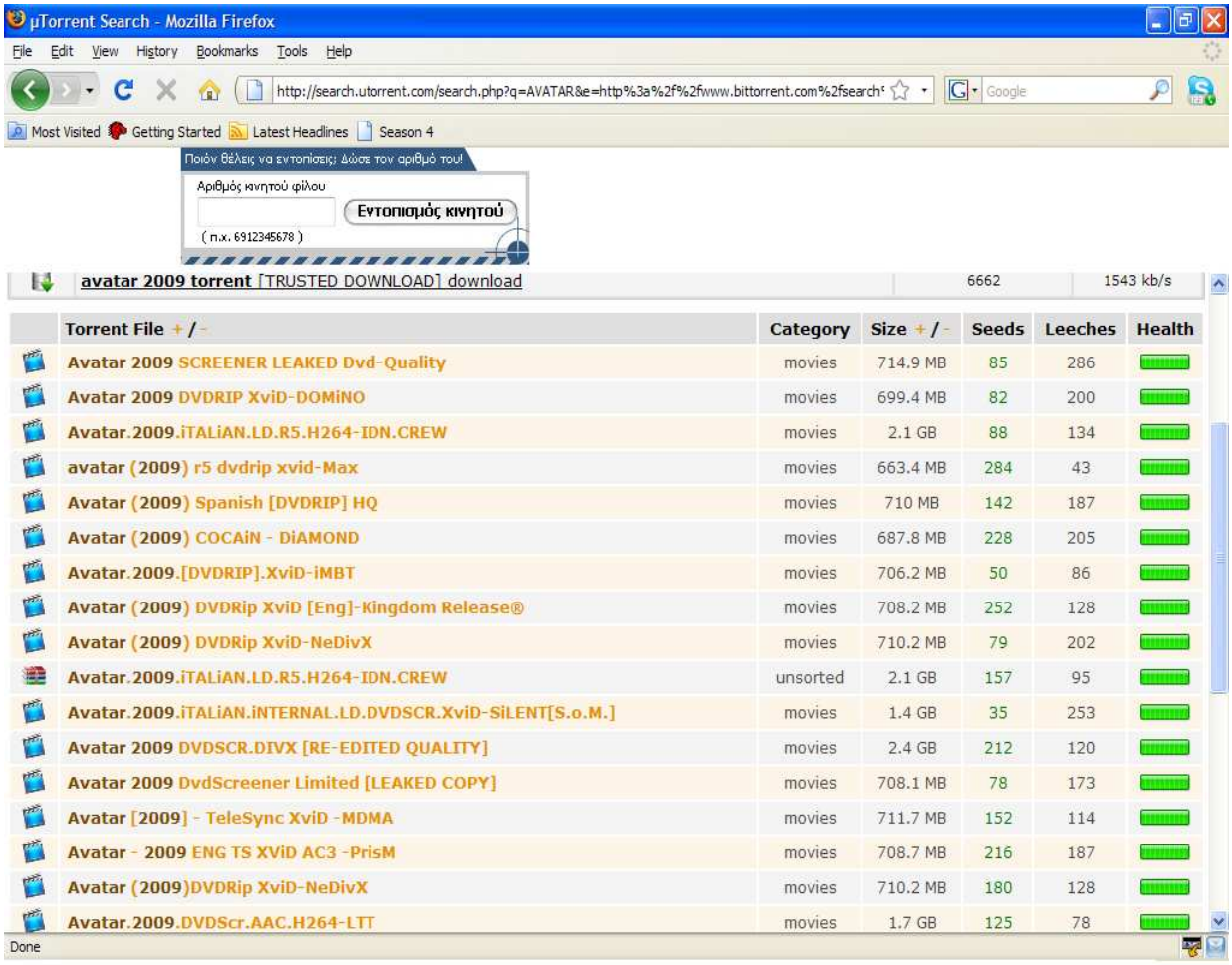
Ας πούμε λοιπόν ότι θέλουμε να βρούμε το Torrent αρχείο για την ταινία Avatar.



Εικόνα 33.Search στο μTorrent

[49]Query: http://en.wikipedia.org/wiki/Query_language

Και εν τέλει το πρώτο από τα αποτελέσματα μας βγάζει τα παρακάτω αρχεία Torrent τα οποία μας εμφανίζουν και αναλυτικά τα αρχεία με βάση τον συντελεστή leechers προς seeders.Όσο περισσότερο υπερτερούν οι seeders τόσο πιο γρήγορο το download αλλά και τόσο αργό το upload.



Torrent File + / -	Category	Size + / -	Seeds	Leeches	Health
Avatar 2009 SCREENER LEAKED Dvd-Quality	movies	714.9 MB	85	286	
Avatar 2009 DVDRIP XviD-DOMiNO	movies	699.4 MB	82	200	
Avatar.2009.iTALiAN.LD.R5.H264-IDN.CREW	movies	2.1 GB	88	134	
avatar (2009) r5 dvdrip xvid-Max	movies	663.4 MB	284	43	
Avatar (2009) Spanish [DVDRIP] HQ	movies	710 MB	142	187	
Avatar (2009) COCAiN - DiAMOND	movies	687.8 MB	228	205	
Avatar.2009.[DVDRIP].XviD-iMBT	movies	706.2 MB	50	86	
Avatar (2009) DVDRip XviD [Eng]-Kingdom Release®	movies	708.2 MB	252	128	
Avatar (2009) DVDRip XviD-NeDivX	movies	710.2 MB	79	202	
Avatar.2009.iTALiAN.LD.R5.H264-IDN.CREW	unsorted	2.1 GB	157	95	
Avatar.2009.iTALiAN.iNTERNAL.LD.DVDSCR.XviD-SiLENT[S.o.M.]	movies	1.4 GB	35	253	
Avatar 2009 DVDSCR.DIVX [RE-EDITED QUALITY]	movies	2.4 GB	212	120	
Avatar 2009 DvdScreener Limited [LEAKED COPY]	movies	708.1 MB	78	173	
Avatar [2009] - TeleSync XviD -MDMA	movies	711.7 MB	152	114	
Avatar - 2009 ENG TS XViD AC3 -PrisM	movies	708.7 MB	216	187	
Avatar (2009)DVDRip XviD-NeDivX	movies	710.2 MB	180	128	
Avatar.2009.DVDScr.AAC.H264-LTT	movies	1.7 GB	125	78	

Εικόνα 34.Αποτελέσματα του search για το avatar.torrent

3.5.1 Προσθήκη ενός Torrent αρχείου

Μόλις αποκτήσετε το .Torrent αρχείο του περιεχομένου που θέλετε να κατεβάσετε, εισάγετε το απλά στο μTorrent.Υπάρχουν διάφοροι τρόποι για την επίτευξη αυτού :

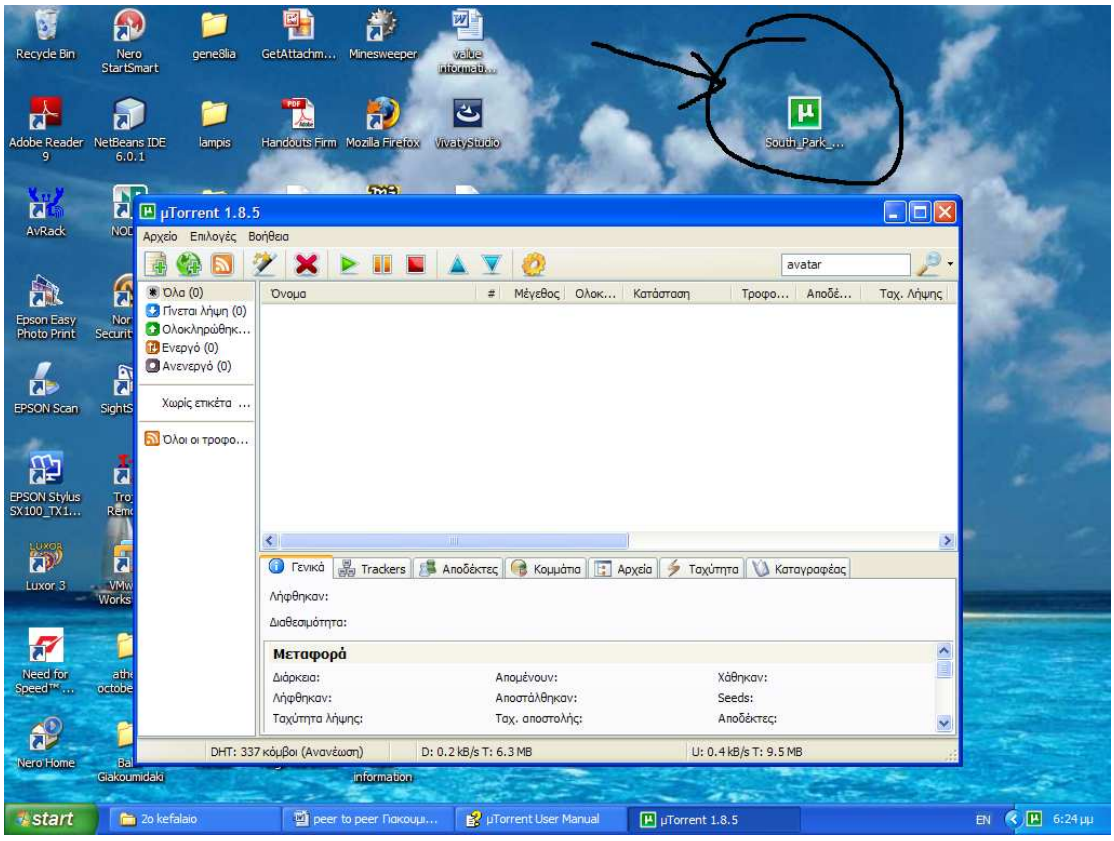
1)Αριστερό κλικ στο "Αρχείο" και "Προσθήκη Torrent " (ή πατήστε Ctrl O) στο μTorrent και ανοίξτε το .Torrent αρχείο.

2)Κάντε διπλό κλικ στο αρχείο .Torrent (μόνο αν είναι αρχείο torrent που σχετίζεται με το μTorrent).

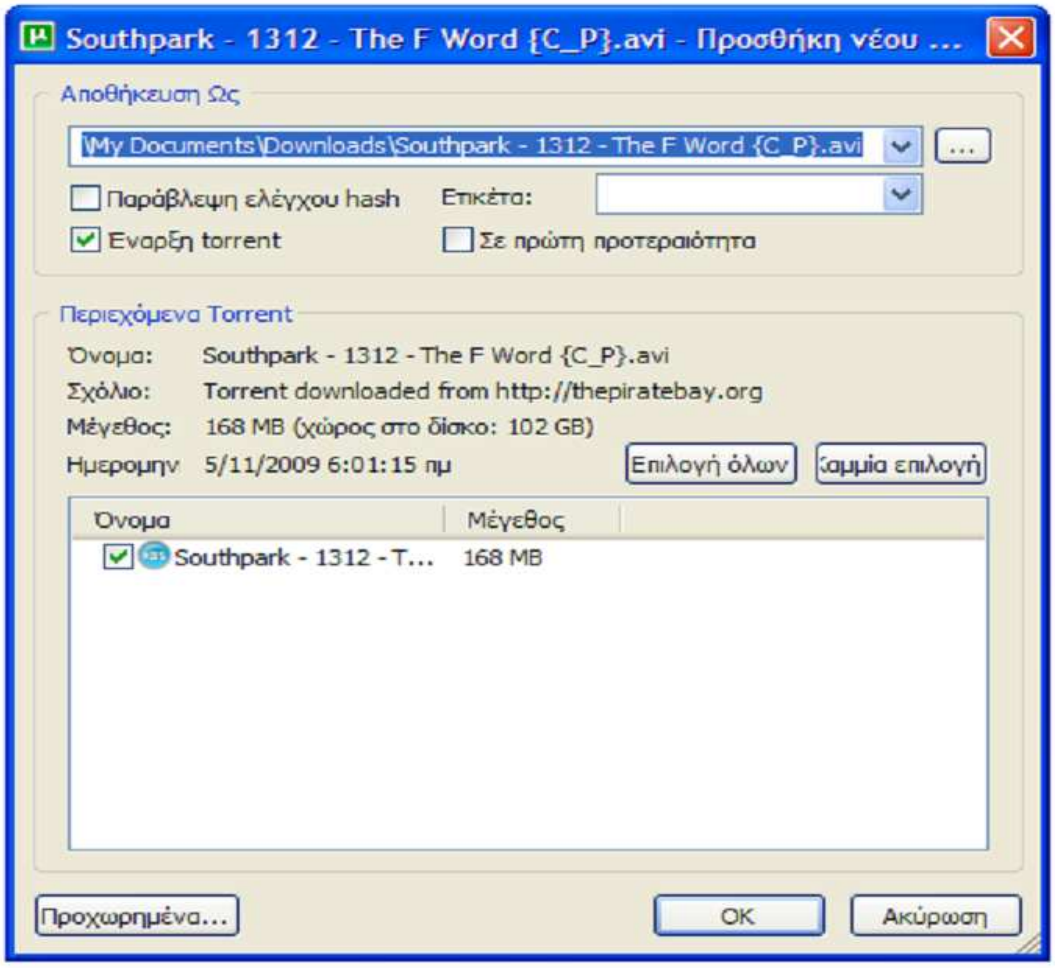
3) Drag-and-drop το αρχείο .Torrent στο κυρίως παράθυρο του μTorrent.

4)Εάν γνωρίζετε τη διεύθυνση URL απευθείας που οδηγεί στο αρχείο .Torrent, αλλά δεν το έχει στο σκληρό δίσκο, μπορείτε να επιλέξετε "Αρχείο" , "Προσθήκη Torrent από URL" (ή πατήστε το πλήκτρο Ctrl U) και να πληκτρολογήσετε την διεύθυνση URL του .Torrent αρχείου.

Μετά το άνοιγμα του. Torrent αρχείου, δίνουμε εντολή στο μTorrent, για το πού θα θέλαμε το περιεχόμενο να σωθεί. Αν το download δεν αρχίσει αυτόματα, μπορούμε να το κάνουμε με manual τρόπο πατώντας απλώς το κουμπί της έναρξης. Ακολουθεί η διαδικασία σε εικόνες για το κατέβασμα ενός επεισοδίου South park.

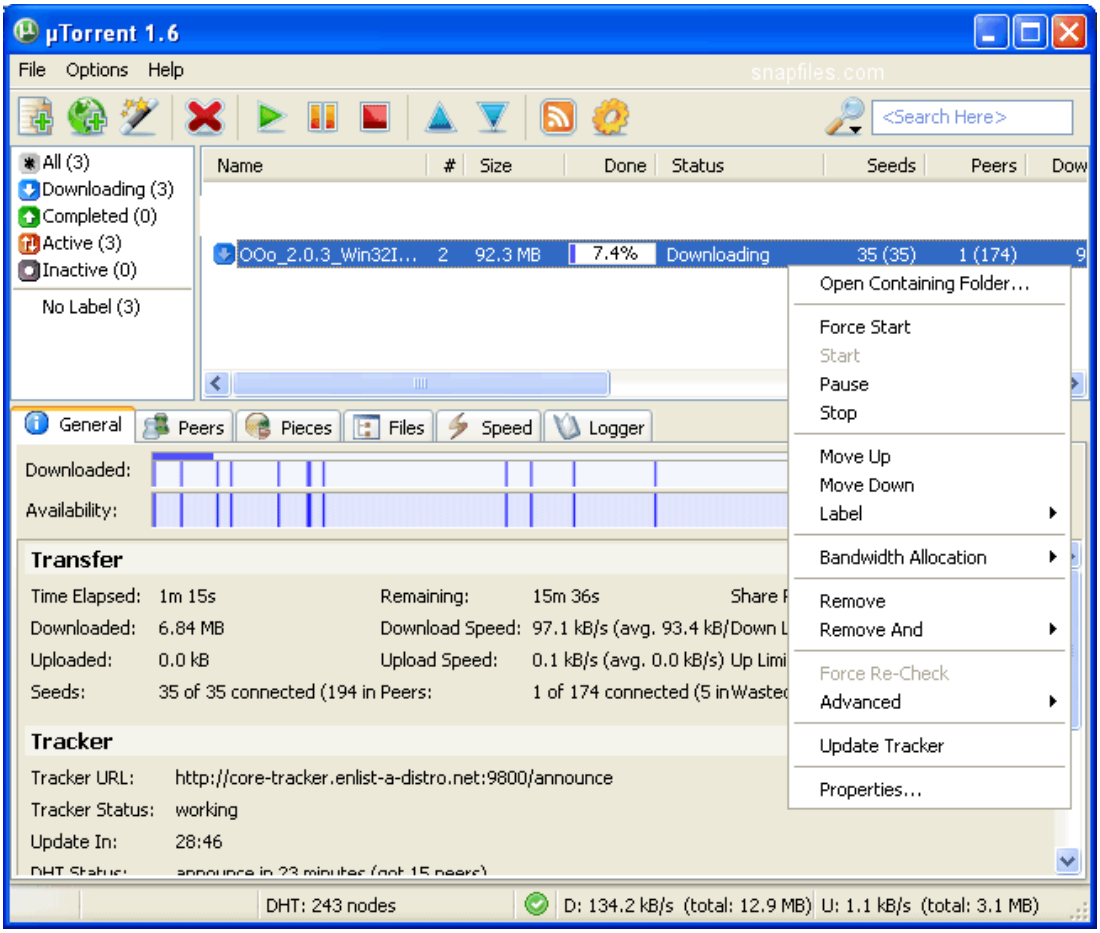


Εικόνα 35.Το Torrent αρχείο στην επιφάνεια

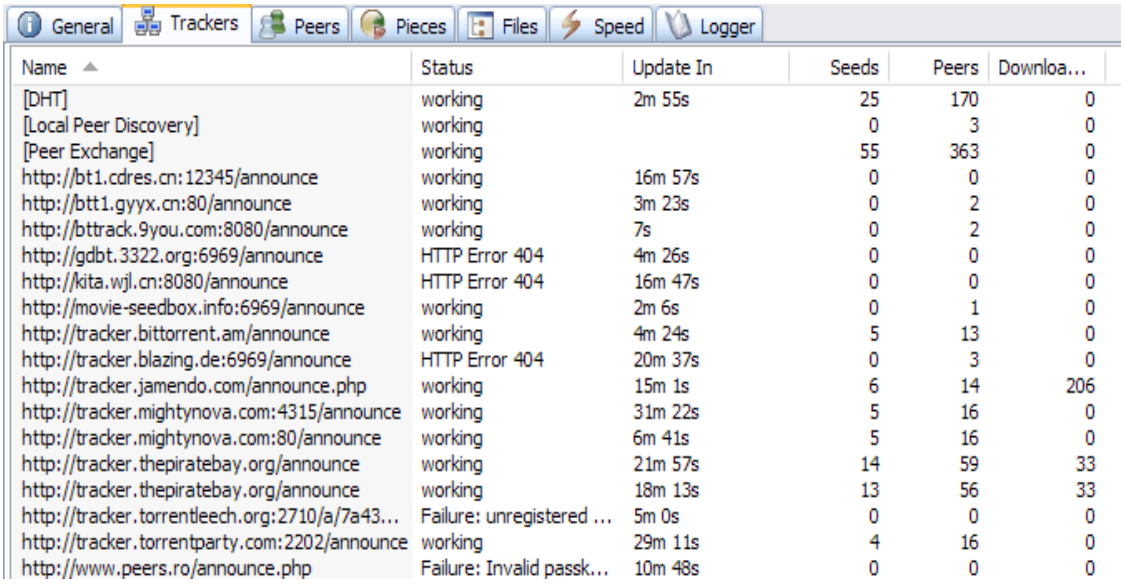


Εικόνα 36.Οι λεπτομέρειες του αρχείου και download επιλογές.

Από ότι βλέπουμε στην κορυφή φαίνεται το path στο οποίο θα αποθηκευτεί το αρχείο που θα κατεβάσουμε.Μπορούμε να δώσουμε και ένα συγκεκριμένο όνομα αν θέλουμε στο TextField Label.Επίσης γίνεται να παραλείψουμε τον Hash Check αλλά δεν προτείνεται.Είναι καλύτερο να ξέρουμε μέσω του Hash αλγορίθμου που περιγράψαμε και παραπάνω αν το αρχείο είναι corrupted ή όχι.Δίνεται η δυνατότητα προτεραιότητας στα queue's για το αρχείο αυτό και η επιλογή αν θέλουμε κάποιων από τα αρχεία που περιέχει.Στα Προχωρημένα είναι πράγματα που θα δούμε παρακάτω.



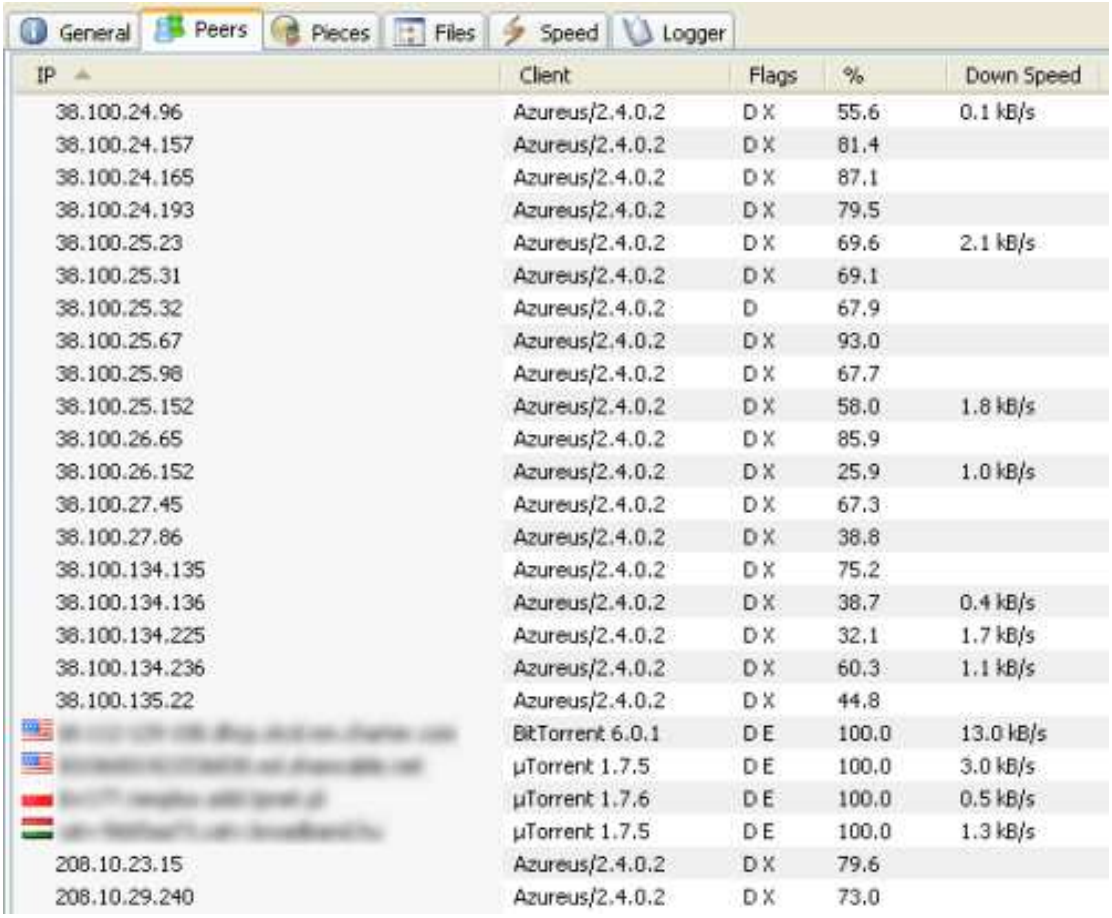
Εικόνα 37.Έναρξη της διαδικασίας του download.



Name	Status	Update In	Seeds	Peers	Downloa...
[DHT]	working	2m 55s	25	170	0
[Local Peer Discovery]	working		0	3	0
[Peer Exchange]	working		55	363	0
http://bt1.cdres.cn:12345/announce	working	16m 57s	0	0	0
http://btt1.gyyx.cn:80/announce	working	3m 23s	0	2	0
http://bttrack.9you.com:8080/announce	working	7s	0	2	0
http://gdbt.3322.org:6969/announce	HTTP Error 404	4m 26s	0	0	0
http://kita.wjl.cn:8080/announce	HTTP Error 404	16m 47s	0	0	0
http://movie-seedbox.info:6969/announce	working	2m 6s	0	1	0
http://tracker.bittorrent.am/announce	working	4m 24s	5	13	0
http://tracker.blazing.de:6969/announce	HTTP Error 404	20m 37s	0	3	0
http://tracker.jamendo.com/announce.php	working	15m 1s	6	14	206
http://tracker.mightynova.com:4315/announce	working	31m 22s	5	16	0
http://tracker.mightynova.com:80/announce	working	6m 41s	5	16	0
http://tracker.thepiratebay.org/announce	working	21m 57s	14	59	33
http://tracker.thepiratebay.org/announce	working	18m 13s	13	56	33
http://tracker.torrentleech.org:2710/a/7a43...	Failure: unregistered ...	5m 0s	0	0	0
http://tracker.torrentparty.com:2202/announce	working	29m 11s	4	16	0
http://www.peers.ro/announce.php	Failure: Invalid passk...	10m 48s	0	0	0

Εικόνα 38.Παρουσίαση των χρησιμοποιούμενων Trackers.

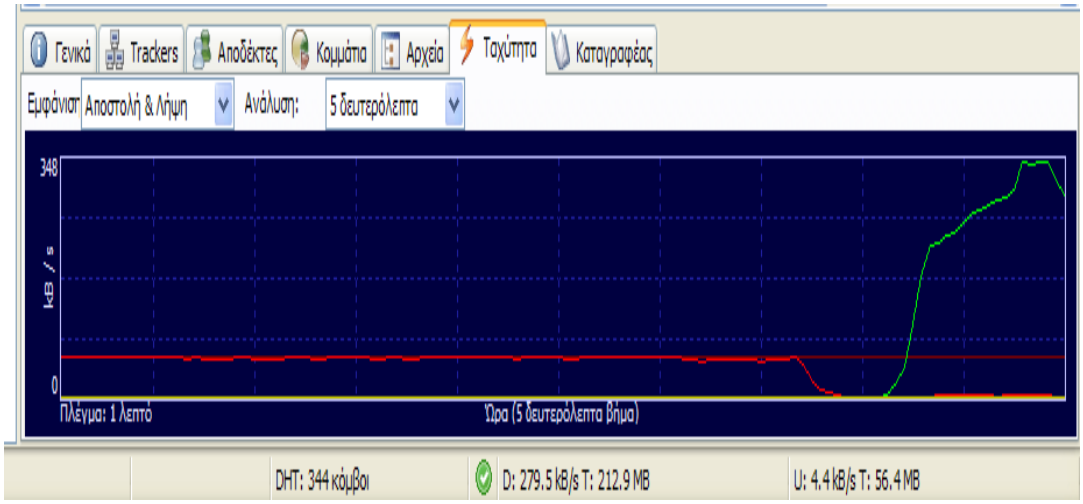
Παραπάνω βλέπουμε τους Trackers που έχουν το συγκεκριμένο αρχείο,αν δουλεύουν ή όχι,τον χρόνο που απομένει για το επόμενο update τους και τους seeds peers και αριθμούς download του συγκεκριμλενου αρχείου.



IP	Client	Flags	%	Down Speed
38.100.24.96	Azureus/2.4.0.2	D X	55.6	0.1 kB/s
38.100.24.157	Azureus/2.4.0.2	D X	81.4	
38.100.24.165	Azureus/2.4.0.2	D X	87.1	
38.100.24.193	Azureus/2.4.0.2	D X	79.5	
38.100.25.23	Azureus/2.4.0.2	D X	69.6	2.1 kB/s
38.100.25.31	Azureus/2.4.0.2	D X	69.1	
38.100.25.32	Azureus/2.4.0.2	D	67.9	
38.100.25.67	Azureus/2.4.0.2	D X	93.0	
38.100.25.98	Azureus/2.4.0.2	D X	67.7	
38.100.25.152	Azureus/2.4.0.2	D X	58.0	1.8 kB/s
38.100.26.65	Azureus/2.4.0.2	D X	85.9	
38.100.26.152	Azureus/2.4.0.2	D X	25.9	1.0 kB/s
38.100.27.45	Azureus/2.4.0.2	D X	67.3	
38.100.27.86	Azureus/2.4.0.2	D X	38.8	
38.100.134.135	Azureus/2.4.0.2	D X	75.2	
38.100.134.136	Azureus/2.4.0.2	D X	38.7	0.4 kB/s
38.100.134.225	Azureus/2.4.0.2	D X	32.1	1.7 kB/s
38.100.134.236	Azureus/2.4.0.2	D X	60.3	1.1 kB/s
38.100.135.22	Azureus/2.4.0.2	D X	44.8	
[redacted]	BitTorrent 6.0.1	D E	100.0	13.0 kB/s
[redacted]	µTorrent 1.7.5	D E	100.0	3.0 kB/s
[redacted]	µTorrent 1.7.6	D E	100.0	0.5 kB/s
[redacted]	µTorrent 1.7.5	D E	100.0	1.3 kB/s
208.10.23.15	Azureus/2.4.0.2	D X	79.6	
208.10.29.240	Azureus/2.4.0.2	D X	73.0	

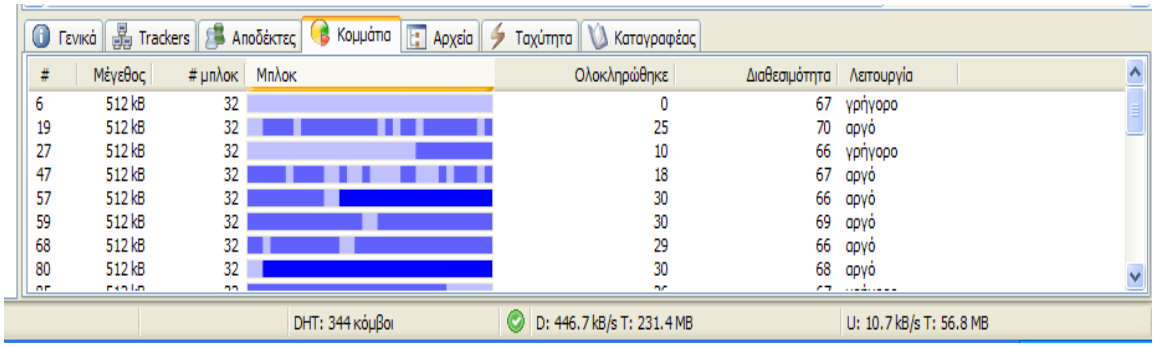
Εικόνα 39.Στο ίδιο σημείο παρομοίως οι άλλοι ταυτόχρονοι αποδέκτες και στοιχεία τους.

Στην μια στήλη έχουμε τα IP των peers του swarm,τον client που χρησιμοποιούν και τέλος το ποσοστό του αρχείου που έχουν κατεβάσει καθώς και την τρέχουσα ταχύτητά τους.



Εικόνα 40.Γραφική παράσταση της ταχύτητας.

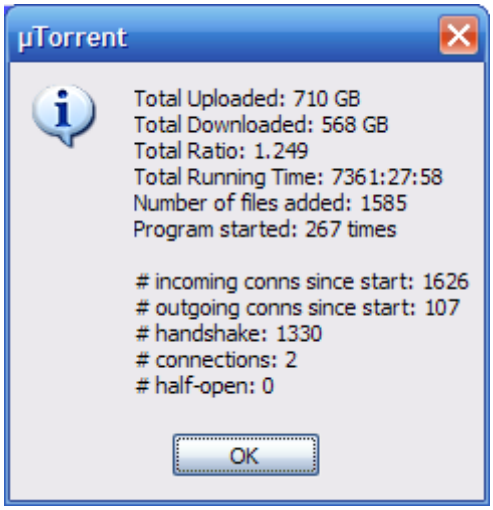
Βλέπουμε δηλαδή στην αμέσως παραπάνω εικόνα ότι η ταχύτητα είναι γύρω στα 270 και έφτασε μέχρι και 600 Kbps οπότε συμβαδίζει με το speed test που παρατέθηκε προηγουμένως. Συνεπώς έγιναν σωστά οι ρυθμίσεις ταχύτητας.



