Τ.Ε.Ι. Δυτικής Ελλάδας
Τμήμα Μηχανικών Πληροφορικής Τ.Ε

ΤΙΤΛΟΣ ΕΡΓΑΣΙΑΣ

"ΑΝΑΛΥΣΗ ΔΙΚΤΥΑΚΗΣ ΚΙΝΗΣΗΣ ΚΑΙ ΕΞΑΓΩΓΗ ΣΥΜΠΕΡΑΣΜΑΤΩΝ ΣΕ ΕΠΙΠΕΔΟ ΕΦΑΡΜΟΓΗΣ."

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ:

ΓΙΩΡΓΟΣ ΓΚΙΝΟΠΟΥΛΟΣ, Α.Μ. 0494

ΕΥΘΥΜΙΟΣ ΠΑΠΑΔΟΠΟΥΛΟΣ, Α.Μ. 0588

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ

ΒΑΣΙΛΕΙΟΣ ΤΣΑΚΑΝΙΚΑΣ

ΝΑΥΠΑΚΤΟΣ 2014

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ	**ΥΠΟΓΡΑΦΕΣ**
1.	
2.	
3.	

ΠΕΡΙΛΗΨΗ

Σκοπός της πτυχιακής εργασίας είναι η αναγνώριση της δικτυακής κίνησης που παράγεται από τον τελικό χρήστη, δηλαδή να μπορούμε να αναγνωρίσουμε αν η κίνηση που παράγεται είναι VoIP, παρακολούθηση κάποιου Video, απλή περιήγηση σε κάποιο ιστότοπο κλπ. Για το σκοπό αυτό, δημιουργήσαμε ένα πρόγραμμα, με τη χρήση της γλώσσας προγραμματισμού Java, το οποίο καταγράφει την κίνηση που παράγεται από τον εκάστοτε server στον τελικό χρήστη, μετά από αίτηση σύνδεσης του τελευταίου στο server. Επίσης, εμφανίζει γραφικές παραστάσεις που αφορούν το μέγεθος πακέτου, το πρωτόκολλο μεταφοράς που χρησιμοποιεί το κάθε πακέτο, και το μέγεθος του TCP Window. Συγκεκριμένα, αυτό που γίνεται είναι καταγραφή όλων των πακέτων που γίνονται λήψη από την κάρτα δικτύου του υπολογιστή, εξαγωγή των πληροφοριών του κάθε πακέτου σε κάποια text αρχεία και στη συνέχεια γραφική απεικόνιση της κίνησης.

Στο **Κεφάλαιο 1** της εργασίας, γίνεται μια εισαγωγή στα δίκτυα υπολογιστών, τα δίκτυα επικοινωνιών και το Διαδίκτυο. Συγκεκριμένα, δίνεται ο ορισμός των παραπάνω εννοιών, γίνεται μια μικρή ανάλυση για το καθένα.

Στο **Κεφάλαιο 2**, γίνεται αναφορά στο μοντέλο OSI και ακολουθεί πλήρης τεχνική και λογική περιγραφή κάθε επιπέδου του μοντέλου. Συγκεκριμένα αναλύεται ο τρόπος λειτουργίας και επικοινωνίας και των εφτά επιπέδων.

Στο **Κεφάλαιο 3**, γίνεται η περιγραφή και η ανάλυση των σημαντικότερων πρωτοκόλλων που χρησιμοποιούνται στο Διαδίκτυο από το κάθε επίπεδο του μοντέλου OSI.

Στο **Κεφάλαιο 4**, γίνεται θεωρητική περιγραφή των χαρακτηριστικών κίνησης των σημαντικότερων διαδικτυακών εφαρμογών, καθώς και αναφορά στα πρωτόκολλα που χρησιμοποιούν.

Στο **Κεφάλαιο 5**, εξηγούμε τη διαδικασία της πειραματικής διαδικασίας που εκτελέσαμε, παραθέτουμε τα αποτελέσματα των μετρήσεων, και αναλύουμε τα συμπεράσματα που προέκυψαν από τις γραφικές παραστάσεις.

ABSTRACT

The purpose of this graduate theses is the recognition of the network traffic witch is produced by the end user, that is to say that we can acknowledge, whether the traffic that is being produced is a VoIP, monitoring (watching) of a Video, simply browsing in some site e.c.t. For this purpose, we created a program with the use of the program language Java, witch record the traffic that is being produced by server side to the end user, after the connect request to the Server. Moreover, it appears graphs that have to do with the size of the package, the transfer protocol that every package uses and the size of the TCP Window. Specifically, what takes place is a recording of all the packages that are being received from the computer network card, extraction of the information of every package in text files and a graphic depiction of the traffic.

In the **first chapter** of the theses is being done an introduction to the Computers Network, the Communications Network and the Internet. Specifically, is being given the definition of the above and a small analysis for each one of them.

In the **second chapter** of the theses there is a cite of the OSI model followed by a complete, technical and logical, description of every level of this model. Specifically, is being analyzed, the way of operation and communication of all seven layers.

The **third chapter** contains the description and the analysis of the most important protocols that are being used in the Internet from every level of the OSI model.

The **forth chapter** contains a theoretical description of the characteristics of the traffic of the most important Internet applications and a report to the protocols that are being used.

In the **fifth chapter** we explain the experimental process that we followed. We quote the results of the measurements and we analyze the conclusions that have arisen from the graphs.

Ευχαριστίες

Με την ευκαιρία της ολοκλήρωσης της πτυχιακής μας εργασίας, θα θέλαμε να ευχαριστήσουμε τον επιβλέποντα καθηγητή μας κ. Βασίλη Τσακανίκα για την πολύτιμη καθοδήγησή του καθ' όλη τη διάρκεια της και για τις χρήσιμες και ενδιαφέρουσες συζητήσεις που είχαμε.

Επίσης, θα θέλαμε να ευχαριστήσουμε όλους τους καθηγητές του τμήματος, για τις πολύτιμες γνώσεις που μας προσέφεραν όλα αυτά τα χρόνια.

Τέλος, ένα μεγάλο ευχαριστώ στις οικογένειές μας, για την εμπιστοσύνη και τη στήριξη που μας έδειξαν, όλα αυτά τα χρόνια των σπουδών μας.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΙΝΑΚΑΣ ΕΙΚΟΝΩΝ

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

1.1 ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

1.1.1 Τι είναι ένα δίκτυο υπολογιστών

Ένα δίκτυο υπολογιστών είναι ένα τηλεπικοινωνιακό σύστημα από αυτόνομους ή μη αυτόνομους διασυνδεδεμένους υπολογιστές. Οι υπολογιστές, θεωρούνται διασυνδεδεμένοι όταν είναι σε θέση να ανταλλάξουν πληροφορίες μεταξύ τους και αυτόνομοι όταν δεν είναι δυνατό κάποιος υπολογιστής, να ελέγξει τη λειτουργία (π.χ. εκκίνηση, τερματισμό) κάποιου άλλου.

1.1.2 Σκοπός των Δικτύων

Τα δίκτυα δημιουργήθηκαν για να εξυπηρετήσουν τις ανάγκες που προέκυψαν, από την εξάπλωση της χρήσης υπολογιστών. Βασικός σκοπός της ύπαρξης των δικτύων, είναι ο διαμοιρασμός των πόρων του δικτύου και η ανταλλαγή πληροφοριών κάθε μορφής (προγράμματα, αρχεία, δεδομένα). Ο όρος πόρος αναφέρεται, είτε σε υλικό (hardware) , π.χ. εκτυπωτές είτε σε λογισμικό (software), π.χ. προγράμματα εφαρμογών.

1.1.3 Αρχιτεκτονική των Δικτύων

Η αρχιτεκτονική των δικτύων καθορίζει τον τρόπο με τον οποίο οι υπολογιστές και οι υπόλοιπες συσκευές, συνδέονται μεταξύ τους για να σχηματίσουν ένα σύστημα επικοινωνίας που θα επιτρέπει στους χρήστες, να διαμοιράζονται πληροφορίες και συσκευές του δικτύου. Σε ένα δίκτυο περιλαμβάνονται:

- Τερματικοί κόμβοι. Ελέγχουν τους πόρους του δικτύου.
- Υποδίκτυα. Φυσικά μέσα μετάδοσης, πρωτόκολλα επικοινωνίας, τοπολογία, τερματικοί κόμβοι, πόροι που μπορεί να διαφέρουν πολύ ανά υποδίκτυο.
- Συσκευές διασύνδεσης. Διασύνδεουν τα ετερογενή υποδίκτυα, έτσι ώστε να διασφαλίζεται η επικοινωνία τερματικών κόμβων που βρίσκονται σε διαφορετικά υποδίκτυα.

1.1.4 Είδη Δικτύων

Τα δίκτυα μπορούμε να τα κατατάξουμε σε διάφορες κατηγορίες. Ανάλογα με το φυσικό μέσο διασύνδεσής τους χαρακτηρίζονται ως:

- **Ενσύρματα δίκτυα**. Η ενσύρματη επικοινωνία, περιλαμβάνει εναέριες, επίγειες και υπόγειες συνδέσεις.
- **Ασύρματα δίκτυα**. Οι συνδέσεις πραγματοποιούνται μέσω ηλεκτρομαγνητικών κυμάτων και όχι μέσω καλωδίων.

Με βάση τη γεωγραφική τους ανάπτυξη διακρίνονται σε:

- **Τοπικά δίκτυα (Local Area Networks - LAN)**, που καλύπτουν μικρές αποστάσεις (μερικών εκατοντάδων μέτρων ή λίγων χιλιομέτρων) και περιορίζονται στα πλαίσια μίας επιχείρησης.
- **Αστικά Δίκτυα (Metropolitan Area Networks - MAN)**, τα οποία είναι δίκτυα που δεν ξεπερνούν τα σύνορα μιας πόλης. Είναι ταχύτερα από τα τοπικά δίκτυα και μπορούν να μεταδίδουν εικόνα, φωνή και δεδομένα αποδοτικότερα.
- **Δίκτυα ευρείας περιοχής** (**Wide Area Networks - WAN**), που καλύπτουν αποστάσεις μερικών χιλιομέτρων στην ίδια πόλη, μέχρι χιλιάδων χιλιομέτρων σε διαφορετικές πόλεις-κράτη-ηπείρους.

Με βάση τον τηλεπικοινωνιακό φορέα εξυπηρέτησης διακρίνονται σε :

- **Ιδιωτικά δίκτυα (Private Networks)**. Ανήκουν εξ' ολοκλήρου σε ιδιωτικούς οργανισμούς και χρησιμοποιούν είτε αποκλειστικές γραμμές επικοινωνίας δημόσιων τηλεπικοινωνιακών φορέων (leased lines) χωρίς να τις μοιράζονται με άλλους χρήστες ή ιδιόκτητες γραμμές επικοινωνίας.
- **Δημόσια δίκτυα (Public Networks)**, που εξυπηρετούν τις διασυνδέσεις μεταξύ απομακρυσμένων σημείων. Χρησιμοποιούνται όταν η απόσταση είναι μεγάλη και καθίσταται απαγορευτική, λόγω κόστους, η χρήση αποκλειστικών γραμμών ή όταν ο φόρτος μεταξύ των σημείων δεν είναι μεγάλος και επιτυγχάνεται έτσι μεγάλη ταχύτητα μεταφοράς.

1.1.5 Τοπολογίες Δικτύων

Το βασικότερο χαρακτηριστικό ενός δικτύου είναι η τοπολογία του. Αυτή χωρίζεται στην φυσική και λογική τοπολογία. Στην φυσική τοπολογία, περιγράφεται η γεωγραφική του κατανομή, ενώ στην λογική ο τρόπος της δρομολόγησης των σημάτων μεταξύ των μελών του δικτύου. Από αυτήν εξαρτάται το είδος της τεχνολογίας που θα χρησιμοποιηθεί. Στις διάφορες τοπολογίες χρησιμοποιείται και διαφορετική τεχνική για την επικοινωνία μεταξύ των υπολογιστών. Οι βασικότερες τεχνικές είναι:

- **Peer - to - peer**: Με την τεχνική αυτή, οι υπολογιστές του δικτύου επικοινωνούν άμεσα μεταξύ τους. Το πλεονέκτημα, είναι πως το κόστος υλοποίησης είναι μικρό αλλά η διαχείριση του δικτύου (πόροι, δικαιώματα πρόσβασης και η ασφάλεια γενικότερα) είναι χρονοβόρα και όχι τόσο αποτελεσματική χωρίς την ύπαρξη ενός κεντρικού εξυπηρετητή αφού θα πρέπει να ρυθμιστεί ο κάθε σταθμός ξεχωριστά.

- **Client - Server**: Στην τεχνική αυτή υπάρχει ένας (ή περισσότεροι) κεντρικός εξυπηρετητής, με τον οποίο επικοινωνούν όλοι οι σταθμοί. Ο εξυπηρετητής διαχειρίζεται τους πόρους και τις υπηρεσίες στις οποίες έχουν πρόσβαση οι σταθμοί. Η διαχείριση του δικτύου με την τεχνική αυτή, είναι εύκολη και καθόλου χρονοβόρα αφού αρκεί να ρυθμιστεί μια φορά ο εξυπηρετητής για όλο το δίκτυο. Επίσης, αλλαγές που θα γίνουν αργότερα στους λογαριασμούς των σταθμών γίνονται μια μόνο φορά στον εξυπηρετητή και ισχύουν για όλο το δίκτυο. Η διαχείριση του δικτύου δηλαδή είναι κεντρική. Το μειονέκτημα, είναι το υψηλό κόστος και η περίπτωση στην οποία το δίκτυο καταρρέει όταν ο κεντρικός εξυπηρετητής είναι εκτός λειτουργίας λόγω, π.χ. κάποιας βλάβης.

- **Application - Server**: Η τεχνική αυτή είναι ίσως η παλαιότερη από όλες τις υπόλοιπες, αφού απαιτεί πολύ λιγότερο και φτηνό υλικό για την υλοποίηση του. Πάλι χρησιμοποιείται ένας κεντρικός εξυπηρετητής, αλλά οι σταθμοί είναι «κουτά» τερματικά, δεν έχουν δηλαδή αποθηκευτικά μέσα ούτε επεξεργαστική ισχύ. Όλα τα δεδομένα αποθηκεύονται στον server ο οποίος αναλαμβάνει και όλη την επεξεργασία.

Οι πιο γνωστές τοπολογίες είναι:

- **Τοπολογία διαύλου (Bus Network):** Στην τοπολογία διαύλου, όλα τα μέλη του δικτύου επικοινωνούν μέσω ενός κοινού διαύλου που τα ενώνει σειριακά. Αυτό σημαίνει πως το σήμα μεταδίδεται από μέλος σε μέλος, έως να βρεθεί ο σωστός παραλήπτης, ο οποίος τελικά λαμβάνει και το πακέτο. Στα δύο άκρα του διαύλου συνδέονται αντιστάσεις που τον τερματίζουν. Ένα από τα μειονεκτήματα της τοπολογίας αυτής, είναι πως σε περίπτωση βλάβης ενός σταθμού «σπάει» ο δίαυλος και το δίκτυο καταρρέει.

- **Τοπολογία δακτυλίου (Ring Network):** Η τοπολογία δακτυλίου είναι παρόμοια της τοπολογίας διαύλου, με την μόνη διαφορά πως αντί για αντιστάσεις στα άκρα του διαύλου ενώνονται τα δύο ακριανά μέλη του δικτύου μεταξύ τους (το πρώτο και το τελευταίο δηλαδή), σχηματίζοντας έτσι σχήμα δακτυλίου.

- **Τοπολογία δακτυλίου με κουπόνι (Token Ring):** Η τοπολογία δακτυλίου με κουπόνι είναι μία παραλλαγή του κανονικού δακτυλίου, με τη διαφορά πως

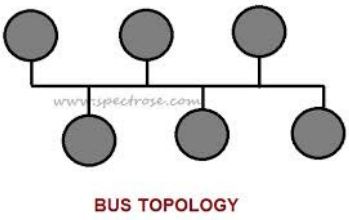
χρησιμοποιείται ένα κουπόνι το οποίο μετακινείται με συγκεκριμένη φορά από σταθμό εργασίας σε σταθμό εργασίας και μένει σε αυτόν για συγκεκριμένο χρονικό διάστημα. Όσο ο σταθμός έχει στην κατοχή του το κουπόνι έχει και το δικαίωμα πρόσβασης στο μέσο, μπορεί δηλαδή να στείλει ή να λάβει δεδομένα. Το μεγαλύτερο πλεονέκτημα στην τοπολογία αυτή είναι πως οι συγκρούσεις (η απόπειρα ταυτόχρονης πρόσβασης στο μέσο μετάδοσης άνω του ενός μέλους) είναι θεωρητικά ανύπαρκτες. Το μειονέκτημα είναι πως ενώ ένας ή και περισσότεροι σταθμοί εργασίας μπορεί να μην χρειάζονται πρόσβαση στο μέσο, θα έχουν στην κατοχή τους το κουπόνι μειώνοντας έτσι το ποσοστό αξιοποίησης των πόρων του δικτύου.

- **Τοπολογία αστέρα (Star Network):** Στην τοπολογία αστέρα όλοι οι σταθμοί εργασίας συνδέονται άμεσα με έναν κεντρικό υπολογιστή, τον εξυπηρετητή (server) ή κάποια δικτυακή συσκευή όπως π.χ. έναν δρομολογητή (router) ή hub, μέσω του οποίου ανταλλάσσουν δεδομένα. Ένα μεγάλο πλεονέκτημα είναι πως το δίκτυο δεν εξαρτάται από την κατάσταση του κάθε σταθμού εργασίας αλλά μόνο από την κατάσταση της κεντρικής μονάδας στην οποία συνδέονται όλα τα μέλη. Το μειονέκτημα είναι πως στην περίπτωση δυσλειτουργίας της κεντρικής μονάδας η επικοινωνία διακόπτεται πλήρως. Αυτό βέβαια μπορεί να αντιμετωπιστεί με την εγκατάσταση περισσότερων κεντρικών μονάδων έτσι ώστε σε περίπτωση δυσλειτουργίας της μίας να συνεχίζει η άλλη.

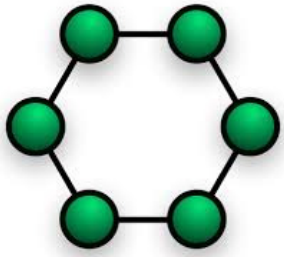
- **Πλεκτή τοπολογία (Mesh Network):** Η πλεκτή τοπολογία χωρίζεται στην πλήρως πλεκτή (full mesh) και μερικώς πλεκτή (partial mesh). Στην πλήρως πλεκτή κάθε σταθμός εργασίας συνδέεται απευθείας με όλους τους υπόλοιπους σταθμούς, επικοινωνεί δηλαδή άμεσα με κάθε έναν από αυτούς. Στην μερικώς πλεκτή κάποιοι σταθμοί επικοινωνούν άμεσα με όλους ή μερικούς από τους υπόλοιπους ενώ κάποιοι άλλοι μόνο με τους γειτονικούς. Το πλεονέκτημα, εδώ είναι πως ακόμα και σε περίπτωση μερικής καταστροφής του μέσου υπάρχει η δυνατότητα επικοινωνίας δύο σταθμών μέσω εναλλακτικών διαδρομών. Το μειονέκτημα είναι η περιττή καλωδίωση και το κόστος στην περίπτωση που το μέσο είναι το καλώδιο.

- **Τοπολογία δέντρου (Tree Network):** Στην τοπολογία δέντρου πρόκειται για δύο ή περισσότερα δίκτυα αστέρα των οποίων οι κεντρικοί σταθμοί επικοινωνούν μεταξύ τους μέσω ενός κοινού διαύλου. Είναι δηλαδή, ένα δίκτυο διαύλου που αποτελείται από δίκτυα αστέρα.

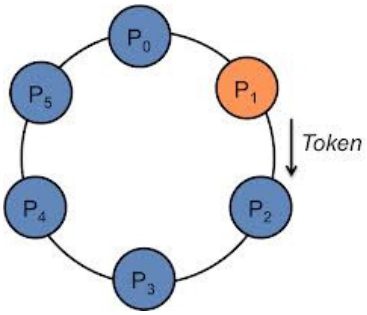
Παρακάτω, παρουσιάζονται εικόνες, που αποδίδουν σχηματικά τις παραπάνω τοπολογίες.