Εικόνα 41.Τα μπλοκ των 512KB χαρακτηριστικό του πρωτοκόλλου Bit-Torrent.

Τι γίνεται αφότου ολοκληρωθεί η λήψη;

Μετά που ολοκληρωθεί η λήψη του αρχείου , μπορείτε να δείτε τα αρχεία που έχετε κατεβάσει. Ενώ μπορείτε επίσης να τα αφαιρέσετε από την λίστα του μTorrent εάν το επιθυμείτε. Πάντως ενθαρρύνονται ιδιαίτερα οι χρήστες να αφήσουν το Torrent job να κάνει seeding μετά που αποκτηθούν όλα τα κομμάτια του αρχείου ώστε να αρχίσει να τα κάνει upload . Αν και το χρονικό διάστημα που θα πρέπει να περιμένετε για το seeding δεν ορίζεται συγκεκριμένα(estimated time άπειρο), συνιστάται να γίνεται upload η ποσότητα των δεδομένων η οποία προηγουμένως έγινε download, για την επίτευξη του 1,0 ratio . Ο λόγος αυτός υπολογίζεται διαιρώντας το ποσό των δεδομένων που έχει γίνει upload από το ποσό που έχει γίνει download. Τεχνικά βέβαια είναι αδύνατο να πετύχουν όλοι οι συμμετέχοντες αυτό το ratio καθώς υπάρχουν πάρα πολλοί που κάνουν upload ένα πολύ μικρό ποσοστό σε σχέση με το download η διακόπτουν το Torrent job αμέσως μετά την λήψη. Αυτοί λοιπόν είναι οι λεγόμενοι leechers[50] που έχουμε αναφέρει και παραπάνω.Να αναφερθεί ότι διάφοροι trackers μπορεί να απαγορεύουν τους leechers κάνοντας ban στην IP address τους.Βεβαίως ο όρος αναφέρεται και στα άτομα των οποίων το κατέβασμα είναι σε εξέλιξη αλλά με βάση το ratio (π.χ κατω απο 0.2) μπορεί να πέσει πέλεκυς.



Εικόνα 42.Στατιστικά χρήσης του προγράμματος

[50]Leechers: http://en.wikipedia.org/wiki/Leech_(computing)

3.6 Το πρωτόκολλο SSL

Το μTorrent client χρησιμοποιεί το πρωτόκολλο SSL για την ασφαλή μετάδοση της πληροφορίας μέσα στα swarm που δημιουργούνται.

Το πρωτόκολλο SSL (Secure Sockets Layer) αναπτύχθηκε από την εταιρεία Netscape και σχεδιάστηκε για να παρέχει ασφάλεια κατά την μετάδοση ευαίσθητων δεδομένων στο διαδίκτυο. Η έκδοση 3.0 του πρωτοκόλλου κυκλοφόρησε από την Netscape το 1996 και αποτέλεσε την βάση για την μετέπειτα ανάπτυξη του πρωτοκόλλου TLS[51] (Transport Layer Security), το οποίο πλέον τείνει να αντικαταστήσει το SSL. Τα δύο αυτά πρωτόκολλα χρησιμοποιούνται ευρέως για ηλεκτρονικές αγορές και χρηματικές συναλλαγές μέσω του διαδικτύου.

Το SSL χρησιμοποιεί μεθόδους κρυπτογράφησης των δεδομένων που ανταλλάσσονται μεταξύ δύο συσκευών (συνηθέστερα Ηλεκτρονικών Υπολογιστών) εγκαθιδρύοντας μία ασφαλή σύνδεση μεταξύ τους μέσω του διαδικτύου. Το πρωτόκολλο αυτό χρησιμοποιεί το TCP/IP [52]για τη μεταφορά των δεδομένων και είναι ανεξάρτητο από την εφαρμογή που χρησιμοποιεί ο τελικός χρήστης. Για τον λόγο αυτό μπορεί να παρέχει υπηρεσίες ασφαλούς μετάδοσης πληροφοριών σε πρωτόκολλα ανώτερου επιπέδου όπως για παράδειγμα το HTTP, το FTP, το Telnet κοκ.

Η μετάδοση πληροφοριών μέσω του διαδικτύου γίνεται ως επί το πλείστον χρησιμοποιώντας τα πρωτόκολλα TCP/IP (Transfer Control Protocol / Internet Protocol). Το SSL λειτουργεί πριν το TCP/IP και μετά τις εφαρμογές υψηλού επιπέδου, όπως είναι για παράδειγμα το HTTP (προβολή ιστοσελίδων), το FTP (μεταφορά αρχείων) και το IMAP[53] (e-mail). Άρα λοιπόν αυτό που ουσιαστικά κάνει το SSL είναι να παίρνει τις πληροφορίες από τις εφαρμογές υψηλότερων επιπέδων, να τις κρυπτογραφεί και στην συνέχεια να τις μεταδίδει στο Internet προς τον Η/Υ που βρίσκεται στην απέναντι πλευρά και τις ζήτησε.

Το SSL προσφέρει συνοπτικά τις ακόλουθες υπηρεσίες:

- Πιστοποίηση του server από τον client.
- Πιστοποίηση του client από τον server.
- Εγκαθίδρυση ασφαλούς κρυπτογραφημένου διαύλου επικοινωνίας μεταξύ των δύο μερών.

Οι κρυπτογραφικοί αλγόριθμοι που υποστηρίζονται από το πρωτόκολλο είναι οι εξής: DES - Data Encryption Standard, DSA - Digital Signature Algorithm, KEA - Key Exchange Algorithm, MD5 - Message Digest, RC2/RC4, RSA, SHA-1 - Secure Hash Algorithm, SKIPJACK, Triple-DES.

---

[51] TLS:http://en.wikipedia.org/wiki/Transport_Layer_Security
[52] TCP/IP:http://el.wikipedia.org/wiki/Συζήτηση:TCP/IP
[53]IMAP: http://en.wikipedia.org/wiki/Internet_Message_Access_Protocol

3.6.1 Λειτουργία του SSL

Το πρωτόκολλο SSL χρησιμοποιεί έναν συνδυασμό της κρυπτογράφησης δημοσίου και συμμετρικού κλειδιού . Η κρυπτογράφηση συμμετρικού κλειδιού είναι πολύ πιο γρήγορη και αποδοτική σε σχέση με την κρυπτογράφηση δημοσίου κλειδιού, παρ' όλα αυτά όμως η δεύτερη προσφέρει καλύτερες τεχνικές πιστοποίησης. Κάθε σύνδεση SSL ξεκινά πάντα με την ανταλλαγή μηνυμάτων από τον server και τον client έως ότου επιτευχθεί η ασφαλής σύνδεση, πράγμα που ονομάζεται χειραψία (handshake)[54]. Η χειραψία επιτρέπει στον server να αποδείξει την ταυτότητά του στον client χρησιμοποιώντας τεχνικές κρυπτογράφησης δημοσίου κλειδιού[55] και στην συνέχεια επιτρέπει στον client και τον server να συνεργαστούν για την δημιουργία ενός συμμετρικού κλειδιού που θα χρησιμοποιηθεί στην γρήγορη κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων που ανταλλάσσονται μεταξύ τους. Προαιρετικά η χειραψία επιτρέπει επίσης στον client να αποδείξει την ταυτότητά του στον server. Αναλυτικότερα, η διαδικασία χειραψίας έχει ως εξής:

1. Αρχικά ο client στέλνει στον server την έκδοση του SSL που χρησιμοποιεί, τον επιθυμητό αλγόριθμο κρυπτογράφησης, μερικά δεδομένα που έχουν παραχθεί τυχαία και οποιαδήποτε άλλη πληροφορία χρειάζεται ο server για να ξεκινήσει μία σύνδεση SSL.

2. Ο server απαντά στέλνοντας παρόμοιες πληροφορίες συμπεριλαμβανομένου όμως και του ψηφιακού πιστοποιητικού, το οποίο τον πιστοποιεί στον client. Προαιρετικά μπορεί να ζητήσει και το ψηφιακό πιστοποιητικό του client.

3. Ο client λαμβάνει το ψηφιακό πιστοποιητικό του server και το χρησιμοποιεί για να τον πιστοποιήσει. Εάν η πιστοποίηση αυτή δεν καταστεί δυνατή, τότε ο χρήστης ενημερώνεται με ένα μήνυμα σφάλματος και η σύνδεση SSL ακυρώνεται. Εάν η πιστοποίηση του server γίνει χωρίς προβλήματα, τότε η διαδικασία της χειραψίας συνεχίζεται στο επόμενο βήμα.

4. Ο client συνεργάζεται με τον server και αποφασίζουν τον αλγόριθμο κρυπτογράφησης που θα χρησιμοποιηθεί στην ασφαλή σύνδεση SSL. Επίσης ο client δημιουργεί το συμμετρικό κλειδί που θα χρησιμοποιηθεί στον αλγόριθμο κρυπτογράφησης και το στέλνει στον server κρυπτογραφημένο, χρησιμοποιώντας την τεχνική κρυπτογράφησης δημοσίου κλειδιού. Δηλαδή χρησιμοποιεί το δημόσιο κλειδί του server που αναγράφεται πάνω στο ψηφιακό του πιστοποιητικό για να κρυπτογραφήσει το συμμετρικό κλειδί και να του το στείλει. Στην συνέχεια ο server χρησιμοποιώντας το ιδιωτικό του κλειδί μπορεί να αποκρυπτογραφήσει το μήνυμα και να αποκτήσει το συμμετρικό κλειδί που θα χρησιμοποιηθεί για την σύνδεση.

5. Ο client στέλνει ένα μήνυμα στον server ενημερώνοντάς τον ότι είναι έτοιμος να ξεκινήσει την κρυπτογραφημένη σύνδεση.

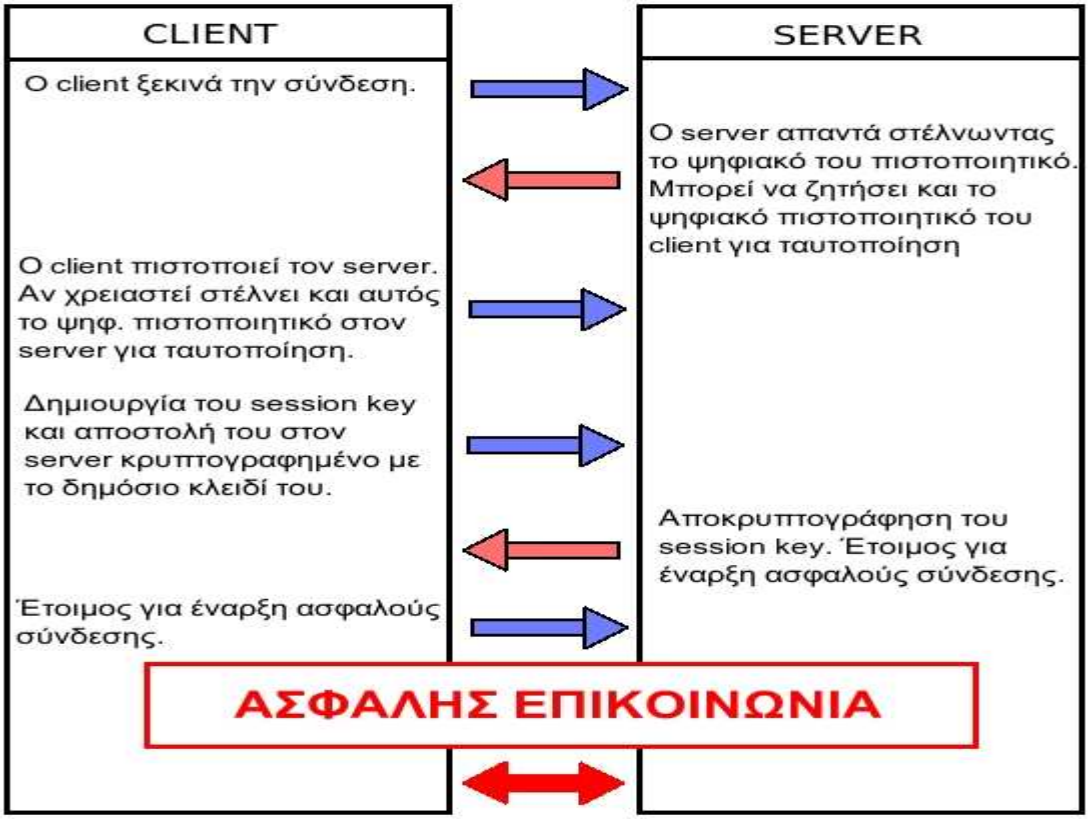
---

[54] Handshake:http://support.microsoft.com/kb/257591
[55] Public Key Infrastructure:http://docs.sun.com/source/816-6154-10/contents.htm

6. Ο server στέλνει ένα μήνυμα στον client ενημερώνοντάς τον ότι και αυτός είναι έτοιμος να ξεκινήσει την κρυπτογραφημένη σύνδεση.

7. Από εδώ και πέρα η χειραψία έχει ολοκληρωθεί και τα μηνύματα που ανταλλάσσουν τα δύο μηχανήματα (client - server) είναι κρυπτογραφημένα.

Η διαδικασία της χειραψίας φαίνεται πιο παραστατικά στο σχήμα που ακολουθεί.



Εικόνα 43.Η SSL Επικοινωνία βήμα βήμα

3.7 Δημιουργία Torrent

Μια πάρα πολύ σημαντική λειτουργία του μTorrent είναι η δημιουργία ενός δικού μας Torrent αρχείου. Η κοινή χρήση δεδομένων στο πρωτόκολλο Bit-Torrent είναι λίγο πιο περίπλοκη από ό, τι με άλλες εφαρμογές P2P. Αυτό είναι ο λόγος που κάνει αυτό το σύστημα διανομής τόσο αποτελεσματικό. Το Bit-Torrent μοιράζει το περιεχόμενο μετά από σπάσιμο αυτού ,σε μικρά κομμάτια και η διανομή τους γίνεται τυχαία μεταξύ των peers. Αυτοί οι peers κατόπιν μοιράζονται αυτά τα κομμάτια μεταξύ τους. Αυτό γλιτώνει τον seeder από τον κόπο της αποστολής ίδιων κομματιών ξανά και ξανά σε διαφορετικούς peers και επιτρέπει σε όλους τους peers σε ένα σμήνος να συμμετάσχουν στη διανομή των αρχείων, ανεξάρτητα από το ποσοστό που απέχουν από την ολοκλήρωση του download ο καθένας χωριστά.

Όπως αναφέρθηκε και παραπάνω, προκειμένου για όλους εκείνους τους peers ,να γνωρίζουν πώς να τοποθετήσουν όλα αυτά τα κομμάτια πίσω στη σωστή σειρά και να κάνουν χρήση του περιεχομένου, οι Bit-Torrent clients απαιτούν ένα ειδικό αρχείο αναφοράς που ονομάζεται Torrent. Το torrent είναι αυτό που κάνετε λήψη από την τοποθεσία και το οποίο ανοίχτηκε με το μTorrent. Όλοι οι peers και οι seeders που εμπλέκονται στη διανομή οποιουδήποτε αρχείου έχουν το ίδιο torrent αρχείο φορτωμένο στον client που χρησιμοποιούν. Για να μοιράζεται κάποιο δικό μας περιεχόμενο μέσω του δικτύου Bit-Torrent, χρειάζεται να δημιουργήσουμε ένα torrent αρχείο για αυτό το περιεχόμενο.

Πράγματα που πρέπει να ληφθούν υπόψη

1. Πριν την δημιουργία ενός Torrent ,θα ήταν σώφρον να διαλέξουμε πρώτα ένα site και να δούμε το FAQ section του που παρέχει σημαντικές πληροφορίες για απορίες που μπορεί να προκύψουν καθώς και τους κανονισμούς χρήσης.
2. Το site της επιλογής μας για παράδειγμα μπορεί να έχει θέσει απαγορευτικό σε συγκεκριμένου είδους υλικό(πχ πορνογραφικό υλικό)ή να ειδικεύεται σε συγκεκριμένα είδη όπως cartoon ή μουσική.
3. Επίσης είναι πιθανό το συγκεκριμένο site να έχει συγκεκριμένες απαιτήσεις σχετικά με την δημιουργία του torrent αρχείου όπως την απαίτηση signature files etc.
4. Άλλα sites απαιτούν να γίνει πρώτα register πριν το upload.
5. Είναι σημαντικό επίσης να σκεφτεί κανείς το μέγεθος του περιεχομένου που θα ανεβάσει επειδή 1)Δεν έχει ο καθένας αρκετό χώρο στο δίσκο για μεγάλα torrent files και 2)Μεγαλύτερα αρχεία torrent σημαίνει μεγαλύτερος χρόνος για seeding.Βασικό λοιπόν να γίνεται upload το περιεχόμενο τακτοποιημένο και διαχωρισμένο.
6. Πριν από την δημιουργία του torrent πρέπει να επιλεγεί προσεκτικά η τοποθεσία του καθώς θα χρειαστεί να μείνει εκεί για αρκετή ώρα(τουλάχιστον κατά την διάρκεια του initial seeding).
7. Τα αρχεία που αποτελούν το περιεχόμενο δεν πρέπει να τροποποιηθούν αφότου γίνει το torrent file και κατά την διάρκεια του seeding καθώς αυτό θα προκαλέσει corruption στο αρχείο.
8. Να είμαστε σίγουροι ότι εκείνη την στιγμή δεν γίνεται χρήση του περιεχομένου αυτού με οποιονδήποτε τρόπο.
9. Δεν υπάρχει πιο ενοχλητικό πράγμα από το multiple compression.Εκτός του ότι δεν έχει διαφορά σε σχέση με το απλό compression,εκνευρίζει και αρκετούς down loaders.Συναντάται πολλές φορές στο κατέβασμα υποτίτλων όπου μπορεί να κάνουμε και 4 extract για να φτάσουμε στο αρχείο υποτίτλων.

Ας δούμε λοιπόν και πρακτικά τα βήματα για να πραγματοποιήσουμε ένα torrent αρχείο:

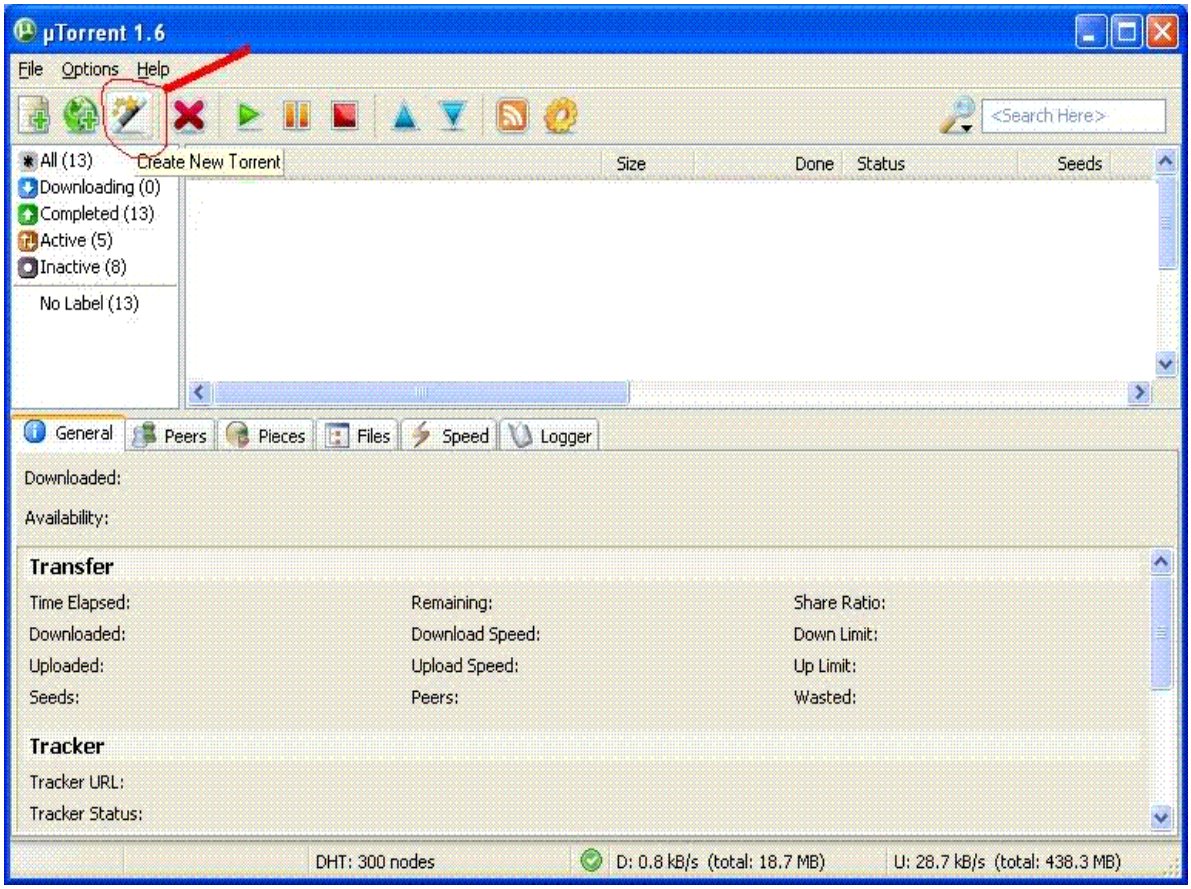
Η πηγή

Εδώ είναι το σημείο όπου μπορούμε να καθορίσουμε τη θέση του περιεχομένου που θέλουμε να μοιράσουμε. Πριν από την επιλογή της διαδρομής πρέπει να επιλέξουμε αν κάνουμε torrent ένα αρχείο ή πολλαπλά αρχεία Αν κάνουμε ένα torrent με πάνω

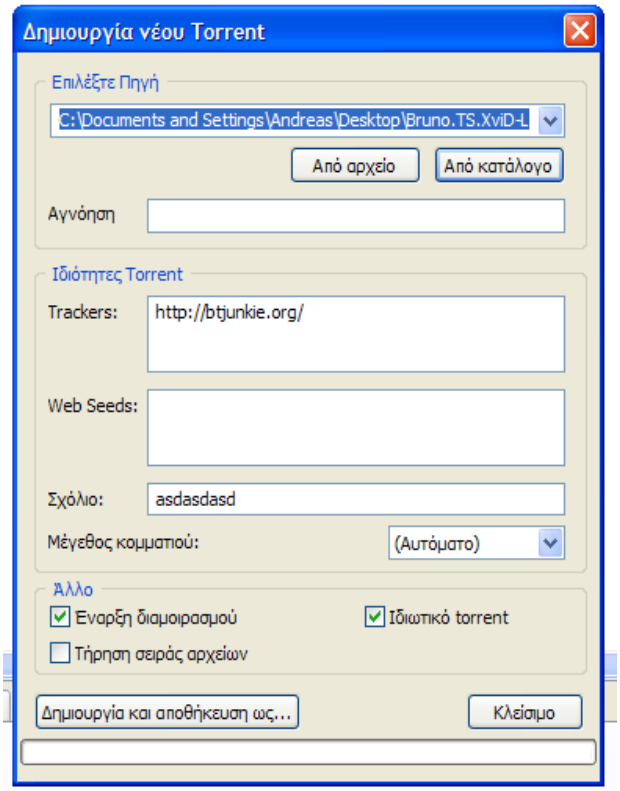
από ένα αρχείο τα αρχεία πρέπει να βρίσκονται σε ένα φάκελο, που δεν θα περιέχει τίποτα άλλο μέσα του.

i) Από το κύριο παράθυρο του μTorrent λοιπόν επιλέγουμε δημιουργία νέου Torrent.
ii) "Προσθήκη αρχείου" ή "Προσθήκη καταλόγου."
iii) Επιλέγουμε την τοποθεσία του αρχείου ή του καταλόγου που θέλουμε να μοιραστούμε.

Στην συγκεκριμένη περίπτωση έχουμε τον Bruno folder στην επιφάνεια εργασίας που περιέχει 3 SRT files (υπότιτλοι) και το AVI της ταινίας.



Εικόνα 44.Επιλογή για δημιουργία Torrent.



Εικόνα 45.Επιλογή του προς Torrent φακέλου.

Ο Tracker

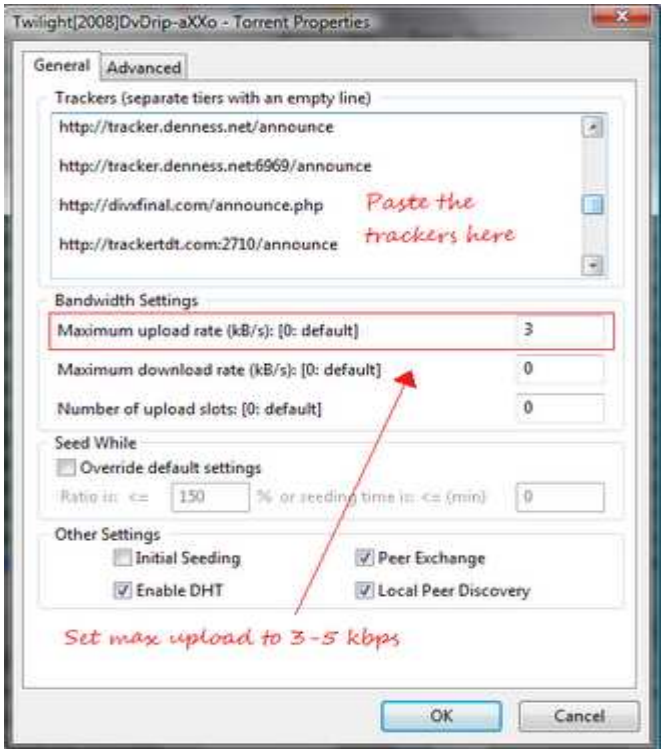
Ένας tracker είναι μια εφαρμογή ή script σε ένα σύστημα το οποίο μεταδίδει πληροφορίες σύνδεσης σχετικά με τους peers για ένα δεδομένο Torrent αρχείο. Ωστόσο, είναι πολύ σημαντικό διότι χωρίς αυτό οι Bit-Torrent clients δεν θα ήξεραν πώς να βρουν άλλους clients που μοιράζονται το ίδιο αρχείο. Το μTorrent ξέρει με ποιόν Tracker να επικοινωνήσει με την ανάγνωση του announce URL στο Torrent file.Οι Trackers γενικά μοιάζουν με οποιαδήποτε άλλη διεύθυνση στο διαδίκτυο (HTTP / /address: port number / announce).

Εάν χρειάζεστε Tracker μπορείτε να:

1)Επιλέξετε την τοποθεσία όπου θέλετε να ανεβάσετε το Torrent.

2)Να αναφερθεί ότι συνήθως, ιδιωτικά sites παρέχουν το δικό τους tracker.

Το μTorrent υποστηρίζει HTTP και HTTPS (SSL) trackers. UDP trackers δεν υποστηρίζονται. Επίσης υποστηρίζει να υπάρχουν πολλοί Trackers ταυτόχρονα.Trackers από τον ίδιο Server (με παρόμοια URLs) πρέπει να ομαδοποιηθούν και εκείνοι που προέρχονται από διαφορετικούς Server, χωρίζονται με μια κενή γραμμή μεταξύ τους.Παρακάτω παρατίθονται τα περιεχόμενα που μπορούμε να δούμε από ένα αρχείο torrent τη στιγμή που το ανοίγουμε με το utorrent και επιλέγοντας το Advanced.



Εικόνα 46.Καθορισμός των Trackers σε ένα Torrent.

Επίσης το μTorrent περιέχει έναν "ενσωματωμένο tracker" που προορίζεται για άτομα που επιθυμούν να μοιραστούν τα αρχεία τους με μια μικρή ομάδα για ένα σύντομο χρονικό διάστημα. Αυτό δεν πρέπει να χρησιμοποιείται για την ανταλλαγή torrent πάνω από Public και private sites.

1)Το URL του ενσωματωμένου Tracker είναι: http://your_ip_address:port/announce (όπου IP σας είναι η διεύθυνση IP και port είναι η port που έχει επιλεγεί να ακούει το μTorrent)

2)Το ενσωματωμένο tracker πρέπει να είναι ενεργοποιημένο, οπότε κάνουμε τα εξής: μTorrent μενού> επιλογές> προτιμήσεις> Advanced> bt.enable_tracker: να οριστεί σε "true".

Εικόνα 47.Ενεργοποίηση του embedded Tracker.

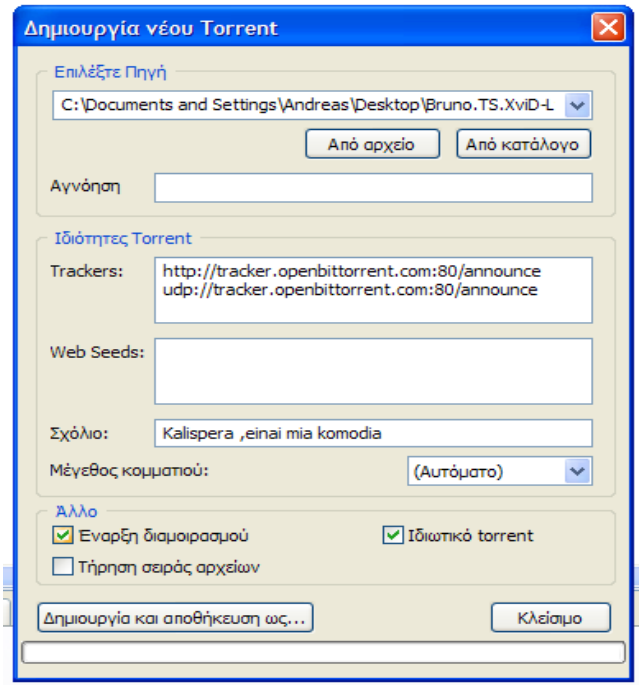
Warning: Χρησιμοποιώντας το ενσωματωμένο tracker απαιτεί από εσάς να έχετε την ίδια διεύθυνση IP και την ίδια θύρα όσο το upload του Torrent είναι ενεργό. Αυτό σημαίνει ότι αν χρησιμοποιείτε μια δυναμική IP και ένα τυχαίο Port και αποσυνδεθείτε από το διαδίκτυο, το torrent αρχείο θα καταστραφεί(τουλάχιστον online).

Σχόλια

Ένα κομμάτι ίσως όχι και το σημαντικότερο είναι και τα σχόλια, προσθέστε λοιπόν κάτι που κατά κύριο λόγο να δίνει πληροφορίες για τον Tracker και για τον seeder.Σε κάποια αυστηρά ιδιωτικά sites όπως IPTorrents όμως, είναι σημαντικό να το περιγράφεις καλά.

Μέγεθος κομματιών

Καθώς φτιάνεται ένα αρχείο Torrent, το περιεχόμενό του κομματιάζεται σε μικρά μέρη για ευκολότερη μετάδοση και διαχείριση(συνήθως των 512kb). Αυτή η επιλογή λοιπόν χρησιμοποιείται για να επιλέξουμε πιο θα είναι το μέγεθος των κομματιών. Όσο μεγαλύτερο το περιεχόμενο τόσο μεγαλύτερα πρέπει να είναι και τα κομμάτια .Ας το αφήσουμε όμως αυτό στο auto-detect καθώς δεν υπάρχει μια de facto αναλογία.



Εικόνα 48.Αμέσως πριν την δημιουργία του Torrent file.

Λοιπά

Όπως βλέπουμε και στην εικόνα παραπάνω πρέπει να έχουμε ticked τα παρακάτω 2 checkboxes:

Η "Εναρξη διαμοιρασμού" θα φορτώσει αυτόματα το νέο torrent στο μTorrent όταν έχετε ολοκληρώσει τη διαδικασία και αν φυσικά δεν υπάρχει κάποιο λάθος στα παραπάνω. Κάποιοι μπορεί να θέλουν να το απενεργοποιήσουν εξαιτίας των Trackers που απαιτούν το re-download του torrent για να αρχίσει το seeding, (αυτό συμβαίνει με ορισμένους δικτυακούς τόπους που απαιτούν κωδικό πρόσβασης ή cookies).Εάν δεν επιλεχτεί το κουτί αυτό τότε θα πρέπει να κάνουμε το seeding με manual τρόπο.