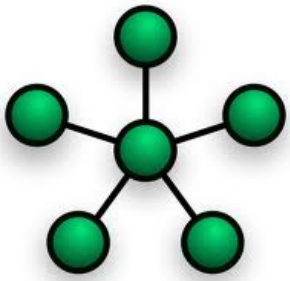
Εικόνα 1: Bus Network



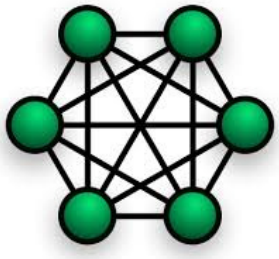
Εικόνα 2: Ring Network



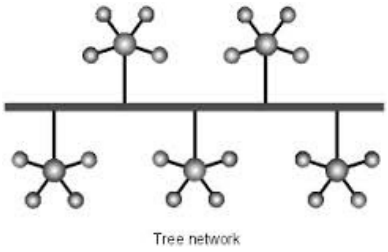
Εικόνα 3: Token ring Network



Εικόνα 4: Star Network



Εικόνα 5: Mesh Network



Εικόνα 6: Tree Network

1.2 Δίκτυα Επικοινωνιών

1.2.1 Τα επικοινωνιακά δίκτυα και οι ανάγκες που εξυπηρετούν

Η ανάγκη των ανθρώπων να επικοινωνούν μεταξύ τους ξεκινάει από πολύ παλιά. Για την επικοινωνία δύο συσκευών απαιτείται να υπάρχει μεταξύ τους σύνδεση από σημείο σε σημείο. Η σύνδεση αυτή μπορεί να υλοποιείται με καλώδιο, οπτική ίνα ή ραδιοζεύξη. Όταν ο αριθμός των συσκευών αυξάνει και πρέπει να είναι δυνατή η επικοινωνία μεταξύ δύο οποιονδήποτε συσκευών, προφανώς δεν είναι πρακτική λύση να υπάρχουν συνδέσεις

από σημείο σε σημείο για όλες αυτές τις συσκευές. Έτσι, με την αύξηση των συνδρομητών, έγινε προφανής η ανάγκη του τηλεφωνικού δικτύου, όπου δεν υπάρχουν άπειρες συνδέσεις από σημείο σε σημείο αλλά γίνεται από κοινού εκμετάλλευση του υπάρχοντος εξοπλισμού και των τηλεπικοινωνιακών γραμμών.

Το ίδιο πρόβλημα υπάρχει και στις συνδέσεις υπολογιστών. Στην αρχή υπήρχαν συνδέσεις από σημείο σε σημείο. Όταν, όμως, ο αριθμός άρχισε να αυξάνεται και έγινε αντιληπτό το όφελος από τη διασύνδεση των υπολογιστών, άρχισαν να δημιουργούνται τα δίκτυα δεδομένων (data networks). Γενικότερα, η λύση στο πρόβλημα της επικοινωνίας είναι η ύπαρξη επικοινωνιακού δικτύου του οποίου τις γραμμές, τους κόμβους και γενικότερα τους πόρους να μπορεί να χρησιμοποιεί οποιαδήποτε συσκευή που θέλει να επικοινωνήσει.

1.2.2 Επικοινωνιακά Δίκτυα

Επικοινωνιακό δίκτυο είναι ένα σύνολο κόμβων διασυνδεδεμένων με γραμμές επικοινωνίας, έτσι ώστε να επιτρέπεται η ανταλλαγή πληροφορίας. Οι κόμβοι μπορεί να είναι τερματικές συσκευές, όπως τηλεφωνικές συσκευές, υπολογιστές, εκτυπωτές, εξυπηρετητές αρχείων. Μπορεί, επίσης, να είναι συσκευές επικοινωνίας, όπως τηλεφωνικά κέντρα, δρομολογητές κ.α. Γενικά, υπάρχουν δύο είδη κόμβων: οι τερματικοί και οι επικοινωνιακοί κόμβοι. Οι τερματικοί κόμβοι παράγουν ή καταναλώνουν την πληροφορία που μεταφέρεται στο δίκτυο. Οι επικοινωνιακοί κόμβοι μεταφέρουν την πληροφορία, αλλά ούτε την παράγουν ούτε την καταναλώνουν. Μερικά από τα οφέλη από τη χρήση των δικτύων επικοινωνίας είναι:

- Διαμοιρασμός πόρων.
- Υψηλή αξιοπιστία.
- Εξοικονόμηση χρημάτων.
- Επικοινωνία.

1.2.3 Υπηρεσίες Δικτύου Επικοινωνίας

Ένα δίκτυο επικοινωνιών έχει σκοπό να παρέχει υπηρεσίες στους χρήστες του. Τέτοια υπηρεσία είναι για παράδειγμα, η υπηρεσία τηλεφωνικής επικοινωνίας, με την οποία γίνεται εφικτή η σύνδεση μιας τηλεφωνικής συσκευής με οποιαδήποτε άλλη, όπου και αν βρίσκεται.

Τα δίκτυα δεδομένων παρέχουν και αυτά πολλές υπηρεσίες. Για παράδειγμα, στον περιορισμένο γεωγραφικά χώρο ενός τοπικού δικτύου, η υπηρεσία εξυπηρέτησης εκτυπώσεων επιτρέπει σε όλους τους υπολογιστές του τοπικού δικτύου να χρησιμοποιούν από κοινού το διαθέσιμο εκτυπωτή. Η υπηρεσία εξυπηρέτησης αρχείων επιτρέπει σε όλους τους χρήστες του τοπικού δικτύου να χρησιμοποιούν αρχεία που βρίσκονται σε ένα διαθέσιμο για το σκοπό αυτό υπολογιστή (file server) . Αλλά και στον ευρύτερο χώρο, π.χ. του Internet, παρέχονται διάφορες υπηρεσίες όπως η υπηρεσία ηλεκτρονικού ταχυδρομείου (e-mail), η οποία επιτρέπει στους χρήστες να ανταλλάσουν μηνύματα, η υπηρεσία μεταφοράς αρχείων (file transfer), η οποία επιτρέπει τη μεταφορά αρχείων από έναν υπολογιστή σε άλλον κοκ. Συνεπώς, ένα δίκτυο επικοινωνίας προσφέρει ποικίλες και αρκετά διαφοροποιημένες υπηρεσίες.

Ανάλογα με την υπηρεσία, η μεταφορά των bits μπορεί να είναι περισσότερο ή λιγότερο αξιόπιστη και να διαρκεί περισσότερο ή λιγότερο χρόνο. Τις διαφορετικές αυτές απαιτήσεις, εξυπηρετεί το δίκτυο χρησιμοποιώντας λίγες μόνο διαφορετικές κατηγορίες υπηρεσιών επικοινωνίας.

1.2.4 Κατηγορίες Υπηρεσιών Επικοινωνίας

Από την πλευρά του χρήστη οι υπηρεσίες επικοινωνίας μπορεί να είναι είτε σύγχρονες είτε ασύγχρονες.

Σύγχρονη υπηρεσία επικοινωνίας:

- Σταθερός ρυθμός μετάδοσης της πληροφορίας.
- Κάθε bit φτάνει στο δέκτη με την ίδια καθυστέρηση που φεύγει από τον πομπό.

Παράδειγμα: Τηλεφωνία

Ασύγχρονη υπηρεσία επικοινωνίας:

- Η σειρά από bits διαιρείται σε πακέτα.
- Το κάθε πακέτο μεταδίδεται ανεξάρτητα από το άλλο.

Η ασύγχρονη υπηρεσία επικοινωνίας χωρίζεται σε ασύγχρονη υπηρεσία με σύνδεση και ασύγχρονη υπηρεσία χωρίς σύνδεση.

Ασύγχρονη υπηρεσία με σύνδεση:

- Παρέχει αξιόπιστη σύνδεση.

- Τα πακέτα μεταφέρονται με τη σειρά που στάλθηκαν.
- Μπορεί να υπάρχει εγγύηση.

Παράδειγμα: επικοινωνία Η/Υ (chat)

Ασύγχρονη υπηρεσία χωρίς σύνδεση:

- Η μεταφορά των πακέτων γίνεται με τυχαία σειρά.
- Μπορεί να υπάρξουν απώλειες - λάθη κατά τη μεταφορά.
- Υπάρχει μηχανισμός επιβεβαίωσης λήψης.

Παράδειγμα: e-mail

Υπάρχουν δύο βασικές τεχνικές για τη μεταφορά της πληροφορίας μέσα από το δίκτυο κι βοηθούν στην αξιοποίηση των διαθέσιμων πόρων του δικτύου. Αυτές είναι η μεταγωγή και η πολυπλεξία.

1.2.5 Μεταγωγή

Με τη μεταγωγή (**switching**), η πληροφορία που στέλνει ένας σταθμός εργασίας περνάει από διαδοχικούς κόμβους του δικτύου, για να φτάσει τελικά στο σταθμό προορισμού. Έτσι, χωρίς να είναι ανάγκη να υπάρχουν γραμμές που να συνδέουν όλους τους σταθμούς μεταξύ τους, παρέχεται από το δίκτυο μα υπηρεσία επικοινωνίας όπου κάθε σταθμός είναι δυνατό να ανταλλάξει πληροφορία με οποιοδήποτε σταθμό του διαδικτύου.

Οι κόμβοι μεταγωγής δεν ασχολούνται με το περιεχόμενο της πληροφορίας, αλλά μόνο με το πώς θα προωθήσουν την πληροφορία κατάλληλα από κόμβο σε κόμβο, μέχρι αυτή να φτάσει στον προορισμό της. Υπάρχουν δύο τεχνικές μεταγωγής. Η μεταγωγή κυκλώματος και η μεταγωγή πακέτου.

Μεταγωγή κυκλώματος

Η μεταγωγή κυκλώματος, είναι μια τεχνική που χρησιμοποιείται σε δίκτυα επικοινωνίας με σκοπό να προωθηθεί μια πληροφορία από ένα πομπό σε ένα δέκτη. Στην μεταγωγή κυκλώματος, για να επικοινωνήσουν δυο σταθμοί αποκαθίσταται μια αποκλειστική φυσική σύνδεση μεταξύ τους, που διατηρείται σταθερή σε όλη την διάρκεια της επικοινωνίας. Αποτελείται από μια σειρά συνδέσεων, μεταξύ των κόμβων του δικτύου. Περιλαμβάνει τρεις φάσεις, την **αποκατάσταση κυκλώματος**, τη **μεταφορά πληροφορίας** και τον **τερματισμό κυκλώματος**. Η τεχνική της μεταγωγής κυκλώματος μπορεί να είναι αρκετά αναποτελεσματική. Η χωρητικότητα του τηλεπικοινωνιακού

καναλιού, ένας αρκετά πολύτιμος πόρος ενός δικτύου, αφιερώνεται σε όλη τη διάρκεια της επικοινωνίας των δύο σταθμών, ακόμη κι αν δεν μεταδίδεται πληροφορία.

Μεταγωγή πακέτου

Η μεταγωγή πακέτου (packet switching), είναι μια τεχνική που χρησιμοποιείται σε δίκτυα επικοινωνίας με σκοπό να προωθηθεί μια πληροφορία από ένα πομπό σε ένα δέκτη. Στην μεταγωγή πακέτου, τα προς μετάδοση μηνύματα τεμαχίζονται σε πακέτα μικρού αριθμού bytes. Το τυπικό μέγιστο μήκος πακέτου είναι τα 1000 bytes. Κάθε πακέτο, περιέχει τμήμα της ωφέλιμης πληροφορίας του χρήστη και επιπλέον μια διεύθυνση προορισμού (destination address) κι ένα αριθμό σειράς (sequence number). Κάθε κόμβος του δικτύου, που λέγεται και **κόμβος μεταγωγής πακέτου** (Packet Switching Node, PSN), χρησιμοποιεί τη διεύθυνση προορισμού του πακέτου, για να αποφασίσει σε ποιον κόμβο θα το προωθήσει. Οι αριθμοί σειράς των πακέτων χρησιμοποιούνται από το σταθμό προορισμού, για να ανακατασκευάσει το αρχικό μήνυμα από τα κομμάτια που έχει λάβει μέσα στα πακέτα.

Υπάρχουν δύο μέθοδοι δρομολόγησης των πακέτων σε ένα δίκτυο μεταγωγής πακέτων: το **αυτοδύναμο πακέτο** και το **νοητό κύκλωμα.**

1. **Αυτοδύναμο πακέτο** (**datagram**): Είναι το κάθε πακέτο που ακολουθεί το δικό του δρόμο στο δίκτυο.
2. **Εικονικό κύκλωμα** (**virtual circuit**) : Πριν αρχίσει η ανταλλαγή των πακέτων, επιλέγεται η καλύτερη διαδρομή. Αυτή τη διαδρομή ακολουθούν όλα τα πακέτα και έρχονται ταξινομημένα με τη σειρά που στάλθηκαν.

1.2.6 Σύγκριση μεθόδων μεταγωγής

Κάνοντας σύγκριση των μεθόδων που αναφέραμε προηγουμένως προκύπτουν τα εξής συμπεράσματα:

- Η μεταγωγή κυκλώματος είναι ιδανική μέθοδος για μετάδοση συνεχών σημάτων μεγάλης διάρκειας, π.χ. για μετάδοση φωνής (τηλεφωνικό δίκτυο) και εικόνας. Αυτό οφείλεται στο γεγονός ότι στην περίπτωση αυτή δεν απαιτείται καμία επεξεργασία των σημάτων από τη στιγμή που εγκαθίσταται το κύκλωμα (φυσικό κανάλι). Τέτοιες επεξεργασίες καθυστερούν τη μετάδοση, πράγμα που δεν είναι επιθυμητό για μεγάλα και συνεχή μηνύματα.

• Η μεταγωγή κυκλώματος δεν είναι αποδοτική για μετάδοση μηνυμάτων μικρής διάρκειας και σποραδικής φύσεως. Στην περίπτωση αυτή, ο χρόνος που απαιτείται για να συνδεθούν οι χρήστες για κάθε σύντομη μετάδοση θα ήταν σημαντική επιβάρυνση, ενώ η διατήρηση της σύνδεσης μεταξύ διαδοχικών μεταδόσεων θα σήμαινε σπατάλη ενός μεγάλου ποσοστού της χωρητικότητας της γραμμής. Στη συγκεκριμένη περίπτωση, ενδείκνυται η μεταγωγή πακέτων.

• Η τεχνική εικονικού κυκλώματος, συνδυάζει χαρακτηριστικά των προαναφερθέντων τύπων.

• Όσον αφορά την αξιοπιστία του συστήματος η τεχνική datagram, είναι πολύ καλύτερη, γιατί σε περίπτωση βλάβης (π.χ. καταστροφής ενός κόμβου) το μήνυμα θα φτάσει στον προορισμό του μέσω άλλων εναλλακτικών διαδρομών. Αντίθετα, στη μεταγωγή κυκλώματος, καταστροφή του διαθέσιμου καναλιού θα έχει σαν αποτέλεσμα την απώλεια του μηνύματος. Στη μεταγωγή εικονικού κυκλώματος, υπάρχει μεγάλη πιθανότητα απώλειας του μηνύματος ή ανάγκη επαναμετάδοσης του, αφού σε περίπτωση που καταστραφεί κάποιος κόμβος όλα τα μηνύματα που διέρχονται από αυτόν θα χαθούν.

1.2.7 Πολυπλεξία

Πολυπλεξία (**multiplexing**), είναι η τεχνική που επιτρέπει δεδομένα από πολλές πηγές να μεταδίδονται μέσα από την ίδια γραμμή επικοινωνίας.

Πολυπλέκτης: Συνθέτει (πολυπλέκει), τα δεδομένα από τις n γραμμές εισόδου και τα μεταδίδει μέσα από γραμμή μεγαλύτερης χωρητικότητας.

Αποπολυπλέκτης: Λαμβάνει την πολυπλεγμένη ροή δεδομένων, χωρίζει τα δεδομένα ανάλογα με το κανάλι, στο οποίο ανήκουν και τα οδηγεί στις αντίστοιχες γραμμές εξόδου.

1.3 Διαδίκτυο – Ιστορική εξέλιξη

1.3.1 Διαδίκτυο (Internet) και Παγκόσμιος Ιστός (Web): Δύο Διακριτές έννοιες

Στη γενική του έννοια, **το Διαδίκτυο** είναι ένα παγκόσμιο δίκτυο ηλεκτρονικών υπολογιστών που (δια) συνδέει άλλα δίκτυα. Ο αντίστοιχος αγγλικός όρος Internet προκύπτει από τη σύνθεση των λέξεων inter - network. Στην πιο εξειδικευμένη και περισσότερο χρησιμοποιούμενη μορφή, με τους όρους Διαδίκτυο ή Internet περιγράφεται το παγκόσμιο πλέγμα διασυνδεδεμένων υπολογιστών περιλαμβανομένων και των

υπηρεσιών και πληροφοριών που παρέχει στους χρήστες του. Οι χρήστες του Διαδικτύου μπορούν εύκολα και γρήγορα να περιηγηθούν σε μια τεράστια βάση πληροφοριών, να αποστείλουν και να λάβουν αρχεία, να κάνουν χρήση της ηλεκτρονικής αλληλογραφίας, και γενικά να χρησιμοποιήσουν ένα πλήθος υπηρεσιών που έχουν στη διάθεση τους. Το Διαδίκτυο χρησιμοποιεί τη μεταγωγική μετάδοση πακέτων (packet switching) και το βασικό πρωτόκολλο επικοινωνίας TCP/IP (Transmission Control Protocol / Internet Protocol). Κάθε πληροφορία που ταξιδεύει στο διαδίκτυο, διακινείται μέσω μιας ποικιλίας από «γλώσσες» γνωστές ως πρωτόκολλα.

Ο Παγκόσμιος Ιστός (World Wide Web ή WWW ή Web ή Παγκόσμιας εμβέλειας ιστός ή και απλά Ιστός) είναι ένα κατανεμημένο πληροφοριακό σύστημα οργάνωσης και πρόσβασης πληροφοριών που υλοποιεί τις βασικές αρχές οργάνωσης του υπερκειμένου. Ως πληροφοριακό σύστημα παρέχει ένα συγκεκριμένο μοντέλο δεδομένων το οποίο βασίζεται σε κόμβους και υπερσυνδέσμους. Δημιουργήθηκε από τον Tim Berners-Lee στα τέλη της δεκαετίας του 1980 και απέκτησε ευρεία διάδοση στα μέσα της δεκαετίας του 1990. Η επίδραση του σε σχεδόν όλες τις πτυχές της ανθρώπινης δραστηριότητας υπήρξε τόσο μεγάλη που θεμελίωσε την ψηφιακή επανάσταση στον 20^{ο} αιώνα.

Ο όρος Παγκόσμιος Ιστός συνήθως θεωρείται συνώνυμο του όρου διαδίκτυο, παρόλο που αποτελούν δύο διακριτές έννοιες. Ο Παγκόσμιος Ιστός είναι ένα μοντέλο διαμοίρασης πληροφορίας (σε οποιαδήποτε ψηφιακή μορφή, αλλά κυρίως σε HTML σελίδες) που χρησιμοποιεί το Διαδίκτυο ως υποδομή για να παρέχει κατανεμημένη οργάνωση και πρόσβαση των πληροφοριών. Για τη διακίνηση της πληροφορίας ο Ιστός χρησιμοποιεί το HTTP πρωτόκολλο, που είναι μια μόνο από τις <<γλώσσες>> που μιλιούνται στο Διαδίκτυο. Χωρίς το διαδίκτυο και τις υπηρεσίες που αυτό παρέχει , ο Παγκόσμιος Ιστός δεν μπορεί να λειτουργήσει, αλλά από την άλλη μεριά ο Ιστός αποτελεί το μεγαλύτερο, το δημοφιλέστερο και το ταχύτερα αναπτυσσόμενο κομμάτι του Διαδικτύου.