Η επιλογή "Ιδιωτικό Torrent" θα απενεργοποιήσει το DHT (Distributed Hash Table) και το PEX[56] (Peer Exchange), οι οποίες είναι ένα εναλλακτικό μέσο για να λαμβάνονται δεδομένα από άλλους peers εκτός από τον tracker. Αυτό είναι ιδιαίτερα χρήσιμο όταν ο tracker δεν είναι διαθέσιμος για κάποιο λόγο. Ωστόσο, ορισμένες ιδιωτικές ιστοσελίδες δεν το επιτρέπουν γιατί αποτελεί εμπόδιο στην παρακολούθηση των χρηστών, στην ενημερότητα του συνολικού τους ratio και στην δυνατότητα που δίνεται να καθίσταται επικοινωνία με unregistered users(peers).

Τέλος είναι πολύ σημαντικό μετά την δημιουργία του torrent file να δώσουμε ένα χαρακτηριστικό όνομα το οποίο θα περιέχει στοιχεία που θα ενημερώνουν τους επίδοξους downloads:

i) Όνομα αρχείου
ii) Χρονολογία
iii) Ποιότητα
iv) Format
v) Δημιουργός
Ένα παράδειγμα θα ήταν , "My Vacation movies_1996_CAM_MPG_BYME.torrent"

Αυτό που ακολουθεί είναι να επισκεφτούμε το site του Tracker που επιλέξαμε και να κάνουμε upload το Torrent file.

Υπενθύμιση: Μετά το upload δεν πρέπει να αλλάξουμε τουλάχιστον όχι μέχρι να γίνει το πρώτο seed την τοποθεσία του αρχείου, για παράδειγμα εγώ πρέπει να το έχω στην επιφάνεια εργασίας καθώς αλλάζει το URL στα χαρακτηριστικά του και γίνεται unreachable.Έπειτα θα αναλάβουν άλλοι seeders για λογαριασμό μας.

3.8 Προβλήματα

Έλλειψη περιεχομένου

Παρόλο που τα swarming scales είναι ικανά να υποστηρίξουν τα πλήθη για δημοφιλές περιεχόμενο, είναι λιγότερο χρήσιμα για μη δημοφιλές περιεχόμενο. Οι Peers που φθάνουν μετά το αρχικό seeding, είναι πιθανόν να βρουν το περιεχόμενο μη διαθέσιμο και να πρέπει να περιμένουν την άφιξη ενός νέου seeder για την ολοκλήρωση της λήψης τους. Η άφιξή ενός seeder όμως, με τη σειρά του μπορεί να κάνει πολύ χρόνο για να συμβεί, δεδομένου ότι η διατήρηση των seeder για τέτοιο περιεχόμενο είναι μια μη οικονομική λύση ως προς το bandwidth .

Έλλειψη ανωνυμίας

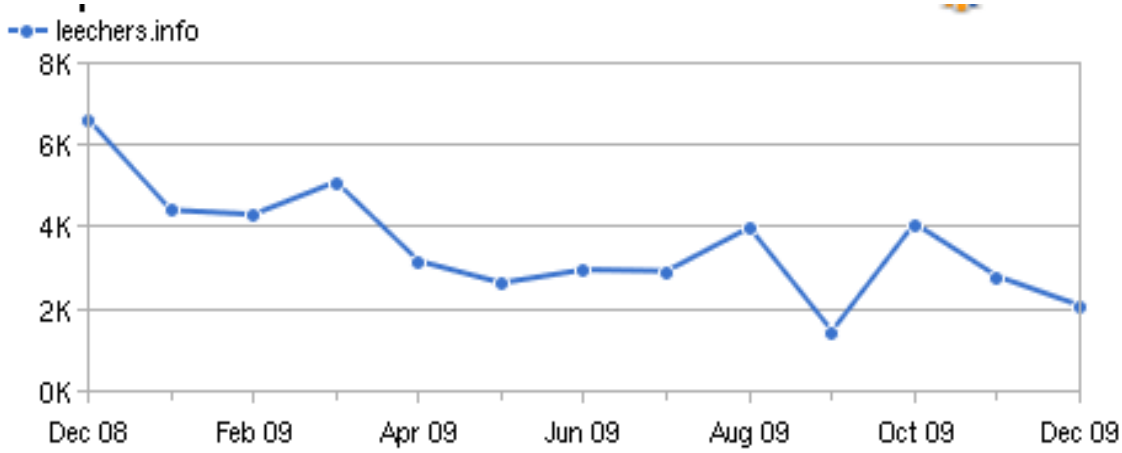
Το Bit-Torrent δεν προσφέρει στους χρήστες του ανωνυμία .Είναι δυνατόν κάποιος να λάβει τις διευθύνσεις IP όλων των προς στιγμή, και, ενδεχομένως, των, προηγούμενων peers που ήταν συμμετέχοντες σε ένα swarm σε έναν συγκεκριμένο Tracker.Αυτό μπορεί να εκθέσει τους χρήστες με ανασφαλή συστήματα σε επιθέσεις.

[56] PEX: http://en.wikipedia.org/wiki/Peer_exchange

Επίσης υπάρχει πάντα ο κίνδυνος μήνυσης από τον ιδιοκτήτη για παράνομη διαχείριση και διανομή του υλικού του, καθώς δεν πρέπει να ξεχνάμε το Napster και τους Metallica στην δίκη[57] για τα πνευματικά δικαιώματα και τις κατηγορίες εναντίον κάποιον πανεπιστημίων για downloads από το δίκτυο του campus.Επίσης μήνυση [58]είχαμε για downloaders της ταινίας Hurtlocker από την παραγωγό εταιρία τον Μάιο του 2010

Το πρόβλημα του leech

Κάποιοι χρήστες του Bit-Torrent μπορούν να επιλέγουν συχνά να εγκαταλείψουν το swarm από τη στιγμή που έχει γίνει πλήρες download απελευθερώνοντας bandwidth για τους άλλους. Αν αρκετοί χρήστες ακολουθήσουν αυτό το παράδειγμα, τα torrent swarms σταδιακά πεθαίνουν, πράγμα που σημαίνει μικρότερη δυνατότητα απόκτησης παλιότερων torrent αρχείων . Ορισμένες ιστοσελίδες που υποστηρίζουν το Bit-Torrent προσπάθησαν να αντιμετωπίσουν αυτό το φαινόμενο, καταγράφοντας το upload και download ratio του κάθε χρήστη, έτσι οι χρήστες που τουλάχιστον ήταν λίγο συνεπείς(ratio 1.0) ανταμείβονταν με πρόσβαση σε καινούργια torrent αρχεία ενώ οι άλλοι μπορούσαν να τιμωρηθούν ακόμη και με ban της IP τους(όπως στο IPTORRENTS[59] που αναφέρθηκε στο 1^{ο} κεφάλαιο). Αυτό έχει φέρει μια πτώση των leechers στατιστικά σε όλα τα sites καθώς χαρακτηριστικό είναι ότι στο IPTORRENTS το ποσοστό τους είναι σχεδόν 0. Πάντως οι παραπάνω αυστηροί Trackers δείχνουν κατανόηση σε περιπτώσεις dial up χρηστών με πολύ περιορισμένες upload δυνατότητες.



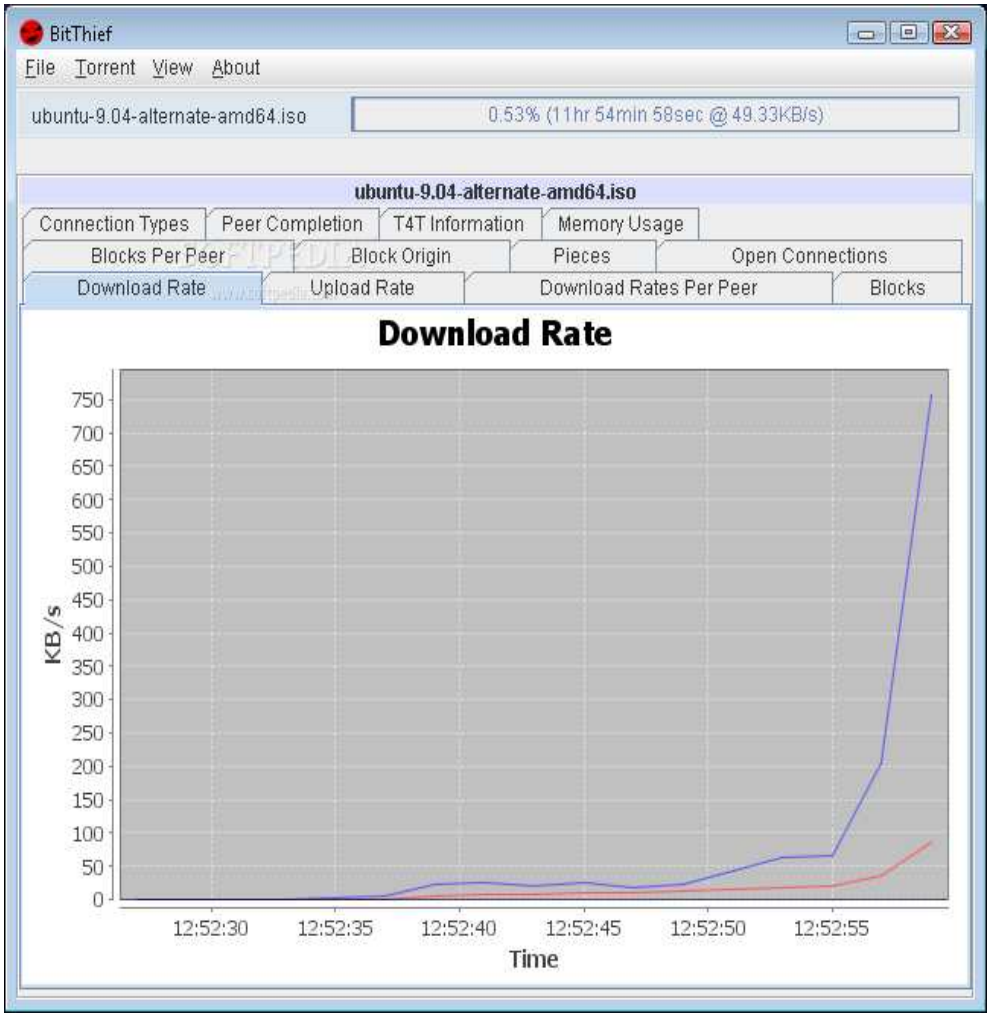
Εικόνα 49.Απεικόνηση της μείωσης του leeching.[60]

Πρόβλημα με cheaters

[57] MetallicaVSNapster: http://guitar.about.com/library/weekly/aa051500a.htm
[58] HurtLocker Sue: http://www.tgdaily.com/business-and-law-features/49998-hurt-locker-producer-sues-5000-bittorerent-users
[59] IPTorrents:http://www.iptorrents.com/indexipt.php
[60]About leechers reduction: http://www.compete.com/

Υπάρχουν cheater Bit-Torrent clients όπως το Bit Thief[61] που ισχυρίζεται ότι είναι σε θέση να κάνει download χωρίς μετά να απαιτείται upload. Τέτοιου είδους εκμετάλλευση, επηρεάζει αρνητικά το πνεύμα συνεργασίας του Bit-Torrent πρωτοκόλλου, αν και θα μπορούσε να αποδειχθεί χρήσιμο για τους ανθρώπους σε χώρες όπου τα πνευματικά δικαιώματα επιτρέπουν το download υλικού αλλά απαγορεύουν το upload.

Επίσης υπάρχουν τεχνικές για spoofing[62] του πραγματικού ratio του χρήστη μέσα από τον client με χρήση προγραμμάτων όπως το Ratio Master το οποία μέσα από ορισμένα βήματα[63] παρουσιάζει ψεύτικο υψηλό ratio σε σχέση με αυτό που έχει ο user.Μπορεί όμως πολλές φορές να γίνει αντιληπτό με μια ματιά στα πρόσφατα στατιστικά του εκάστοτε επιτηδείου για κάποιο Torrent file.



Εικόνα 50.Τα τεράστια download rates του Bit Thief

[61]BitThief: http://www.dcg.ethz.ch/projects/bitthief/
[62] Spoofing:http://en.wikipedia.org/wiki/Spoofing_attack
[63] Spoofing steps: http://www.raymond.cc/blog/archives/2006/07/27/how-to-cheat-bittorrent-ratio-by-spoofing/

Πρόβλημα ταχύτητας

Ο μέσος όρος του download speed στο Bit-Torrent είναι συνήθως το σύνολο της εν λόγω ταχύτητας upload από τον συγκεκριμένο peer και ένα δίκαιο μερίδιο από το σύνολο του upload των peers που ανήκουν στο swarm (peers συνδεδεμένοι με τον tracker που έχει ένα πλήρες αντίγραφο του αρχείου). Οι seeders στην προσπάθεια τους να παράσχουν δίκαια κομμάτια αυτού του upload speed προχωρούν σε διασκορπισμό σε μια ευρεία επιλογή από peers με καλή απόδοση. Βέβαια αυτό έχει να κάνει με αλγόριθμους του μTorrent.

Από την άλλη οι ISP παρέχουν συχνά ασύμμετρες συνδέσεις με το Διαδίκτυο, με πολύ υψηλότερο rate σε download ταχύτητες από ότι σε upload. Δεδομένου ότι ένας peer πρέπει να κατεβάσει δεδομένα τα οποία έχουν ανεβαστεί από κάποιον άλλο φέρνει το Bit-Torrent πρωτόκολλο σε ένα αδιέξοδο. Αυτό το ζήτημα των επιδόσεων γίνεται πιο προφανές κατά τη διάρκεια της εναρκτήριας διαδικασίας ενός σμήνους όπου υπάρχει ένας seeder ο οποίος έχει το πλήρες αντίγραφο του αρχείου torrent και όλοι οι συμμετέχοντες peers έχουν λάβει μέχρι στιγμής τα ίδια κομμάτια του. Όταν ενταχθεί κάποιος σε ένα τέτοιο swarm αρχικά θα επιτυγχάνει πολύ υψηλές ταχύτητες download, καθώς κάθε άλλος peer θα στέλνει κομμάτια με την ελπίδα ότι υπάρχει κάτι να τους σταλεί σαν αντάλλαγμα. Αυτό μάλλον θα συνεχιστεί μέχρι τη στιγμή προσαρμογής με το σμήνος οπότε και η κατά μέσο όρο ταχύτητα λήψης θα πέφτει ακριβώς στα ίδια επίπεδα με την ταχύτητα upload των seeder.

Αν όλοι οι peers στο swarm έχουν συμμετρικές συνδέσεις γίνεται πολύ πιο σταθερό. Κατά την εκκίνηση το swarm θα είναι σε θέση να αντλήσει νέες αφίξεις για το τρέχων ανώτατο επίπεδο, ώστε όλοι να γίνονται seeder .Η ισορροπία μεταξύ της upload και της download speed σημαίνει ότι οδηγούμαστε σε μεγαλύτερες ταχύτητες download κατά μέσο όρο ως αποτέλεσμα των πολλών seeder και ίσως στον αποδεκατισμό των leechers που κατά ένα μεγάλο ποσοστό εγκαταλείπουν το swarm από βαρεμάρα λόγω χαμηλής ταχύτητας μετά το download

Άλλα αναφερθέντα προβλήματα.

Browsing problems.

Σε πάρα πολλά forum παγκοσμίως έχει αναφερθεί ότι όταν τρέχει το μTorrent και ιδιαίτερα εάν κατεβάζει πάνω από ένα αρχείο ταυτόχρονα παρουσιάζεται τεράστιο πρόβλημα στο browsing καθώς οι ταχύτητες είναι πάρα πολύ αργές στο φόρτωμα των sites.Χειρότερες είναι οι περιπτώσεις που αναφέρονται όπου έχουμε και πλήρη διακοπή στο Internet με μόνη προσωρινή λύση όπως αναφέρεται το reboot.

Incompatibility with AMDX64

Επίσης έχει αναφερθεί από άτομα ότι κατά την χρήση του μTorrent ακόμα και όταν γινόταν η λήψη μόνο ενός αρχείου το PC τους «πάγωνε» για ένα χρονικό διάστημα την στιγμή που επιτυγχανόταν το μέγιστο πιθανό download Rate.Κοινό όλων ήταν η χρήση του hardware AMDX64 Dual core και μίας ασυμβατότητας με την συγκεκριμένη μνήμη cache αυτού του επεξεργαστή.

Security flaw[64]

Παρόλο λοιπόν που πολλοί είναι χρήστες του μTorrent και μάλιστα φανατικοί, ήρθε η ώρα να μάθουν το εξής :Η εταιρία διαδικτυακής ασφάλειας SECUNIA[65] ανακάλυψε μια μεγάλη τρύπα στην ασφάλεια του μTorrent η οποία επιτρέπει σε έναν επιτιθέμενο να λαμβάνει τον απόλυτο έλεγχο του μολυσμένου συστήματος .Η συγκεκριμένη εταιρία το χαρακτήρισε ως κόκκινο συναγερμό για τους φανατικούς του download τονίζοντας ότι η προβληματική έκδοση ήταν η 1.6 χωρίς βέβαια να αποκλείεται η μετάσταση σε άλλες εκδόσεις.

Αυτή η αδυναμία του μTorrent απέναντι σε hackers ήταν το αποτέλεσμα ενός σφάλματος κατά την επεξεργασία των .Torrent αρχείων η οποία μπορούσε να αξιοποιηθεί με την χρήση ενός συγκεκριμένου torrent αρχείου με πολύ μεγάλο announce field(4800 Bytes) και το οποίο προκαλούσε stack buffer overflow[66] δηλαδή αποθήκευση δεδομένων εκτός της μνήμης που έχει προοριστεί αρχικά από τον χρήστη με συνέπεια το crush του προγράμματος.

Κατά τα άλλα δεν έχει αναφερθεί άλλο security περιστατικό καθιστώντας το μTorrent ως τον μακρά πιο ασφαλή Bit-Torrent client που βρίσκεται εγκατεστημένος στο 5% των PC παγκοσμίως. Πάντως είναι γεγονός αναπόφευκτο ότι σε δημόσιους και όχι private trackers αλλά και σε διάφορες άλλες σελίδες που φιλοξενούν torrent αρχεία χωρίς έλεγχο, ο καθένας μπορεί να ανεβάσει ότι αρχείο θέλει με ότι περιγραφή θέλει. Πολλές φορές τα comments σώζουν, άλλες όχι.

Προβλήματα λόγω SSL

Η χρήση του πρωτοκόλλου SSL αυξάνει τα διακινούμενα πακέτα μεταξύ των δύο μηχανών και καθυστερεί την μετάδοση των πληροφοριών επειδή χρησιμοποιεί μεθόδους κρυπτογράφησης και αποκρυπτογράφησης. Ειδικότερα οι διάφορες καθυστερήσεις εντοπίζονται στα εξής σημεία:

1. Στην αρχική διαδικασία χειραψίας όπου κανονίζονται οι λεπτομέρειες της σύνδεσης και ανταλλάσσονται τα κλειδιά της συνόδου.

2. Στην διαδικασία κρυπτογράφησης και αποκρυπτογράφησης που γίνεται στους δύο υπολογιστές με αποτέλεσμα να δαπανώνται υπολογιστικοί πόροι και χρόνος.

3. Στην καθυστέρηση μετάδοσης των κρυπτογραφημένων δεδομένων αφού αυτά αποτελούνται από περισσότερα bytes σε σχέση με την αρχική μη κρυπτογραφημένη πληροφορία.

[64] Utorrent Security:http://news.softpedia.com/news/uTorrent-Vulnerable-To-Attacks-46957.shtml
[65] Secunia:http://secunia.com/
[66] Buffer OverFlow:http://en.wikipedia.org/wiki/Buffer_overflow

4. Λόγω αυτών των επιβαρύνσεων που εισάγει το πρωτόκολλο SSL, χρησιμοποιείται πλέον μονάχα σε περιπτώσεις όπου πραγματικά χρειάζεται ασφαλής σύνδεση (πχ μετάδοση κωδικών χρήστη ή αριθμών πιστωτικών καρτών μέσω του διαδικτύου) και όχι σε περιπτώσεις απλής επίσκεψης σε μία ιστοσελίδα.

3.9 Λήψη μέτρων ασφαλείας

Γενικά όταν κάποιος βρίσκεται μέσα σε ένα swarm κατά τη διάρκεια του download είναι εκτεθειμένος καθώς η IP address του γνωστοποιείται στους υπολοίπους peers του swarm.

Συνεπώς καταλαβαίνουμε πως πάντα πρέπει να ακολουθάμε κάποιους παραδοσιακούς κανόνες προστασίας:

- Δεν χρησιμοποιούμε ποτέ Torrent αρχεία που προέρχονται από Trackers τους οποίους δεν έχουμε ποτέ ξαναχρησιμοποιήσει και δεν είναι γνωστοί.

- Παρακολουθούμε Blogs στο διαδίκτυο που αναφέρονται σε Torrent sites για να έχουμε πρόσφατη πληροφόρηση πάντα.

- Πάντα έχουμε ενεργοποιημένο το Firewall και ιδιαίτερα κατά την διαδικασία του upload όπου και πραγματοποιούνται αρκετές συνδέσεις με εμάς.
- Scan τακτικά σε download folders αλλά και όλων των αρχείων κυρίως εκτελέσιμων πριν να τα χρησιμοποιήσουμε.

- Χρήση ορισμένων εξειδικευμένων εργαλείων, όπως το peerblock.

Το peerblock είναι μια open source εφαρμογή που αυτό που κάνει κυρίως είναι να μπλοκάρει τις εξερχόμενες και εισερχόμενες ύποπτες συνδέσεις. Στην ουσία είναι ένας IP blocker .Πρακτικά μιλώντας λοιπόν ,παρακολουθεί τις εξερχόμενες και εισερχόμενες συνδέσεις που κάνουμε με άλλους peers και συγκρίνει τις IP address τους με τις IP που βρίσκονται σε μια block list η οποία ενημερώνεται online όπως τα antivirus κυρίως από την iblocklist.com.Αυτή η λίστα περιέχει ύποπτους διανομείς malware , ψευδο-αρχείων κτλ.

Πάντως είναι σημαντικό να ξέρουμε πως το peerblock[67] είναι καλό στην δουλειά που κάνει και μόνο.Δηλαδή να μας δίνει την δυνατότητα μέσω των blocklists,που βρίσκονται στο διαδίκτυο,να επικοινωνούμε με συγκεκριμένες IP.Υπάρχουν λοιπόν δύο βασικά ερωτήματα:

- Υπάρχει 100% προστασία?

[67] PeerBlock:http://www.peerblock.com/

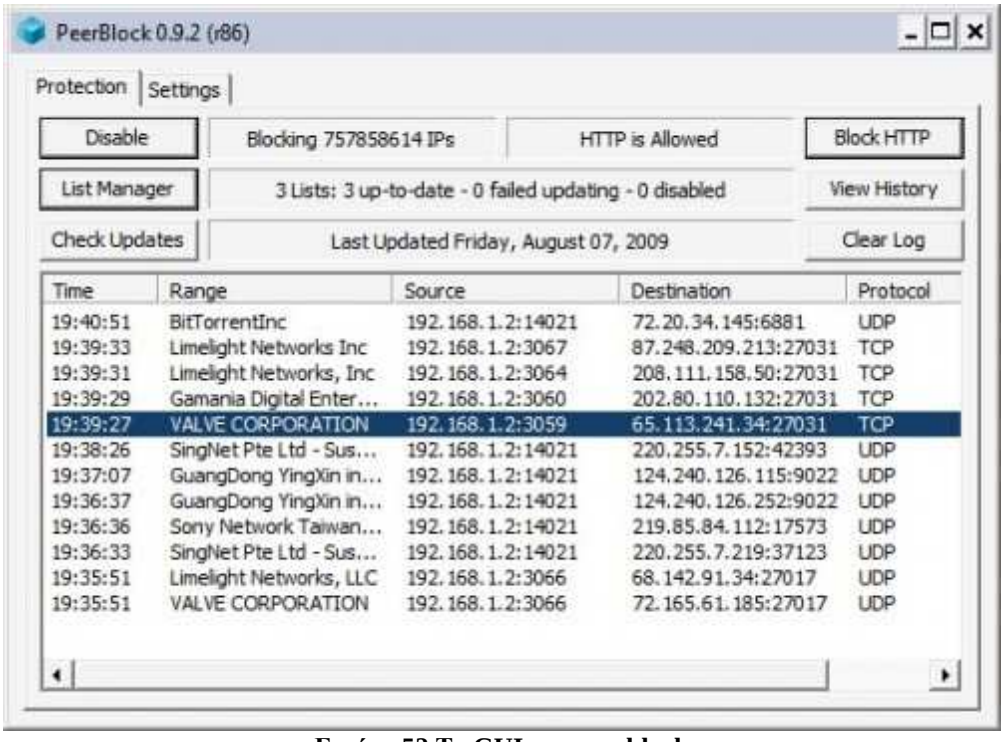
- Μας προσφέρει ασφάλεια τουλάχιστον για το download copyright δεδομένων?

  Απάντηση 1η : Όχι γιατί εξαρτώμαστε πάντα από την εκάστοτε BlockList.

  Απάντηση 2η :Όχι καθώς σύμφωνα με την παραπάνω απάντηση έχουμε πιθανότητες εντοπισμού από εταιρίες όπως η παραγωγή της ταινίας HurtLocker που αναφέραμε παραπάνω.

  Πάντως ώς λύση ασφαλείας απέναντι σε κακόβουλο λογισμικό, είναι ένα πολύ καλό εργαλείο.

Εικόνα 51 Το λογότυπο του peerblock



Εικόνα 52 Το GUI του peerblock

Κεφάλαιο 4

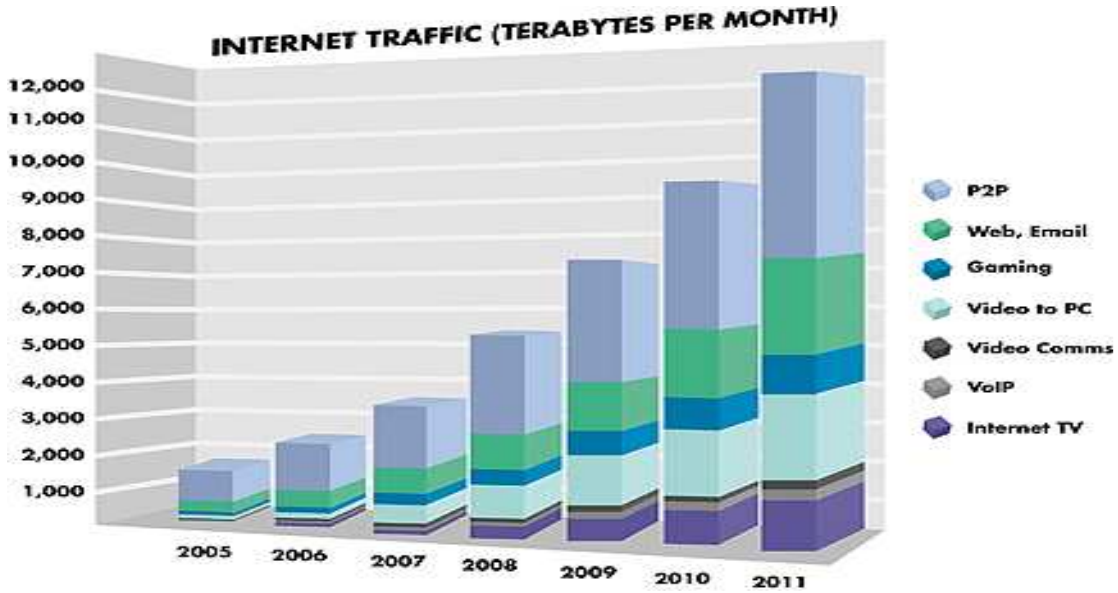
4.0 Εισαγωγή

Όπως αναφέρθηκε και στο προηγούμενο κεφάλαιο κυρίως μετά το 2001 υπάρχει μια έξαρση στην χρήση peer to peer εφαρμογών είτε αυτές είναι για file-sharing είτε για instant messaging[68] κ.τ.λ. Αυτές οι αλλαγές που επέφερε η χρήση peer to peer εφαρμογών έχουν αντίκτυπο στην χρήση του παγκόσμιου ιστού γενικότερα, αλλά και στην πολιτική που εφαρμόζουν οι Internet Service Providers(ISP's).Παρακάτω θα παρατεθούν κάποια ενδιαφέροντα στατιστικά στοιχεία που προκύπτουν από την χρήση peer to peer εφαρμογών.

4.1 Στατιστικά P2P traffic σε πολυπληθείς αγορές.

Γενικά οι εφαρμογές P2P βρίσκονται σε άνοδο. Στην Αμερική μόνο, εκτιμάται ότι 50 εκατομμύρια χρήστες, ή λίγο πάνω από 1/3 των χρηστών του διαδικτύου της Αμερικής κάνουν χρήση κάποιας μορφής δικτύου P2P. Το eDonkey για παράδειγμα, το πιο δημοφιλές δίκτυο P2P, έχει ρεκόρ των περίπου πέντε εκατομμύρια χρηστών σε απευθείας σύνδεση ταυτόχρονα.

Παραδόξως, περισσότερο από το 50% των downloaded αρχείων και από το 80% των στοιχείων που γίνονται upload στο Διαδίκτυο είναι μέσω ενός δικτύου P2P. Από αυτά, το 46% είναι βίντεο, μόνο το 13% είναι τα τραγούδια και το 37% είναι οτιδήποτε άλλο, συμπεριλαμβανομένου του λογισμικού και e-books.Όλα ρα παραπάνω σύμφωνα με το PC Magazine(τεύχος Μαρτίου 2010)



Εικόνα 53 Στατιστική πρόβλεψη του Internet Traffic(2005-2011)

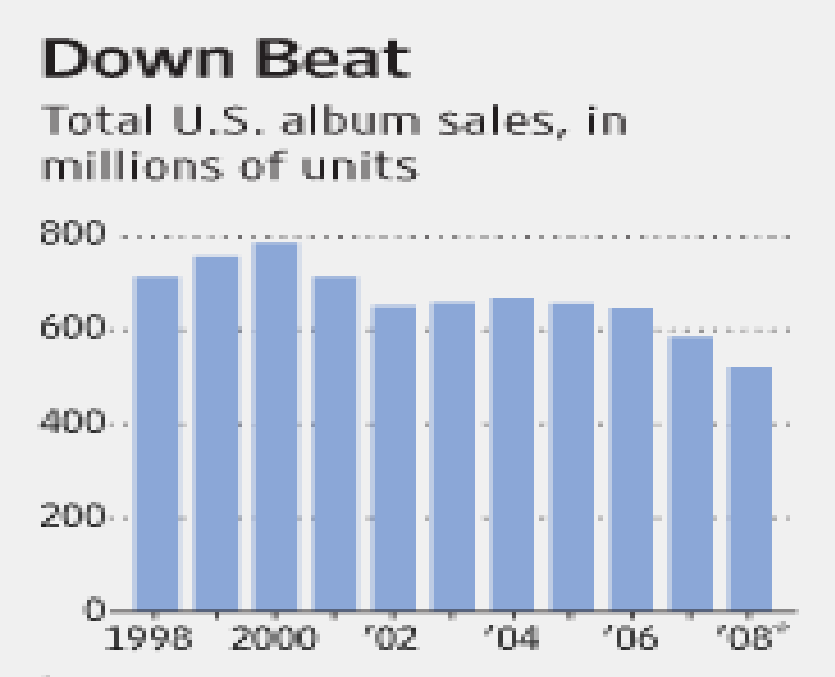
Παρά πολύ βαριά νομική δράση κατά των P2P δικτύων είναι σε εξέλιξη και φυσικά προέρχεται από τις εταιρίες και από τους κατόχους των πνευματικών δικαιωμάτων video, music etc.,Πάντως αυτό δεν δείχνει να οδηγεί σε κάποιο αποτέλεσμα. Το

[68] Instant Messaging:http://en.wikipedia.org/wiki/Instant_messaging

Kazaa[69] απαγορεύεται τώρα στην Αυστραλία, αλλά πολλές εναλλακτικές λύσεις υπάρχουν ,ας μην ξεχνάμε τα torrents και τους αμέτρητους clients που αναφέρθηκαν στο προηγούμενο κεφάλαιο. Η νομική μάχη κατά των P2P εφαρμογών παραμένει όμως και δεν θα σταματήσει οποτεδήποτε σύντομα παρόλο που φαίνεται να είναι μια λερναία Ύδρα.