1.3.2 Ιστορική Αναδρομή

Οι πρώτες απόπειρες για την δημιουργία ενός διαδικτύου ξεκίνησαν στις ΗΠΑ κατά την διάρκεια του ψυχρού πολέμου. Η Ρωσία είχε ήδη στείλει στο διάστημα τον δορυφόρο Σπούτνικ 1 (Sputnik 1) κάνοντας τους Αμερικανούς να φοβούνται όλο και περισσότερο για την ασφάλεια της χώρας τους. Θέλοντας λοιπόν να προστατευτούν από μια πιθανή πυρηνική επίθεση των Ρώσων δημιούργησαν την υπηρεσία προηγμένων

αμυντικών ερευνών ARPA (Advanced Research Project Agency) γνωστή ως DARPA (Defense Advanced Research Projects Agency) στις μέρες μας. Αποστολή της συγκεκριμένης υπηρεσίας ήταν να βοηθήσει τις στρατιωτικές δυνάμεις των ΗΠΑ να αναπτυχθούν τεχνολογικά και να δημιουργηθεί ένα δίκτυο επικοινωνίας το οποίο θα μπορούσε να επιβιώσει σε μια ενδεχόμενη πυρηνική επίθεση.

Το αρχικό θεωρητικό υπόβαθρο δόθηκε από τον Τζ. Λικλάιντερ (Joseph Carl Robnett Licklider *)* που ανέφερε σε συγγράμματά του το «γαλαξιακό δίκτυο». Η θεωρία αυτή υποστήριζε την ύπαρξη ενός δικτύου υπολογιστών που θα ήταν συνδεδεμένοι μεταξύ τους και θα μπορούσαν να ανταλλάσσουν γρήγορα πληροφορίες και προγράμματα. Το επόμενο θέμα που προέκυπτε ήταν ότι το δίκτυο αυτό θα έπρεπε να ήταν αποκεντρωμένο έτσι ώστε ακόμα κι αν κάποιος κόμβος του δεχόταν επίθεση να υπήρχε δίοδος επικοινωνίας για τους υπόλοιπους υπολογιστές. Τη λύση σε αυτό έδωσε ο Πωλ Μπάραν (Paul Baran) με τον σχεδιασμό ενός κατανεμημένου δικτύου επικοινωνίας που χρησιμοποιούσε την ψηφιακή τεχνολογία. Πολύ σημαντικό ρόλο έπαιξε και η θεωρία ανταλλαγής πακέτων του Λέοναρντ Κλαίηνροκ (Leonard Kleinrock), που υποστήριζε ότι πακέτα πληροφοριών που θα περιείχαν την προέλευση και τον προορισμό τους μπορούσαν να σταλούν από έναν υπολογιστή σε έναν άλλο.

Στηριζόμενο λοιπόν σε αυτές τις τρεις θεωρίες, δημιουργήθηκε το πρώτο είδος διαδικτύου γνωστό ως ARPANET. Εγκαταστάθηκε και λειτούργησε για πρώτη φορά το 1969 με 4 κόμβους μέσω των οποίων συνδέονται 4 μίνι υπολογιστές, του πανεπιστημίου της Καλιφόρνια στην Σάντα Μπάρμπαρα, του πανεπιστημίου της Καλιφόρνια στο Λος Άντζελες, το SRI στο Στάνφορντ και το πανεπιστήμιο της Γιούτα. Η ταχύτητα του δικτύου έφθανε τα 50 kbps και έτσι επιτεύχθηκε η πρώτη dial up σύνδεση μέσω γραμμών τηλεφώνου. Μέχρι το 1972 οι συνδεδεμένοι στο ARPANET υπολογιστές έχουν φτάσει τους 23, οπότε και εφαρμόζεται για πρώτη φορά το σύστημα διαχείρισης ηλεκτρονικού ταχυδρομείου (e-mail).

Παράλληλα δημιουργήθηκαν και άλλα δίκτυα, τα οποία χρησιμοποιούσαν διαφορετικά πρωτόκολλα (όπως το x.25 και το UUCP) τα οποία συνδέονταν με το ARPANET. Το πρωτόκολλο που χρησιμοποιούσε το ARPANET ήταν το NCP (Network Control Protocol), το οποίο, όμως, είχε το μειονέκτημα ότι λειτουργούσε μόνο με συγκεκριμένους τύπους υπολογιστών. Έτσι, δημιουργήθηκε η ανάγκη στις αρχές του 1970 για ένα πρωτόκολλο που θα ένωνε όλα τα δίκτυα που είχαν δημιουργηθεί μέχρι τότε.

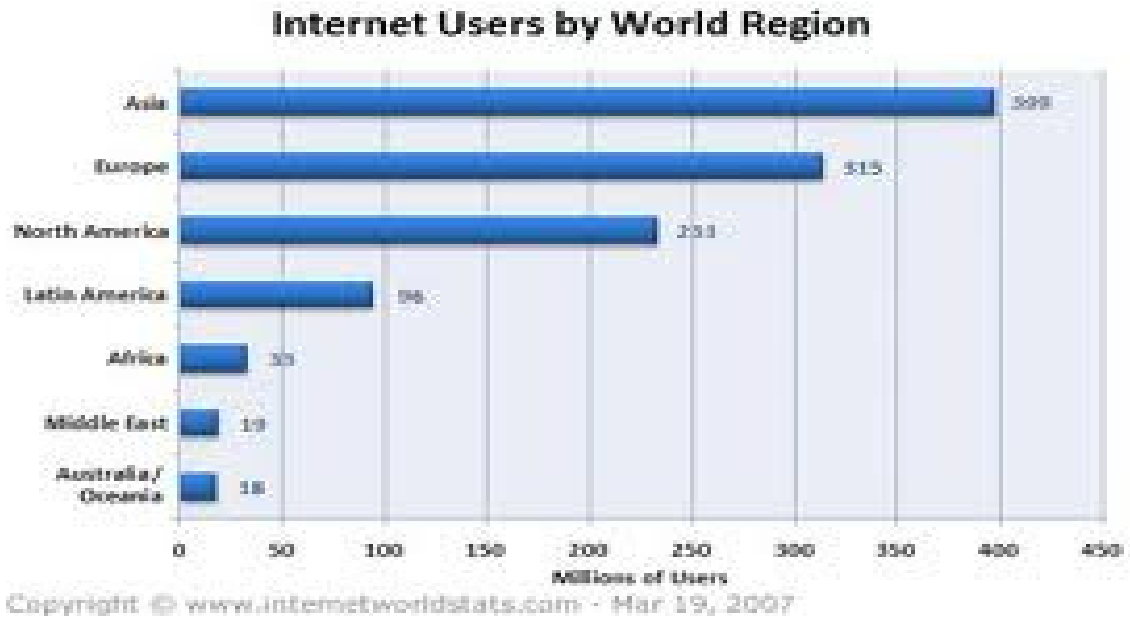
Το 1974 λοιπόν, δημοσιεύεται η μελέτη των Βιντ Σερφ (Vint Cerf) και Μπομπ Κάαν (Bob Kahn) από την οποία προέκυψε το πρωτόκολλο TCP (Transmission Control Protocol) που αργότερα το 1978 έγινε TCP/IP, προσετέθη δηλαδή το Internet Protocol (IP), ώσπου το 1983 έγινε το μοναδικό πρωτόκολλο που ακολουθούσε το ARPANET.

Το 1984 υλοποιείται το πρώτο DNS (Domain Name System) σύστημα στο οποίο καταγράφονται 1000 κεντρικοί κόμβοι και οι υπολογιστές του διαδικτύου πλέον αναγνωρίζονται από διευθύνσεις κωδικοποιημένων αριθμών. Ένα ακόμα σημαντικό βήμα στην ανάπτυξη του Διαδικτύου έκανε το Εθνικό Ίδρυμα Επιστημών (National Science Foundation, NSF) των ΗΠΑ, το οποίο δημιούργησε την πρώτη διαδικτυακή πανεπιστημιακή ραχοκοκαλιά (backbone), το NSFNet, το 1986. Ακολούθησε η ενσωμάτωση άλλων σημαντικών δικτύων, όπως το Usenet, το Fidonet και το Bitnet.

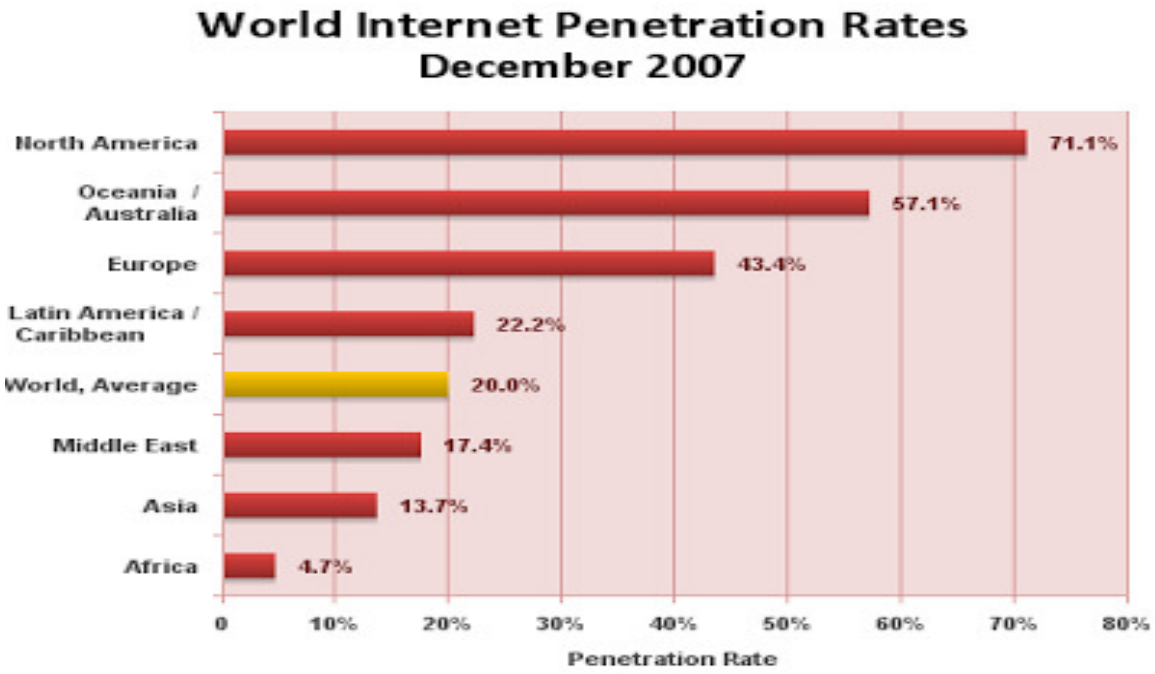
Ο όρος Διαδίκτυο - Internet ξεκίνησε να χρησιμοποιείται ευρέως την εποχή που συνδέθηκε το APRANET με το NSFNet και Internet σήμαινε οποιοδήποτε δίκτυο χρησιμοποιούσε TCP/IP. Η μεγάλη άνθιση του Διαδικτύου όμως, ξεκίνησε με την εφαρμογή της υπηρεσίας του Παγκόσμιου Ιστού από τον Tim Berners-Lee στο ερευνητικό ίδρυμα CERN το 1989, το οποίος είναι στην ουσία, η "πλατφόρμα", η οποία κάνει εύκολη την πρόσβαση στο Internet, ακόμα και στη μορφή που είναι γνωστό σήμερα.

1.3.3 Η σημερινή κατάσταση με αριθμούς

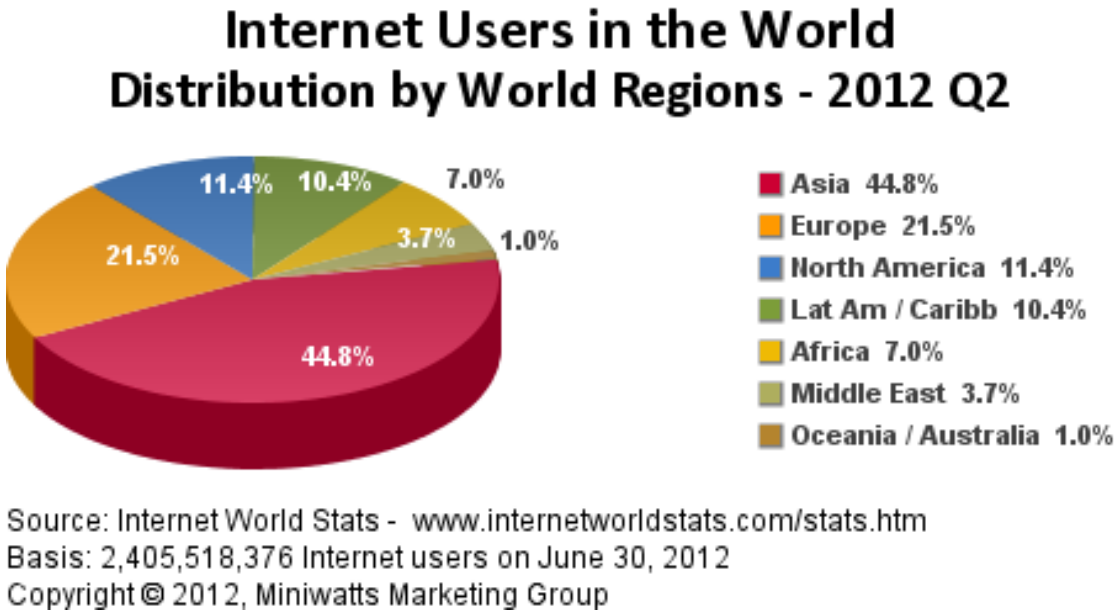
Στις εικόνες που ακολουθούν παρουσιάζεται η σημερινή κατάσταση με αριθμούς.



Εικόνα 7: Πλήθος χρηστών ανά περιοχή



Εικόνα 8: Ποσοστό χρηστών Internet ανά περιοχή



Εικόνα 9: Ποσοστό χρηστών Internet σε παγκόσμιο επίπεδο

1.4 Βιβλιογραφία & πηγές

Βιβλία

[1] Andrew S. Tanenbaum Τέταρτη Αμερικάνικη Έκδοση <<Δίκτυα Υπολογιστών>>

[2] Σημειώσεις Θεωρίας Προγραμματισμός Διαδικτύου, Δρ. Χριστοδούλου Σωτήριος

Links

[1] http://el.wikipedia.org/wiki/Δίκτυο Υπολογιστών

[2] http://el.wikipedia.org/wiki/Διαδίκτυο

[3] http://www.cnc.uom.gr

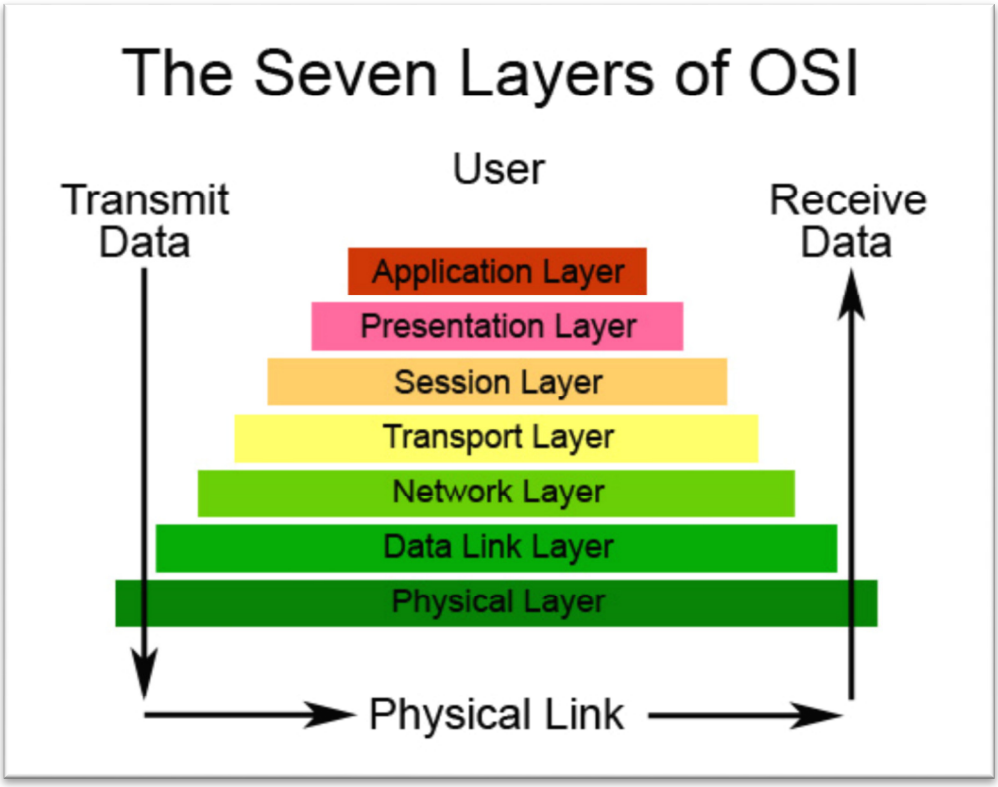
[4] http://www.ekoletsou.gr/pdfFiles/NETWORKS2.pdf

ΚΕΦΑΛΑΙΟ 2: ΔΟΜΗ ΕΠΙΠΕΔΩΝ OSI

2.1 Εισαγωγή

Το μοντέλο OSI (Open Systems Interconnection) αποτελεί ένα εργαλείο αναφοράς με σκοπό την κατανόηση της ανταλλαγής δεδομένων μεταξύ οποιωνδήποτε δύο δικτυακών συστημάτων. Διαχωρίζει τις επικοινωνιακές διεργασίες σε εφτά επίπεδα όπως φαίνεται και στην Εικόνα 10. Κάθε επίπεδο εκτελεί συγκεκριμένες λειτουργίες για την υποστήριξη των από πάνω επιπέδων και ταυτόχρονα παρέχει υπηρεσίες στα από κάτω επίπεδα. Τα τρία χαμηλότερα επίπεδα εστιάζουν στο να μεταβιβάζουν τα δεδομένα από το δίκτυο στο τελικό σύστημα. Τα τέσσερα ανώτερα επίπεδα υπεισέρχονται για την ολοκλήρωση της διεργασίας στο τελικό σύστημα. Ένα μοντέλο δικτύου προσφέρει τα γενικά μέσα για τον διαχωρισμό των δικτυακών λειτουργιών των υπολογιστών σε πολλαπλά επίπεδα. Κάθε ένα από αυτά τα επίπεδα παρέχει δυνατότητες στα παρακάτω επίπεδα και υποστηρίζει τα από πάνω επίπεδα. Ένα τέτοιο μοντέλο, διαβαθμισμένης λειτουργικότητας, καλείται στοίβα πρωτοκόλλων ή σουίτα πρωτοκόλλων. Το μοντέλο ορίζεται από το στάνταρντ 7498-1 του οργανισμού ISO (International Organization for Standardization). Επιτρέπει τη συνεργασία των στοιχείων ενός δικτύου ανεξάρτητα με το ποια πρωτόκολλα χρησιμοποιούνται και από ποιους κατασκευαστές υπολογιστών υποστηρίζονται. Τα κύρια πλεονεκτήματα του μοντέλου OSI περιλαμβάνουν τα ακόλουθα.

- Βοηθάει τους χρήστες να κατανοήσουν το δίκτυο συνολικά.
- Βοηθάει τους χρήστες να κατανοήσουν την συνεργασία μεταξύ του hardware και του software.
- Διευκολύνει την επίλυση προβλημάτων χωρίζοντας το δίκτυο σε διαχειρίσιμα τμήματα.
- Διευκρινίζει τους όρους με τους οποίους οι ειδικοί μπορούν να συγκρίνουν τις βασικές λειτουργικές σχέσεις στα διαφορετικά δίκτυα.
- Βοηθά τους χρήστες να καταλάβουν νέες τεχνολογίες καθώς αυτές αναπτύσσονται.
- Ενισχύει την λειτουργικότητα των προϊόντων.