Τα P2P δίκτυα δίνουν τη δυνατότητα στους χρήστες να κατεβάσουν το λογισμικό, έτσι ώστε παρά το τεράστιο συνήθως μέγεθος των περισσότερων αρχείων να μπορούν να γίνουν download μέσα σε λίγες ώρες(αυτό βέβαια εξαρτάται από την δυνατότητα της σύνδεσης του χρήστη) .

Στην περίπτωση της μουσικής, το πρόβλημα δεν είναι τόσο σοβαρό. Τρεις στους τέσσερις χρήστες δέχονται να αγοράσουν ένα CD, μετά τη λήψη του σε απευθείας σύνδεση. Σύμφωνα με μελέτες, η απώλεια από την μουσική πειρατεία είναι πολύ λιγότερη από ό, τι πίστευαν παλαιότερα. Οι περισσότεροι άνθρωποι που κατεβάζουν μουσική από το διαδίκτυο, δεν θα είχαν αγοράσει το CD, ακόμη και αν οι αντίστοιχες εφαρμογές P2P και το διαδίκτυο δεν υπήρχαν. Η Offline μουσική πειρατεία ανέρχεται στο 14% των πωλήσεων. Πάντως έχει σημειωθεί μια μικρή πτώση όπως βλέπουμε στην παρακάτω εικόνα, στις πωλήσεις των CD στην Αμερική μετά το 2006(δηλαδή μετά την ευρεία χρήση του BitTorrent) .



Εικόνα 54 Παρουσίαση της μείωσης πωλήσεων CD στην Αμερική[70]

Επίσης οι P2P χρήστες αυξάνονται κατά 4% κάθε χρόνο και το eDonkey[71] είναι το # 1 δίκτυο, με μεγάλη διαφορά.

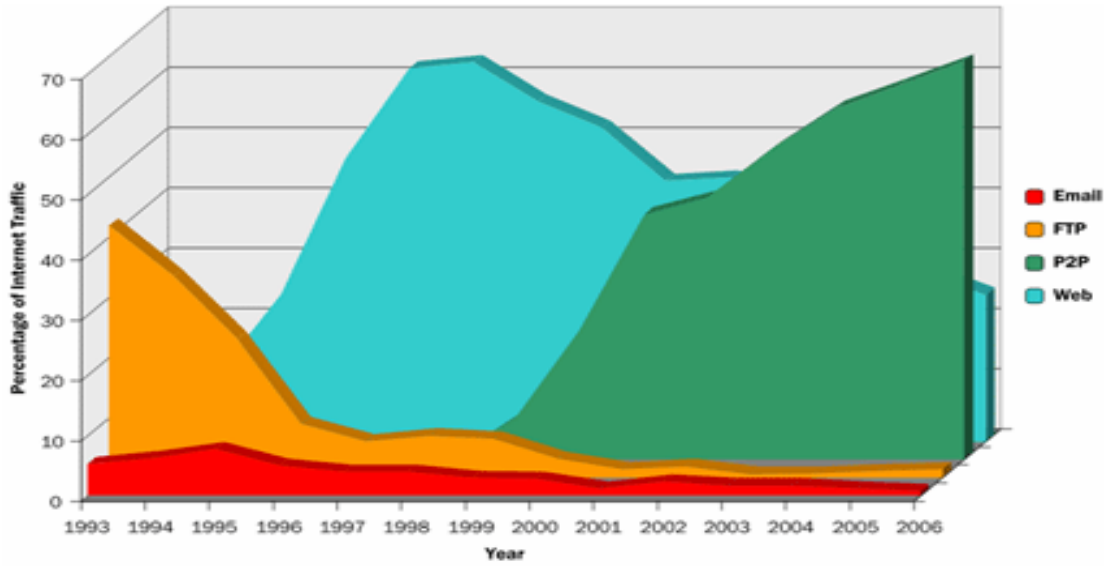
[69] Kazza:http://www.kazaa.com/
[70]DownBeat Research: http://online.wsj.com/article/SB122966038836021137.html
[71] E-donkey:http://en.wikipedia.org/wiki/EDonkey_network

Συνοψίζοντας λοιπόν έχουμε τα εξής για την κίνηση συνολικά σε περιοχές όπως η Ευρώπη η Αμερική και η Κίνα:

Σχετικά με το ποσοστό των δεδομένων(World-Wide peer to peer Market)

Το 50-65% της συνολικής κίνησης downloaded αρχείων στο διαδίκτυο έχει να κάνει με peer to peer δίκτυα.

Το 75-90% της συνολικής κίνησης upload επίσης σχετίζεται με peer to peer.



Εικόνα 55 Το μερίδιο του p2p στο παγκόσμιο εύρος ζώνης

Σχετικά με το πλήθος των χρηστών

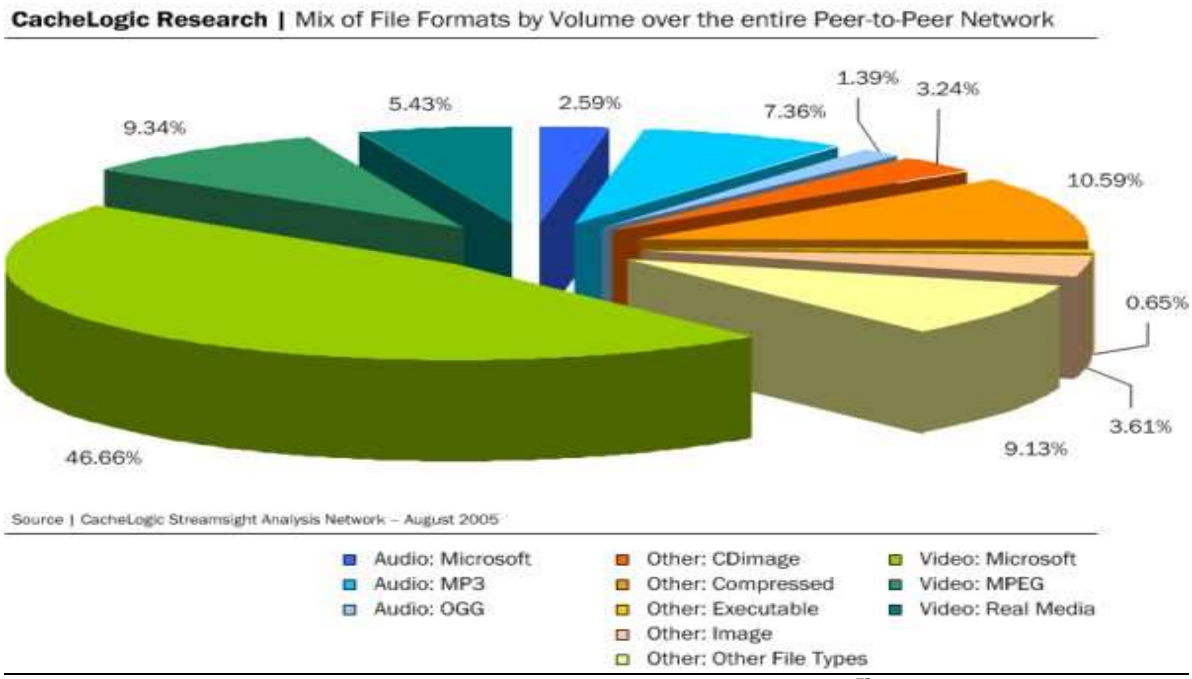
Το 2004 ένας Cache Logic Server[72]** είχε κάνει ρεκόρ κάνοντας register 3.000.000 IP διευθύνσεις σε 30 ημέρες.

Το 2006 ένας Cache Logic Server είχε έκανε κάτι παρόμοιο κάνοντας register 3.000.000 IP διευθύνσεις σε 8 ημέρες.

**Cache Logic Servers να σημειωθεί ότι είναι μια σειρά servers που καταγράφει την peer to peer κίνηση στις δημοφιλέστερες κυρίως εφαρμογές.

Σχετικά με το είδος των downloaded δεδομένων
Το 46.66% είναι αρχεία video
Το 11,3 % είναι αρχεία audio
Το 27,2% είναι παιχνίδια, λογισμικό ,βιβλία κτλ. .
Ο μέσος όρος του μέγεθος των παραπάνω αρχείων είναι το 1 Gigabyte

[72] Cache Logic Server:http://whois.domaintools.com/cachelogic.info



Εικόνα 56 Καταμερισμός των διακινούμενων αρχείων[73]

4.2 Security stats

Όπως έχουμε δει και από το πρώτο κεφάλαιο η φιλοσοφία των peer to peer δικτύων δημιουργεί από την φύση της security risks,τα οποία ότι και να κάνουμε πάντα θα υπάρχουν. Μπορούν να συμβούν είτε μέσα από εφαρμογές instant messaging είτε μέσα από spamming γενικότερα. Επίσης θα καταλάβουμε και το τόσο μένος των εταιριών απέναντι στις peer to peer εφαρμογές . Ας δούμε μερικά στατιστικά που έχουν προκύψει κατά καιρούς από διάφορες έρευνες αναφερόμενες στο βιβλίο "Server and peer to peer trends in western Europe".

Το 55% δηλώνει μολυσμένο από Spyware.

Το 55% των online χρηστών δήλωσαν ότι είχαν προσβληθεί από spyware [74]τουλάχιστον μια φορά, και το 82% πίστευε ότι το γεγονός αυτό αποτελούσε απειλή για την online προστασία της ιδιωτικής ζωής.

22% δηλώνει ότι μείωσε την χρήση εφαρμογών Instant messaging.

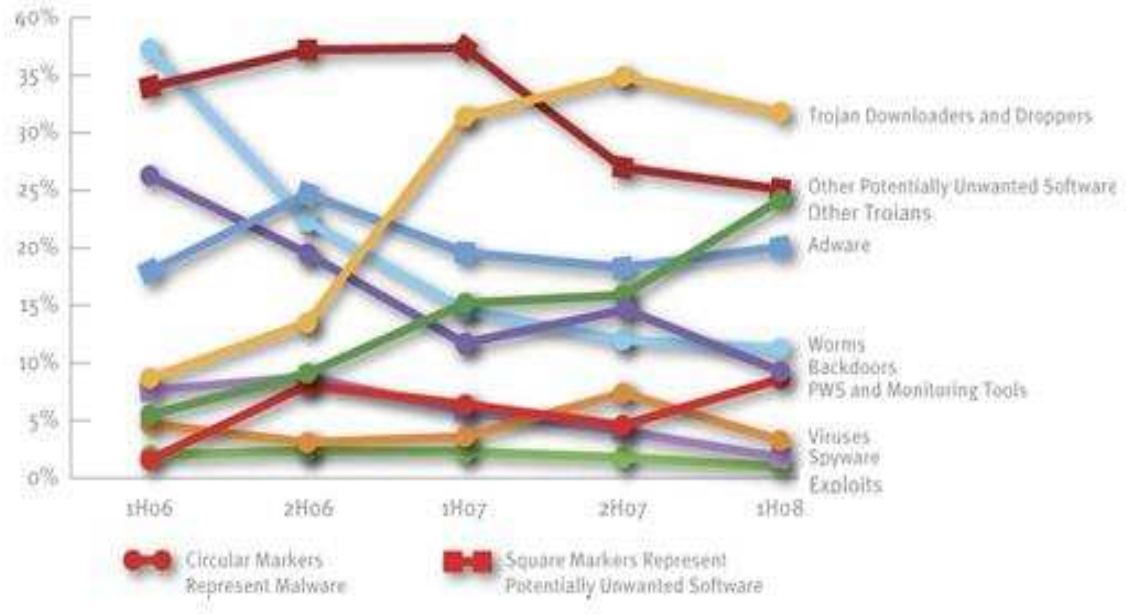
Το 53% των ενηλίκων χρηστών instant messaging στις Ηνωμένες Πολιτείες, τώρα δηλώνουν ότι εμπιστεύονται τις εφαρμογές αυτές λιγότερο λόγω των spam με αποτέλεσμα πτώση κάτω από 38% στη χρηστικότητα πριν από 6 χρόνια(2004) και περίπου το ίδιο τον Ιούνιο του 2003.Πάντως περίπου 53 εκ. Αμερικάνοι χρησιμοποιούν Instant Messaging ,σύμφωνα με την Pew Internet[75] .

[73] CacheLogic Research: http://www.afterdawn.com/news/index.cfm/2005/08/
[74] Spyware:http://www.microsoft.com/hellas/athome/security/spyware/spywarewhat.mspx
[75] Pew Internet Research: http://www.pewinternet.org/Reports/2004/How-Americans-Use-Instant-Messaging.aspx

Το 22% των παραπάνω χρηστών δηλώνουν ότι ξοδεύουν λιγότερο χρόνο , λόγω του spam, κάτω από το 29% που είχε την προηγούμενη χρονιά.

Malicious Software στις μεγάλες αγορές

Κατά το δεύτερο εξάμηνο του 2004, η Symantec παρακολουθεί τον αριθμό των υπολογιστών που συμμετέχουν σε peer to peer εφαρμογές και που έχουν παραβιαστεί από επιβλαβές λογισμικό. Το 25,2% του συνόλου των μολυσμένων υπολογιστών που η εταιρεία ανακάλυψε είχαν βάση στο Ηνωμένο Βασίλειο, με τις ΗΠΑ να ακολουθούν μια ανάσα πίσω στενά με 24,6%, και η Κίνα στην Τρίτη θέση με 7,8%. Τον Ιούλιο του 2004 η Symantec έκανε την διαπίστωση ότι κατά μέσο όρο 30.000 υπολογιστές μολύνονταν κάθε μέρα από malicious software με τον αριθμό αυτό να μειώνεται στις 5000 τον Δεκέμβριο του ίδιου έτους.



Εικόνα 57 Στοιχεία του Malicious Software

Το 33% των εταιριών δίνει πρόσβαση σε instant messaging στο προσωπικό

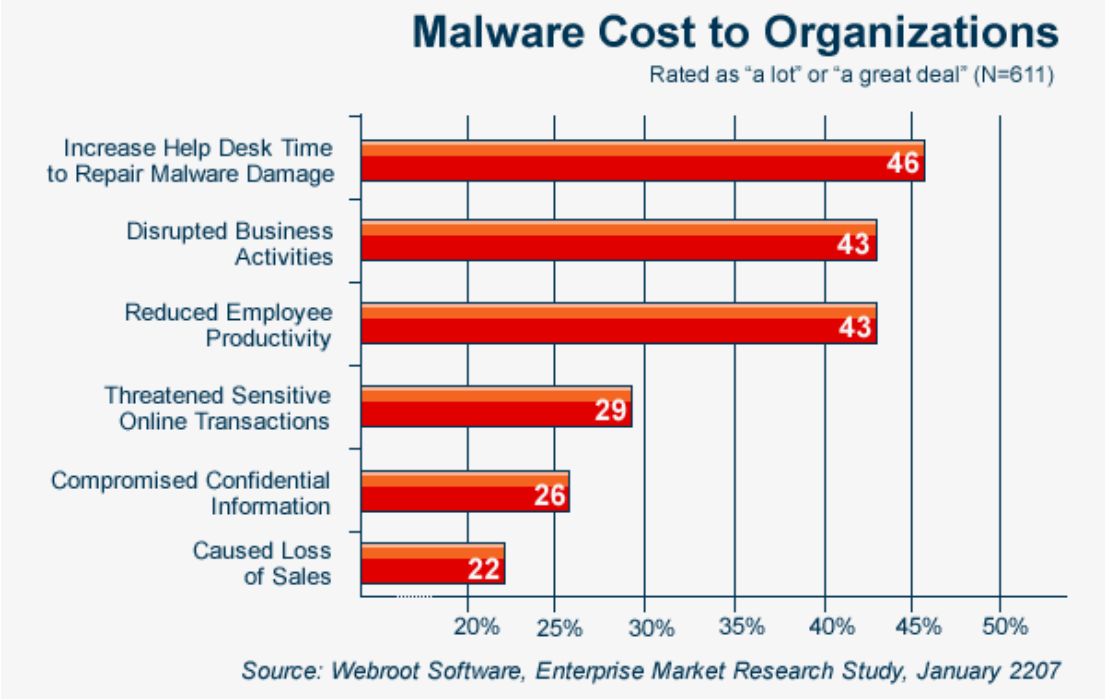
Ο Αγγλικός IT Observer[76] εισαγάγει στατιστικά στοιχεία του Ηνωμένου Βασιλείου σχετικά με τη χρήση Instant messaging εφαρμογών . Η έρευνα διεξήχθη από το Manchester Business School .33% των βρετανικών εταιρειών παρέχουν πρόσβαση του προσωπικού σε υπηρεσίες άμεσων μηνυμάτων, σε σύγκριση με το 84% που έχουν εταιρικό intranet. Ενώ περισσότερο από το ήμισυ των εταιρειών με IM θεώρησε ότι θα είχε όφελος από αυτό (58%), μόνο το 3% αυτών ανέφερε ότι είχε χρησιμοποιηθεί ως επίσημο εργαλείο επικοινωνίας.

Το τεράστιο κόστος του Malware

Τα Malware, συμπεριλαμβανομένων των ιών, worms και trojans, αύξησαν το κόστος

[76] It Observer: http://www.it-observer.com/

αρκετών παγκόσμιων επιχειρήσεων μεταξύ 13 δισ. δολάρια και 13.5 δισ. δολάρια το 2007 συνολικά[77]. Με περίπου 600 εκ. υπολογιστές βασισμένους στα Windows σε όλο τον κόσμο, συμπεραίνεται ένα ποσό της τάξεως των 281 έως 340 δολαρίων ανά μηχάνημα σε ζημιές .Ίσως αυτός είναι και ο κύριος λόγος που αρκετές εταιρίες απαγορεύουν την χρήση p2p εφαρμογών.

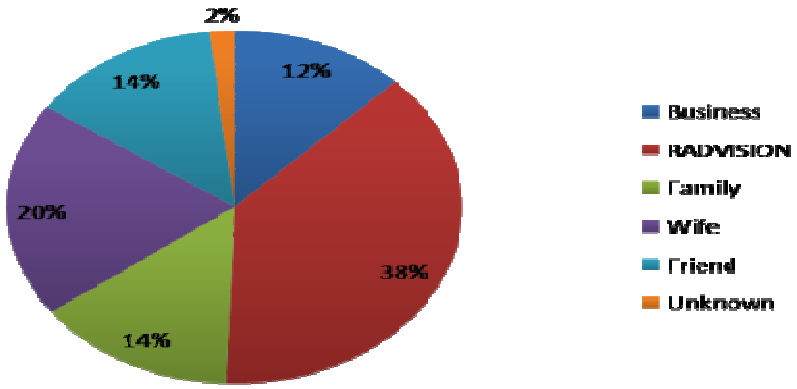


Εικόνα 58 Το κόστος του Malware για τις εταιρίες

Instant messaging: απειλές για την ασφάλεια με διπλασιασμό κάθε 6 μήνες

Η Gartner προέβλεψε ότι μέχρι το τέλος του 2005, τα άμεσα μηνύματα θα ξεπεράσουν το e-mail ως πρωταρχικό τρόπο που οι άνθρωποι επικοινωνούν ηλεκτρονικά. Το Radicati Group αναφέρει ότι "πάνω από το 33% του συνόλου των επιχειρήσεων χρησιμοποιούν εφαρμογές άμεσων μηνυμάτων για τις επιχειρήσεις". Η Symantec ισχυρίζεται επίσης ότι οι instant messengers και γενικά οι peer-to-peer εφαρμογές χρησιμοποιούνται σε 7 από τις 10 κορυφαίες απειλές στο Διαδίκτυο το 2004, με την χρήση IM οι απειλές για την ασφάλεια αυξάνονται κατά 100% κάθε έξι μήνες.

[77] Malware Damage: http://www.computereconomics.com/article.cfm?id=1225



Εικόνα 59 Η χρήση του IM ανάμεσα στις κοινωνικές ομάδες

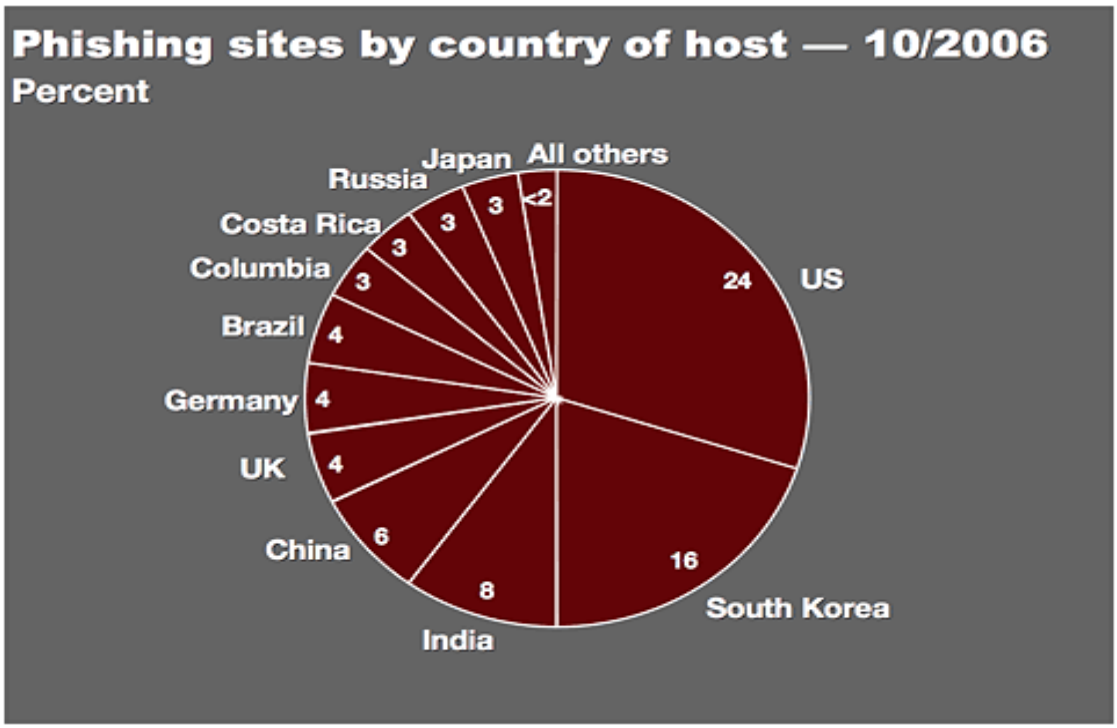
Η μόλυνση από Spyware θα φθάσει το 25% των υπολογιστών των επιχειρήσεων

Η Forrester Research προβλέπει ότι τα επίπεδα μόλυνσης από Spyware θα φθάσουν το 25% σε 12 μήνες(2006), προτρέποντας το 65% των επιχειρήσεων που ερωτήθηκαν να λένε ότι θα επενδύσουν σε anti-spyware εργαλεία και αναβαθμίσεις εντός του τρέχοντος έτους. Περίπου στο 80% των επιχειρήσεων που ερωτήθηκαν έχουν ήδη αναπτυχθεί εξειδικευμένα εργαλεία για την αντιμετώπιση του προβλήματος.

Το 24% των phishing sites φιλοξενούνται στις ΗΠΑ

Πολύ συχνό φαινόμενο στις p2p εφαρμογές αλλά και στο Internet γενικότερα είναι το phishing. Σύμφωνα με μια Anti-Phishing Working Group (APWG) έκθεση τον Ιανουάριο του 2005 επάνω στην phishing[78] δραστηριότητα ,έδειξε ότι το 24% των τοποθεσιών Web που «ψάρευαν» ήταν εγκαταστημένες στις Ηνωμένες Πολιτείες. Η Νότιος Κορέα βρέθηκε να είναι στη δεύτερη θέση, με 16%, με την Κίνα και την Ινδία στην τρίτη και τέταρτη θέση με 8% και 6% αντίστοιχα.

[78] Phising:http://en.wikipedia.org/wiki/Phishing



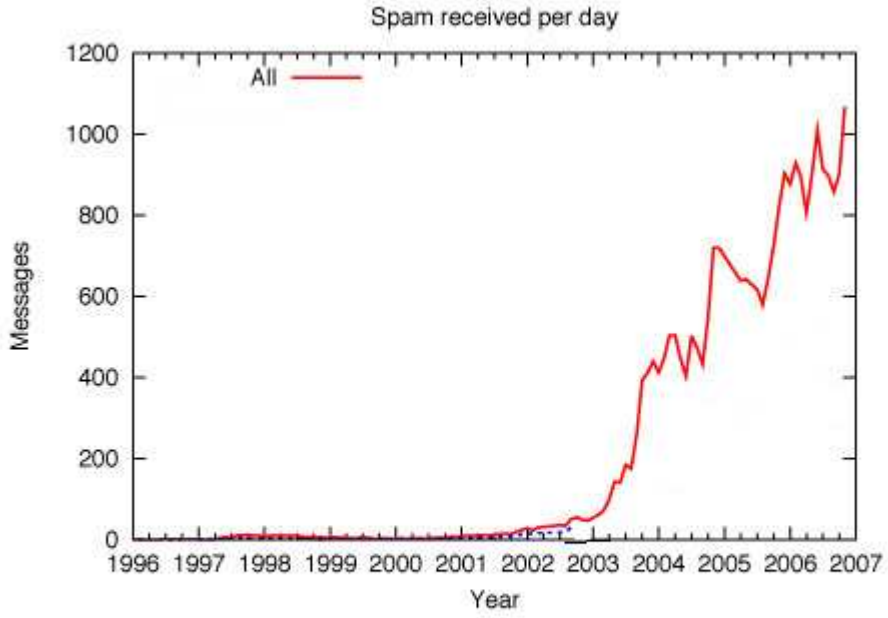
Εικόνα 60 Ποσοστό των phishing hosts ανά χώρα

65% των επιχειρήσεων προτίθεται να δαπανήσουν χρήματα για anti-spyware

Το 65% των επιχειρήσεων δήλωσαν ότι προτίθενται να θέσουν χρήματα για την προστασία των συστημάτων τους από τα αδιάκριτα και κακόβουλα προγράμματα λογισμικού για το 2005. Ενώ το 69% των μεγάλων επιχειρήσεων δήλωσαν ότι θα αγόραζαν anti-spyware εργαλεία το 2005, μόνο το 53% των μικρών και μεσαίων επιχειρήσεων δήλωσαν ότι θα λάμβαναν την προστασία αυτή. Σχεδόν το 40% των ερωτηθέντων παρέλειψε να θέσει έναν συνολικό αριθμό των μηχανημάτων τους που έχουν μολυνθεί. Περίπου το 17% των συστημάτων τους είχαν ήδη υποφέρει από spyware .

14% των χρηστών διαβάσει τα spam messages, και το 4% αγοράζει προϊόντα που διαφημίζονται σε spam

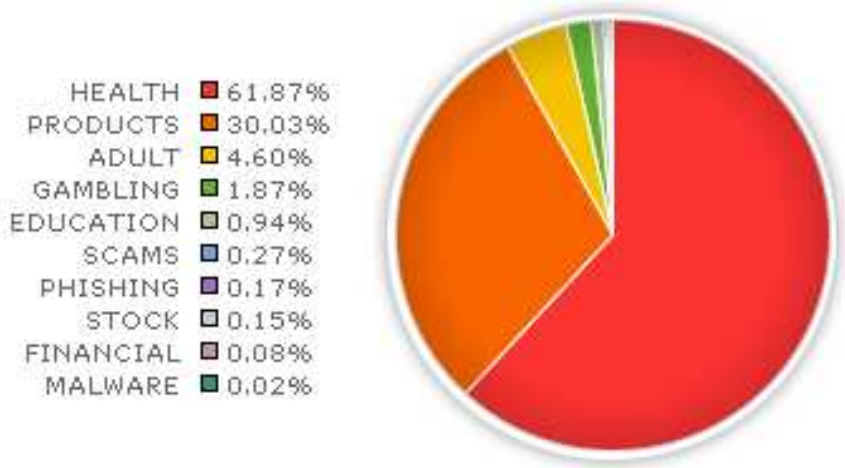
Ο χρόνος που σπαταλιέται για την διαγραφή ανεπιθύμητης ηλεκτρονικής αλληλογραφίας από τις αμερικανικές επιχειρήσεις φέρνει κόστος περίπου 22 δις $ το χρόνο(Server and peer to peer trends in western Europe). Μια τηλεφωνική έρευνα που έγινε σε ενήλικους που χρησιμοποιούν το Internet διαπιστώθηκε ότι πάνω από το 75% λαμβάνει spam καθημερινά. Ο μέσος όρος μηνυμάτων spam ημερησίως είναι 18,5 και ο μέσος χρόνος που δαπανάται ανά ημέρα διαγραφή τους είναι 2,8 λεπτά. Η απώλεια της παραγωγικότητας είναι ισοδύναμη με 21,6 δολάρια δισ. ευρώ ετησίως κατά τον μέσο όρο των μισθών των ΗΠΑ, σύμφωνα με μια έρευνα που έγινε από το Maryland Business School.Το 14% των spam receivers διαβάζει αυτά τα μηνύματα για να δει τι λένε, και το 4% έχουν αγοράσει κάτι που διαφημίζεται μέσω spam κατά το παρελθόν έτος(2005). Φυσικά το κακό με το Spam άρχισε μετά το 2003 σε μεγάλο βαθμό, όταν οι εφαρμογές peer to peer ήταν σε έξαρση.



Εικόνα 61 Η ποσότητα λήψης Spam σε καθημερινή βάση διαχρονικά(1996-2007)

4.6% των spam τον Ιανουάριο του 2005 ήταν πορνό

Σύμφωνα με στοιχεία που δόθηκαν από το BitTorrent και αφορούσαν τις παρατηρήσεις πελατών , το πορνογραφικό spam έχει εκτοξευθεί από το 1% του συνόλου των αυτόκλητων ηλεκτρονικών μηνυμάτων τον Δεκέμβριο του 2004 σε 4.6% τον Ιανουάριο του 2005. Το Spam αυξήθηκε κατά περίπου 40% από το Νοέμβριο, ενώ η κυκλοφορία των ιών μειώνεται σταθερά. Περισσότερα από τρία στα πέντε ηλεκτρονικά μηνύματα spam σχετίζονται με ιατρικά θέματα(61.87%). Αντίθετα, το spam που αφορά διαφήμιση χρηματοπιστωτικών υπηρεσιών μειώθηκε από 2% του συνόλου των spam τον Δεκέμβριο του 2004 σε μόλις 0,08% τον Ιανουάριο του 2005.Ο βασιλιάς του spam είναι συνήθως οι σελίδες των Trackers.



Εικόνα 62 Διαφημιζόμενα είδη μέσω Spam

Τα πιο δημοφιλή μηνύματα spam για το 2007 ταξινομημένα:

1. We bring you the most famous drugs for arthritis (Vioxx).

2. You got a Kiss! (phishing).

3. You've got 17 new messages (phishing).

4. Steamy HOT LESBIAN ΔΡΑΣΗ LIVE ON CAMERA!

5. Digital Filters HURRY (ισχυρίζεται ότι μπορεί να αποκωδικοποιήσει ψηφιακά κανάλια καλωδιακής τηλεόρασης).

6. YOU ARE THE 1.000.000th visitor, Congratulations.

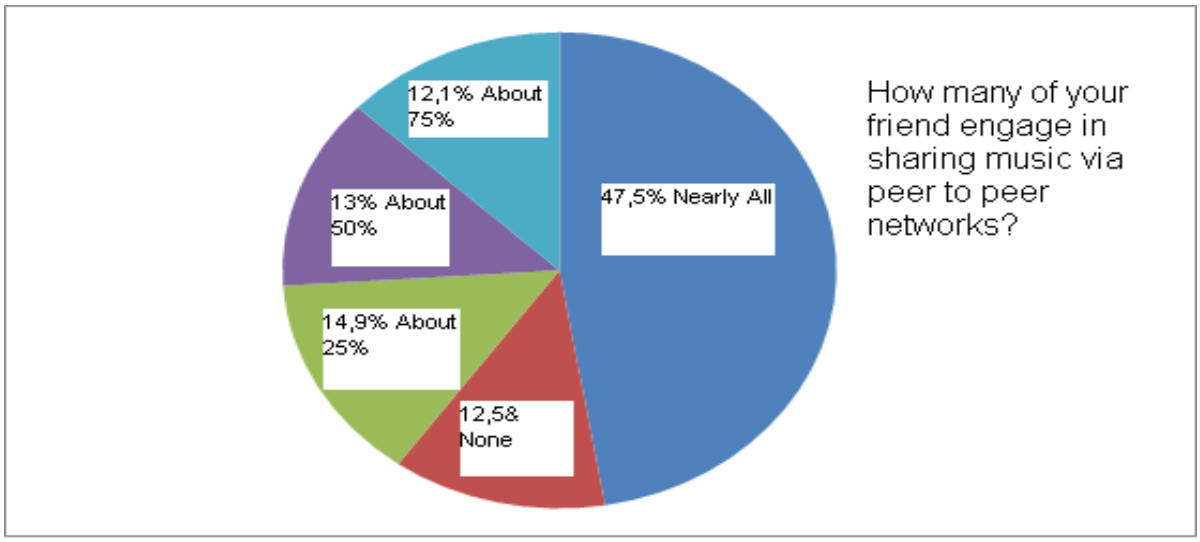
7. HURRY HURRY Hot (pop-up).

8. Έκτακτη είδηση(απλά και ξερά).

4.3 Διάφορα γενικά στατιστικά για τις File-Sharing εφαρμογές

4.3.1 Διαφήμιση μέσω peer to peer για τα διαφημισμένα μουσικά αρχεία

Μια μελέτη από την ιστοσελίδα της PRS for Music's και της Big Champagne Media Measurement's από τον Eric Garland, με τον τίτλο The Long Tail of P2P[79] ,βρίσκει ότι οι peer to peer file sharing εφαρμογές το μόνο που κάνουν είναι να κάνουν την δημοφιλή μουσική ακόμα πιο δημοφιλή ενώ στην ουσία δεν βοηθάνε underground συγκροτήματα και άσημους μουσικούς. Το λογικό αυτού του ισχυρισμού φαίνεται και από το παρακάτω σχήμα που δείχνει τον όγκο των down loaders



Εικόνα 63 Ο όγκος των downloaders μουσικών αρχείων μέσω p2p

Η μελέτη αυτή επίσης έδειξε ότι τα πιο δημοφιλή πειρατικά τραγούδια είναι πάντα στην κορυφή των music charts όπως το Billboard την ίδια χρονική περίοδο, αντιθέτως κάποια άλλα πιο άγνωστα μουσικά σχήματα και κομμάτια ούτε βοηθήθηκαν ούτε και καταρρακώθηκαν από τις peer to peer εφαρμογές. Αυτό το file sharing έχει γίνει πλέον ένα αρκετά ικανοποιητικό broadcasting network που χρησιμοποιείται και για online ραδιόφωνο.

Η πειρατεία που πραγματοποιείται με το μανιώδες παράνομο κατέβασμα τόσων πολλών αρχείων πάντως δεν αντιμετωπίζεται με τον ίδιο τρόπο όπως παλιότερα Αυτό που τελικά ισχυρίζονται όλο και περισσότερα άτομα είναι ότι οι δισκογραφικές

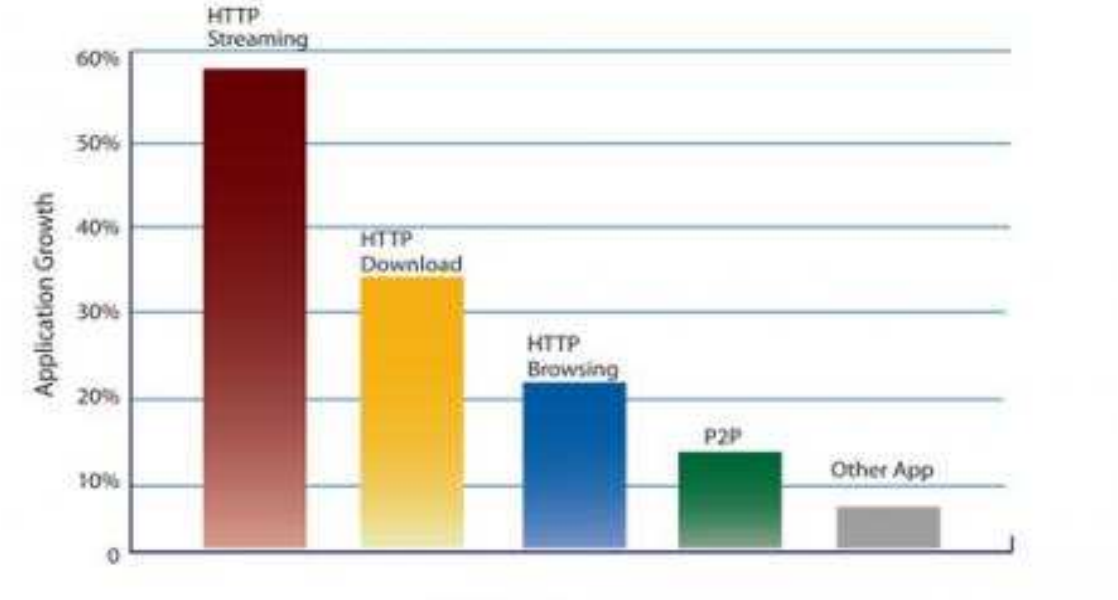
[79] The long tail of peer to peer: http://www.wired.com/epicenter/2009/05/report-challenges-long-tail-theory-on-p2p-networks/

εταιρίες είναι ότι η πειρατεία δεν είναι πλέον απειλή για τις πωλήσεις ,αλλά ένα μέσο διαφήμισης.

4.3.2 Μη δημοφιλές το p2p στο mobile Broadband

Η Allot communications κυκλοφόρησε πρόσφατα την πρώτη παγκόσμια έκθεση κυκλοφορίας του Mobile Broadband η οποία διαπίστωσε, μεταξύ άλλων, ότι το Streaming έχει τα σκήπτρα στην κατάληψη εύρους ζώνης σε σχέση με τα p2p στα mobile δίκτυα.

Τα peer to peer δίκτυα ανέκαθεν θεωρούνταν ο κύριος ένοχος για την κυκλοφοριακή συμφόρηση στο δίκτυο των mobile broadband, αλλά μια νέα υπηρεσία κάνει το ντεμπούτο της ,τα streaming multimedia.Το HTTP streaming ήταν η ταχύτερα αναπτυσσόμενη εφαρμογή από την άποψη mobile broadband στο δεύτερο τρίμηνο του 2008 και αντιπροσώπευε σχεδόν το ένα τέταρτο της παγκόσμιας κίνησης του δικτύου 3G.

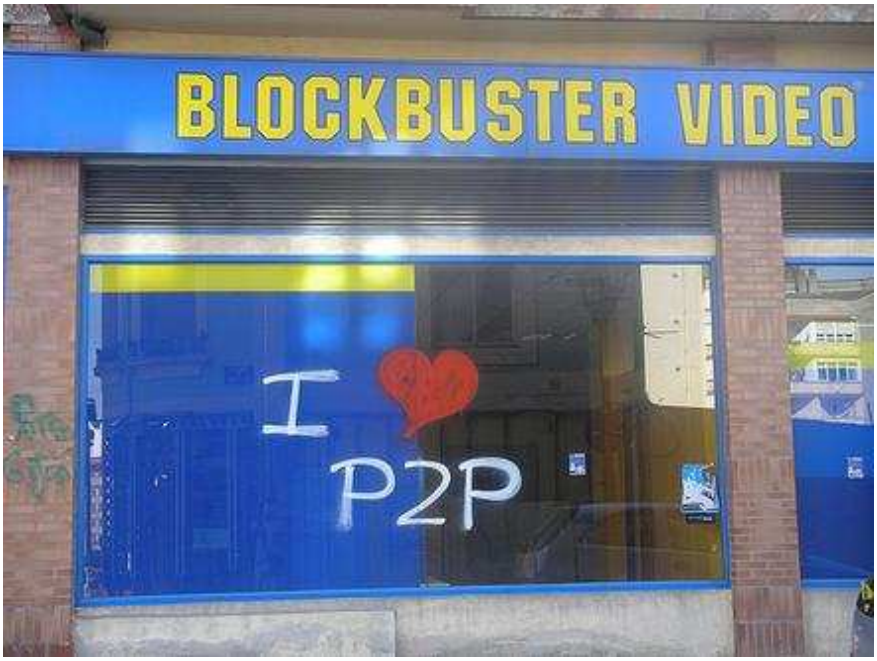


Εικόνα 64 Στατιστικά για τα mobile broadband δίκτυα

Πάντως η P2P κίνηση επηρεάζει αυτά τα κινητά δίκτυα .Αν και αντιπροσωπεύει μόλις το 17 % του εύρους ζώνης του μέσου όρου των mobile cells, καταλαμβάνει το 42% του εύρους ζώνης στα πιο πληγμένα από συμφόρηση mobile cells.Από τη φύση της δηλαδή ή μάλλον από την φύση των χρηστών της η peer to peer τεχνολογία συνεχίζει σε όλα τα δίκτυα να αποτελεί σχεδόν πάντα τον λόγο συμφόρησης όντας συνεπώς εχθρός των ISP.

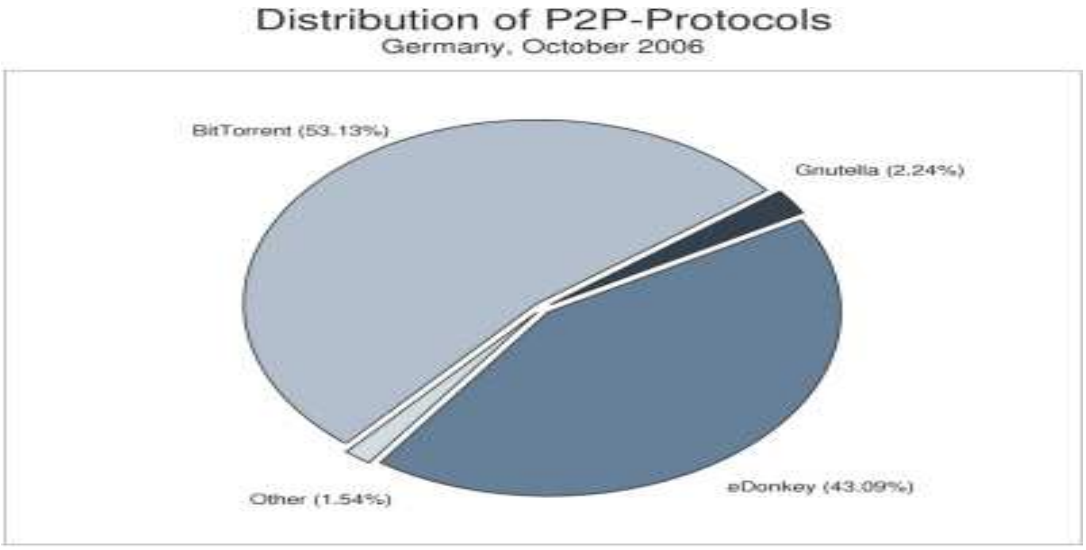
4.3.3 Το peer to peer στην Ευρώπη και στην μέση Ανατολή

Σε μια ωραία μελέτη που έκανε η , Ipoque, ένας Internet provider και παράλληλα data analyzer, έδειξε ότι ένα πολύ μεγάλο μέρος χρηστών από όλο τον κόσμο χρησιμοποιεί peer to peer εφαρμογές. Ως εδώ τίποτα καινούργιο, πάντως με την γλώσσα των αριθμών μπορούμε να καταλάβουμε κάτι παραπάνω.



Εικόνα 65 Χωρίς λόγια

Ισχυρίζεται λοιπόν ότι με τον ένα ή με τον άλλο τρόπο οι ευρωπαίοι χρησιμοποιούν peer to peer εφαρμογές σε ποσοστό 20% το ίδιο περίπου με τους χρήστες της Μέσης ανατολής. Αυτό φυσικά αντιπροσωπεύει ένα μεγάλο ποσοστό ανθρώπων αν αναλογιστεί κανείς ότι σε αυτές τις περιοχές του πλανήτη το file sharing γενικά φτάνει στο 85% της συνολικής online χρηστικότητας και αγγίζει το 90% τις βραδινές ώρες.
Επίσης παρατηρήθηκε ότι το 20% των χρηστών αυτών χρησιμοποιούν encrypted setting για τους e-donkey και Bit Torrent clients ενώ η χρήση πρωτοκόλλων εκτός από Bit Torrent ποικίλει ανάλογα την περιοχή που βρίσκονται.

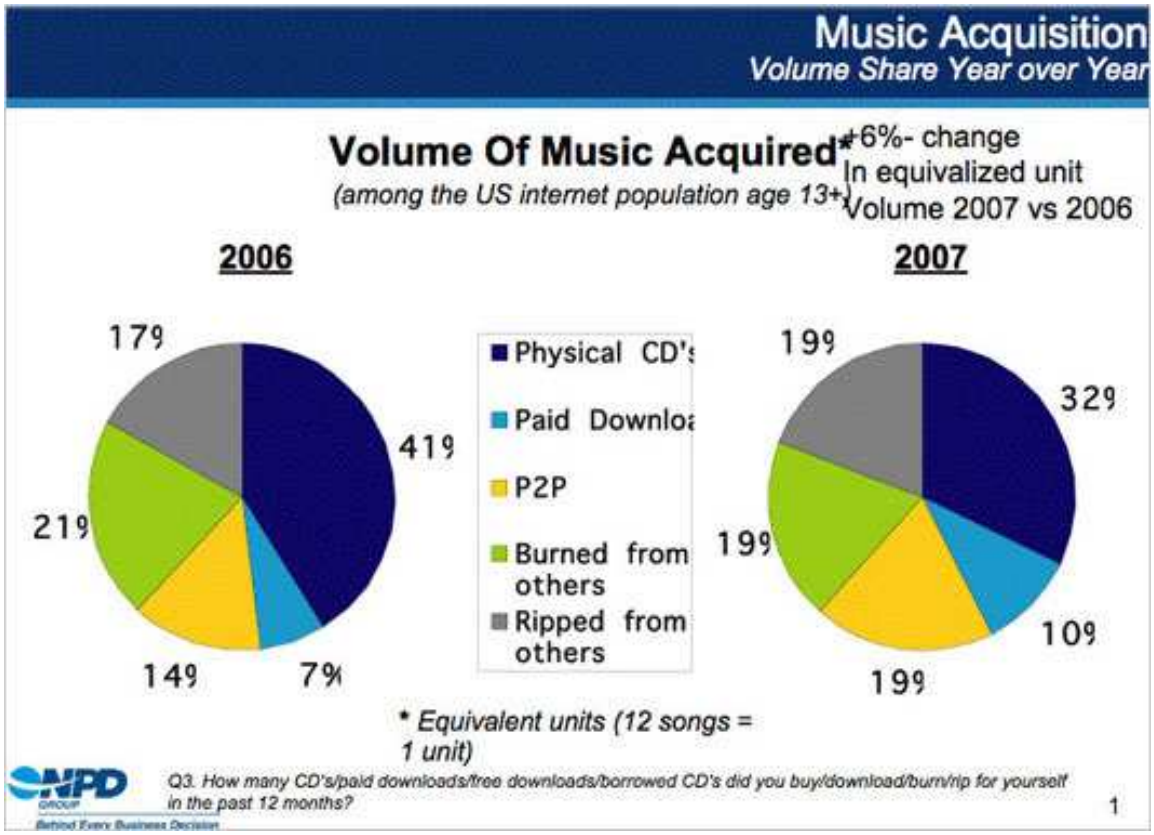


Εικόνα 66 Κατανομή πρωτοκόλλων στην Γερμανία

4.3.4 Το peer to peer στην Ιταλία

Ιταλοί ερευνητές με ερωτήσεις που έκαναν στους καταναλωτές της χώρας έβγαλαν ένα συμπέρασμα για την σχέση μεταξύ P2P και πωλήσεων CD. Διαπίστωσαν ότι μόνο μια μειοψηφία των file sharers, 30 τοις εκατό, μείωσε την αγορά μουσικών CD για αυτόν τον λόγο ενώ ένα μικρό 6% αύξησε αυτές τις αγορές.

Ένας συντριπτικός αριθμός της τάξης του 77% των Ιταλών στην έρευνα παραδέχονται πως κάνουν χρήση peer to peer λογισμικού σε σύγκριση με το 23% το οποίο προτιμάει να καταβάλει χρηματικά ποσά για να κάνει την ίδια δουλειά σε υπηρεσίες όπως το ITunes. Οι Ιταλοί προτιμούν γενικότερα το emule, το οποίο συγκέντρωσε 51 τοις εκατό των P2P χρηστών. Επόμενο ήταν το WinMX (25 τοις εκατό) και Kazaa (13 τοις εκατό).



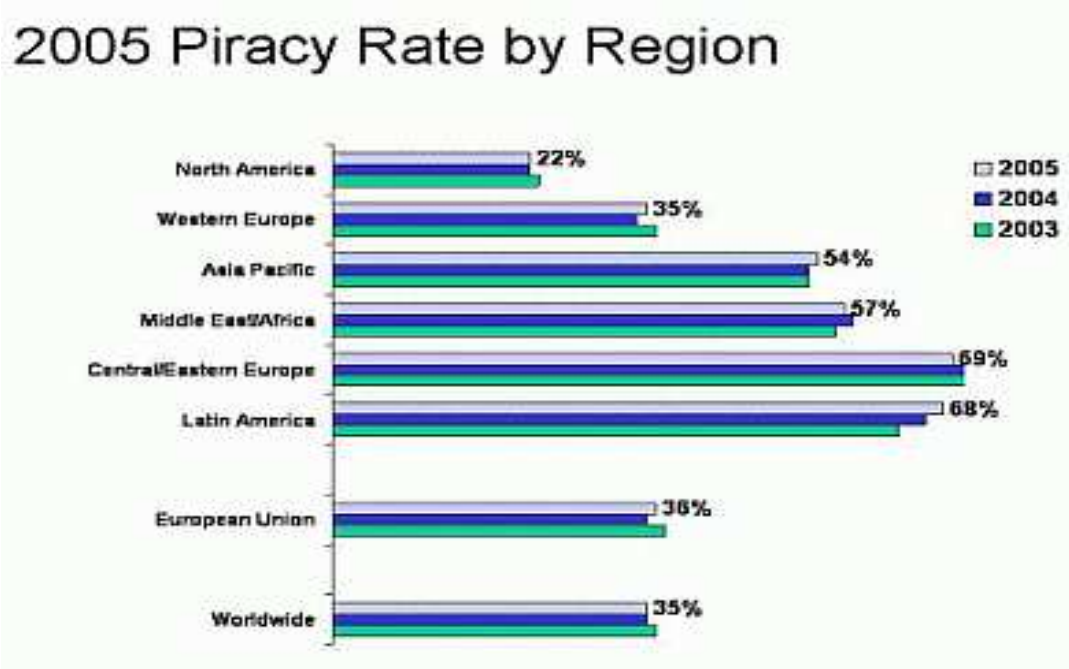
Εικόνα 67 Δείγμα της μουσικής αγοράς

4.3.5 Αθώωση των File Sharing εφαρμογών

Μια πρόσφατη έρευνα από το NPD Group επιβεβαιώνει τις έρευνες που γίνονταν και από άλλες πηγές ,ότι δηλαδή δεν είναι οι εφαρμογές peer to peer ο πρώτος που πρέπει να κατηγορηθεί για παράνομο download και παραβίαση πνευματικών δικαιωμάτων. Τα παραπάνω έχουν προκαλέσει πόλεμο μεταξύ των δισκογραφικών εταιριών και πολλών εφαρμογών στοχευόμενοι πολλές φορές στην δραστηριότητα μεγάλων κολεγιακών δικτύων.

Η ίδια έρευνα επίσης έδειξε πως το φυσιολογικό μεταξύ φίλων και γνωστών Rip and Burn σε CD με την χρήση προγραμμάτων όπως το Nero-το οποίο λαμβάνει χώρα offline εκτός ελέγχου από οποιαδήποτε αρχή είναι υπεύθυνο για το 37% της συνολικής παράνομης μουσικής δραστηριότητας δηλαδή αρκετά παραπάνω από το file sharing.

Επίσης όπως είναι φυσικό η δραστηριότητα αυτή συνεχώς αυξάνεται με την ανάπτυξη και την αύξηση της χωρητικότητας των USB αλλά και των rewritable media,δηλαδή CD DVD Portable hard disks etc.H peer to peer τεχνολογία είναι φανερό πως δεν είναι δα και κάτι το απειλητικό για την μουσική βιομηχανία. Παρακάτω βλέπουμε και τις περιοχές με αυξημένη πειρατεία το 2005.



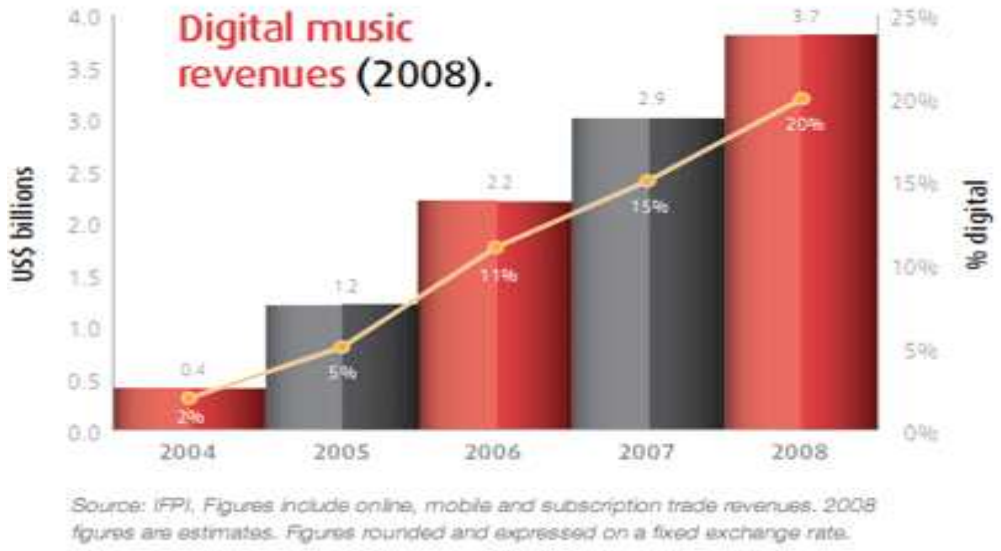
Εικόνα 68 Πειρατεία ανά περιοχές (NPD Group)

4.3.6 Ανάλογη αύξηση Web και peer to peer music download(2006)

Αριθμοί που δόθηκαν στο τέλος του έτους από το NPD Group και το IFPI (International Federation of the Phonographic Industry) δείχνουν ότι και το web αλλά και το peer to peer music downloading αυξάνονται. Στο διαδίκτυο τα νόμιμα τραγούδια διπλασιάστηκαν σε 4 εκατομμύρια ενώ τα συνολικά downloads ξεπέρασαν τα 800 εκατομμύρια με τα 610 από αυτά να γίνονται από Αμερική.

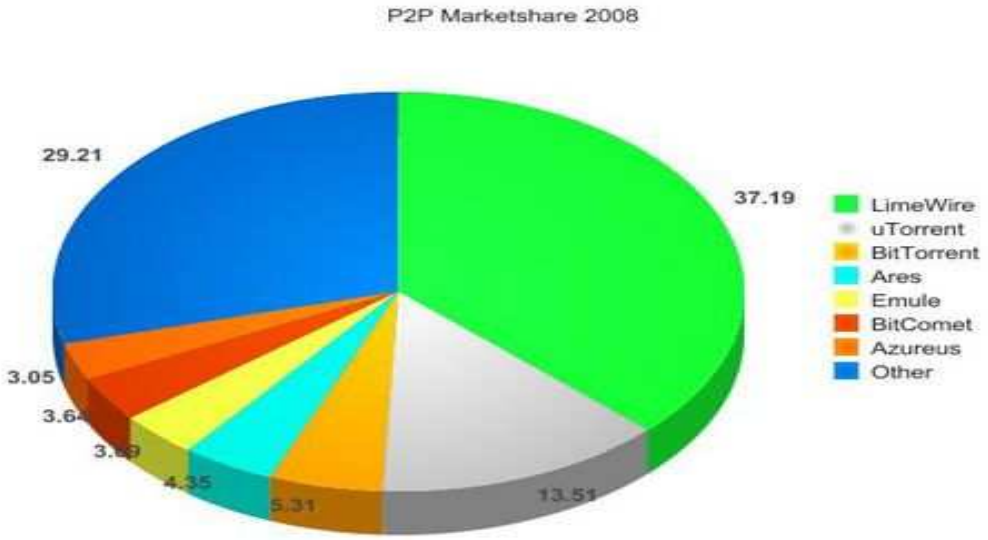
Η ITunes υποστήριξε ότι το 70% αυτής της ψηφιακής αγοράς μέσω download της ανήκε. Πάντως ο μέσος χρήστης του ITunes χρησιμοποίησε την υπηρεσία για download 11% λιγότερο εκείνη την χρονιά. Το Wal-mart και το Kazaa έχασαν μερίδιο αγοράς ενώ το yahoo έμεινε στα ίδια.

Με το τέλος του 2006 ,47 εκατομμύρια Αμερικάνικα νοικοκυριά είχαν τουλάχιστον ένα μέλος το οποίο χρησιμοποιούσε ψηφιακή μουσική. Το 32% από αυτούς έχει τουλάχιστον κατεβάσει ένα τραγούδι χρησιμοποιώντας peer to peer file sharing εφαρμογές .



Εικόνα 69 Ποσοστιαία αύξηση της ψηφιακής μουσικής δραστηριότητας το 2008

Στον κόσμο του peer to peer το Limewire[80] έχει γίνει η κυρίαρχη εφαρμογή μετά που το eDonkey και το kazaa αντιμετώπισαν νομικές πιέσεις και εξασθένισαν στην αγορά. Το Limewire κατέχει το 37.19% του μεριδίου αγοράς .Ο μέσος χρήστης Limewire κατέβασε 309 μουσικά αρχεία το 2006.



Εικόνα 70 Μερίδιο αγοράς P2P(2008)

[80] Limewire:http://www.limewire.com/el

4.3.7 Πληρωμένο peer to peer

Μια Νότιο-Κορεάτικη εφαρμογή peer to peer η Soribada[81] αναγκάστηκε να κλείσει(15 Νοεμβρίου 2005) λόγω του ότι παρείχε δωρεάν service.Όταν ξανάνοιξε τον Ιούλιο του ίδιου χρόνου που είχε κλείσει είχαν υπογραφεί συμβόλαια με 350 μουσικούς παραγωγούς κάτι που του έδινε μια μεγάλη μουσική γκάμα.

Στο ζενίθ της η Soribada(2008) είχε 22 εκατομμύρια δωρεάν χρήστες. Όταν πλέον δεν ήταν δωρεάν ,είχαν κάνει sign up 500.000 μέλη τα οποία πλήρωναν 3.000 Won ή 3.14 δολάρια για να έχουν απεριόριστη χρήση. Αυτό απέφερε περίπου 1,5 εκατομμύρια δολάρια τον μήνα. Πάντως αυτή η εξέλιξη στην μουσική βιομηχανία δεν ακούστηκε καθόλου καλά αφού οι εταιρίες πλέον δεν είχαν τα νόμιμα επιχειρήματα για τα πνευματικά δικαιώματα και έπρεπε να βρουν τρόπους να κάνουν το προϊόν τους πιο ανταγωνιστικό. Κάτι τέτοιο φυσικά δεν είναι δυνατό.

Οι εταιρίες επίσης απαιτούν να γίνονται authorized μεταφορές αρχείων χωρίς να υπάρχουν ανώνυμοι users.Αυτό τουλάχιστον είναι λογικό και δεν είναι και δύσκολο καθώς κατά το login μπορούν να γίνονται authorizes από το Soribada το οποίο είναι centralized peer to peer εφαρμογή όπως και το Napster.

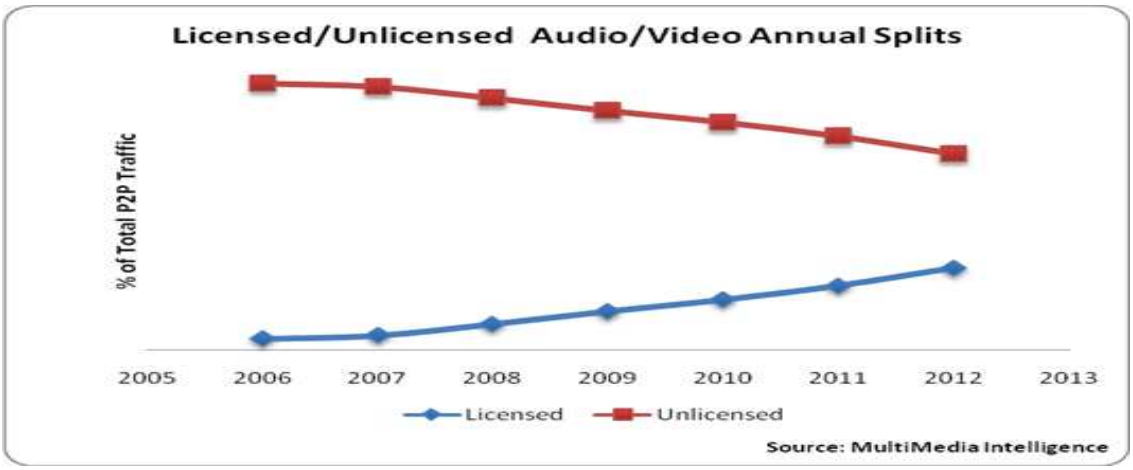
Άσχετα πάντως με τα νομικά θέματα, είναι ξεκάθαρο ότι οι καταναλωτές όχι μόνο προτίθενται να πληρώνουν για αντίστοιχες εφαρμογές, αλλά και να τις διαφημίζουν. Εάν αυτό ληφθεί σοβαρά υπόψη τότε μπορούν να σημειωθούν κέρδη εκατομμυρίων ευρώ ενώ παράλληλα να λήξει ο κανιβαλισμός πολλών καναλιών με fake content etc.

Εικόνα 71 Το λογότυπο της Soribada

[81]Soribada: http://en.wikipedia.org/wiki/Soribada

4.3.8 P2P:Ένα μικρό κομμάτι της online πειρατείας[82]

Σύμφωνα με μια έρευνα της Pew το 16% των ερωτηθέντων είπαν πως κάνουν download μουσική και video μέσω P2P ,ενώ το 17% λένε ότι έχουν χρησιμοποιήσει P2P εφαρμογές στο παρελθόν. Δεδομένης της αύξησης της file-sharing δραστηριότητας κάτι δεν πάει καλά καθώς αρκετοί άλλοι χρήστες δεν υπολογίζονται. Το 20% λαμβάνουν τα αρχεία μέσω e-mail και instant messaging και το 15% μέσω κάποιου mp3 player ενός γνωστού. Και τα δύο περιέχουν ουσιαστικά παράνομη διακίνηση αρχείων .Η P2P ενοχή και διακίνηση παράνομου υλικού κατέχει μόνο το 31% του συνόλου .Ίσα ίσα από το 2006 και μετά η κίνηση authorized peer to peer traffic αυξάνεται ενώ η αντίστοιχη unauthorized μειώνεται.