Εικόνα 10: Τα εφτά επίπεδα του μοντέλου OSI

2.2 Επίπεδο 1: Φυσικό Επίπεδο (Physical Layer)

Το φυσικό επίπεδο (**Physical Layer**) είναι το χαμηλότερο επίπεδο της ιεραρχίας όπως απεικονίζεται και στην Εικόνα 10. Το επίπεδο αυτό προδιαγράφει τις μηχανικές, ηλεκτρικές και χρονικές διασυνδέσεις με το δίκτυο. Σε αυτές περιλαμβάνονται οι σχηματισμοί των ακίδων, οι επιτρεπτές τάσεις, οι προδιαγραφές των καλωδίων κλπ. Η μετάδοση μπορεί να γίνει μέσω των τριών ειδών που υπάρχουν: τα κατευθυνόμενα (χάλκινα σύρματα και οπτικές ίνες), ασύρματα (επίγεια ραδιοκύματα) και τα δορυφορικά. Οι κύριες λειτουργίες του φυσικού επιπέδου είναι:

- **Ο καθορισμός των χαρακτηριστικών του υλικού:** Καθορίζει τα μηχανικά και ηλεκτρικά χαρακτηριστικά της διασύνδεσης του σταθμού εργασίας με το μέσο μετάδοσης. Έτσι καθορίζει τον τύπο των συνδέσεων που χρησιμοποιούνται, το ρόλο του κάθε ακροδέκτη, τις διαστάσεις τους, τις χρησιμοποιούμενες τάσεις, τον τύπο και τα χαρακτηριστικά των καλωδίων, τους συγκεντρωτές, τους επαναλήπτες, τις κάρτες δικτύου κλπ.

- **Η κωδικοποίηση και σηματοδότηση**: Διαμόρφωση και αποδιαμόρφωση των ψηφιακών δεδομένων κατά τη μετάδοση από συσκευή σε συσκευή. Για παράδειγμα, τα ψηφιακά ηλεκτρικά σήματα μπορεί να ταξιδέψουν ως αναλογικά σε χάλκινο καλώδιο, μετά σαν φως σε μία οπτική ίνα, μετά να μεταδοθούν από ραδιοζεύξη ή δορυφορικά, να μεταδοθούν πάλι αναλογικά σε χάλκινο καλώδιο και να γίνουν ψηφιακά στον παραλήπτη.

- **Εκπομπή και λήψη δεδομένων**:
    - Ανίχνευση φορέα και εντοπισμός συγκρούσεων.
    - Αντιστάθμιση του σήματος, έτσι ώστε να εξασφαλιστούν αξιόπιστες συνδέσεις και να διευκολυνθεί η πολυπλεξία.
    - Συγχρονισμός των bit σε σύγχρονες σειριακές επικοινωνίες.
    - Έναρξη και τερματισμός της ηλεκτρικής σύνδεσης μιας μετάδοσης.
    - Συμμετοχή σε διαδικασίες, όπου οι επικοινωνιακές συσκευές εξυπηρετούν πολλούς χρήστες (πολυπλεξία). Επιλύονται προβλήματα προτεραιότητας πρόσβασης και ελέγχου ροής δεδομένων.

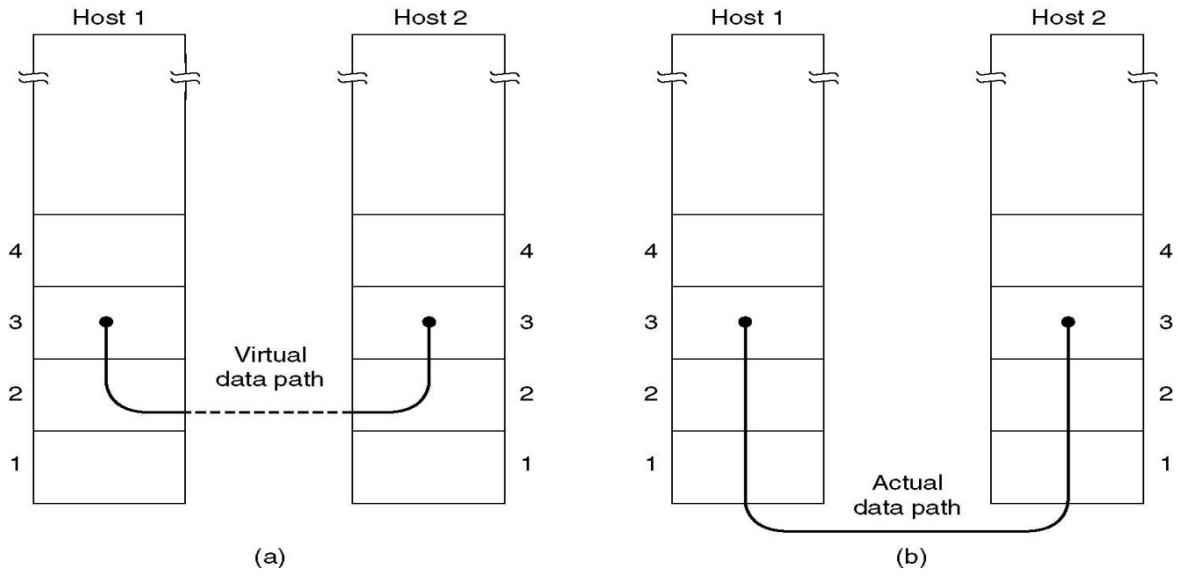
- **Τοπολογία και φυσικός σχεδιασμός του δικτύου:** Το φυσικό επίπεδο είναι η βάση όλων των δικτύων. Οι τεχνολογίες που χρησιμοποιεί βρίσκονται στο χαμηλότερο επίπεδο και ασχολούνται με τα 0 και 1 που αποστέλλονται στο δίκτυο. Συσκευές διασύνδεσης που χρησιμοποιούν το φυσικό επίπεδο είναι οι επαναλήπτες, οι πομποδέκτες και οι συγκεντρωτές. Το επίπεδο αυτό δεν έχει καμία γνώση για το περιεχόμενο του μηνύματος, απλώς παίρνει τα δεδομένα που του έρχονται από το $2^{ο}$ επίπεδο τα μετατρέπει σε bit και τα εκπέμπει στην συσκευή διασύνδεσης, η οποία με την σειρά της τα μετατρέπει στην κατάλληλη μορφή για το μέσο μετάδοσης και τα εκπέμπει στην έξοδο της.

2.3 Επίπεδο 2: Επίπεδο Συνδέσμου Μετάδοσης Δεδομένων (Data Link Layer - DLL)

Το επίπεδο συνδέσμου μετάδοσης δεδομένων (**Data Link Layer - DLL**) είναι το δεύτερο επίπεδο του μοντέλου δικτύωσης OSI και ο στόχος του είναι να παρέχει υπηρεσίες στο επίπεδο δικτύου, αξιοποιώντας τις υπηρεσίες του φυσικού επιπέδου. Το DLL μπορεί να υλοποιεί διάφορες λειτουργίες και σε αυτές περιλαμβάνονται οι ακόλουθες:

1. Παροχή μιας καλά ορισμένης διασύνδεσης υπηρεσίας στο επίπεδο δικτύου.
1. Αντιμετώπιση των σφαλμάτων μετάδοσης.
2. Ρύθμιση των δεδομένων έτσι ώστε αργοί παραλήπτες να μην κατακλύζονται από τους γρήγορους αποστολείς.

Για να πετύχει τους στόχους αυτούς, το DLL παίρνει τα δεδομένα που δέχεται από το επίπεδο δικτύου και τα ενθυλακώνει σε **πλαίσια** (**frames**) προς μετάδοση. Κάθε πλαίσιο περιέχει μία κεφαλίδα πλαισίου, ένα πεδίο ωφέλιμου φορτίου μέσα στο οποίο περιέχονται τα δεδομένα και ένα επίμετρο (trailer) πλαισίου. Η διαχείριση πλαισίων είναι ο πυρήνας του επιπέδου συνδέσμου μετάδοσης δεδομένων. Η βασική του υπηρεσία είναι η μεταφορά δεδομένων από το επίπεδο δικτύου της μηχανής προέλευσης στο επίπεδο δικτύου της μηχανής προορισμού όπως απεικονίζεται στην Εικόνα 11.



Εικόνα 11: (a) Εικονική διαδρομή δεδομένων, (b) Πραγματική διαδρομή δεδομένων

Το επίπεδο συνδέσμου μετάδοσης δεδομένων παρέχει τρεις τρόπους λειτουργίας ως προς την αποστολή των πλαισίων. Οι τρόποι αυτοί αναλύονται παρακάτω:

1. **Ασυνδεσμική υπηρεσία χωρίς επιβεβαιώσεις**: Η υπηρεσία αυτή συνίσταται στο να βάζουμε τη μηχανή προέλευσης να στέλνει αυτόνομα πλαίσια στην μηχανή προορισμού χωρίς να ζητάμε από τη μηχανή προορισμού να επιβεβαιώνει τη λήψη τους. Δεν εγκαθιδρύεται κάποια λογική σύνδεση. Αν χαθεί κάποιο πλαίσιο λόγω θορύβου γραμμής, δεν γίνεται κάποια απόπειρα ανίχνευσης ή επιδιόρθωσης της απώλειας από το DLL. Αυτή η κατηγορία υπηρεσιών είναι κατάλληλη για περιπτώσεις όπου ο ρυθμός σφαλμάτων είναι πολύ χαμηλός, άρα η επανόρθωση τους αφήνεται στα ανώτερα επίπεδα, και για κυκλοφορία πραγματικού χρόνου στην οποία τα καθυστερημένα δεδομένα δεν έχουν λόγο για επανάληψη της αποστολής.
2. **Ασυνδεσμική υπηρεσία με επιβεβαιώσεις:** Όταν παρέχεται αυτή η υπηρεσία πάλι δεν χρησιμοποιούνται λογικές συνδέσεις, αλλά κάθε πλαίσιο που στέλνεται επιβεβαιώνεται αυτόνομα. Με αυτό τον τρόπο ο αποστολέας ενημερώνεται εάν ένα πλαίσιο έχει φτάσει σωστά, αν το πλαίσιο δεν φτάσει μέσα σε ένα ορισμένο χρονικό διάστημα, μπορεί να σταλεί ξανά. Η υπηρεσία αύτη είναι χρήσιμη στα μη αξιόπιστα κανάλια, όπως αυτά των ασύρματων συστημάτων.
3. **Συμδεσμοστρεφής υπηρεσία με επιβεβαιώσεις:** Με την υπηρεσία αυτή, πριν μεταδοθούν οποιαδήποτε δεδομένα οι μηχανές προέλευσης και προορισμού εγκαθιδρύουν μια σύνδεση. Κάθε πλαίσιο που στέλνεται μέσω του καναλιού αριθμείται, και το επίπεδο συνδέσμου μετάδοσης δεδομένων εγγυάται ότι κάθε πλαίσιο που στέλνεται θα λαμβάνεται πραγματικά. Επιπλέον, εγγυάται ότι κάθε πλαίσιο θα λαμβάνεται ακριβώς μία φορά, καθώς και ότι όλα τα πλαίσια θα λαμβάνονται με τη σωστή σειρά. Όταν χρησιμοποιείται η συνδεσμοστρεφής υπηρεσία, η μεταφορά περνά από τρεις διακριτές φάσεις. Στην πρώτη φάση γίνεται η εγκαθίδρυση της σύνδεσης, στη δεύτερη γίνεται η πραγματική μετάδοση ενός ή περισσότερων πλαισίων και στη τρίτη, και τελευταία φάση, απελευθερώνεται η σύνδεση, αποδεσμεύοντας τις μεταβλητές, τις περιοχές προσωρινής αποθήκευσης και όποιους άλλους πόρους χρησιμοποιούνται για τη διατήρηση της σύνδεσης.

Αν και η βασική υπηρεσία του DLL είναι να μεταφέρει τα πακέτα από έναν κόμβο σε έναν γειτονικό κόμβο επάνω σε μια ζεύξη, οι λεπτομέρειες αυτής της υπηρεσίας

υλοποιούνται από ένα πρωτόκολλο επιπέδου ζεύξης και πιθανές υπηρεσίες που μπορεί να προσφέρει περιλαμβάνουν:

Πλαισίωση

Για να παρέχει τις υπηρεσίες του στο επίπεδο δικτύου, το DLL πρέπει να χρησιμοποιήσει τις υπηρεσίες που του παρέχονται από το φυσικό επίπεδο. Αυτό που κάνει το φυσικό επίπεδο είναι να δέχεται μια ανεπεξέργαστη ροη bit και να προσπαθεί να τη μεταδώσει στο προορισμό της. Αυτή η ροή δεν είναι εγγυημένο ότι δεν περιέχει σφάλματα. Είναι θέμα του DLL να ανιχνεύσει και, εφόσον απαιτείται, να διορθώσει τα σφάλματα. Η συνηθισμένη προσέγγιση είναι να τεμαχίζεται η ροη των bit σε διακριτά πλαίσια και να υπολογίζεται ένα άθροισμα ελέγχου (**checksum**) για κάθε πλαίσιο. Όταν το πλαίσιο φτάσει στον προορισμό του υπολογίζεται ξανά το άθροισμα ελέγχου και αν διαφέρει από εκείνο που περιέχεται στο πλαίσιο, το DLL γνωρίζει ότι έχει συμβεί κάποιο σφάλμα και κάνει κάποιες ενέργειες για να το αντιμετωπίσει. Υπάρχουν πολλές μέθοδοι οι οποίοι είναι υπεύθυνοι για τον τεμαχισμό της ροής των bit σε πλαίσια. Οι τέσσερις βασικοί είναι:

- **Μετρητές χαρακτήρων**, χρησιμοποιεί ένα πεδίο στην επικεφαλίδα, το οποίο προσδιορίζει το πλήθος των χαρακτήρων στο πλαίσιο. Όταν το DLL στον προορισμό βλέπει αυτόν το μετρητή χαρακτήρων, καταλαβαίνει πόσοι χαρακτήρες ακολουθούν και κατά συνέπεια εντοπίζει που βρίσκεται το τέλος του πλαισίου. Το βασικό πρόβλημα αυτής της μεθόδου είναι ότι αν γίνει κάποιο σφάλμα μετάδοσης επάνω στο μετρητή χαρακτήρων ο προορισμός θα χάσει το συγχρονισμό και δεν θα είναι σε θέση να εντοπίσει την αρχή του επόμενου πλαισίου.

- **Byte σημαίας, με συμπλήρωση byte,** η μέθοδος αυτή παρακάμπτει το πρόβλημα του συγχρονισμού προσθέτοντας στην αρχή και στο τέλος του πλαισίου κάποια ειδικά byte, τα οποία ονομάζονται byte σημαίας (flag byte). Με τον τρόπο αυτό αν ο παραλήπτης χάσει κάποια στιγμή το συγχρονισμό, μπορεί να αναζητήσει το byte σημαίας για να βρει το τέλος του πλαισίου. Στη μέθοδο αυτή εμφανίζεται ένα σοβαρό πρόβλημα όταν μεταδίδονται δυαδικά δεδομένα, γιατί μπορεί εύκολα η ακολουθία των bit του byte σημαίας να υπάρχει στα δεδομένα και έτσι να δημιουργούνται παρεμβολές στην πλαισίωση.

- **Σημαίες αρχής και τέλους, με συμπλήρωση bit,** ένας τρόπος να λυθεί το παραπάνω πρόβλημα είναι να εισάγει το DLL του αποστολέα ένα ειδικό byte διαφυγής

(escape byte ή ESC) πριν από κάθε byte σημαίας το οποίο εμφανίζεται και στα δεδομένα. Το DLL του παραλήπτη απομακρύνει αυτά τα byte πριν παραδώσει τα δεδομένα στο επίπεδο δικτύου.

- **Παραβιάσεις της κωδικοποίησης του φυσικού επιπέδου,** η μέθοδος αυτή εφαρμόζεται μόνο σε δίκτυα όπου η κωδικοποίηση στο φυσικό μέσο εμφανίζει πλεονασμό.

Έλεγχος ροής

Οι κόμβοι σε κάθε πλευρά της ζεύξης έχουν μια περιορισμένη χωρητικότητα καταχώρησης πλαισίων. Αυτό είναι ένα πιθανό πρόβλημα, επειδή ένας κόμβος λήψης μπορεί να δεχθεί πλαίσια μ' έναν ρυθμό ταχύτερο από όσο μπορεί να επεξεργαστεί τα πλαίσια μέσα σε ένα χρονικό διάστημα. Χωρίς τον έλεγχο ροής, ο ενταμιευτής του δέκτη μπορεί να υπερχειλίσει και να χαθούν πλαίσια. Δύο είναι οι προσεγγίσεις που χρησιμοποιούνται συνήθως προκειμένου να αποτραπούν τέτοιες καταστάσεις. Στην πρώτη, τον βασιζόμενο σε ανάδραση έλεγχο ροής (**feedback - based flow control**), ο παραλήπτης επιστρέφει περιοδικά πληροφορίες στον αποστολέα δίνοντας του την άδεια να στείλει περισσότερα δεδομένα ή τουλάχιστον ενημερώνοντας τον σε τη κατάσταση είναι ο παραλήπτης. Στην δεύτερη, τον βασιζόμενο σε ρυθμό έλεγχο ροής (**rate - based flow control**), το πρωτόκολλο έχει έναν ενσωματωμένο μηχανισμό ο οποίος περιορίζει το ρυθμό με τον οποίο οι αποστολείς μπορούν να μεταδίδουν δεδομένα, χωρίς να χρειάζεται ανάδραση από τον παραλήπτη.

Ανίχνευση και διόρθωση σφαλμάτων

Ο δέκτης ενός κόμβου μπορεί να αποφασίσει λανθασμένα ότι ένα bit μέσα σε ένα πλαίσιο είναι μηδέν, ενώ μεταδόθηκε σαν ένα και το αντίστροφο. Τέτοια εσφαλμένα bit εισάγονται από εξασθένηση σήματος και ηλεκτρομαγνητικό θόρυβο. Οι σχεδιαστές δικτύων έχουν αναπτύξει δύο βασικές στρατηγικές για την αντιμετώπιση των σφαλμάτων. Ο ένας τρόπος είναι να περιλαμβάνονται αρκετές πλεονάζουσες πληροφορίες σε κάθε αποστελλόμενη ομάδα δεδομένων, έτσι ώστε ο παραλήπτης να μπορεί να συμπεράνει ποια πρέπει να ήταν τα δεδομένα που μεταδόθηκαν. Ο άλλος τρόπος είναι να περιλαμβάνεται αρκετός πλεονασμός ώστε να μπορεί ο παραλήπτης να συμπεράνει ότι συνέβη ένα σφάλμα, αλλά όχι πιο σφάλμα, έτσι ώστε να μπορεί να ζητά αναμετάδοση των δεδομένων. Η πρώτη στρατηγική χρησιμοποιεί κωδικούς διόρθωσης σφαλμάτων (**error correcting codes**), ενώ η δεύτερη χρησιμοποιεί κωδικούς ανίχνευσης σφαλμάτων (**error detecting**

codes). Σε κανάλια που είναι εξαιρετικά αξιόπιστα είναι οικονομικότερη η χρήση ενός κωδικού ανίχνευσης σφαλμάτων και η αναμετάδοση των λίγων ομάδων που εντοπίζονται ότι είναι εσφαλμένες. Σε κανάλια, όμως στα οποία παρουσιάζονται πολλά σφάλματα, είναι καλύτερα να προστίθεται αρκετός πλεονασμός σε κάθε ομάδα έτσι ώστε ο παραλήπτης να μπορεί να υπολογίσει ποια ήταν η αρχική ομάδα, αντί να απαιτεί αναμετάδοση.