Εικόνα 72 Νόμιμη/Παράνομη διακίνηση υλικού μέσω P2P σε σύγκριση.(2006-2012)

Εικόνα 73 Τοποθεσίες με μεγάλη online πειρατεία

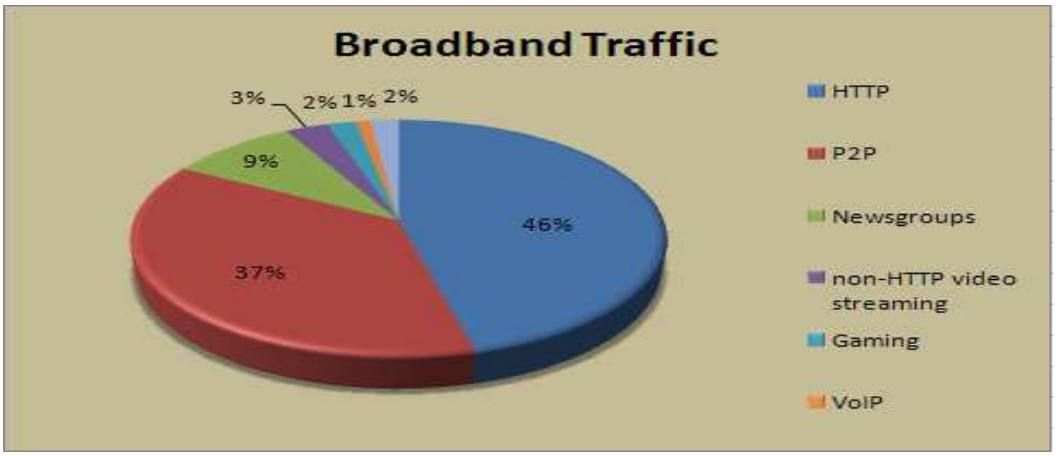
[82]Oniline Piracy: http://www.wisegeek.com/what-is-online-piracy.htm

4.4 «2009»: P2P-Streaming Media σημειώσατε 2

Έρευνα για το διαδίκτυο δείχνει πως σε παγκόσμιο επίπεδο σημειώνεται μια αλλαγή της συμπεριφοράς των χρηστών: το video streaming παίρνει τα σκήπτρα της κίνησης κατά τις απογευματινές ώρες μεταξύ 7 και 10 (οι ώρες αιχμής για τα δίκτυα) από την παραδοσιακά βαριά χρήση των δικτύων p2p δηλαδή συμπεριλαμβανομένου των δικτύων διαμοιρασμού αρχείων. Η έρευνα αυτή(World Wide Peer to Peer Market) αφορά περισσότερα από 20 διαφορετικά δίκτυα παρόχων και 24 εκατομμύρια συνδρομητές σε 5 διαφορετικές περιοχές του πλανήτη: Ευρώπη, Βόρεια Αμερική, Καραϊβική και Λατινική Αμερική, Νοτιοανατολική Ασία, Μέση Ανατολή και Αφρική.

Οι μετρήσεις αφορούν DSL και καλωδιακές συνδέσεις και συλλέχθηκαν μέσα στον Σεπτέμβριο. Να σημειωθεί πως η έρευνα ήταν ανώνυμη, δεν καταγράφτηκαν οι διευθύνσεις IP και τα μόνα στοιχεία που μετρήθηκαν είναι bits ανά δευτερόλεπτο ανά πρωτόκολλο. Τέλος την έρευνα διεξήγαγε η εταιρεία Sandvine. Πρόκειται για την έκτη κατά σειρά τέτοια έρευνα της εταιρείας από το 2002.

Η αλλαγή αυτή στα πρωτεία της κίνησης από τα p2p στο http video streamingαποτελεί μια μεγάλη αλλαγή στην κατανάλωση bandwidth και έχει μεγάλες επιπτώσεις στην διαχείριση των δικτύων των παρόχων. Το γεγονός αυτό δίνει ακόμα μεγαλύτερο ενδιαφέρον στην συζήτηση γύρω από την δικτυακή ουδετερότητα (net neutrality) η οποία βρίσκεται στο επίκεντρο του ενδιαφέροντος της κυβέρνησης των Η.Π.Α.



Εικόνα 74 2η θέση για peer to peer σε ότι αφορά την παγκόσμια κίνηση(2008)

Παρόμοιες πρόσφατες έρευνες από την Cisco και την Arbor Networks επιβεβαιώνουν την έρευνα της Sandvine: η κίνηση από το http video steaming ολοένα και αυξάνεται. Συγκεκριμένα η κίνηση εφαρμογών ψυχαγωγίας σε πραγματικό χρόνο (live) όπως η μετάδοση βίντεο, η μετάδοση ήχου ή εφαρμογές flash, αποτελεί το 26.6% της συνολικής κίνησης στο διαδίκτυο. Πέρσι(2001) η ίδια κίνηση αποτελούσε μόνο το 12.6%. Το μερίδιο αυτό ανεβαίνει στο 32.8% τις απογευματινές ώρες αιχμής. Στην ίδια

κατηγορία εφαρμογών κατατάσσονται και άλλες live εφαρμογές όπως το Voip και το online gaming που δεν καταναλώνουν μεγάλες ποσότητες bandwidth σε σύγκριση με την εικόνα και τον ήχο.

Την ίδια στιγμή η κίνηση των p2p εφαρμογών έπεσε από το 32% του 2008 στο 20% το 2009.

Ο κόσμος άλλαξε μέσα σε έναν μόνο χρόνο. Η αλλαγή έγινε σταδιακά κατά την διάρκεια του χρόνου αλλά μοιάζει εντυπωσιακή αν απλώς δεις τις δυο μετρήσεις (Σεπτέμβριο 2008-Σεπτέμβριο 2009)", δήλωσε ο Dave Caputo, συνιδρυτής, Πρόεδρος και Διευθύνων Σύμβουλος της Sandvine. "Άλλαξε ο τρόπος με τον οποίο χρησιμοποιούν το διαδίκτυο άμεσα. Θέλουν να δουν ένα βίντεο, την αγαπημένη τους εκπομπή και θέλουν να την δουν εκείνη ακριβώς στιγμή. Είναι μία μετακίνηση από το "το κατεβάζω τώρα και το βλέπω αργότερα" στο "το βλέπω τώρα". “

Η φράση του Caputo "το κατεβάζω τώρα-το βλέπω αργότερα" αποτελεί ευθεία αναφορά στα δίκτυα p2p και ειδικά στην κίνηση από τα BitTorrent τα οποία έχουν ενοχοποιηθεί από τους παρόχους για κατανάλωση δυσανάλογου εύρους ζώνης από αυτό που τους αναλογεί στην τεχνολογία dsl. Η έρευνα έδειξε μετατόπιση προς το video streaming όχι μόνο των χρηστών p2p αλλά και ευρύτερα. Για την ακρίβεια οι p2p χρήστες, σύμφωνα με τον Dave Caputo, μετάθεσαν το κατέβασμα αρχείων από p2p σε ώρες μη αιχμής.

ο Dave Caputo συνεχίζει λέγοντας: "Με την μελλοντική ευρεία χρήση εφαρμογών όπως το Hulu.com, πλέον όλοι θα είμαστε καταναλωτές μεγάλων ποσοτήτων bandwidth και όχι μόνο οι p2p χρήστες".

Όπως γίνεται αντιληπτό ,τα νέα ίσως να μην είναι τόσο ευχάριστα για τους παρόχους όσο πιθανόν να νομίζει κάποιος, αφού η κίνηση από εφαρμογές όπως το βίντεο και το voip είναι πολύ πιο ευαίσθητη σε αντίθεση με την κίνηση από p2p εφαρμογές όπου στην χειρότερη περίπτωση ο χρήστης περίμενε λίγο περισσότερο για να κατέβει το αρχείο.

"Θα είναι όλο και περισσότερο σημαντικό για τον πάροχο ευρυζωνικών υπηρεσιών να προσφέρει υπηρεσίες κατάλληλα διαμορφωμένες στις ανάγκες του πελάτη. Δηλαδή ο πελάτης να μπορεί να ορίζει ανάλογα με την ώρα ποια εφαρμογή έχει προτεραιότητα για αυτόν", δήλωσε ο D. Caputo.

Πιστεύεται πως αρκετοί καταναλωτές θα προτιμήσουν να δώσουν προτεραιότητα στις μετρήσεις του latency[83] και του jitter[84]. Κάτι τέτοιο θα μπορούσε να οδηγήσει στο τέλος εποχής του τύπου ,κατανάλωσε όσο εύρος ζώνης μπορείς.

[83]Latency: http://en.wikipedia.org/wiki/Latency_(engineering)
[84] Jitter:http://en.wikipedia.org/wiki/Jitter

Κεφάλαιο 5

5.0 Εισαγωγή

Το JXTA[85] είναι ένα σύνολο ανοικτών, γενικευμένων peer-to-peer (P2P) πρωτοκόλλων που επιτρέπουν σε οποιοδήποτε δικτυωμένο σύστημα - αισθητήρες, κινητά τηλέφωνα, PDA, φορητούς υπολογιστές, σταθμούς εργασίας, servers και υπερυπολογιστές - να επικοινωνούν και να συνεργάζονται μεταξύ τους σαν peers. Τα πρωτόκολλα JXTA είναι ανεξάρτητα από την γλώσσα προγραμματισμού, και πολλαπλές εφαρμογές, επίσης γνωστές ως bindings, υπάρχουν ανάλογα με το λειτουργικό περιβάλλον. Η κοινή χρήση των πρωτόκολλων JXTA σημαίνει ότι όλοι είναι πλήρως διαλειτουργικοί. Σε αυτό το κεφάλαιο θα δούμε τι είναι η τεχνολογία JXTA, ποια πρωτόκολλα και ποια στοιχεία αποτελούν ένα JXTA διομότιμο δίκτυο, καθώς και εφαρμογή κώδικα για την εκτέλεση διάφορων λειτουργιών με την χρήση NetBeans[86]. Τα στοιχεία που παρατίθενται παρακάτω έχουν πηγές από το βιβλίο JXTA in a nutshell και από το Manual JXTA[87].

5.1 Λόγοι χρήσης της JXTA τεχνολογίας

Καθώς το Διαδίκτυο συνεχίζει να αυξάνεται τόσο στο περιεχόμενο αλλά και στον αριθμό των συνδεδεμένων συσκευών, η peer to peer τεχνολογία διαδίδεται όλο και περισσότερο όπως έχουμε αναφέρει και παραπάνω. Δημοφιλή παραδείγματα περιλαμβάνουν την κοινή χρήση αρχείων, κατανεμημένα συστήματα πληροφορικής, και instant messaging εφαρμογές. Ενώ κάθε μία από αυτές τις εφαρμογές εκτελεί διαφορετικά καθήκοντα, όλοι μοιράζονται πολλές ίδιες ιδιότητες, όπως η ανακάλυψη των peers, αναζήτηση και μεταφορά δεδομένων ή αρχείων. Πάντως ένας πολύ μεγάλος αριθμός εφαρμογών είναι σχεδιασμένος για συγκεκριμένα λειτουργικά συστήματα προκαλώντας έτσι πρόβλημα στην επικοινωνία μεταξύ τους.Το JXTA λοιπόν μας παρέχει μία πλατφόρμα που ενσωματώνει τις βασικές λειτουργίες δικτύου P2P. Ως εκ τούτου, το JXTA ξεπερνά τις ελλείψεις πολλών από τα υφιστάμενα συστήματα P2P που βρίσκονται στη αγορά:

Διαλειτουργικότητα – Η JXTA τεχνολογία έχει σχεδιαστεί για να επιτρέψει στους peers που χρησιμοποιούν P2P υπηρεσίες , να εντοπίσουν ο ένας τον άλλον και να επικοινωνήσουν μεταξύ τους ανεξάρτητα από network addressing και φυσικά πρωτόκολλα.

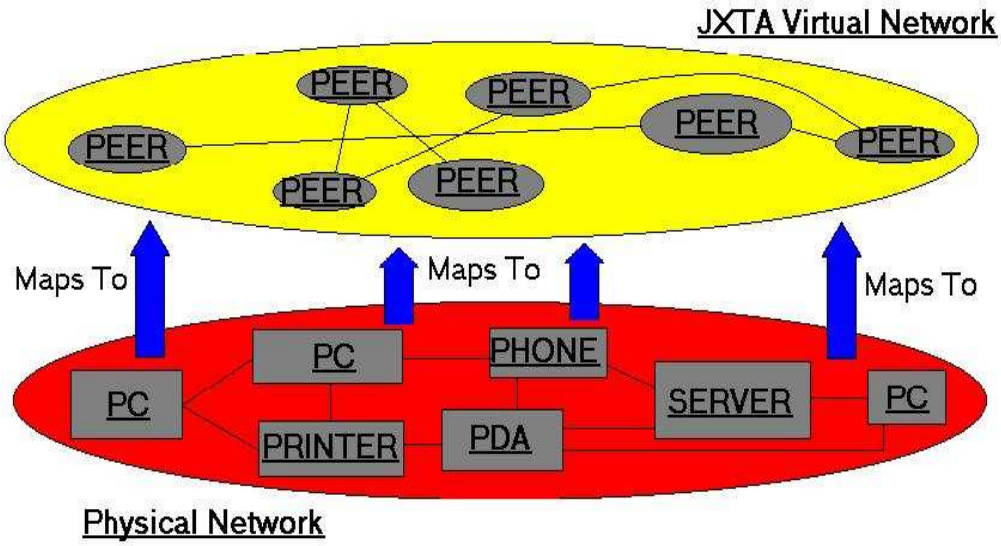
Ανεξαρτησία της Πλατφόρμας -Η JXTA τεχνολογία έχει επίσης σχεδιαστεί για να είναι ανεξάρτητη από γλώσσες προγραμματισμού, πρωτόκολλα μεταφοράς του δικτύου και τις πλατφόρμες ανάπτυξης.

Παρουσία πληθώρας συσκευών –Ένα δίκτυο με χρήση JXTA πρωτοκόλλων έχει

[85] Jxta:http://en.wikipedia.org/wiki/JXTA
[86] NetBeans:http://www.cs.uoi.gr/~zarras/se-notes/NetBeansPresentation.pdf
[87] JXTA Programmes Guide: https://jxta.dev.java.net/

σχεδιαστεί για να είναι προσβάσιμο από οποιαδήποτε συσκευή με digital heartbeat τπου χρησιμοποιεί δηλαδή ψηφιακό ρολόι).

Το JXTA παρέχει επιπλέον στους peers ενός δικτύου την τροφοδότηση ενός παγκοσμίως μοναδικού σχήματος διευθύνσεων των peers που είναι ανεξάρτητο των παραδοσιακών name services. Μέσω της χρήσης JXTA ID's[88] οι διάφοροι peers μπορούν να μεταναστεύσουν σε όλα τα φυσικά δίκτυα, αλλάζοντας τις διευθύνσεις δικτύου, και έχουν την δυνατότητα ακόμη και όταν είναι προσωρινά αποσυνδεδεμένοι να εξακολουθούν να είναι προσπελάσιμοι από άλλους peers.Θα δούμε παρακάτω στο κεφάλαιο την δημιουργία ID's .



Εικόνα 75 Αναπαράσταση της JXTA δικτύωσης.

5.2 Η JXTA τεχνολογία και αρχιτεκτονική

Η JXTA είναι λοιπόν όπως είπαμε μια ανοικτή πλατφόρμα πληροφορικής σχεδιασμένη για peer to peer δικτύωση διαφόρων υπολογιστικών και όχι μόνο συσκευών.
Το όνομα "JXTA" δεν είναι ένα αρκτικόλεξο. Είναι συντόμευση του juxtapose , όπως λέμε δηλαδή το ένα δίπλα στο άλλο. Είναι μια αναγνώριση ότι η τεχνολογία P2P προστίθεται στο μοντέλα client-server ή Web-based , το οποίο αποτελεί ένα παραδοσιακό μοντέλο που διανέμεται σήμερα .

Παρέχει επίσης ένα κοινό σύνολο ανοικτών πρωτοκόλλων που υποστηρίζονται με εφαρμογές ανοιχτού κώδικα για την ανάπτυξη των peer-to-peer εφαρμογών. Τα πρωτόκολλα JXTA έχουν τυποποιήσει τον τρόπο με τον οποίο peers:

- Ανακαλύπτουν ο ένας τον άλλον\
- Αυτοργανόνονται σε ομάδες peers
- Διαφημίζονται(μέσω μηνύματος δηλαδή) για να ανακαλύψουν τους πόρους του δικτύου

[88] JXTA ID'S:http://java.sun.com/developer/technicalArticles/Networking/jxta2.0/index.html

- Επικοινωνούν μεταξύ τους
- Παρακολουθούν ο ένας τον άλλον

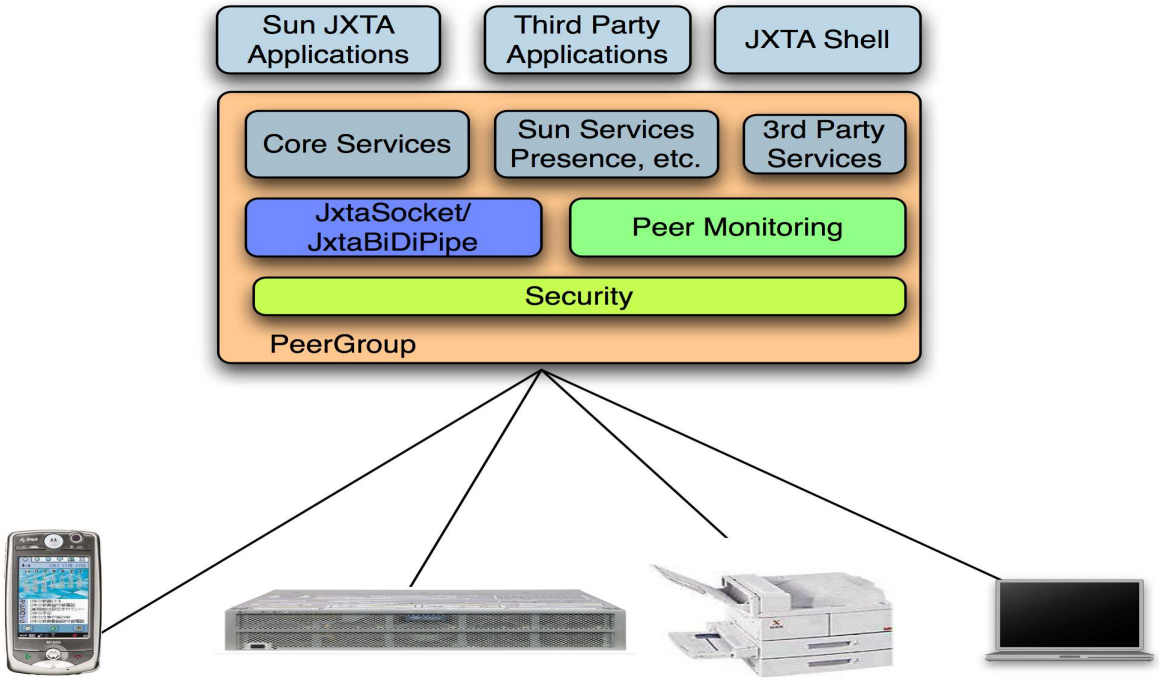
Τα πρωτόκολλα JXTA έχουν σχεδιαστεί ώστε να είναι ανεξάρτητα από γλώσσες προγραμματισμού και από πρωτόκολλα μεταφορών.

Μερικά σημαντικά πράγματα που μπορεί κανείς να πετύχει με την χρήση αυτής της τεχνολογίας είναι:

- Να βρει άλλους peers στο δίκτυο με δυναμική ανακάλυψη μέσα από τείχη προστασίας και NAT.
- Να έχει διαμοιρασμό πόρων εύκολα και γρήγορα με οποιονδήποτε σε ολόκληρο το δίκτυο
- Δημιουργία ενός peer group το οποίο θα παρέχει μια υπηρεσία
- Καταγραφή δραστηριοτήτων των άλλων peers
- Ασφαλής επικοινωνία με άλλους peers στο δίκτυο

Η JXTA αρχιτεκτονική λοιπόν μπορεί να χωριστεί σε 3 κύρια επίπεδα:

1) Στον πυρήνα του JXTA(Jxta core)
2) Στο επίπεδο υπηρεσιών
3) Στο επίπεδο εφαρμογών



Εικόνα 76 Απεικόνιση των επιπέδων της JXTA αρχιτεκτονικής

JXTA Core

Ο πυρήνας JXTA συμπυκνώνει τα ελάχιστα και απαραίτητα στοιχεία που είναι κοινά για P2P δίκτυα. Περιλαμβάνει δομικά στοιχεία για να μπορέσουν κύριοι μηχανισμοί για P2P εφαρμογές, συμπεριλαμβανομένης της ανακάλυψης, της μεταφοράς δεδομένων και της επικοινωνίας να εφαρμοστούν.

Services Layer

Το στρώμα υπηρεσιών περιλαμβάνει υπηρεσίες δικτύου που μπορεί να μην είναι απολύτως απαραίτητες για ένα δίκτυο P2P για να λειτουργήσει, αλλά μπορεί να είναι επιθυμητά σε ένα περιβάλλον P2P. Παραδείγματα δικτυακών υπηρεσιών περιλαμβάνουν την αναζήτηση και το indexing, ευρετήριο, συστήματα αποθήκευσης, κοινή χρήση αρχείων, κατανεμημένα συστήματα αρχείων, συγκέντρωση των πόρων, μετάφραση πρωτοκόλλου, ο έλεγχος γνησιότητας και PKI[89] (Public Key Infrastructure) για τις υπηρεσίες.

Applications Layer

Το σκέλος των εφαρμογών περιλαμβάνει την υλοποίηση ολοκληρωμένων εφαρμογών, όπως P2P instant messaging, εγγράφων και του καταμερισμού των πόρων, την διαχείριση περιεχομένου ψυχαγωγίας, P2P συστήματα e-mail, κατανεμημένα συστήματα δημοπρασίας, και πολλά άλλα.

Τα όρια μεταξύ των υπηρεσιών και εφαρμογών, δεν είναι απαράβατα. Η εφαρμογή ενός πελάτη μπορεί να θεωρηθεί ως υπηρεσία σε έναν άλλο πελάτη. Το όλο σύστημα έχει σχεδιαστεί ώστε να μπορεί να λειτουργήσει αρθρωτά, επιτρέποντας στους προγραμματιστές να επιλέξουν από μια συλλογή υπηρεσιών και εφαρμογών που ταιριάζει στις ανάγκες τους.

Βασικά Σημεία της Αρχιτεκτονικής JXTA

Τέσσερις βασικές πτυχές της αρχιτεκτονικής JXTA που τη διαφοροποιούν από άλλα μοντέλα είναι :

- Η χρήση XML εγγράφων (advertisements) για να περιγράψουν τους πόρους του δικτύου.
- Η οργάνωση με χρήση pipes και endpoints πάνω στους peers , χωρίς την εξάρτηση από μία κεντρική ονοματοδοσία / διευθυνσιοδότηση όπως το DNS.
- Ένα μοναδικό σχήμα διευθυνσιοποίησης (IDs).
- Μια αποκεντρωμένη υποδομή αναζήτησης των peers βασισμένη στο Distributed Hash Table (DHT) [90]μοντέλο.

[89] PKI:http://archive.opengroup.org/public/tech/security/pki/index.htm
[90] DHT:http://en.wikipedia.org/wiki/Distributed_hash_table

Όπως έχουμε λοιπόν καταλάβει πρόκειται για μια αρχιτεκτονική η οποία περιλαμβάνει διάφορα στοιχεία τα οποία παρόλο που είναι κοινά έως ένα σημείο με οποιαδήποτε εφαρμογή peer to peer δικτύωσης, διαφοροποιούνται και εξειδικεύονται σε συγκεκριμένες λειτουργίες. Ας δούμε λοιπόν τα στοιχεία αυτά.

5.3 JXTA components

5.3.1 Peers

Peer είναι οποιοδήποτε δικτυωμένη οντότητα που εφαρμόζει ένα ή περισσότερα από τα πρωτόκολλα JXTA. Οι peers μπορεί να μεταφράζονται σε αισθητήρες, τηλέφωνα, PDAs και, καθώς επίσης και Η / Υ, servers κ.α. Κάθε peer λειτουργεί ανεξάρτητα και ασύγχρονα από όλους τους άλλους και χαρακτηρίζεται μονοσήμαντα από ένα Peer ID.

Εδώ πέρα λοιπόν έχουμε τις εξής κατηγορίες peers:

- Minimal-edge peers: Peers που εφαρμόζουν μόνο τις απαιτούμενες βασικές υπηρεσίες JXTA και μπορεί να στηρίζονται σε άλλους peers για να ενεργούν ως πληρεξούσιοι για άλλες υπηρεσίες(proxy)ώστε να συμμετάσχουν πλήρως σε ένα JXTA δίκτυο. Οι proxy peers λειτουργούν ως υποκατάστατο για μη βασικές υπηρεσίες. Τέτοιοι peers συνήθως είναι συσκευές αισθητήρων και συσκευές οικιακού αυτοματισμού

- Full-edge Peers: Peers που υλοποιούν όλες τις βασικές και τυποποιημένες υπηρεσίες JXTA και μπορούν να συμμετέχουν σε όλα τα πρωτόκολλα JXTA. Αυτοί οι peers αποτελούν την πλειοψηφία σε ένα δίκτυο JXTA και μπορεί να περιλαμβάνουν κινητά τηλέφωνα, υπολογιστές, servers, κλπ.
- Super-Peers: Peers που παρέχουν πόρους οι οποίοι βοηθούν την ανάπτυξη και την λειτουργία ενός δικτύου JXTA.

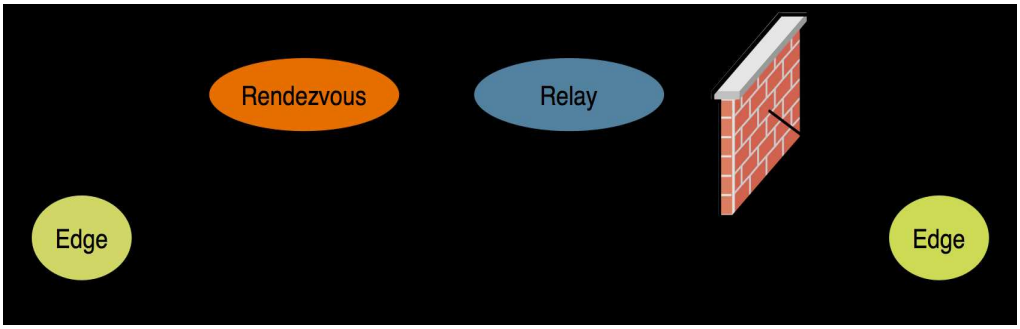
- Υπάρχουν τρεις βασικές λειτουργίες για έναν JXTA Super Peer. Μια ή και περισσότερες λειτουργίες που μπορούν να εφαρμοστούν από τον κάθε peer

- Relay: Χρησιμοποιείται για την αποθήκευση και προώθηση μηνυμάτων μεταξύ των peers που δεν έχουν απευθείας σύνδεση λόγω firewalls ή NAT. Μόνο οι peers που δεν είναι σε θέση να λάβουν συνδέσεις από άλλους peers απαιτούν το relay service.

- Rendezvous: [91]Διατηρεί τα συνολικά advertisement indexes του δικτύου και βοηθά τους edge και proxied peers με advertisement search. Επίσης χειρίζεται και message broadcasting.

[91] Rendezvouz:http://en.wikipedia.org/wiki/JXTA

- Proxy: Χρησιμοποιείται από τους Minimal-edge peers ώστε να αποκτήσουν πρόσβαση σε όλες τις λειτουργίες του δικτύου JXTA.



Εικόνα 77 Ο ρόλος των διαφόρων ειδών peers.

5.3.2 Peer Groups

Μια ομάδα peers είναι μια συλλογή των peers που έχουν συμφωνήσει σε ένα κοινό σύνολο υπηρεσιών, ή ενδιαφερόντων. Οι peers λοιπόν αυτό-οργανώνονται σε ομάδες, κάθε μία από τις οποίες χαρακτηρίζεται μονοσήμαντα από μία peer group ID. Το κάθε peer group χαράζει την δική του πολιτική και είναι ανοιχτό για όποιον peer θέλει να κάνει join.Προϋπόθεση φυσικά είναι να ακολουθεί κατά γράμμα το πρωτόκολλο.

Οι peers μπορεί να ανήκουν σε περισσότερες από μία ομάδες ταυτόχρονα. Εξ ορισμού, η πρώτη ομάδα που σχηματίζεται είναι το Network Peer Group. Όλοι οι peers που ανήκουν στο Network Peer Group μπορούν να επιλέξουν να ενταχθούν σε επιπλέον ομάδες ανά πάσα στιγμή.

Υπάρχουν βεβαίως αρκετοί λόγοι για σχηματισμό peer group:

• Για τη δημιουργία ενός ασφαλούς περιβάλλοντος

Οι ομάδες δημιουργούν έναν τομέα ελέγχου στον οποίο μια συγκεκριμένη πολιτική ασφάλειας μπορεί να εκτελεστεί. Η πολιτική ασφάλειας μπορεί να είναι τόσο απλή όσο ένα απλό όνομα χρήστη text και ενδεχομένως ένα password, ή πολύπλοκη, κρυπτογραφία δημόσιου κλειδιού. Υπάρχουν οριοθετήσεις οι οποίες ορίζουν το κατά πόσο ένας peer έχει το δικαίωμα στην πρόσβαση και στην δημοσίευση συγκεκριμένου περιεχομένου.

• Για να δημιουργηθεί ένα περιβάλλον οριοθέτησης

Οι ομάδες επιτρέπουν τη δημιουργία ενός τοπικού τομέα της εξειδίκευσης. Για παράδειγμα, οι peers μπορούν να σχηματίσουν ένα group με σκοπό τον διαμοιρασμό αρχείων ή τον διαμοιρασμό υπολογιστικών πόρων. Τα peer groups χρησιμεύουν για την υποδιαίρεση του δικτύου σε περιοχές που κάθε μια από τις οποίες έχει ένα συγκεκριμένο ρόλο.

• Για να δημιουργηθεί ένα περιβάλλον παρακολούθησης

Τα peer groups αναθέτουν κάποιες φορές σε κάποιους peers να παρακολουθούν μια σειρά από άλλους peers για οποιοδήποτε ιδιαίτερο σκοπό (π.χ., Digital heartbeat, παρακολούθηση κυκλοφορίας κ.α).

5.3.3 Network Services

Οι Peers συνεργάζονται και επικοινωνούν για να δημοσιεύουν, να ανακαλύπτουν, και εν τέλει να χρησιμοποιήσουν τις υπηρεσίες του δικτύου στο οποίο ανήκουν. Μπορούν να δημοσιευτούν πολλαπλές υπηρεσίες οι οποίες, με τη σειρά τους, ανακαλύπτονται μέσω του Peer Discovery πρωτοκόλλου.

Τα πρωτόκολλα JXTA αναγνωρίζουν δύο επίπεδα υπηρεσιών δικτύου:

Peer Services

Η υπηρεσία είναι προσβάσιμη μόνο μέσω των peers που δημοσιεύουν την εν λόγω υπηρεσία. Αν αυτοί αποσυνδεθούν ή οτιδήποτε άλλο τότε η υπηρεσία χάνεται. Πολλά στιγμιότυπα μιας υπηρεσίας μπορούν να τρέχουν ταυτόχρονα σε διαφορετικούς peers αλλά τα ανάλογα advertisements αφορούν τον κάθε peer ξεχωριστά.

Peer Group services

Μια peer group service αποτελείται από μια συλλογή των στιγμιότυπων της υπηρεσίας, που πιθανόν να συνεργάζονται μεταξύ τους εκτελούμενα στους διάφορους peers του hosting group. Εάν κάποιος από τους peers πάθει οτιδήποτε, η συλλογική υπηρεσία δεν θίγεται εφ 'όσον η υπηρεσία είναι ακόμα διαθέσιμη από τουλάχιστον ένα μέλος του group.Οι Peer group services δημοσιεύονται με ένα ενιαίο advertisement την ομάδας.