2.4 Επίπεδο 3: Επίπεδο Δικτύου (Network Layer)

Το επίπεδο δικτύου ασχολείται με τη μεταφορά πακέτων από την προέλευση τους μέχρι τον προορισμό τους. Για να φτάσουν τα πακέτα στον προορισμό τους, μπορεί να χρειαστεί πολλά άλματα (**hops**) μέσω ενδιάμεσων δρομολογητών που υπάρχουν στη διαδρομή. Η λειτουργία αυτή είναι σαφώς διαφορετική από εκείνη του επιπέδου συνδέσμου μετάδοσης δεδομένων, το οποίο έχει ως στόχο να μετακινεί απλώς πλαίσια από το ένα άκρο του καναλιού στο άλλο. Έτσι, το επίπεδο δικτύου είναι το κατώτερο επίπεδο που ασχολείται με τη μετάδοση απ' άκρου εις άκρο (end to end). Για να πετύχει τους στόχους του, το επίπεδο δικτύου πρέπει να γνωρίζει την τοπολογία του υποδικτύου επικοινωνίας και να επιλέγει τις κατάλληλες διαδρομές μέσα από αυτό. Θα πρέπει επίσης να προσέχει όταν επιλέγει δρομολόγια, έτσι ώστε να αποφεύγει την υπερφόρτωση κάποιων γραμμών επικοινωνίας και δρομολογητών ενώ άλλοι παραμένουν αδρανείς. Το επίπεδο δικτύου παρέχει υπηρεσίες στο επίπεδο μεταφοράς και αυτές έχουν σχεδιαστεί ακλουθώντας τους παρακάτω στόχους:

1. Οι υπηρεσίες πρέπει να είναι ανεξάρτητες από την τεχνολογία του δρομολογητή.
2. Το επίπεδο μεταφοράς δεν πρέπει να γνωρίζει το πλήθος, τον τύπο και την τοπολογία των υπαρχόντων δρομολογητών.
3. Οι διευθύνσεις δικτύου που διατίθενται στο επίπεδο μεταφοράς πρέπει να χρησιμοποιούν ένα ομοιόμορφο σχέδιο αριθμοδότησης, ακόμα και ανάμεσα σε διαφορετικά LAN και WAN.

Με δεδομένους αυτούς τους στόχους το επίπεδο δικτύου μπορεί να παρέχει συνδεσμοστρεφή ή ασυνδεσμική υπηρεσία. Αν προσφέρεται ασυνδεσμική υπηρεσία, τα πακέτα εισάγονται μεμονωμένα στο υποδίκτυο και δρομολογούνται ανεξάρτητα το ένα από το άλλο και δεν χρειάζεται κάποια εκ των προτέρων συνεννόηση. Στο περιβάλλον αυτό τα πακέτα ονομάζονται αυτοδύναμα πακέτα (**datagrams**) και το υποδίκτυο

ονομάζεται υποδίκτυο αυτοδύναμων πακέτων (**datagram subnet**). Όταν χρησιμοποιείται συνδεσμοστρεφής υπηρεσία, πριν σταλούν οποιαδήποτε πακέτα δεδομένων θα πρέπει να εγκαθιδρυθεί μια διαδρομή από το δρομολογητή προέλευσης μέχρι τον δρομολογητή προορισμού. Αυτή η σύνδεση ονομάζεται εικονικό κύκλωμα ή VC (**virtual circuit**) και το υποδίκτυο ονομάζεται υποδίκτυο εικονικών κυκλωμάτων (**virtual circuit subnet**). Τόσο τα εικονικά κυκλώματα όσο και τα αυτοδύναμα πακέτα έχουν τους υποστηρικτές τους και τους κατήγορους τους. Οι βασικές τους διαφορές παρατίθενται στην Εικόνα 12.

Ζήτημα	**Υποδίκτυο αυτοδύναμων πακέτων**	**Υποδίκτυο εικονικών κυκλωμάτων**
Εγκαθίδρυση σύνδεσης	Δεν χρειάζεται	Απαραίτητη
Διευθυνσιοδότηση	Κάθε πακέτο περιέχει την πλήρη διεύθυνση προέλευσης και προορισμού	Κάθε πακέτο περιέχει ένα μικρό αριθμό εικονικού κυκλώματος
Πληροφορίες κατάστασης	Οι δρομολογητές δεν διατηρούν πληροφορίες κατάστασης για τις συνδέσεις	Κάθε εικονικό κύκλωμα απαιτεί χώρο στους πίνακες δρομολόγησης ανά σύνδεση
Δρομολόγηση	Κάθε πακέτο δρομολογείται ανεξάρτητα	Το δρομολόγιο επιλέγεται όταν εγκαθιδρύεται το κύκλωμα, και όλα τα πακέτα το ακολουθούν
Επιπτώσεις κατάρρευσης δρομολογητών	Καμία, εκτός από τα πακέτα που χάνονται κατά την κατάρρευση	Όλα τα κυκλώματα τα οποία περνούσαν από το δρομολογητή που κατάρρευσε τερματίζονται
Ποιότητα υπηρεσιών	Δύσκολη	Εύκολη, εφόσον μπορούν να εκχωρηθούν προκαταβολικά επαρκείς πόροι για κάθε εικονικό κύκλωμα
Έλεγχος συμφόρησης	Δύσκολη	Εύκολη, εφόσον μπορούν να εκχωρηθούν προκαταβολικά επαρκείς πόροι για κάθε εικονικό κύκλωμα

Εικόνα 12: Σύγκριση υποδικτύων αυτοδύναμων πακέτων και εικονικών κυκλωμάτων

Η κύρια λειτουργία του επιπέδου δικτύου είναι η δρομολόγηση πακέτων από τη μηχανή προέλευσης στη μηχανή προορισμού. Οι αλγόριθμοι επιλογής των δρομολογίων και οι δομές δεδομένων που χρησιμοποιούν είναι ένας σημαντικός τομέας στη σχεδίαση του επιπέδου δικτύου. Ο **αλγόριθμος δρομολόγησης** (**routing algorithm**) είναι το τμήμα λογισμικού του επιπέδου δικτύου που είναι αρμόδιο να αποφασίσει σε ποια γραμμή εξόδου θα μεταδοθεί ένα εισερχόμενο πακέτο. Είναι χρήσιμο να γίνει η διάκριση ανάμεσα στη δρομολόγηση, η οποία είναι η λήψη της απόφασης σχετικά με τα δρομολόγια που θα χρησιμοποιούνται, και της προώθησης, η οποία είναι η ενέργεια που εκτελείται όταν φτάσει ένα πακέτο. Μπορεί να θεωρηθεί ότι ο δρομολογητής έχει εσωτερικά δύο διεργασίες. Η μια αντιμετωπίζει το κάθε πακέτο καθώς φτάνει, αναζητώντας στους

πίνακες δρομολόγησης την εξερχόμενη γραμμή που θα χρησιμοποιήσει για το πακέτο και ονομάζεται **προώθηση** (**forwarding**). Η άλλη διεργασία είναι υπεύθυνη για τη συμπλήρωση και την ενημέρωση των πινάκων δρομολόγησης και αυτό το κάνει ο αλγόριθμος δρομολόγησης. Οι αλγόριθμοι δρομολόγησης μπορούν να ομαδοποιηθούν σε δύο μεγάλες κατηγορίες τους μη προσαρμοστικούς και τους προσαρμοστικούς. Οι μη προσαρμοστικοί αλγόριθμοι δεν βασίζουν τις αποφάσεις δρομολόγησης σε μετρήσεις ή εκτιμήσεις της τρέχουσας κίνησης και τοπολογίας. Αντιθέτως, η επιλογή του δρομολογίου που θα χρησιμοποιηθεί για να φτάσουμε από έναν κόμβο σε έναν άλλο υπολογίζεται προκαταβολικά και μεταφέρεται στους δρομολογητές κατά την εκκίνηση του δικτύου. Αντίθετα, οι προσαρμοστικοί αλγόριθμοι μεταβάλλουν τις αποφάσεις δρομολόγησης έτσι ώστε να αντανακλούν τις αλλαγές στην τοπολογία, και συνήθως και στην κίνηση. Οι προσαρμοστικοί αλγόριθμοι διαφέρουν ως προς το από πού λαμβάνουν τις πληροφορίες τους, ως προς το πότε αλλάζουν τα δρομολόγια και ως προ το μέτρο σύγκρισης που χρησιμοποιείται για τη βελτιστοποίηση. Στα δίκτυα υπολογιστών χρησιμοποιούνται πολλοί αλγόριθμοι δρομολόγησης. Οι βασικοί στατικοί αλγόριθμοι είναι η συντομότερη διαδρομή και η πλημμύρα, ενώ οι βασικοί δυναμικοί αλγόριθμοι είναι η δρομολόγηση με διανύσματα απόστασης και η δρομολόγηση με κατάσταση συνδέσμων. Άλλα σημαντικά θέματα δρομολόγησης είναι η ιεραρχική δρομολόγηση, η δρομολόγηση των εκπομπών, η δρομολόγηση πολυδιανομής, η δρομολόγηση για κινητούς υπολογιστές υπηρεσίας και η δρομολόγηση σε ομότιμα δίκτυα. Στην **ιεραρχική δρομολόγηση** οι δρομολογητές διαιρούνται σε περιφέρειες (regions), με κάθε δρομολογητή να γνωρίζει όλες τις λεπτομέρειες σχετικά με το πώς πρέπει να δρομολογούνται τα πακέτα προς τους προορισμούς μέσα στην περιφέρεια του, χωρίς να γνωρίζει τίποτα για την εσωτερική δομή των άλλων περιφερειών. Η **δρομολόγηση εκπομπών** (broadcast routing) χρησιμοποιείται για να μπορεί μια υπηρεσία να στέλνει μηνύματα προς πολλούς ή προς όλους τους άλλους κόμβους. Για την υλοποίηση αυτής της υπηρεσίας μπορούν να χρησιμοποιηθούν διάφοροι μέθοδοι δρομολόγησης όπως η πλημμύρα, η δρομολόγηση πολλαπλών προορισμών, ο αλγόριθμος εκπομπής με την χρήση του δέντρου απαγωγής και η προώθηση αντίστροφης διαδρομής. Η **δρομολόγηση πολυδιανομής** (multicast routing) χρησιμοποιείται για μπορούν διεργασίες οι οποίες είναι απομακρυσμένες μεταξύ τους να δουλεύουν μαζί σε ομάδες. Απαιτεί κάποια μέθοδο δημιουργίας και καταγραφής ομάδων και κάποια μέθοδο προσχώρησης και αποχώρησης από αυτές. Η **δρομολόγηση για κινητούς υπολογιστές υπηρεσίας** χρησιμοποιείται για υπολογιστές υπηρεσίας οι οποίοι λειτουργούν εν κινήσει

και θέλουν να διατηρούν τις συνδέσεις τους καθώς μετακινούνται. Τα υποδίκτυα μπορεί να υποστούν εύκολα συμφόρηση, οπότε αυξάνεται η καθυστέρηση και μειώνεται η διεκπεραιωτική ικανότητα (throughput) για τα πακέτα. Μερικές τεχνικές αποφυγής της συμφόρησης είναι η πολιτική αναμετάδοσης, οι κρυφές μνήμες και ο έλεγχος ροής. Αν όμως εμφανιστεί συμφόρηση υπάρχουν και τρόποι αντιμετώπισης της όπως: η επιστροφή πακέτων αποπνιγμού και η αποβολή φορτίου. Εκτός από την αντιμετώπιση της συμφόρησης, υπάρχει κ η προσπάθεια επίτευξης κάποιας συμφωνημένης ποιότητας υπηρεσιών. Οι μέθοδοι που μπορεί να χρησιμοποιηθούν για το σκοπό αυτόν περιλαμβάνουν την προσωρινή αποθήκευση στον πελάτη, τη μορφοποίηση κίνησης, τη δέσμευση πόρων και τον έλεγχο αποδοχής. Οι προσεγγίσεις που έχουν σχεδιαστεί για να παρέχουν καλή ποιότητα υπηρεσιών περιλαμβάνουν τις ενοποιημένες υπηρεσίες, τις διαφοροποιημένες υπηρεσίες και το MPLS.

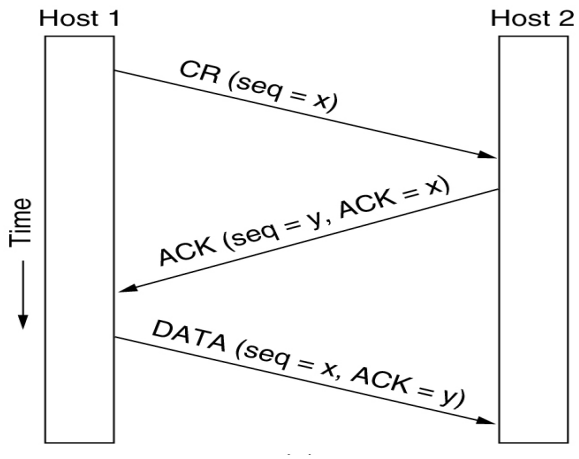
2.5 Επίπεδο 4: Επίπεδο Μεταφοράς (Transport Layer)

Το επίπεδο μεταφοράς δεν είναι απλώς ένα ακόμη επίπεδο, είναι η καρδιά ολόκληρης της ιεραρχίας των πρωτοκόλλων. Ο στόχος του επιπέδου μεταφοράς είναι να παρέχει αποδοτικές, αξιόπιστες, και οικονομικές ως προς το κόστος υπηρεσίες στους χρήστες του, οι οποίοι συνήθως είναι διεργασίες του επιπέδου εφαρμογών. Για να πετύχει το στόχο αυτό, το επίπεδο μεταφοράς αξιοποιεί τις υπηρεσίες που παρέχονται από το επίπεδο δικτύου. Το υλικό/λογισμικό του επιπέδου μεταφοράς που κάνει αυτή την δουλειά ονομάζεται οντότητα μεταφοράς. Όπως υπάρχουν δύο τύποι υπηρεσίας δικτύου, συνδεσμοστρεφής και ασυνδεσμική, έτσι υπάρχουν και δύο τύποι υπηρεσιών υπηρεσίας μεταφοράς. Η συνδεσμοστρεφής υπηρεσία μεταφοράς είναι σε πολλά σημεία παρόμοια με την συνδεσμοστρεφής υπηρεσία δικτύου. Και στις δύο περιπτώσεις οι συνδέσεις έχουν τρεις φάσεις: εγκαθίδρυση, μεταφορά δεδομένων, αποσύνδεση. Η διευθυνσιοδότηση και ο έλεγχος ροής είναι επίσης παρόμοιοι και στα δύο επίπεδα. Η μεγάλη διαφορά στην υπηρεσία του επιπέδου μεταφοράς σε σχέση με το επίπεδο δικτύου είναι ότι ο κώδικας μεταφοράς εκτελείται πλήρως στις μηχανές των χρηστών, ενώ ο κώδικας δικτύου εκτελείται κυρίως στους δρομολογητές. Το επίπεδο μεταφοράς έχει ως κύρια λειτουργία τη λήψη και τον τεμαχισμό των δεδομένων του επιπέδου συνόδου και το πέρασμά τους στο επίπεδο δικτύου με επιτυχία. Επίσης, κάθε ενέργεια πρέπει να γίνεται έτσι ώστε τα ανώτερα στρώματα να απομονώνονται από τα κατώτερα, για την αποφυγή τυχόν αλλαγών

στο υλικό. Το επίπεδο μεταφοράς δημιουργεί μία σύνδεση ανάμεσα στο επίπεδο συνόδου και στο επίπεδο δικτύου. Ανάλογα με το throughput, μπορεί να υφίστανται και περισσότερες συνδέσεις, ή να γίνεται πολυπλεξία (multiplexing) για ελάττωση του κόστους. Καθορίζει επίσης ποια υπηρεσία προσφέρει το στρώμα συνόδου. Η πιο σημαντική είναι η υπηρεσία ενός διαύλου σημείου προς σημείο (point to point), ενώ υπάρχουν και άλλες υπηρεσίες, όπως η μεταφορά μηνυμάτων χωρίς εγγύηση ορθής λήψης ή η πολλαπλή εκπομπή μηνυμάτων. Στο σημείο αυτό, αξίζει να σημειωθεί ότι το επίπεδο μεταφοράς είναι ένα επίπεδο από άκρο σε άκρο (end to end) από την αφετηρία στον προορισμό. Το επίπεδο μεταφοράς είναι υπεύθυνο για το σχηματισμό και τον τερματισμό των συνδέσεων ενός δικτύου, καθώς και τη ρύθμιση της ροής της πληροφορίας ανάμεσα στους hosts, έτσι ώστε ένας αργός host να μην «πνίγεται» από έναν γρήγορο.

2.5.1 Εγκαθίδρυση συνδέσεων

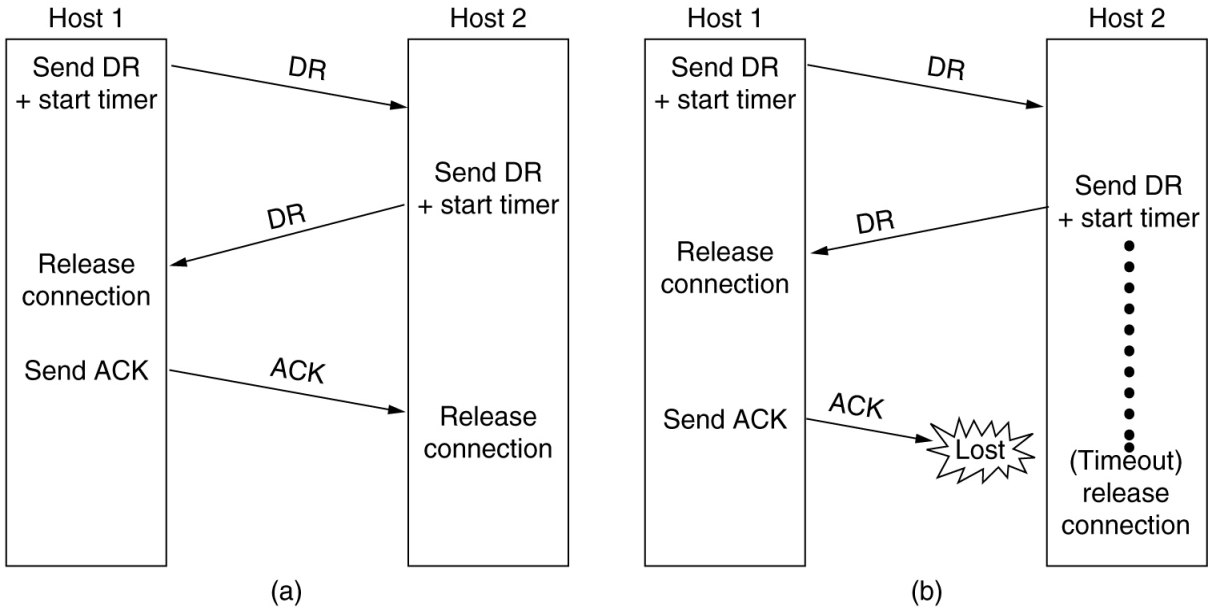
Για την εγκαθίδρυση συνδέσεων στο επίπεδο μεταφοράς χρησιμοποιείται το πρωτόκολλο της τριπλής χειραψίας (three-way handshake). Η κανονική διαδικασία εγκαθίδρυσης όταν η σύνδεση ξεκινά από έναν υπολογιστή υπηρεσίας φαίνεται στην Εικόνα 13. Ο υπολογιστής υπηρεσίας επιλέγει έναν αριθμό ακολουθίας x και στέλνει σε έναν άλλο υπολογιστή υπηρεσίας μια TPDU ΑΙΤΗΣΗ ΣΥΝΔΕΣΗΣ που περιέχει τον αριθμό αυτόν. Ο δεύτερος υπολογιστής υπηρεσίας απαντά με μια TPDU επιβεβαίωσης του x, η οποία ανακοινώνει επιπλέον το δικό της αρχικό αριθμό ακολουθίας y. Τέλος, ο πρώτος υπολογιστής υπηρεσίας επιβεβαιώνει την επιλογή του αρχικού αριθμού ακολουθίας του δεύτερου υπολογιστή υπηρεσίας στην πρώτη TPDU δεδομένων που στέλνει.



Εικόνα 13: Εγκαθίδρυση σύνδεσης με τριπλής χειραψία σε κανονική λειτουργία

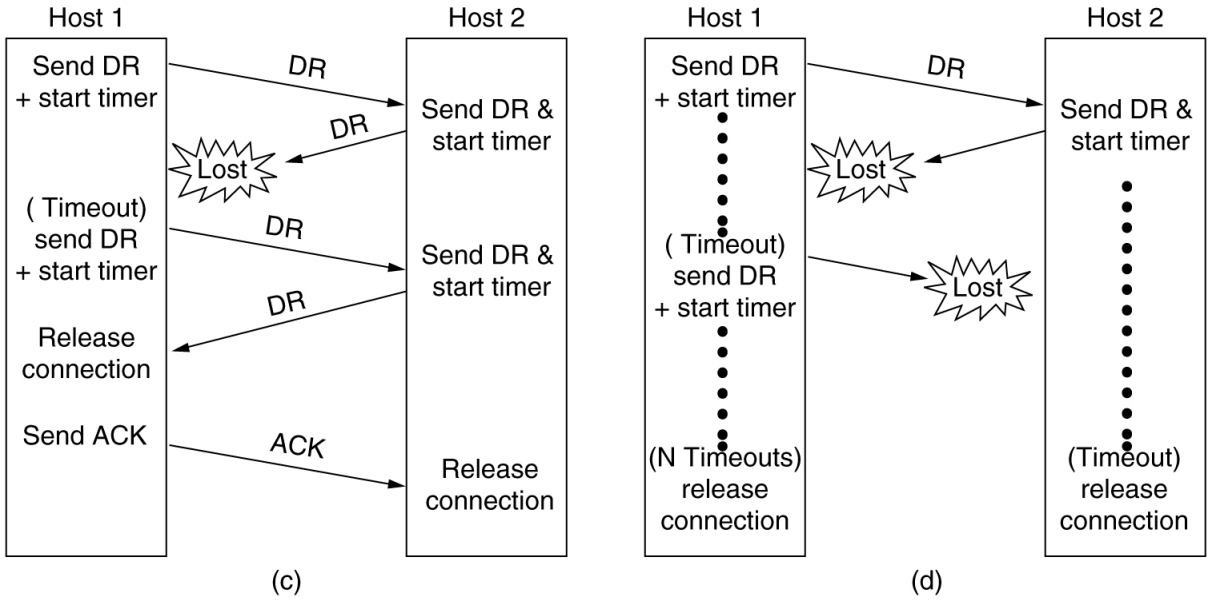
2.5.2 Αποδέσμευση συνδέσεων

Η αποδέσμευση μιας σύνδεσης είναι ευκολότερη από την εγκαθίδρυση μιας σύνδεσης. Υπάρχουν δύο είδη τερματισμού συνδέσεων: ασύμμετρη και συμμετρική αποδέσμευση. Η ασύμμετρη είναι ο τρόπος που λειτουργεί το τηλεφωνικό σύστημα: όταν η μια πλευρά κατεβάζει το τηλέφωνο, η σύνδεση τερματίζεται. Η συμμετρική αποδέσμευση μεταχειρίζεται τη σύνδεση σαν να ήταν δύο ξεχωριστές μονόδρομες συνδέσεις και απαιτεί να αποδεσμευτεί χωριστά η κάθε μια τους. Οι εικόνες 14 και 15 απεικονίζουν τέσσερα σενάρια αποδέσμευσης που χρησιμοποιούν την τριπλή χειραψία. Αν και το πρωτόκολλο αυτό δεν είναι αλάνθαστο, είναι συνήθως επαρκές. Στην Εικόνα 14 (a) βλέπουμε την κανονική περίπτωση, στην οποία ένας από τους χρήστες στέλνει μία TPDU ΑΑ (ΑΙΤΗΣΗ ΑΠΟΣΥΝΔΕΣΗΣ) για να ξεκινήσει την αποδέσμευση της σύνδεσης. Όταν φτάσει η αίτηση, ο παραλήπτης επιστρέφει με τη σειρά του μια TPDU και ξεκινά ένα χρονόμετρο, για την περίπτωση που θα χαθεί το μήνυμα ΑΑ. Όταν φτάσει αυτή η ΑΑ, ο αρχικός αποστολέας στέλνει μία TPDU ΕΠΙΒΕΒΑΙΩΣΗΣ και αποδεσμεύει τη σύνδεση. Τέλος, όταν φτάσει η TPDU ΕΠΙΒΕΒΑΙΩΣΗΣ ο παραλήπτης αποδεσμεύει και αυτός τη σύνδεση. Αποδέσμευση της σύνδεσης σημαίνει ότι η οντότητα μεταφοράς διαγράφει τις πληροφορίες για τη σύνδεση αυτή από τον πίνακα με τις τρέχουσες ανοικτές συνδέσεις και ενημερώνει με κάποιον τρόπο τον ιδιοκτήτη της σύνδεσης.



Εικόνα 14: Αποδέσμευση σύνδεσης (a) Κανονική περίπτωση τριπλής χειραψίας (b) Απώλεια της τελικής επιβεβαιωσης

Αν χαθεί η τελική TPDU ΕΠΙΒΕΒΑΙΩΣΗΣ, όπως φαίνεται στην Εικόνα 14 (b), η κατάσταση διασώζεται από το χρονόμετρο. Όταν λήξει ο χρόνος αναμονής, η σύνδεση αποδεσμεύεται σε κάθε περίπτωση. Θεωρήστε τώρα την περίπτωση που χάνεται η δεύτερη ΑΑ. Ο χρήστης που ξεκίνησε την αποδέσμευση δεν θα λάβει την αναμενόμενη απάντηση, θα λήξει ο χρόνος αναμονής του, και η διαδικασία θα ξεκινήσει από την αρχή. Στην Εικόνα 15 (c) βλέπουμε πώς λειτουργεί αυτή η διαδικασία, υποθέτοντας ότι τη δεύτερη φορά δεν χάνεται καμία TPDU και ότι όλες οι TPDU παραδίδονται σωστά και στην ώρα τους. Το τελευταίο σενάριο, η Εικόνα 15 (d), είναι ίδιο με την Εικόνα 15 (c) με τη διαφορά ότι στην περίπτωση αυτή υποθέτουμε ότι όλες οι επόμενες προσπάθειες αναμετάδοσης της ΑΑ αποτυγχάνουν λόγω απώλειας των TPDU Μετά από N προσπάθειες, ο αποστολέας τα παρατάει και αποδεσμεύει τη σύνδεση. Εν τω μεταξύ λήγει και ο χρόνος αναμονής του παραλήπτη, οπότε τα παρατάει και αυτός.



Εικόνα 15: Αποδέσμευση σύνδεσης (c) Απώλεια απάντησης (d) Απώλεια απάντησης και επόμενων ΑΑ

2.5.3 Έλεγχος ροής και προσωρινή αποθήκευση

Ένα από τα βασικά ζητήματα στο επίπεδο μεταφοράς είναι η διαχείριση των συνδέσεων όσο αυτές βρίσκονται σε χρήση: ο έλεγχος ροής. Ο μηχανισμός ελέγχου ροής θα πρέπει να εφαρμόζεται στον αποστολέα, για να τον αποτρέπει από το να έχει ταυτόχρονα σε εκκρεμότητα πάρα πολλές μη επιβεβαιωμένες TPDU. Ο Belsnes (1975) πρότεινε τη χρήση μιας μεθόδου ελέγχου ροής με κυλιόμενο παράθυρο, στην οποία ο

αποστολέας προσαρμόζει δυναμικά το μέγεθος του παραθύρου έτσι ώστε να ανταποκρίνεται στη χωρητικότητα μεταφοράς του δικτύου. Αν το δίκτυο μπορεί να αντιμετωπίσει *c* TPDU/sec και ο χρόνος κύκλου (ο οποίος περιλαμβάνει τη μετάδοση, τη διάδοση, την αναμονή σε ουρές, την επεξεργασία στον παραλήπτη, και την επιστροφή της επιβεβαίωσης) είναι r, τότε το παράθυρο του αποστολέα θα πρέπει να είναι *c*r*. Με ένα παράθυρο αυτού του μεγέθους ο αποστολέας συνήθως διατηρεί γεμάτο το κανάλι προς τον παραλήπτη. Κάθε μικρή μείωση στην απόδοση του δικτύου θα τον κάνει να μπλοκαριστεί. Για να μπορεί να προσαρμόζεται περιοδικά το μέγεθος του παραθύρου, ο αποστολέας μπορεί να παρακολουθεί και τις δύο παραπάνω παραμέτρους και να υπολογίζει στη συνέχεια το επιθυμητό μέγεθος του παραθύρου. Η χωρητικότητα μεταφοράς μπορεί να προσδιοριστεί με απλή καταμέτρηση του πλήθους TPDU που επιβεβαιώνονται κατά τη διάρκεια κάποιας χρονικής περιόδου και διαίρεση αυτού του αριθμού με τη διάρκεια της χρονικής περιόδου. Κατά τη διάρκεια των μετρήσεων ο αποστολέας θα πρέπει να στέλνει όσο πιο γρήγορα μπορεί, για να εξασφαλίσει ότι ο παράγοντας που περιορίζει το ρυθμό των επιβεβαιώσεων είναι η χωρητικότητα μεταφοράς του δικτύου, και όχι ο χαμηλός ρυθμός αποστολής. Ο χρόνος που απαιτείται για την επιβεβαίωση μιας TPDU που μεταδόθηκε μπορεί να μετρηθεί με ακρίβεια, και είναι εφικτό να διατηρείται ένας τρέχων μέσος όρος. Αφού η διαθέσιμη χωρητικότητα του δικτύου για κάθε δεδομένη ροή μεταβάλλεται με το χρόνο, το μέγεθος του παραθύρου θα πρέπει να προσαρμόζεται συχνά, παρακολουθώντας τις αλλαγές στη χωρητικότητα μεταφοράς.

2.6 Επίπεδο 5: Επίπεδο Συνόδου (Session Layer)

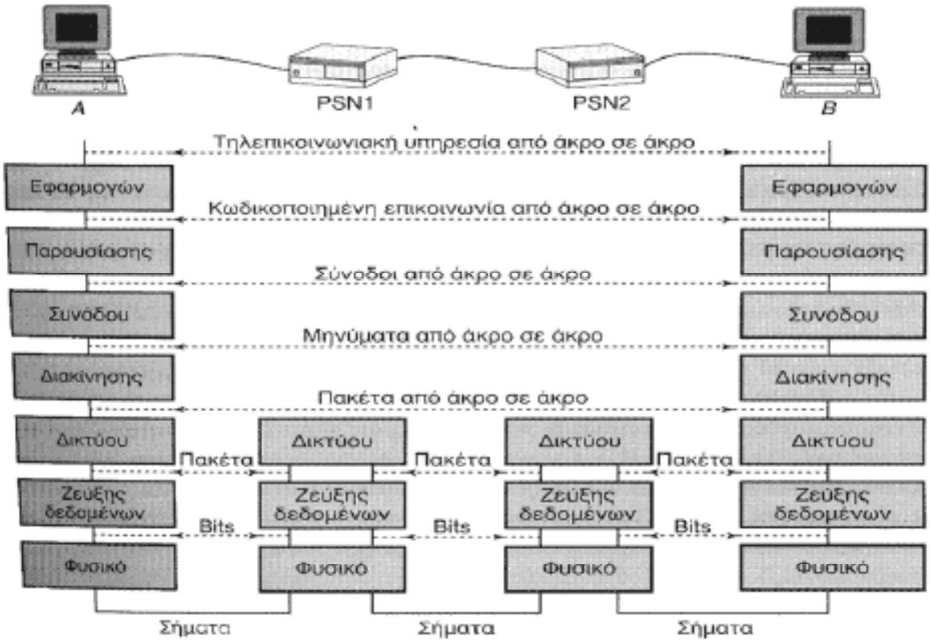
Το επίπεδο συνόδου είναι υπεύθυνο για τη σωστή αποκατάσταση των συνόδων σε ένα δίκτυο. Αυτό πρακτικά σημαίνει τη διευθέτηση ενεργειών, όπως για παράδειγμα τη μεταφορά αρχείων, οι οποίες μπορεί να χρειαστεί να γίνουν ταυτόχρονα από πολλούς χρήστες. Έτσι, με την ονομαζόμενη **διαχείριση σκυτάλης** (**token management**), στην περίπτωση που περισσότεροι του ενός χρήστες επιθυμούν να μεταφέρουν αρχεία, το επίπεδο συνόδου αποδίδει την κατάλληλη προτεραιότητα στον αντίστοιχο χρήστη. Τέλος, μια άλλη υπηρεσία είναι ο **συγχρονισμός** (**synchronization**) που έχει να κάνει με την εισαγωγή σημείων ελέγχου στα μεταφερόμενα δεδομένα, ώστε η μετάδοσή τους να επανεκκινεί σε περίπτωση διακοπής της σύνδεσης ή άλλης βλάβης.

2.7 Επίπεδο 6: Επίπεδο Παρουσίασης (Presentation Layer)

Το επίπεδο παρουσίασης μετασχηματίζει τα δεδομένα σε τυπική μορφή που την αναμένει το επίπεδο εφαρμογών. Στο επίπεδο αυτό τα δεδομένα υφίστανται κρυπτογράφηση, συμπίεση, κωδικοποίηση MIME και όποια άλλη διαμόρφωση απαιτεί η μορφή δεδομένων ή ο σχεδιαστής του πρωτοκόλλου. Παραδείγματα αποτελούν η μετατροπή αρχείων από κώδικα EBCDIC σε κώδικα ASCII και η μετατροπή της δομής των δεδομένων σε μορφή XML ή αντίστροφα (π.χ. από XML σε έγγραφο τύπου DOC).

2.8 Επίπεδο 7: Επίπεδο Εφαρμογής (Application Layer)

Αφού ολοκληρώσαμε όλα τα προκαταρκτικά, φτάνουμε πια στο επίπεδο όπου βρίσκονται όλες οι εφαρμογές. Τα επίπεδα κάτω από το επίπεδο εφαρμογών είναι απαραίτητα για να παρέχουν αξιόπιστη μεταφορά, δεν κάνουν όμως κάποια πραγματική δουλειά για τους χρήστες. Το επίπεδο εφαρμογής είναι ένα επίπεδο από άκρο σε άκρο (end to end) από την αφετηρία στον προορισμό. Αυτό μπορούμε να το δούμε στην Εικόνα 16.



Εικόνα 16: Επικοινωνία ανάμεσα στα αντίστοιχα επίπεδα OSI δύο τερματικών

Ωστόσο, ακόμα και στο επίπεδο εφαρμογών υπάρχει η ανάγκη για κάποια πρωτόκολλα υποστήριξης, τα οποία θα επιτρέπουν τη λειτουργία των εφαρμογών. Έτσι, πριν αρχίσουμε να ασχολούμαστε με τις ίδιες τις εφαρμογές, θα εξετάσουμε ένα από αυτά. Το εν

λόγω πρωτόκολλο είναι το DNS, το οποίο διαχειρίζεται τα ονόματα στο Internet. Τις σημαντικότερες διαδικτυακές εφαρμογές θα τις περιγράψουμε θεωρητικά στο 4^{ο} κεφάλαιο.

2.8.1 Domain Name System (DNS)

Αν και θεωρητικά τα προγράμματα θα μπορούσαν να αναφέρονται στους υπολογιστές υ-πηρεσίας, τα γραμματοκιβώτια, και τους άλλους πόρους χρησιμοποιώντας τις διευθύνσεις δικτύου τους, οι διευθύνσεις αυτές είναι δύσκολες στην απομνημόνευση για τους ανθρώπους.

Στην εποχή του ARPANET υπήρχε απλώς ένα αρχείο, το hosts.txt το οποίο ανέφερε όλους τους υπολογιστές υπηρεσίας και τις διευθύνσεις IP τους. Κάθε νύχτα όλοι οι υπολογιστές υπηρεσίας έπαιρναν το αρχείο αυτό από την τοποθεσία στην οποία γινόταν η διατήρηση του. Για ένα δίκτυο με μόνο λίγες εκατοντάδες μεγάλες χρονομεριζόμενες μηχανές, η προσέγγιση αυτή λειτουργούσε αρκετά καλά. Όταν όμως συνδέθηκαν στο δίκτυο προσωπικοί υπολογιστές, όλοι συνειδητοποίησαν ότι η προσέγγιση αυτή δεν θα μπορούσε να λειτουργεί για πάντα. Καταρχήν, το μέγεθος του αρχείου θα γινόταν πολύ μεγάλο. Ακόμη πιο σημαντικό ήταν όμως το ότι θα εμφανίζονταν συνεχώς διενέξεις στα ονόματα των υπολογιστών υπηρεσίας, εκτός και αν η διαχείριση των ονομάτων γινόταν κεντρικά κάτι αδιανόητο για ένα τεράστιο διεθνές δίκτυο, λόγω του φορτίου και της καθυστέρησης. Για να λυθούν αυτά τα προβλήματα, επινοήθηκε το **Σύστημα Ονομάτων Περιοχών** ή DNS (**Domain Name System**). Η ουσία του DNS είναι η επινόηση ενός ιεραρχικού συστήματος ονοματολογίας που βα-σίζεται σε περιοχές, καθώς και ενός κατανεμημένου συστήματος βάσεων δεδομένων για την υλοποίηση αυτού του συστήματος ονοματολογίας. Το DNS χρησιμοποιείται κυρίως για την αντιστοίχιση των ονομάτων των υπολογιστών υπηρεσίας και των προορισμών του ηλεκτρονικού ταχυδρομείου σε διευθύνσεις IP, αλλά μπορεί να χρησιμοποιηθεί και για άλλους σκοπούς. Το DNS ορίζεται στα RFC 1034 και 1035.

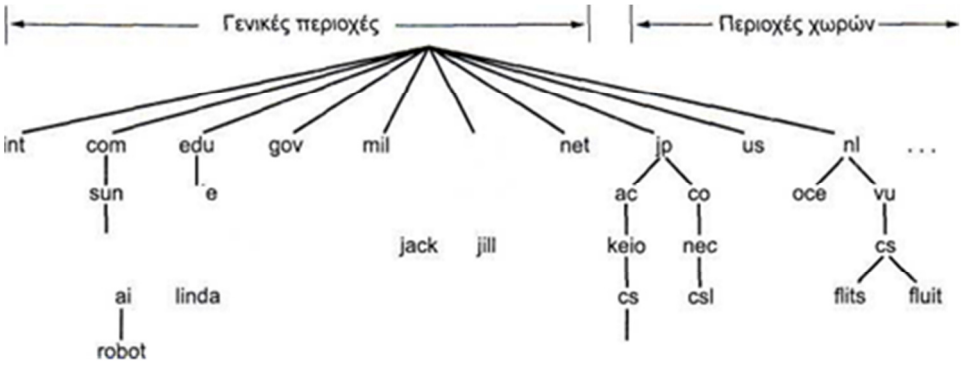
Πολύ συνοπτικά, ο τρόπος χρήσης του DNS είναι ο ακόλουθος. Για να αντιστοιχιστεί ένα όνομα σε μια διεύθυνση IP, το πρόγραμμα εφαρμογής καλεί μια διαδικασία βιβλιοθήκης η οποία ονομάζεται **αναλυτής** (resolver), μεταβιβάζοντας της το όνομα αυτό ως παράμετρο. Ένα τέτοιο παράδειγμα είναι η συνάρτηση gethostbyname. Ο αναλυτής στέλνει ένα πακέτο UDP σε έναν τοπικό διακομιστή DNS, ο οποίος αναζητεί το όνομα και επιστρέφει στον αναλυτή τη διεύθυνση IP, και αυτός την επιστρέφει με τη σειρά του στον καλούντα. Οπλισμένο με αυτή τη διεύθυνση, το πρόγραμμα μπορεί να

εγκαθιδρύσει στη συνέχεια μια σύνδεση TCP με τον προορισμό ή να του στείλει πακέτα UDP.

2.8.2 Ο χώρος ονομάτων του DNS

Η διαχείριση ενός μεγάλου και συνεχώς μεταβαλλόμενου συνόλου ονομάτων είναι ένα δύσκολο πρόβλημα. Στο απλό ταχυδρομικό σύστημα, η διαχείριση των ονομάτων γίνεται με την απαίτηση οι επιστολές να προσδιορίζουν (άμεσα ή έμμεσα) τη χώρα, την πολιτεία ή το νομό, την πόλη, και την οδό και τον αριθμό του παραλήπτη. . Το DNS λειτουργεί με τον ίδιο τρόπο. Από λογική άποψη, το Internet διαιρείται σε περισσότερες από 200 περιοχές (domains) ανωτάτου επιπέδου, όπου η κάθε περιοχή καλύπτει πολλούς υπολογιστές υπηρεσίας. Κάθε περιοχή υποδιαιρείται σε υπό-περιοχές, αυτές υποδιαιρούνται περαιτέρω, και ούτω καθεξής. Όλες αυτές οι περιοχές μπορούν να αναπαρασταθούν με ένα δένδρο, όπως φαίνεται στην Εικόνα 17. Τα φύλλα του δένδρου αυτού παριστάνουν περιοχές οι οποίες δεν έχουν υπό-περιοχές (αλλά περιέχουν, βέβαια, μηχανήματα). Μια περιοχή φύλλου μπορεί είτε να περιέχει έναν μόνο υπολογιστή υπηρεσίας, ή μπορεί να αντιπροσωπεύει μια εταιρεία και να περιέχει χιλιάδες υπολογιστές υπηρεσίας.