Οι υπηρεσίες μπορεί να είναι είτε προεγκατεστημένες σε έναν peer ή να φορτωθούν από το δίκτυο. Η διαδικασία για την εξεύρεση, το κατέβασμα και την εγκατάσταση μιας υπηρεσίας από το δίκτυο είναι ανάλογη με την εκτέλεση μιας αναζήτησης στο Διαδίκτυο για μια ιστοσελίδα, την ανάκτηση της σελίδας και, στη συνέχεια, το οποιοδήποτε plug-in που απαιτείται από τη σελίδα.

Οι core peer group services τις οποίες πρέπει οποιοδήποτε group ,να εφαρμόσει είναι:

Endpoint Service

Το endpoint service χρησιμοποιείται για να σταλούν και να ληφθούν μηνύματα μεταξύ των peers.Αυτή η υπηρεσία εφαρμόζει το Endpoint Routing Protocol[92].

Resolver Service

Η υπηρεσία αυτή χρησιμοποιείται για να σταλούν διάφορα requests σε άλλους peers.Οι peers μέσω αυτής της υπηρεσίας έχουν την δυνατότητα να ανταλλάσουν και να αναγνωρίζουν queries μεταξύ τους ώστε να βρουν οποιαδήποτε πληροφορία την

[92] End-Point Routing Protocol:http://my.safaribooksonline.com/0735712344/ch09lev1sec3

οποία μπορεί να αναζητούν(πχ advertisements και άλλες αναγνωριστικές πληροφορίες)

Τα standard peer group services τα οποία βρίσκονται στα περισσότερα groups είναι τα εξής:

Discovery Service

Το discovery service χρησιμοποιείται από τα μέλη του group για να αναζητήσουν πόρους ενός peer group όπως peers ,τα ίδια τα group ,υπηρεσίες και pipes για τα οποία θα αναφερθούμε αργότερα.

Membership Service

Η υπηρεσία αυτή χρησιμοποιείται από τα μέλη των group για τη δημιουργία ασφαλούς ταυτοποίησης ώστε να υπάρχει εμπιστοσύνη εντός του group.Οι ταυτότητες αυτές επιτρέπουν για τις εφαρμογές και υπηρεσίες να καθορίζεται ποιος είναι ο αιτών και αν θα πρέπει ή μπορεί να χρησιμοποιήσει αυτή την υπηρεσία. Οι αιτήσεις μπορούν να ασκούν το δικό τους έλεγχο πρόσβασης ή μπορούν να χρησιμοποιούν την Access Service.

Access Service

Το access service χρησιμοποιείται για να κάνει έγκυρα τα requests τα οποία γίνονται μεταξύ των peers. Ο peer ο οποίος λαμβάνει το request ελέγχει τα διαπιστευτήρια και τα στοιχεία του αιτούντα ώστε να καθορίσει εάν θα επιτραπεί η χρήση της υπηρεσίας. Να σημειωθεί φυσικά ότι μόνο οι υπηρεσίες οι οποίες εξ ορισμού έχουν κάποιο περιορισμό ελέγχονται με το Access service καθώς είναι κρίμα να σπαταλούνται υπολογιστικοί πόροι όταν δεν χρειάζεται.

Pipe Service

Το pipe service χρησιμοποιείται για να δημιουργήσει και να διαχειριστεί συνδέσεις μεταξύ των peer groups στην συγκεκριμένη περίπτωση.

Monitoring Service

Χρησιμοποιείται για να γίνεται μια παρακολούθηση των δραστηριοτήτων των peersαπό peers του ίδιου και μόνο group.

5.3.4 Messages

Οι υπηρεσίες και οι εφαρμογές JXTA επικοινωνούν μεταξύ τους χρησιμοποιώντας JXTA messages.Αυτά τα μηνύματα είναι η βασική μονάδα δεδομένων που ανταλλάσσεται μεταξύ των peers.Κάθε JXTA πρωτόκολλο καθορίζεται από ένα set μηνυμάτων το οποίο ανταλλάσσεται μεταξύ των peers.Η επικοινωνία αυτή μεταξύ των peers γίνεται με την χρήση του Endpoint service και του Pipe service στα οποία αναφερθήκαμε παραπάνω. Οι περισσότερες βέβαια εφαρμογές δεν χρησιμοποιούν unidirectional pipes(δηλαδή μονής κατεύθυνσης pipes) ούτε κάνουν άμεση χρήση του Endpoint service,αντιθέτως χρησιμοποιούνται πιο πολύ Bidirectional pipes και Sockets για την λήψη και την αποστολή messages καθώς προσφέρουν μεγαλύτερη ασφάλεια επικοινωνίας και διασφάλιση παράδοσης των δεδομένων στον προορισμό τους. .Η μορφή των δεδομένων που μεταδίδονται τα messages είναι είτε

Binary(δυαδική) είτε XML.Το JXSE το οποίο θα δοκιμάσουμε στο τέλος του κεφαλαίου ,χρησιμοποιεί Binary messages.

5.3.5 Pipes

Οι peers στο JXTA μοντέλο χρησιμοποιούν pipes για να μεταδώσουν και να δεχτούν messages.Τα pipes είναι ένας ασύγχρονος και μονής κατεύθυνσης μηχανισμός επικοινωνίας και μεταφοράς δεδομένων. Πρόκειται για τεχνητά κανάλια επικοινωνίας που συνδέουν μεταξύ τους peers που συνήθως δεν έχουν κάποια φυσική σύνδεση στο ενδιάμεσο. Χρησιμοποιούνται για την αποστολή αρκετών τύπων δεδομένων όπως.XML HTML, απλό κείμενο ,images, μουσική ,δυαδικό κώδικα, Java Objects κτλ. Τα pipes προσφέρουν 2 modes επικοινωνίας, Point to Point και Propagate.Επίσης στο JXSE χρησιμοποιούνται και Secure Unicast Pipes.Ας δούμε τι είναι το καθένα από αυτά.

Point-to-point Pipes

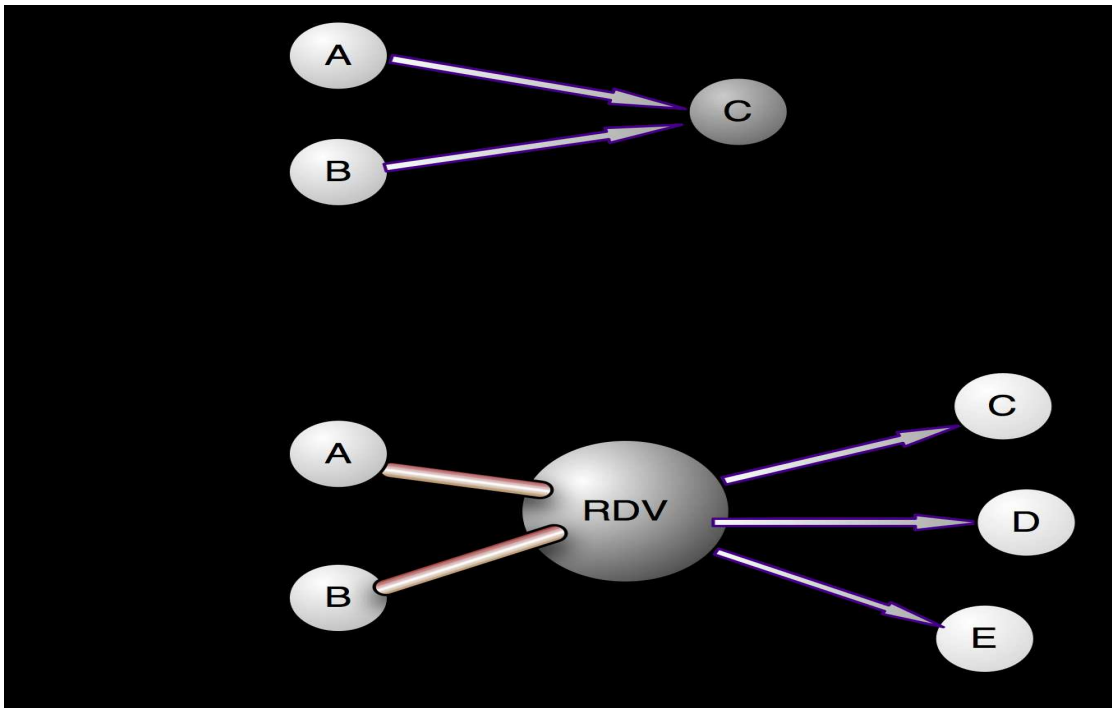
Ένα point to point pipe ενώνει μεταξύ τους δύο pipe endpoints ακριβώς. Το input pipe ενός peer δέχεται messages από το output pipe ενός άλλου.Επίσης γίνεται πολλοί peers να στέλνουν στο input pipe ενός άλλου peer..

Propagate Pipes

Ένα τέτοιο pipe έχει την δυνατότητα να ενώνει ένα output από κάποιον peer με πολλαπλά input σε άλλους peers.

Secure Unicast Pipes

Αυτά τα pipes είναι ένα είδος point to point pipe τα οποία όμως παρέχουν ασφαλή επικοινωνία.



Εικόνα 78 Point to point και από κάτω propagated Pipe.

5.3.6 Advertisements

Όλοι οι πόροι ενός δικτύου JXTA όπως peers, peer groups, pipes και services παρουσιάζονται ως advertisements.Τα advertisement δεν έχουν να κάνουν με γλώσσες προγραμματισμού και είναι ένα είδος meta-data(δηλαδή data των data για να το πούμε απλοϊκά) σε XML μορφή. Τα JXTA πρωτόκολλα χρησιμοποιούν τα advertisements για να δημοσιεύσουν και να περιγράψουν τους πόρους ενός peer.Ο κάθε peer έπειτα με την σειρά του αναζητά advertisements τα οποία ανταποκρίνονται στις ανάγκες του και αναλόγως μπορεί να αποθηκεύσει ορισμένα από τα πιο ενδιαφέροντα.

Το κάθε advertisement γίνεται publish με ένα Lifetime το οποίο χαρακτηρίζει την διαθεσιμότητα των διαφόρων πόρων που προσφέρει η πηγή τους .Όταν αυτό λήξει τότε πλέον τίποτα δεν είναι διαθέσιμο και διαγράφεται χωρίς καμία απαίτηση κεντρικού ελέγχου. Τα advertisement μπορούν να γίνονται republish για να ανανεώνεται ο χρόνος ζωής της διαθεσιμότητας των πηγών τους.Αυτά τα οποία φαίνονται στο advertisement θα αναλυθούν παρακάτω(urn,JXTAUnicast κτλ).

```
<?xml version="1.0"?>
<!DOCTYPE jxta:PipeAdvertisement>
<jxta:PipeAdvertisement xmlns:jxta="http://jxta.org">
<Id>
urn:jxta:uuid-
596162616461626 14E504720503250338E3E786229EA460DADC1A176B69B73150
4
</Id>
<Type>
JxtaUnicast
</Type>
<Name>
TestPipe
</Name>
</jxta:PipeAdvertisement>
```

Εικόνα 79 Δείγμα ενός pipe advertisement

Τα JXTA πρωτόκολλα αναγνωρίζουν αρκετά είδη advertisement εκ των οποίων τα πιο σημαντικά είναι:

Peer Advertisement

Τα οποία περιγράφουν τους πόρους ενός peer. Κύριος ρόλος τους είναι να διατηρούν σημαντικές πληροφορίες για έναν peer όπως όνομα, ID, διαθέσιμα endpoints και οτιδήποτε άλλα χαρακτηριστικά τα οποία μπορεί ένα peer group για παράδειγμα να θέλει να δημοσιεύσει.

Peer Group Advertisement

Πρακτικά είναι ακριβώς τα ίδια πράγματα με το παραπάνω με μια μικρή προσθήκη περιγραφής παραμέτρων των παρεχομένων υπηρεσιών.

Pipe Advertisement

Περιγράφει ένα κανάλι επικοινωνίας και η πληροφορία αυτή αξιοποιείται από τα pipe services για να δημιουργήσουν τα αντίστοιχα output και input pipe endpoints.Κάθε pipe advertisement περιέχει ένα συμβολικό προαιρετικό ID, ένα pipe type(Point to Point, Secure, Propagated) και ένα μοναδικό pipe ID

Rendezvous Advertisement

Περιγράφει ένα peer ο οποίος λειτουργεί ως rendezvous για ένα συγκεκριμένο Peer group.

Peer Info Advertisement

Παρέχει γενικότερες πληροφορίες για ένα peer που συνήθως αφορούν την διακίνηση μηνυμάτων ,το χρόνο τελευταίας διακίνησης, τον αριθμό των μηνυμάτων και γενικά οτιδήποτε έχει να κάνει με την τρέχουσα κατάστασή του.

5.3.7 Security

Σε ότι αφορά την ασφάλεια, το JXTA δίκτυο πρέπει και προσφέρει τα ευκόλως εννοούμενα που απαιτούνται, δηλαδή :

Εμπιστευτικότητα--------Εγγυάται ότι τα περιεχόμενα ενός μηνύματος δεν πρόκειται να γίνουν γνωστά σε μη εξουσιοδοτημένους χρήστες.

Αυθεντικοποίηση--------Εγγυάται ότι ο αποστολέας είναι αυτός που υποστηρίζει ότι είναι.

Εξουσιοδότηση αποστολέα-------Κάνει αυτό ακριβώς που λέει το όνομά του δηλαδή να ελέγχει εάν ο αποστολέας έχει το δικαίωμα να στείλει το συγκεκριμένο μήνυμα,

Αυθεντικότητα δεδομένων-------Εγγυάται ότι κατά την μετάδοση δεν έγινε καμία απολύτως τροποποίηση των δεδομένων,

5.3.8 IDs

Οι peers , τα peer groups , τα pipes και οτιδήποτε άλλοι πόροι πρέπει να είναι μοναδικά αναγνωρίσιμοι. Ένα JXTA ID δίνει αναγνωσιμότητα σε έναν πόρο και επιπλέον έναν τρόπο να απευθύνονται σε αυτόν.
Τα ID’s εκφράζονται με URN’s[93] που είναι ένα είδος URL και παρουσιάζεται σε μορφή κειμένου.

Παράδειγμα JXTA peer ID:

urn:jxta:uuid-
59616261646162614A78746150325033F3BC76FF13C2414CBC0AB663666DA53903

[93] URN: http://en.wikipedia.org/wiki/URN

Παράδειγμα JXTA pipe ID:

urn:jxta:uuid-
59616261646162614E504720503250338E3E786229EA460DADC1A176B69B731504

5.4 Τα πρωτόκολλα JXTA[94]

Το JXTA καθορίζει μια σειρά από XML messages ή πρωτόκολλα για την επικοινωνία μεταξύ των peers.Τα πρωτόκολλα γενικότερα χρησιμοποιούνται από τους peers για την ανακάλυψη άλλων peers, για την ανακάλυψη πόρων δικτύου , για διαφήμιση, για επικοινωνία και για την δρομολόγηση μηνυμάτων.
Υπάρχουν 6 standard πρωτόκολλα:

Peer Discovery Protocol (PDP)

Χρησιμοποιείται από τους peers για να διαφημίσουν τους πόρους τους αλλά και για να ανακαλύψουν πόρους άλλων peers.Όλη αυτή η διαδικασία γίνεται μέσω των advertisements.

Peer Information Protocol (PIP)

Χρησιμοποιείται για να γίνει γνωστό το status άλλων peers (uptime, state, recent traffic κτλ) .

Peer Resolver Protocol (PRP)

Δίνει την δυνατότητα στους peers να στέλνουν queries σε έναν ή περισσότερους peers και να λαμβάνουν ένα ή περισσότερα responses.

Pipe Binding Protocol (PBP)
Χρησιμοποιείται από τους peers για να δημιουργηθεί ένα τεχνητό κανάλι επικοινωνίας ή pipe μεταξύ τους. Επίσης βρίσκει εφαρμογή στην ένωση endpoints μεταξύ τους.

Endpoint Routing Protocol (ERP)

Οι peers το χρησιμοποιούν για να βρουν μονοπάτια προς τα ports του προορισμού τους. Σε αυτήν την διαδικασία εμπλέκονται τα relay peers που έχουν περιγραφεί παραπάνω ώστε να βρεθεί το μονοπάτι.

Rendezvous Protocol (RVP)

Χρησιμοποιείται από τους edge peers για να ξεχωριστούν οι διάφοροι πόροι, να προωθηθούν messages και να γίνει διαφήμιση των πόρων. Από τους rendezvous peers χρησιμοποιούνται για να οργανωθούν με άλλους peers του είδους τους.

Όλα τα παραπάνω πρωτόκολλα είναι στο μοντέλο του «στέλνω ένα ή περισσότερα queries και λαμβάνω μια ή περισσότερες απαντήσεις» .Οι peers υιοθετούν μόνο τα πρωτόκολλα ή το πρωτόκολλο που θα χρησιμοποιήσουν. Πάντως κατά την αποστολή ενός querie σε κάποιον ή κάποιους άλλους peers χρησιμοποιείται ένα μόνο από τα πρωτόκολλα.

---

[94] JXTA Protocols: http://java.sun.com/developer/Books/networking/jxta/jxtap2pch03.pdf

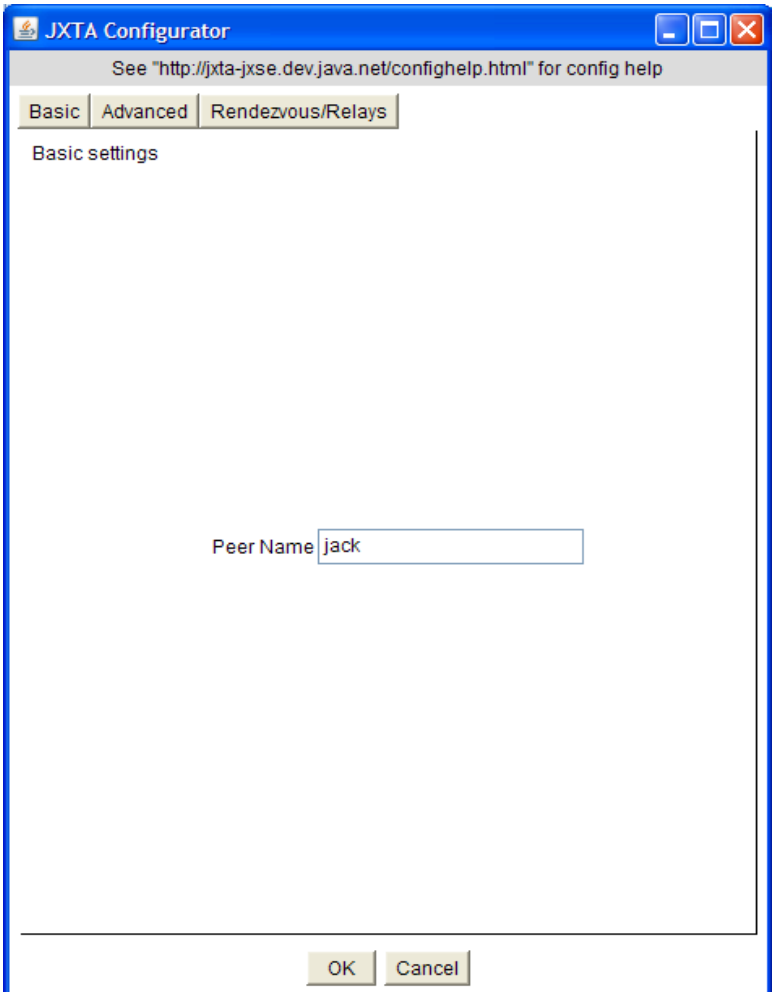
5.5 Εφαρμογή JXTA κώδικα

Σε αυτό το υποκεφάλαιο θα δούμε πώς με την χρήση java μπορούμε να δημιουργήσουμε κάποια από τα components που είδαμε παραπάνω αλλά και να προβούμε σε διάφορες άλλες πράξεις. Στην συνέχεια θα τρέξουμε κώδικα στο NetBeans(http://netbeans.org/downloads/) αφότου κατεβάσουμε τα αντίστοιχα lib και documentation από την επίσημη σελίδα του JXTA, http://download.java.net/jxta/.Τα .java αρχεία για κάθε κομμάτι αυτού του υποκεφαλαίου θα βρίσκονται στον ίδιο φάκελο με το παρόν έγγραφο.Το NetBeans είναι version 6.8 και το JXTA version 2.5.

5.5.0 Προετοιμασία

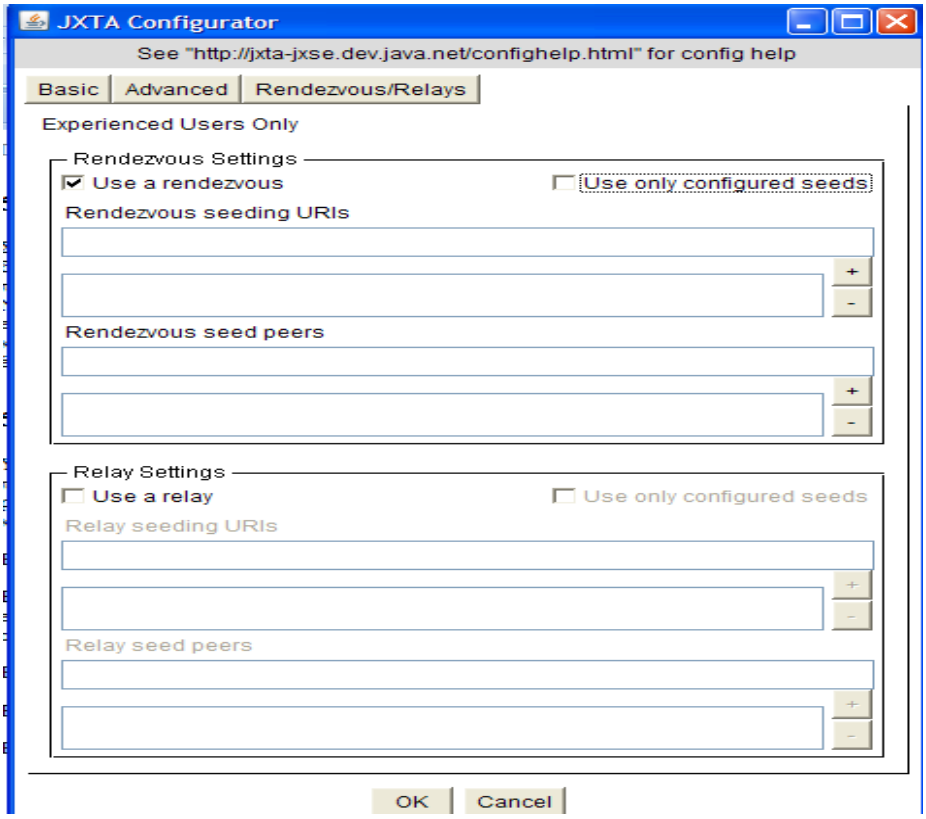
Υπάρχει ένα πρόβλημα γενικότερα με τα rendezvous peers και για τις ανάγκες των παραδειγμάτων χρειάζεται κάποιες φορές να είναι δυνατή η σύνδεση με έναν τέτοιον peer.Για αυτόν τον λόγο θα κάνουμε χρήση του jxta shell το οποίο επίσης θα κατεβάσουμε από την παραπάνω ιστοσελίδα(http://download.java.net/jxta/).

Βήμα 1) Δημιουργούμε τον peer με όποιο όνομα θέλουμε.(εδώ jack)



Εικόνα 80 JXTA configurator

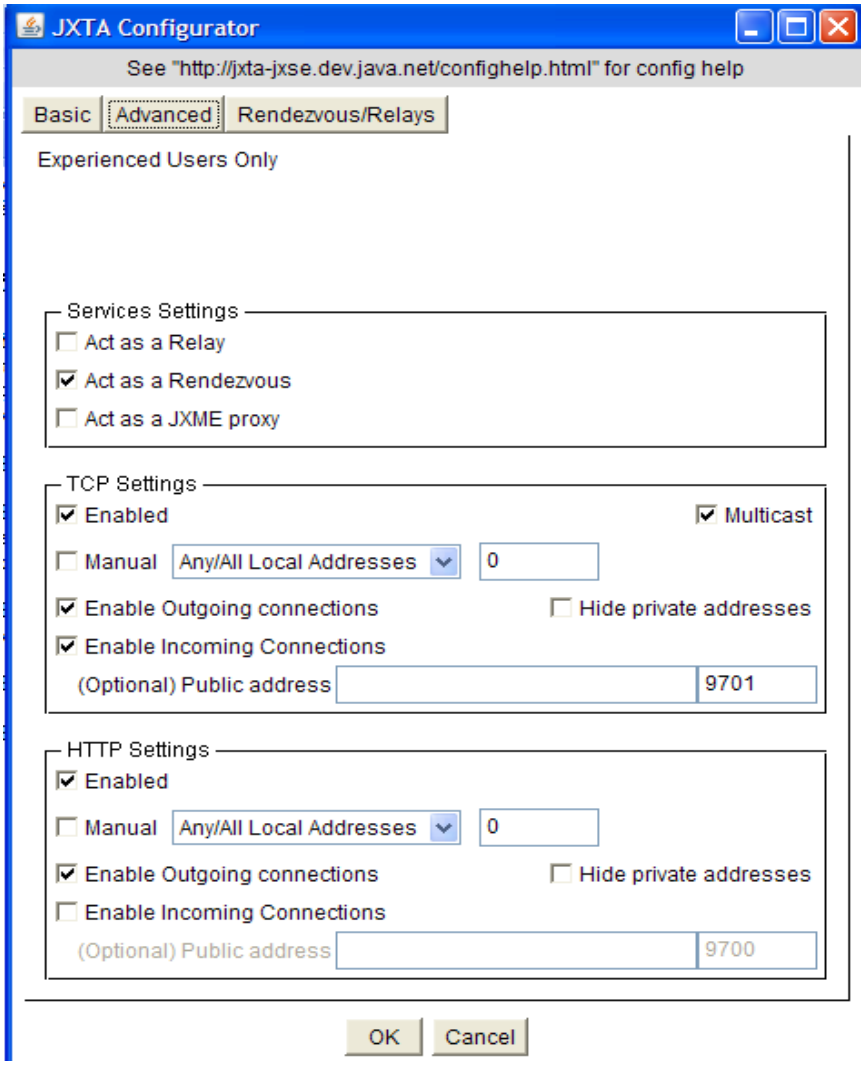
Βήμα 2) Πηγαίνουμε στο tab rendezvous/relay και επιλέγουμε το use a rendezvous, ενώ δεν επιλέγουμε το use only configured seeds και οτιδήποτε έχει να κάνει με relay από κάτω.Με την επιλογή use a rendezvous κάνουμε χρήση υπηρεσιών που προσφέρονται απο rendezvous peers που αναλύθηκαν παραπάνω και θα τις χρειαστούμε για την διασύνδεση μεταξύ των peers .To Use only configured peer είναι στην περίπτωση που δεν επιθυμούμε χρήση υπηρεσιών ή ανταλλαγή messages με peers που δεν έχουμε εμείς δημιουργήσει.Τέλος δεν χρειαζόμαστε relay peers καθώς δεν πρόκειται να έχουμε προβλήματα επικοινωνίας μεταξύ των peer μας(Firewall etc).



Εικόνα 81 JXTA configurator 2

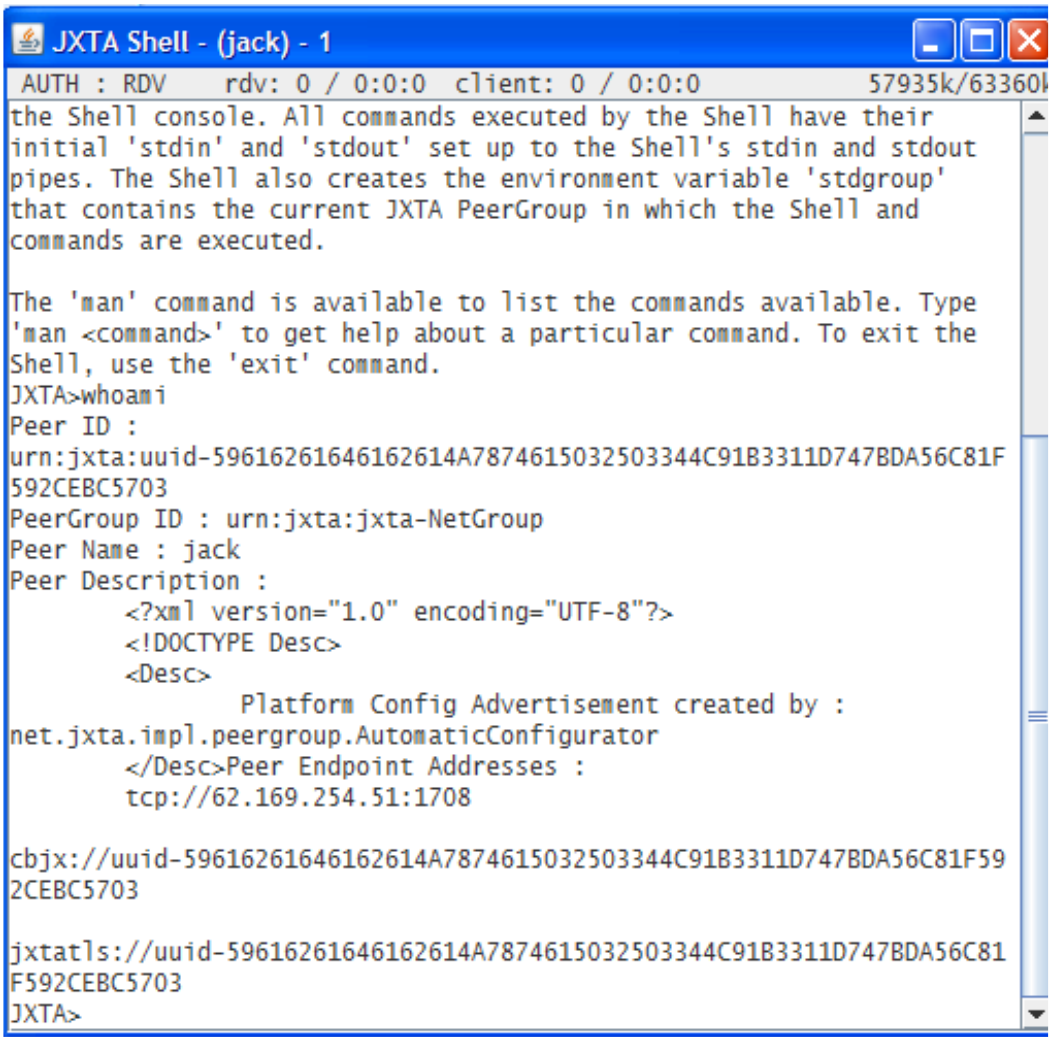
Βήμα 3) Στο tab advanced επιλέγουμε το act as a rendezvous στο services settings ώστε,ο peer jack στην συγκεκριμένη περίπτωση,να έχει τον ρόλο του Rendezvouz peer και όλα τα άλλα τα αφήνουμε ως έχει.Μπορούσαμε να επιλέξουμε είτε as Relay peer είτε ως JXME Proxy[95],δηλαδή να επιτρέπει την επικοινωνία και με συσκευές που δεν είναι υπολογιστές.Στην συγκεκριμένη περίπτωση δεν το χρειαζόμαστε.Από εκεί και πέρα μας επιτρέπεται στα HTTP και TCP settings να ρυθμίσουμε αν θα είναι ενεργοποιημένα αυτά τα 2 πρωτόκολλα,αν η μετάδοση των δεδομένων θα είναι multicast ή σε συγκεκριμένες διευθύνσεις και αν θα επιτρέπεται η σύναψη εξερχόμενων ή/και εισερχόμενων συνδέσεων.Οι επιλογές μας φαίνονται παρακάτω. Τώρα αφού βάλουμε τον κωδικό είμαστε μέσα στο shell.