Οι περιοχές ανωτάτου επιπέδου έχουν δύο τύπους: τις γενικές περιοχές και τις περιοχές χωρών. Οι αρχικές γενικές περιοχές ήταν οι com (commercial , εμπορικές), edu (educational, εκπαιδευτικά Ιδρύματα), gov (government, ομοσπονδιακή κυβέρνηση), int (international, ορισμένοι διεθνείς οργανισμοί), mil (military, ένοπλες δυνάμεις), net (network, φορείς δικτύου), και org (organization, μη κερδοσκοπικοί οργανισμοί). Οι περιοχές χωρών περιλαμβάνουν μία καταχώριση για κάθε χώρα, όπως αυτές ορίζονται στο πρότυπο ISO 3166.



Εικόνα 17: Ένα μέρος του χώρου ονομάτων περιοχών στο Internet.

Τα ονόματα των περιοχών μπορεί να είναι είτε απόλυτα είτε σχετικά. Ένα απόλυτο όνομα περιοχής τελειώνει πάντοτε με μια τελεία (π.χ. eng.sun.com), ενώ ένα σχετικό όνομα δεν τελειώνει με αυτή. Τα σχετικά ονόματα πρέπει να ερμηνευθούν σε σχέση με κάποιο πλαίσιο αναφοράς, προκειμένου να προσδιοριστεί μονοσήμαντα η πραγματική τους σημασία. Και στις δύο περιπτώσεις, η κατονομαζόμενη περιοχή αναφέρεται σε ένα συγκεκριμένο κόμβο του δένδρου, καθώς και σε όλους τους κόμβους που βρίσκονται κάτω από αυτόν. Θεωρητικά, οι περιοχές μπορούν να εισάγονται στο δένδρο με δύο διαφορετικούς τρόπους. Κάθε περιοχή ελέγχει την εκχώρηση των περιοχών που βρίσκονται κάτω από αυτή και διαμορφώνει τα ονόματα σύμφωνα με τον κανόνα που ισχύει για αυτή την περιοχή. Για να δημιουργηθεί μια νέα περιοχή, απαιτείται η άδεια της περιοχής στην οποία θα περιλαμβάνεται. Με αυτόν τον τρόπο αποφεύγονται οι διενέξεις ονομάτων, και η κάθε περιοχή μπορεί να παρακολουθεί όλες τις υπό-περιοχές της. Αφού δημιουργηθεί και καταγραφεί μια νέα περιοχή, μπορεί να δημιουργήσει νέες τις υπό-περιοχές της, χωρίς να χρειάζεται άδεια από όσους βρίσκονται υψηλότερα στο δένδρο. Η ονομασία γίνεται με βάση τα όρια των οργανισμών, και όχι με βάση τα όρια των φυσικών δικτύων.

2.8.3 Εγγραφές πόρων

Κάθε περιοχή, ανεξάρτητα από το αν είναι ένας μόνο υπολογιστής υπηρεσίας ή μια περιοχή ανωτάτου επιπέδου, μπορεί να έχει ένα σύνολο από **εγγραφές πόρων** (resource records) που είναι συσχετισμένες με αυτή. Στην περίπτωση του ενός μόνο υπολογιστή υπηρεσίας, η πιο απλή εγγραφή πόρων είναι απλώς η διεύθυνση IP. Όταν ένας αναλυτής δίνει ένα όνομα περιοχής στο DNS, αυτό που του επιστρέφεται είναι οι εγγραφές πόρων που σχετίζονται με το όνομα αυτό. Έτσι, η πρωταρχική λειτουργία του DNS είναι η αντιστοίχιση ονομάτων περιοχών σε εγγραφές πόρων. Η εγγραφή πόρων είναι μια διατεταγμένη πεντάδα και η οποία αναλύεται παρακάτω:

Όνομα περιοχής (domain_name): το οποίο προσδιορίζει την περιοχή με την οποία σχετίζεται η εγγραφή αυτή. Υπάρχουν συνήθως πολλές εγγραφές για κάθε περιοχή, και κάθε αντίγραφο της βάσης δεδομένων περιέχει πληροφορίες για περισσότερες από μία περιοχές. Αυτό λοιπόν το πεδίο είναι το κύριο κλειδί αναζήτησης που χρησιμοποιείται για την απάντηση στα ερωτήματα. Η σειρά των εγγραφών στη βάση δεδομένων δεν έχει σημασία.

Χρόνος ζωής (time_to_live): δίνει μια ένδειξη σχετικά με το πόσο σταθερή είναι η εγγραφή. Σε πληροφορίες που είναι ιδιαίτερα σταθερές εκχωρείται μια υψηλή τιμή, όπως

το 86400 (το πλήθος δευτερολέπτων σε μία ημέρα). Στις πληροφορίες που είναι ιδιαίτερα ευμετάβλητες εκχωρείται μια μικρή τιμή, όπως το 60 (1 λεπτό).

Τάξη (class): Για τις πληροφορίες του Internet η τάξη είναι πάντα IN. Για πληροφορίες που δεν σχετίζονται με το Internet μπορούν να χρησιμοποιηθούν άλλοι κωδικοί, στην πράξη όμως κάτι τέτοιο το συναντάμε σπάνια.

Τύπος (type): δείχνει τι είδους εγγραφή είναι η τρέχουσα. Οι πιο σημαντικοί τύποι φαίνονται στην Εικόνα 18.

Τύπος	Σημασία	Τιμή
SOA	Έναρξη εξουσιοδότησης	Παράμετροι για τη ζώνη αυτή
A	Διεύθυνση IP ενός υπολογιστή υπηρεσίας	32μπιτος ακέραιος
MX	Σύστημα ανταλλαγής αλληλογραφίας	Προτεραιότητα, περιοχή που είναι πρόθυμη να δεχτεί ηλεκτρονικό ταχυδρομείο
Νδ	Διακομιστής ονομάτων	Όνομα ενός διακομιστή για την περιοχή αυτή
CNAME	Κανονικό όνομα	Όνομα περιοχής
PTR	Δείκτης	Ψευδώνυμο για μια διεύθυνση IP
HINFO	Περιγραφή υπολογιστή υπηρεσίας	Επεξεργαστής και λειτουργικό σύστημα σε A50II
TXT	Κείμενο	Ελεύθερο κείμενο A50II

Εικόνα 18: Οι βασικοί τύποι των εγγραφών πόρων του DNS για το IPv4

Τιμή (value): το πεδίο αυτό μπορεί να είναι ένας αριθμός, ένα όνομα περιοχής, ή ένα αλφαριθμητικό ASCII. Η σημασία του εξαρτάται από τον τύπο της εγγραφής. Στην Εικόνα 18 δίνεται μια σύντομη περιγραφή των πεδίων Τιμή για κάθε έναν από τους βασικούς τύπους εγγραφών.

2.8.4 Διακομιστές ονομάτων

Θεωρητικά τουλάχιστον, ένας μόνο διακομιστής ονομάτων θα μπορούσε να περιέχει ολόκληρη τη βάση δεδομένων του DNS και να απαντά σε όλα τα ερωτήματα προς αυτή. Στην πράξη, όμως, ο διακομιστής αυτός θα ήταν τόσο υπερφορτωμένος που θα καταντούσε να είναι άχρηστος. Επιπλέον, αν ποτέ κατέρρεε θα αχρηστευόταν ολόκληρο το Internet. Για να αποφευχθούν τα προβλήματα που πηγάζουν από την ύπαρξη μίας μοναδικής προέλευσης πληροφοριών, ο χώρος ονομάτων του DNS υποδιαιρείται σε μη επικαλυπτόμενες ζώνες (zones). Κάθε ζώνη περιέχει ένα μέρος του δένδρου, και επιπλέον περιέχει τους διακομιστές ονομάτων οι οποίοι αποθηκεύουν τις πληροφορίες

για τη ζώνη αυτή. Κανονικά μια ζώνη έχει έναν πρωτεύοντα (primary) διακομιστή ονομάτων, ο οποίος λαμβάνει τις πληροφορίες από ένα αρχείο στο δίσκο του, καθώς και έναν ή περισσότερους δευτερεύοντες (secondary) διακομιστές ονομάτων οι οποίοι λαμβάνουν τις πληροφορίες από τον πρωτεύοντα διακομιστή ονομάτων. Για αύξηση της αξιοπιστίας, μερικοί από τους διακομιστές μιας ζώνης μπορεί να βρίσκονται έξω από τη ζώνη.

Η θέση όπου θα τοποθετηθούν τα όρια των ζωνών μέσα σε μια περιοχή είναι θέμα του διαχειριστή της περιοχής αυτής. Η απόφαση αυτή σε μεγάλο βαθμό εξαρτάται από το πλήθος των διακομιστών ονομάτων που επιθυμούμε να έχουμε, καθώς και από τη θέση όπου θέλουμε να βρίσκονται. Όταν ένας αναλυτής έχει ένα ερώτημα σχετικά με κάποιο όνομα περιοχής, στέλνει το ερώτημα σε έναν από τους τοπικούς διακομιστές ονομάτων. Αν η περιοχή που αναζητείται βρίσκεται μέσα στη δικαιοδοσία αυτού του διακομιστή ονομάτων ο διακομιστής επιστρέφει τις επίσημες εγγραφές πόρων. Η **επίσημη εγγραφή** (**authorative record**) είναι μια εγγραφή η οποία προέρχεται από την αρχή που διαχειρίζεται την εγγραφή, και έτσι είναι πάντοτε σωστή. Οι επίσημες εγγραφές αντιδιαστέλλονται με τις εγγραφές που προέρχονται από κρυφές μνήμες, οι οποίες μπορεί να μην είναι ενημερωμένες. Αν όμως η περιοχή είναι απομακρυσμένη και δεν υπάρχει διαθέσιμη τοπικά καμία πληροφορία για τη ζητούμενη περιοχή, ο διακομιστής ονομάτων στέλνει ένα μήνυμα ερωτήματος στο διακομιστή ονομάτων ανωτάτου επιπέδου για τη ζητούμενη περιοχή.

Αν και το DNS είναι εξαιρετικά σημαντικό για τη σωστή λειτουργία του Internet, στην πραγματικότητα το μόνο πράγμα που κάνει είναι να αντιστοιχίζει τα συμβολικά ονόματα των μηχανών με τις διευθύνσεις IP τους. Δεν μας βοηθά γενικά να εντοπίσουμε άτομα, πόρους, υπηρεσίες, ή αντικείμενα. Για τον εντοπισμό αυτών των πραγμάτων έχει προσδιοριστεί μια άλλη υπηρεσία καταλόγου, η οποία ονομάζεται **Ελαφρό Πρωτόκολλο Προσπέλασης Καταλόγου** ή LDAP (Lightweight Directory Protocol Access). Το LDAP είναι μια απλοποιημένη παραλλαγή της υπηρεσίας καταλόγου X.500 του OSI, και περιγράφεται στο RFC 2251. Οργανώνει τις πληροφορίες σε ένα δένδρο και επιτρέπει αναζητήσεις με βάση διάφορες ιδιότητες των αντικειμένων. Μπορεί να θεωρηθεί σαν ένα είδος τηλεφωνικού καταλόγου.

2.9 Βιβλιογραφία & πηγές

Βιβλία

[1] Andrew S. Tanenbaum Τέταρτη Αμερικάνικη Έκδοση <<Δίκτυα Υπολογιστών>>

[2] James Kurose & Keith Ross, 4η Έκδοση <<Δικτύωση Υπολογιστών- Προσέγγιση από Πάνω προς τα Κάτω>>

Links

[1] http://en.wikipedia.org/wiki/Physical_Layer

[2] http://en.wikipedia.org/wiki/Data_link_layer

[3] http://en.wikipedia.org/wiki/Network_layer

[4] http://en.wikipedia.org/wiki/Transport_layer

[5] http://en.wikipedia.org/wiki/Session_layer

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

[7] http://en.wikipedia.org/wiki/Application_layer

[8] http://www.tcpipguide.com/free/t_TransportLayerLayer4-2.htm

[9] http://www.tcpipguide.com/free/t_NetworkLayerLayer3.htm

[10]http://www.highteck.net/EN/Application/Application_Layer_Functionality_and_Protocols.html

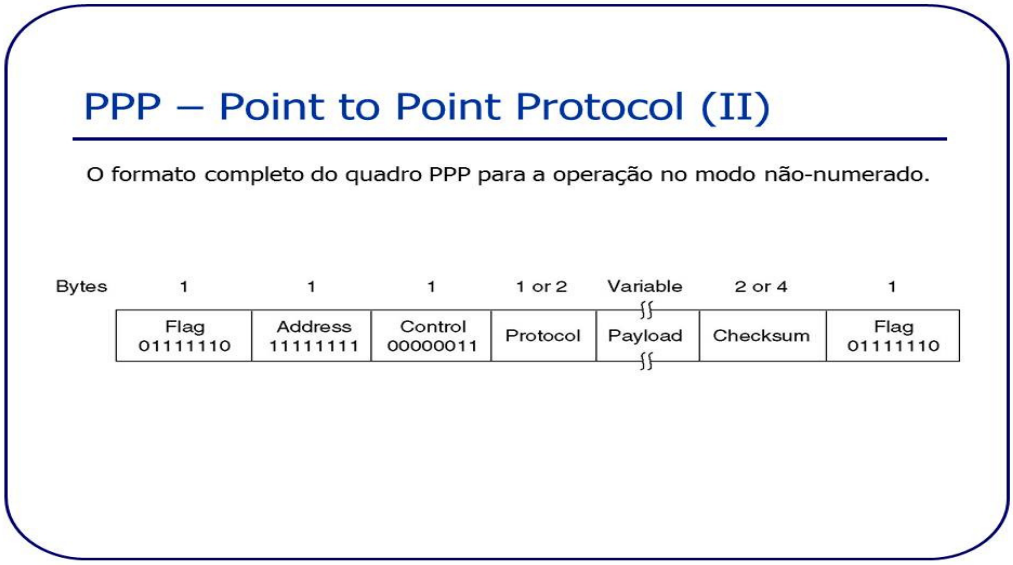
ΚΕΦΑΛΑΙΟ 3: ΣΤΟΙΒΑ ΠΡΩΤΟΚΟΛΛΩΝ OSI ΣΤΟ INTERNET

3.1 Το επίπεδο συνδέσμου μετάδοσης δεδομένων - Data link layer στο Internet

Το Internet χρειάζεται ένα πρωτόκολλο από σημείο σε σημείο για διάφορους σκοπούς, στους οποίους περιλαμβάνεται η κίνηση από δρομολογητή σε δρομολογητή και η κίνηση από τους οικιακούς χρήστες στους ISP. Το πρωτόκολλο αυτό, ονομάζεται **Πρωτόκολλο από Σημείο σε Σημείο** - **PPP** (Point-to-Point Protocol). Το PPP διαχειρίζεται την ανίχνευση σφαλμάτων, υποστηρίζει πολλά πρωτόκολλα, επιτρέπει τη διαπραγμάτευση διευθύνσεων IP κατά τη σύνδεση, επιτρέπει την πιστοποίηση ταυτότητας και έχει ακόμα πολλές δυνατότητες. Το PPP παρέχει τρεις λειτουργίες:

1. Μια μέθοδο πλαισίωσης η οποία οριοθετεί μονοσήμαντα το τέλος του ενός πλαισίου και την αρχή του επόμενου. Η μορφή των πλαισίων καλύπτει επίσης και την ανίχνευση σφαλμάτων.
2. Ένα πρωτόκολλο ελέγχου γραμμής για την ενεργοποίηση της γραμμής, τον έλεγχό της, τη διαπραγμάτευση επιλογών, και την ομαλή της απενεργοποίηση όταν δεν χρειάζεται πλέον. Το πρωτόκολλο αυτό ονομάζεται **Πρωτόκολλο Ελέγχου Συνδέσμου** - **LCP** (Link Control Protocol). Υποστηρίζει τόσο σύγχρονα όσο και ασύγχρονα κυκλώματα, καθώς και κωδικοποιήσεις προσανατολισμένες σε byte ή σε bit.
3. Έναν τρόπο διαπραγμάτευσης των επιλογών του επιπέδου δικτύου που είναι ανεξάρτητος από το πρωτόκολλο επιπέδου δικτύου που χρησιμοποιείται. Η μέθοδος που έχει επιλεγεί είναι να υπάρχει ένα διαφορετικό πρωτόκολλο, το **Πρωτόκολλο Ελέγχου Δικτύου** -**NCP** (Network Control Protocol) για κάθε υποστηριζόμενο επίπεδο δικτύου.

Η προκαθορισμένη μορφή του πλαισίου του PPP είναι:



Εικόνα 19: Πλήρης μορφή πλαισίων του PPP για λειτουργία σε μη αριθμημένη κατάσταση

Όλα τα πλαίσια PPP αρχίζουν με το τυπικό byte **Flag** του HDLC (01111110), το οποίο συμπληρώνεται με byte αν εμφανίζεται μέσα στο πεδίο payload. Στη συνέχεια έχουμε το πεδίο **Address** το οποίο έχει πάντα τη δυαδική τιμή 11111111, ώστε να δείχνει ότι όλοι οι σταθμοί πρέπει να δέχονται το πλαίσιο. Με τη χρήση αυτής τιμής αποφεύγεται η ανάγκη καθορισμού διευθύνσεων συνδέσμου μετάδοσης δεδομένων. Το πεδίο Address ακολουθείται από το πεδίο **Control**, η προεπιλεγμένη τιμή του οποίου είναι 00000011. Η τιμή αυτή υποδηλώνει ένα μη αριθμημένο πλαίσιο. Με άλλα λόγια, το PPP δεν παρέχει εξ ορισμού αξιόπιστη μετάδοση με χρήση αριθμών ακολουθίας και επιβεβαιώσεων. Σε «θορυβώδη» περιβάλλοντα, όπως τα ασύρματα δίκτυα, μπορεί να χρησιμοποιηθεί αξιόπιστη μετάδοση με ενεργοποίηση της αριθμημένης λειτουργίας. Επειδή τα πεδία Address και Control είναι πάντοτε σταθερά στις προεπιλεγμένες διευθύνσεις, το LCP παρέχει τον κατάλληλο μηχανισμό έτσι ώστε τα δύο άκρα να διαπραγματευτούν μια επιλογή με την οποία θα παραλείπουν εντελώς αυτά τα πεδία κα θα εξοικονομούν 2 byte ανά πλαίσιο. Το τέταρτο πεδίο είναι το **Protocol**. Δουλειά του είναι να δείχνει τι είδους πακέτο περιέχεται στο πεδίο payload. Έχουν οριστεί κωδικοί για τα LCP, NCP, IP,I PX, AppleTalk και άλλα πρωτόκολλα. Τα πρωτόκολλα που ξεκινούν με το bit 0 είναι πρωτόκολλα επιπέδου δικτύου όπως τα IP, IPX, OSI CLNP, XNS. Αυτά που αρχίζουν με το bit 1 χρησιμοποιούνται για τη διαπραγμάτευση άλλων πρωτοκόλλων. Σε αυτά περιλαμβάνονται το LCP και ένα διαφορετικό NCP για κάθε υποστηριζόμενο επίπεδο δικτύου. Το προεπιλεγμένο μέγεθος του πεδίου Protocol είναι 2 byte, αλλά μπορεί να

μειωθεί στο 1 byte κατόπιν διαπραγμάτευσης με το LCP. Το πεδίο **Payload** έχει μεταβλητό μήκος, μέχρι κάποιο διαπραγματεύσιμο μέγιστο όριο. Αν κατά την εγκαθίδρυση της γραμμής δεν γίνει διαπραγμάτευση του μήκους μέσω του LCP, χρησιμοποιείται ένα προεπιλεγμένο μήκος 1500 byte. Το payload μπορεί να ακολουθείται από χαρακτήρες συμπλήρωσης (padding), εφόσον χρειάζεται. Μετά το πεδίο payload, ακολουθεί το πεδίο **Checksum**, το οποίο κανονικά καταλαμβάνει 2 byte, αλλά μπορεί να γίνει και διαπραγμάτευση ενός αθροίσματος ελέγχου των 4 byte.