[95] JXME Proxy: http://caribdis.unab.edu.co/pls/portal/docs/PAGE/REVISTACOLOMBIANACOMPUTO/RCC_ESPANOL/NUMEROSANTERIORES/JUNIO2006/R71_ART4_C.PDF



Εικόνα 82 JXTA configurator 3

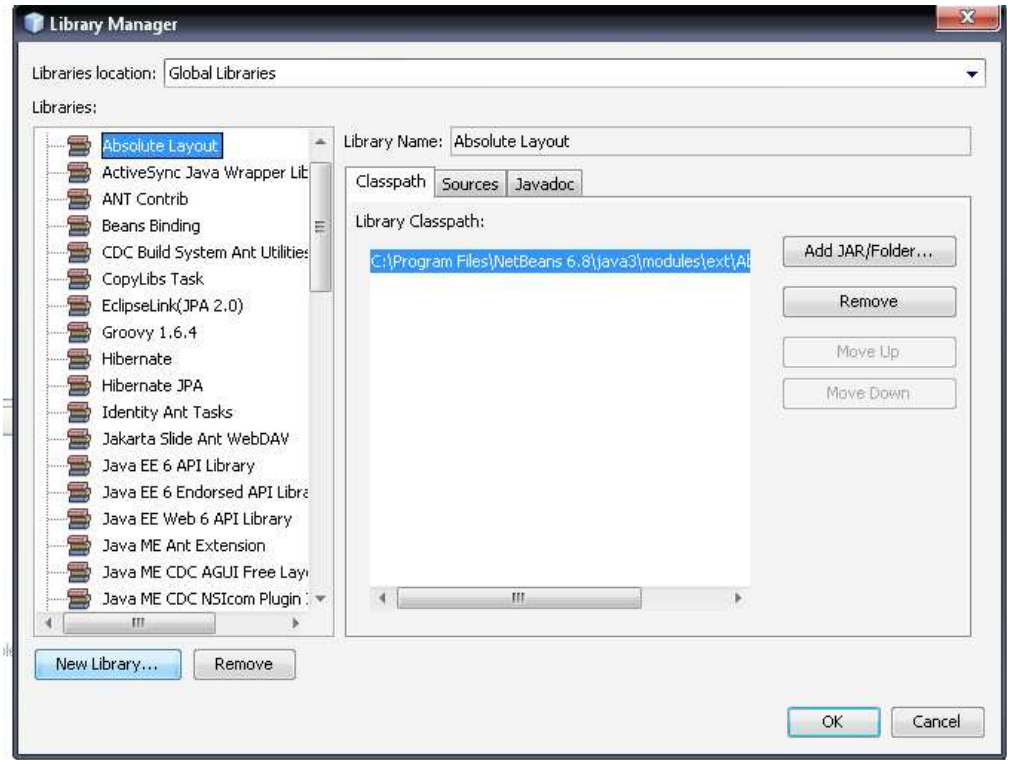
Βήμα 4) Εδώ η πρώτη μας κίνηση είναι να γράψουμε την εντολή whoami ώστε να λάβουμε ορισμένες γενικές πληροφορίες για τον peer μας. Αυτές τις πληροφορίες μπορούμε να τις επαληθεύσουμε ότι είναι οι ίδιες αργότερα την ώρα που θα τρέχουμε τις κλάσεις.Βλέπουμε πληροφορίες για την peer ID του,το όνομα,το peer group ID του,το character enocoding κ.τ.λ.Πλέον κάνουμε μια ελαχιστοποίηση και ανοίγουμε το netbeans και φορτώνουμε το project(JUXTA) το οποίο βρίσκεται στον ίδιο φάκελο με το παρόν έγγραφο.Παρακάτω ενέργειές μας.



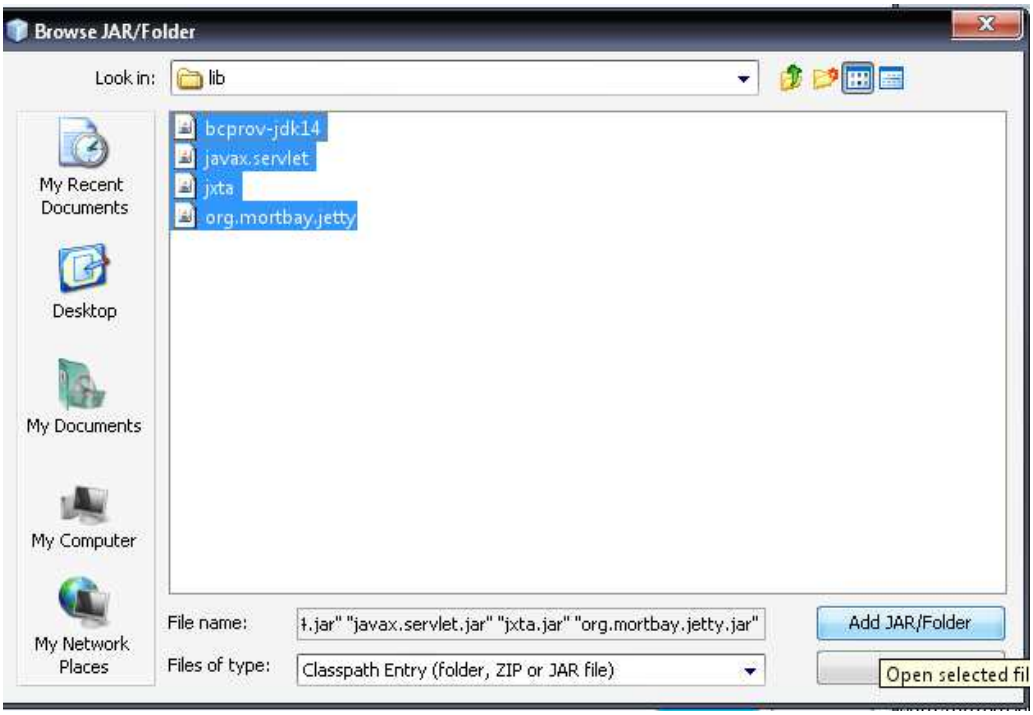
Εικόνα 83 Αναγνώριση του peer.

Εικόνα 84 Φόρτωμα Project JUXTA

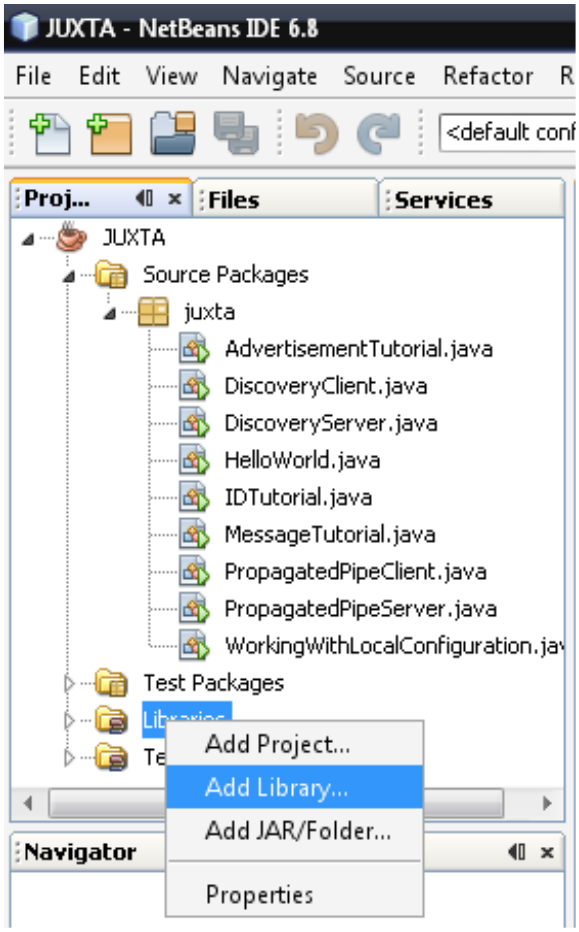
Βήμα 5) Μέσα στο NetBeans πάμε tools-libraries-new library και φορτώνουμε ότι .jar αρχείο βρίσκεται μέσα στο .lib που είναι στον ίδιο φάκελο με το παρόν έγγραφο και μετά το καταχωρούμε ως βιβλιοθήκη πατώντας το OK. Έπειτα πατάμε δεξί click στο libraries του project και προσθέτουμε το library μας.



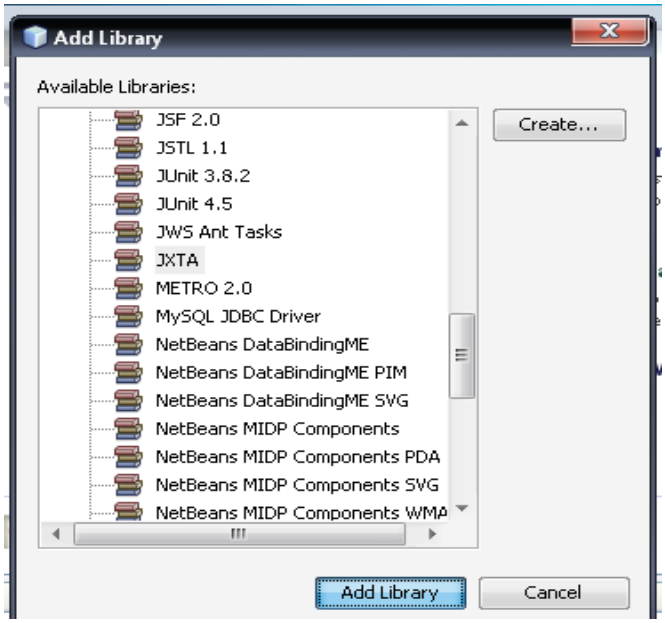
Εικόνα 85 Επιλογή για φόρτωμα Library



Εικόνα 86 Τα JAR αρχεία

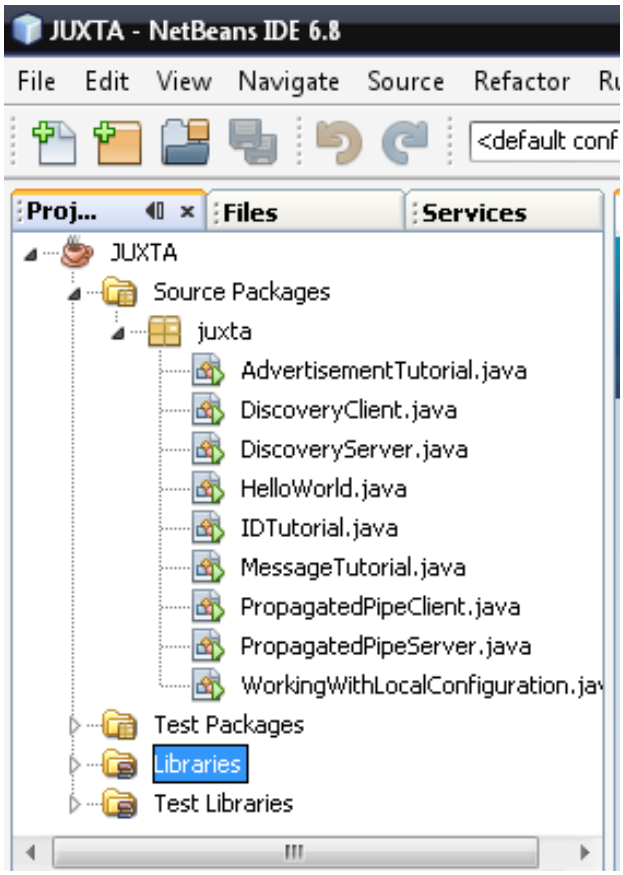


Εικόνα 87 Επιλογή για το νέο Library στο JUXTA Project



Εικόνα 88 Το Library JXTA μέσα από μια πληθώρα Libraries

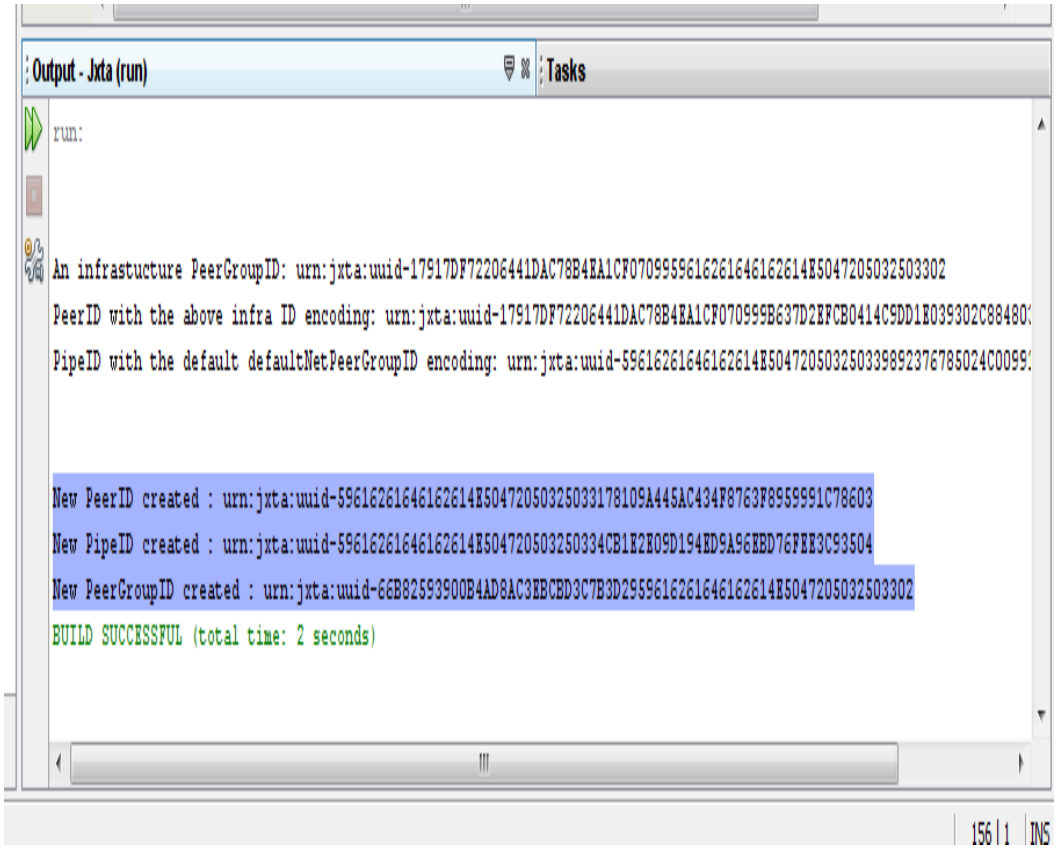
Βήμα 6) Πλέον δεν έχουμε να κάνουμε κάτι άλλο από το να τρέχουμε την κάθε κλάση ξεχωριστά εκτός από αυτές που είναι διπλές με client και server όπου τρέχουμε πρώτα τον client.Ακολουθούν κάποια παραδείγματα.



Εικόνα 89 Οι κλάσεις που περιέχονται στο Project μας

5.5.1 Δημιουργία ID’s

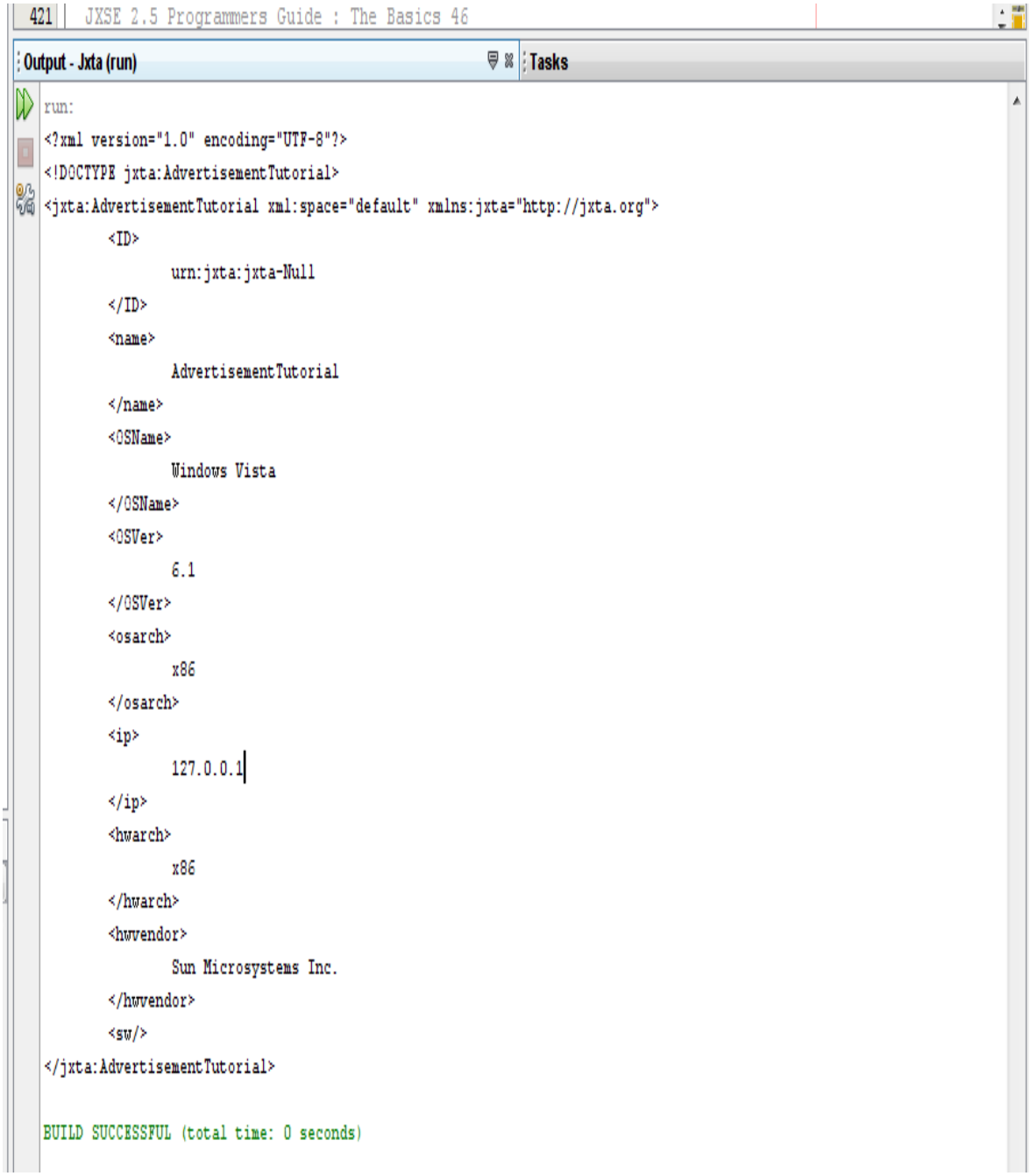
Όπως είδαμε και παραπάνω κάθε component μέσα σε ένα JXTA δίκτυο έχει μια δικιά του μοναδική ID.Κάθε ID είναι δημιουργημένη για το είδος του component το οποίο θα αντιπροσωπεύσει. Σε αυτό το παράδειγμα θα δημιουργήσουμε 3 ID’s ένα για Pipe, ένα για Peer και ένα για Peer Group.Το αποτέλεσμα στο NetBeans φαίνεται στο παρακάτω image.



Εικόνα 90 Αποτέλεσμα δημιουργίας ID’s

5.5.2 Δημιουργία Advertisement

Για να γυρίσουμε πάλι πίσω στην θεωρία θα αναφέρουμε ότι το Advertisement είναι αυτό που ακριβώς δηλώνει, μία διαφήμιση των πόρων και των χαρακτηριστικών των peers , peer groups, services κ.α που διαφημίζει. Είναι ένα XML αρχείο που ανάμεσα στα Tags του περιλαμβάνει τις πληροφορίες που διαφημίζονται. Ορίστε και το αποτέλεσμα.



Εικόνα 91 Δημιουργία Advertisement

Με λίγα λόγια αυτό που μας παρουσιάζεται εδώ είναι ο τύπος του ID του Advertisement στο Tag ID και όσο πάμε προς τα κάτω,το όνομα του Advertisement,το χρησιμοποιούμενο λειτουργικό σύστημα,η ip address(local host από ότι βλέπουμε.) και η πληροφορία για την πηγή ανάπτυξης του κώδικα(Sun Microsystems).

5.5.3 Εκκίνηση και σταμάτημα του JXTA δικτύου

Εδώ έχουμε ένα πολύ απλό παράδειγμα στο οποίο με την χρήση του Network Manager, το οποίο έχει το ρόλο του να ανιχνεύει και να πραγματοποιεί τη σύνδεση με το rendezvous peer, μέσα στην κλάση Helloworld ξεκινάμε το δίκτυο, κάνουμε σύνδεση με έναν rendezvous peer μετά από ένα ορισμένο χρονικό διάστημα(12 δευτερόλεπτα) και τέλος κλείνουμε την σύνδεση.

```
JXTA Started
30 Μαΐ 2010 5:06:18 μμ net.jxta.platform.NetworkManager startNetwork
Waiting for a rendezvous connection
INFO: Started JXTA Network!
Connected :true
Stopping JXTA
```

Εικόνα 92 Σύνδεση με rendezvous peer

5.5.4 Δημιουργία messages

Ένα message από αυτά που ανταλλάσουν μεταξύ τους οι peers αποτελείται από αρκετά message elements.Όπως είπαμε και παραπάνω περιέχονται επιπλέον πληροφορίες και περιεχόμενα πρωτοκόλλου.Παρακάτω βλέπουμε το παράδειγμα ενός message αμέσως μετά το Run της αντίστοιχης κλάσης καθώς και τα περιεχόμενά του.

```
run:
-----------------Begin Message--------------------
Message Size :91
Element : TutorialNameSpace :: String Test
[This is a test]
------------------End Message---------------------
String Value :This is a test
-----------------Begin Message--------------------
Message Size :94
Element : TutorialNameSpace :: long test
[9223372036854775807]
------------------End Message---------------------
long Value :9223372036854775807
-----------------Begin Message--------------------
Message Size :84
Element : TutorialNameSpace :: int test
[2147483647]
------------------End Message---------------------
int Value :2147483647
-----------------Begin Message--------------------
Message Size :105
Element : TutorialNameSpace :: byte test
[ □       □□     □0m      □n   □    ]
------------------End Message---------------------
Read 4096 byte back
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE jxta:PipeAdvertisement>
<jxta:PipeAdvertisement xml:space="default" xmlns:jxta="http://jxta.org">
        <Id>
                urn:jxta:uuid-59616261646162614E50472050325033F6EE7052E8084937B86FEBFF9973CF5604
        </Id>
        <Type>
                JxtaUnicast
        </Type>
</jxta:PipeAdvertisement>

BUILD SUCCESSFUL (total time: 0 seconds)
```

Εικόνα 93 Παράδειγμα message

5.5.5 Χρήση Local Configuration

Σε αυτό εδώ το σημείο θα κάνουμε χρήση του Network configurator επιπλέον με την χρήση του Network Manager που εξηγήσαμε παραπάνω.Ο Network Configurator αυτό που κάνει είναι να κρατά τις ρυθμίσεις που έχουμε κάνει για το δίκτυό μας σταθερές.Ελέγχει εάν υπάρχουν ρυθμίσεις όπως αυτές που κάναμε παραπάνω όταν δημιουργήσαμε τον peer στο shell και εάν ναι τις φορτώνει,εάν όχι ζητάει κωδικό και όνομα που έχουμε βάλει από πριν στο shell και απαιτούνται ρυθμίσεις.Έχουμε μια ρύθμιση και ταυτοποίηση ενός peer και ενός peer group και εν συνεχεία περιμένουμε πάλι για μια σύνδεση με έναν rendezvous peer για να σταματήσει το JXTA.Συνεπώς εδώ απλώς φορτώνουμε τις ρυθμίσεις αφού έχουν βρεθεί(βλέπε εικόνα),ξεκινάει το JXTA δίκτυο,παρουσιάζεται ο peer Helloworld που δημιουργείται μέσω της κλάσης, περιμένουμε για μια σύνδεση του εν λόγω peer με έναν Rendezvouz peer(στην περίπτωσή μας τον jack) και τερματίζεται η σύνδεση.

```
run:
Creating the Network Manager
Network Manager created
PeerID: urn:jxta:uuid-59616261646162614E50472050325033CE8A2D79F0B1425C859B809C2576265203
Retrieving the Network Configurator
30 Μαϊ 2010 8:25:29 μμ net.jxta.platform.NetworkManager configure
INFO: Loading existing configuration. mode = EDGE
Network Configurator retrieved
Local configuration found
Loading found configuration
Configuration loaded
Starting JXTA
```

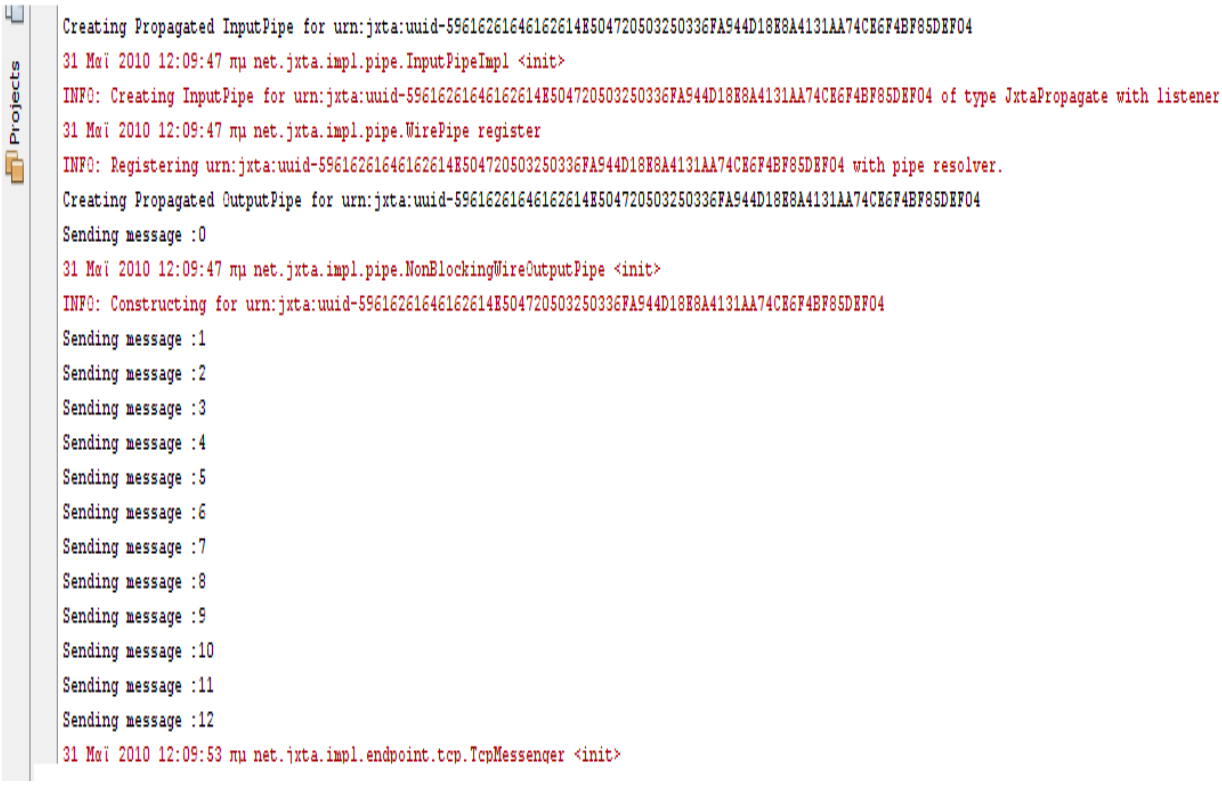
Εικόνα 94 φόρτωμα του Configurator

```
JXTA Started
Peer name : HelloWorld
Peer Group name: NetPeerGroup
Peer Group ID : urn:jxta:uuid-59616261646162614E50472050325033 9CDD1288098746AD9192AA6B96912607 03
Waiting for a rendezvous connection for 25 seconds " + "(maximum)
Connected :true
Stopping JXTA
```

Εικόνα 95 Σύνδεση με rendezvous peer και κλείσιμο

5.5.6 Propagated Pipes

Εδώ έχουμε την δημιουργία ενός propagated output Pipe. Η όλη εφαρμογή αποτελείται από 2 κλάσεις,μια client η οποία δημιουργεί το instance αυτού του pipe το οποίο αρχίζει να στέλνει ασύστολα messages και άλλη μια κλάση server όπου είναι αποδέκτης ενός από τα μηνύματα που στέλνονται κάθε φορά.Να αναφέρουμε πάλι ότι το Propagated pipes είναι διόδοι αποστολής μυνημάτων μεταξύ των peers και τα συγκεκριμένα έχουν την δυνατότητα αποστολής μιας output από ένα peer σε πολλαπλές εισόδους Ας δούμε.



Εικόνα 96 Δημιουργία του Pipe και αποστολή μηνυμάτων 1-12

Εικόνα 97 Λήψη από το input του server και αναγνώριση της πηγής.

Συμπεράσματα

Στην παρούσα πτυχιακή εργασία συναντήσαμε πολλά και διάφορα θέματα που σχετίζονται με τα διομότιμα δίκτυα. Συγκεκριμένα, στην αρχή της εργασίας έγινε μια περιγραφή για το πώς ξεκίνησε το peer to peer με την διάδοση του Internet την δεκαετία του ‘60 και πώς εξαπλώθηκε αργότερα με την εισαγωγή όλο και περισσοτέρων υπολογιστών ιδιωτών.

Στην συνέχεια, παρουσιάσαμε επιγραμματικά τους πιο συχνά χρησιμοποιούμενους BitTorrent clients και αναλυτικά τον UTorrent και την χρήση του,επιπλέον με κάποιους προβληματισμούς.

Επίσης, εμφανίσαμε και αναλύσαμε τα αποτελέσματα πολλών και διαφόρων ερευνών επάνω στα peer to peer συστήματα γενικότερα,περιλαμβανομένου εφαρμογών Instant Messaging και Torrents.Δεν παρελήφθει φυσικά η παρουσίαση στατιστικών στοιχείων για θέματα όπως Online Piracy και το μέλλον των peer to peer εφαρμογών.

Στην συνέχεια της εργασίας αυτής, είδαμε την JXTA peer to peer δικτύωση η οποία αντιπροσωπέυει ένα πρότυπο δικτύωσης πολλών και διαφόρων συσκευών.Αναλύθηκαν θα κυριότερα σημεία που το αποτελούν,η χρησιμότητα αυτών και τα πρωτόκολλα που χρησιμοποιούνται για την εν λόγω δικτύωση

Τέλος, συναντήσαμε τον μεταγλωτιστή Java NetBeans,με σκοπό να υλοποιήσουμε Java κώδικα με την βοήθεια ειδικών βιβλιοθηκών από το Site της εφαρμογής JXTA,παρουσιάσαμε και κατανοήσαμε τα βασικά δικτυακά στοιχεία και εφαρμογές που είχαν αναλυθεί παραπάνω.

Βιβλιογραφία

Έντυπη Βιβλιογραφία

- **Peer-to-Peer: Harnessing the Power of Disruptive Technologies**
- **Peer-to-Peer Computing: Technologies for Sharing and Collaborating on the Net**
- **Peer-to-Peer: Building Secure, Scalable, and Manageable Networks**
- **P2P: How Peer-to-Peer Technology Is Revolutionizing the Way We Do Business**
- **Server and Peer to peer trends in Western europe**
- **Worldwide Peer to peer market**
- **Peer-to-peer, Peer to peer and Internet users outlook in Usa**
- **Web technologies trends in China**
- **PC Magazine**

Ηλεκτρονική βιβλιογραφία και πηγές

- **Πληροφορίες για Peer to Peer**
  http://en.wikipedia.org/wiki/Peer-to-peer
- **Πληροφορίες για JXTA**
  http://en.wikipedia.org/wiki/JXTA
- **JXTA JavaStandard Edition v2.5: Programmers Guide from**
  https://jxta.dev.java.net/
- **Documentation from** http://www.utorrent.com/
- **Peer-to-Peer: Harnessing the Power of Disruptive Technologies**
  http://oreilly.com/catalog/peertopeer/chapter/ch01.html
- **JXTA in a nutshell**
  http://oreilly.com/catalog/jxtaian/chapter/ch02.html