3.2 Το επίπεδο δικτύου - Network layer στο Internet

Ο συνδετικός ιστός του Internet είναι το πρωτόκολλο επιπέδου δικτύου, το **Πρωτόκολλο Internet**- **IP** (Internet Protocol). Σε αντίθεση με τα περισσότερα παλαιότερα πρωτόκολλα επιπέδου δικτύου, το IP σχεδιάστηκε από την αρχή με στόχο τη διαδικτύωση. Ένας καλός τρόπος θεώρησης του επιπέδου δικτύου είναι ο ακόλουθος. Η δουλεία του είναι να παρέχει ένα τρόπο μεταφοράς αυτοδύναμων πακέτων με τη μέθοδο της βέλτιστης προσπάθειας (δηλαδή, όχι εγγυημένα) από την προέλευση στον προορισμό, ανεξάρτητα από το αν οι μηχανές αυτές βρίσκονται στο ίδιο δίκτυο ή αν υπάρχουν άλλα δίκτυα ανάμεσά τους.

3.2.1 Το πρωτόκολλο IP

Το **Πρωτόκολλο Διαδικτύου (IP)**, αποτελεί το κύριο πρωτόκολλο επικοινωνίας για τη μετάδοση datagrams δηλαδή πακέτων δεδομένων, σε ένα διαδίκτυο. Το Πρωτόκολλο IP είναι υπεύθυνο για τη δρομολόγηση των πακέτων δεδομένων ανάμεσα στα διάφορα δίκτυα, ανεξάρτητα από την υποδομή τους, και αποτελεί το κύριο πρωτόκολλο πάνω στο οποίο είναι βασισμένο το διαδίκτυο. Καθορίζει τη μορφή των πακέτων που στέλνονται μέσω ενός διαδικτύου, καθώς και τους μηχανισμούς που χρησιμοποιούνται για την προώθηση των πακέτων από έναν υπολογιστή προς έναν τελικό προορισμό μέσω ενός ή περισσότερων δρομολογητών. Γι' αυτούς τους σκοπούς, το IP, χρησιμοποιεί συγκεκριμένες μεθόδους διευθυνσιοδότησης και δομές για την ενθυλάκωση των πακέτων δεδομένων.

Η πρώτη μεγάλης κλίμακας έκδοση του Πρωτοκόλλου IP, ήταν η έκδοση 4 (**IPv4**) η οποία επικρατεί μέχρι και σήμερα σε όλο το Διαδίκτυο. Ωστόσο, λόγω του ότι δεν επαρκούν πλέον οι διευθύνσεις, τα τελευταία χρόνια, έχει αναπτυχθεί η διάδοχη έκδοση

του πρωτοκόλλου, η έκδοση 6 (**IPv6**), η οποία είναι εν ενεργεία και χρησιμοποιείται εξαπλωνόμενη σε όλο τον κόσμο.

3.2.1.1 Υπηρεσίες του Πρωτοκόλλου IP

Το Πρωτόκολλο IP, είναι υπεύθυνο για τη διευθυνσιοδότηση των κόμβων και την δρομολόγηση των πακέτων από έναν υπολογιστή προς έναν τελικό προορισμό, κατά μήκος ενός ή περισσότερων δικτύων. Για το σκοπό αυτό, το πρωτόκολλο IP, καθορίζει ένα σύστημα διευθυνσιοδότησης, το οποίο έχει δύο λειτουργίες. Έτσι κάθε πακέτο IP, αποτελείται από μια κεφαλίδα και στη συνέχεια ακολουθούν τα δεδομένα. Στη κεφαλίδα αυτή εμπεριέχονται πληροφορίες: πρώτον, για τα δεδομένα που εμπεριέχονται στο πακέτο και δεύτερον, οι διευθύνσεις αφετηρίας και προορισμού. Η διαδικασία προσθήκης της κεφαλίδας σε ένα πακέτο δεδομένων ονομάζεται ενθυλάκωση. Το Πρωτόκολλο IP είναι μια υπηρεσία χωρίς σύνδεση, είναι ανεξάρτητο από την τεχνολογία του υλικού που χρησιμοποιείται σε κάθε δίκτυο, και δεν χρειάζεται να την γνωρίζει πριν την μετάδοση.

Αξιοπιστία

Εκτός από τον ορισμό της μορφής των αυτοδύναμων πακέτων, το Πρωτόκολλο IP ορίζει τη σημασιολογία της επικοινωνίας, και χρησιμοποιεί τον όρο βέλτιστη προσπάθεια, για να περιγράψει την υπηρεσία που παρέχει. Ουσιαστικά το πρότυπο αυτό ορίζει, ότι παρ' όλο που το πρωτόκολλο IP κάνει τη βέλτιστη δυνατή προσπάθεια για να αποδώσει ένα πακέτο στο προορισμό του, το υποκείμενο υλικό από το οποίο είναι φτιαγμένα τα εκάστοτε δίκτυα που διασχίζει, μπορεί να συμπεριφερθεί λανθασμένα. Έτσι, το πρωτόκολλο, δεν εγγυάται ότι θα μπορέσει να αντιμετωπίσει τα παρακάτω προβλήματα:

- Αλλοίωση δεδομένων.
- Απώλεια αυτοδύναμου πακέτου.
- Επανάληψη αυτοδύναμου πακέτου.
- Επίδοση με καθυστέρηση ή εκτός σειράς.

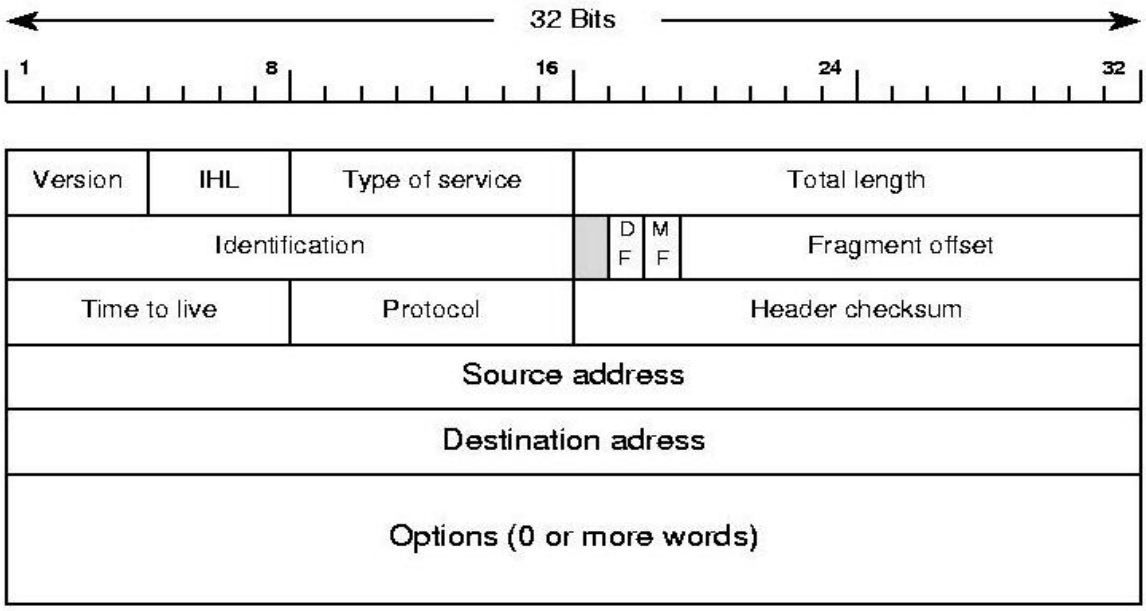
Για την αντιμετώπιση του κάθε ενός από αυτά τα σφάλματα, χρειάζονται πρόσθετα, υψηλότερα επίπεδα λογισμικού πρωτοκόλλων.

Η μόνη διαβεβαίωση που μπορεί να δώσει το πρωτόκολλο IP στην έκδοση 4 (IPv4), είναι το αν τα bit της κεφαλίδας έχουν υποστεί αλλοίωση ή όχι κατά τη διάρκεια της μεταφοράς. Αυτή η πληροφορία εμπεριέχεται σε ένα πεδίο της κεφαλίδας του IP πακέτου, που ονομάζεται Header Checksum. Κάνοντας χρήση του checksum, μπορεί να διαπιστωθεί

εάν η κεφαλίδα έχει μεταφερθεί σωστά ή όχι, και αναλόγως το πακέτο απορρίπτεται ή όχι. Στην έκδοση 6 (IPv6) ωστόσο, έχει εγκαταλειφθεί η χρήση του checksum, προς όφελος της ταχείας προώθησης μέσω ορισμένων στοιχείων δρομολόγησης στο δίκτυο.

Κεφαλίδα του IPv4

Στην Εικόνα 20 που ακολουθεί παρουσιάζεται η μορφή της κεφαλίδας.



Εικόνα 20: Η κεφαλίδα του IPv4

Το πεδίο **Version** δείχνει την έκδοση του πρωτοκόλλου την οποία ακολουθεί το αυτοδύναμο πακέτο. Περιλαμβάνοντας την έκδοση μέσα σε κάθε αυτοδύναμο πακέτο επιτρέπουμε η μετάβαση μεταξύ εκδόσεων να μπορεί να πάρει ακόμα και χρόνια, με μερικές μηχανές να εκτελούν την παλιά έκδοση και μερικές τη νέα.

Επειδή το μήκος της κεφαλίδας δεν είναι σταθερό, παρέχεται ένα πεδίο στην κεφαλίδα, το **IHL** (Internet Header Length), το οποίο δηλώνει πόσο μεγάλη είναι η κεφαλίδα, σε λέξεις των 32 bit.

Το πεδίο **Type of service** προορίζεται για να κάνει διάκριση ανάμεσα σε διαφορετικές τάξεις υπηρεσιών.

Το πεδίο **Total length** περιλαμβάνει όλα τα περιεχόμενα μέσα στο αυτοδύναμο πακέτο-και την κεφαλίδα και τα δεδομένα. Το μέγιστο μήκος είναι 65.535 byte.

Το πεδίο **Identification** είναι ένα πεδίο ταυτότητας και χρησιμεύει για τον μοναδικό προσδιορισμό των κομματιών (fragments) που ανήκουν στο ίδιο αρχικό IP αυτοδύναμο πακέτο.

Στη συνέχεια ακολουθεί ένα μη χρησιμοποιούμενο bit και μετά ακολουθούν δύο πεδία του 1 bit. Το πεδίο **DF** (don't fragment), είναι μια διαταγή προς τους δρομολογητές να μην κατακερματίσουν το αυτοδύναμο πακέτο, επειδή ο προορισμός δεν είναι σε θέση να συναρμολογήσει ξανά όλα τα τμήματα του πακέτου. Το πεδίο **MF** (more fragments), δηλώνει την ύπαρξη περισσότερων κομματιών. Όλα τα κομμάτια εκτός από το τελευταίο έχουν ενεργοποιημένο αυτό το bit. Αυτό απαιτείται έτσι ώστε να γνωρίζουμε πότε έχουν φτάσει όλα τα κομμάτια ενός αυτοδύναμου πακέτου.

Το πεδίο **fragment offset** προσδιορίζει την θέση ενός συγκεκριμένου κομματιού, από την αρχή του αρχικού αυτοδύναμου πακέτου.

Το πεδίο **Time to live** είναι ένας μετρητής που χρησιμοποιείται για τον περιορισμό της ζωής των πακέτων. Υποτίθεται ότι μετρά το χρόνο σε δευτερόλεπτα επιτρέποντας μέγιστο χρόνο ζωής ίσο με 255sec. Θα πρέπει να μειώνεται σε κάθε άλμα και υποτίθεται ότι θα μειώνεται πολλές φορές όταν το πακέτο βρίσκεται για πολλή ώρα στην ουρά ενός δρομολογητή. Στην πράξη απλώς μετρά άλματα. Όταν φτάσει στο μηδέν, το πακέτο απορρίπτεται και επιστρέφεται στον αποστολέα ένα πακέτο προειδοποίησης. Αυτό το χαρακτηριστικό αποτρέπει τα αυτοδύναμα πακέτα να περιπλανούνται για πάντα κάτι που θα μπορούσε να συμβεί αν τύχαινε να αλλοιωθούν οι πίνακες δρομολόγησης.

Το **Header checksum** επαληθεύει μόνο την κεφαλίδα. Μόλις ένα πακέτο φτάσει σε έναν δρομολογητή, ο δρομολογητής υπολογίζει το άθροισμα ελέγχου της κεφαλίδας και το συγκρίνει με το πεδίο αθροίσματος ελέγχου της κεφαλίδας. Εάν δεν ταιριάζουν, τότε ο δρομολογητής απορρίπτει το πακέτο. Σφάλματα στο πεδίο δεδομένων πρέπει να διαχειριστούν από το ενθυλακωμένο πρωτόκολλο.

Τα πεδία **Source address** και **Destination address**, δείχνουν τον αριθμό δικτύου και τον αριθμό υπολογιστή υπηρεσίας.

Τέλος, το πεδίο **Options**, σχεδιάστηκε για να παρέχει ένα τρόπο διαφυγής ο οποίος θα επιτρέπει σε επόμενες εκδόσεις του πρωτοκόλλου να περιέχουν πληροφορίες που δεν υπήρχαν στην αρχική σχεδίαση, θα δίνει στους ερευνητές τη δυνατότητα να δοκιμάζουν

νέες ιδέες και θα αποφεύγει την εκχώρηση bit κεφαλίδας για πληροφορίες που χρειάζονται σπάνια.

3.2.2 Πρωτόκολλα ελέγχου στο Internet

Εκτός από το IP, που χρησιμοποιείται για τη μεταφορά δεδομένων, το Internet διαθέτει και πολλά πρωτόκολλα ελέγχου που χρησιμοποιούνται στο επίπεδο δικτύου, στα οποία περιλαμβάνονται τα ICMP, ARP, RARP, BOOTP και DHCP.

3.2.2.1 Το πρωτόκολλο ICMP

Η λειτουργία του Internet παρακολουθείται προσεκτικά από τους δρομολογητές. Όταν συμβαίνει κάτι απροσδόκητο, το γεγονός αυτό αναφέρεται από το **Πρωτόκολλο Μηνυμάτων Ελέγχου Internet-ICMP** (Internet Control Message Protocol), το οποίο χρησιμοποιείται και για τον έλεγχο του Internet. Έχουν οριστεί γύρω στα δέκα μηνύματα ICMP. Τα πιο σημαντικά από αυτά φαίνονται στην παρακάτω Εικόνα 21. Κάθε τύπος μηνύματος ICMP ενθυλακώνεται σε ένα πακέτο IP.

Τύπος μηνύματος	**Περιγραφή**
Μη προσπελάσιμος προορισμός	Το πακέτο δεν μπορούσε να παραδοθεί
Υπέρβαση Χρόνου	Το πεδίο χρόνου ζωής έφτασε στο 0
Πρόβλημα παραμέτρων	Άκυρο πεδίο κεφαλίδας
Καταστολή προέλευσης	Πακέτο αποπνιγμού
Ανακατεύθυνση	‘‘Μάθημα γεωγραφίας’’ στο δρομολογητή
Αντήχηση	Ρώτα μια μηχανή αν είναι ζωντανή
Απάντηση αντήχησης	Ναι, είμαι ζωντανή
Αίτηση χρονοσφραγίδας	Ίδιο με την Αίτηση αντήχησης, αλλά με χρονοσφραγίδα
Απάντηση χρονοσφραγίδας	Ίδιο με την Αίτηση αντήχησης, αλλά με χρονοσφραγίδα

Εικόνα 21: Οι κύριοι τύποι μηνυμάτων ICMP

Το μήνυμα **Μη προσπελάσιμος προορισμός** (**destination unreachable**), χρησιμοποιείται όταν το υποδίκτυο ή ένας δρομολογητής δεν μπορεί να εντοπίσει τον προορισμό ή όταν ένα πακέτο που έχει ενεργοποιημένο το bit OK, δεν μπορεί να παραδοθεί επειδή υπάρχει στη μέση ένα δίκτυο ‘‘μικρών πακέτων’’.

Το μήνυμα **Υπέρβαση Χρόνου** (**time exceeded**), στέλνεται όταν απορρίπτεται ένα πακέτο επειδή ο μετρητής του έχει φτάσει στο μηδέν. Το γεγονός αυτό είναι ένδειξη ότι τα πακέτα κάνουν κύκλους, ότι υπάρχει τεράστια συμφόρηση, ή ότι έχουν τεθεί πολύ χαμηλές τιμές στο σχετικό χρονόμετρο.

Το μήνυμα **Πρόβλημα παραμέτρων** (**parameter problem**), δείχνει ότι έχει εντοπιστεί μια άκυρη τιμή σε ένα πεδίο κεφαλίδας. Αυτό το πρόβλημα υποδηλώνει κάποιο σφάλμα στο λογισμικό IP του υπολογιστή υπηρεσίας αποστολής ή στο λογισμικό ενός δρομολογητή από τον οποίο πέρασε το πακέτο.

Το μήνυμα **Καταστολή προέλευσης** (**source quench**), το χρησιμοποιούσαν παλαιότερα για να ‘‘συγκρατήσουν’’ τους υπολογιστές υπηρεσίας που έστελναν πάρα πολλά πακέτα. Όταν ένας υπολογιστής υπηρεσίας λάμβανε αυτό το μήνυμα, έπρεπε να επιβραδύνει. Χρησιμοποιείται σπανίως πια, επειδή όταν εμφανίζεται συμφόρηση τα πακέτα αυτά τείνουν να ρίχνουν λάδι στη φωτιά. Πλέον, ο έλεγχος συμφόρησης στο Internet γίνεται σε μεγάλο βαθμό στο επίπεδο μεταφοράς.

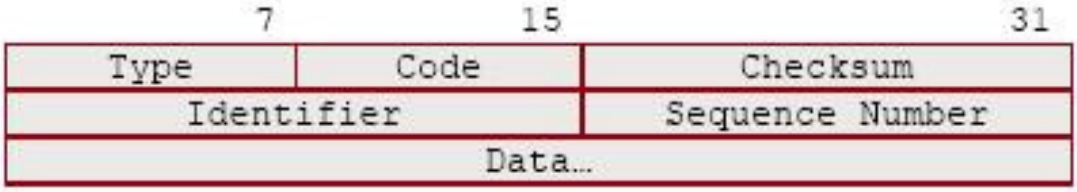
Το μήνυμα **Ανακατεύθυνση** (**redirect**), χρησιμοποιείται όταν ένας δρομολογητής παρατηρήσει ότι κάποιο πακέτο μοιάζει να έχει δρομολογηθεί λανθασμένα. Χρησιμοποιείται από το δρομολογητή για να ενημερώσει τον υπολογιστή υπηρεσίας αποστολής για το πιθανό σφάλμα.

Τα μηνύματα **Αντήχηση** (**echo**) και **Απάντηση αντήχησης** (**echo reply**), χρησιμοποιούνται για να αν κάποιος δεδομένος προορισμός είναι προσπελασμένος και ζωντανός. Όταν λάβει το μήνυμα αντήχηση, ο προορισμός αναμένεται να επιστρέψει ένα μήνυμα απάντηση αντήχησης. Τα μηνύματα **Αίτηση χρονοσφραγίδας** (**timestamp request**) και **Απάντηση χρονοσφραγίδας** (**timestamp reply**), είναι παρόμοια, με τη διαφορά ότι καταγράφονται στην απάντηση ο χρόνος άφιξης του μηνύματος και ο χρόνος αναχώρησης της απάντησης. Αυτή η βοηθητική λειτουργία χρησιμοποιείται για τη μέτρηση της απόδοσης του δικτύου.

Εκτός από αυτά τα μηνύματα, έχουν οριστεί και άλλα. Η πλήρης λίστα βρίσκεται στην τοποθεσία *www.iana.org/assignments/icmp-parameters.*

Δομή πακέτου ICMP

Στην Εικόνα 22 που ακολουθεί φαίνεται η κεφαλίδα (Header) ενός πακέτου ICMP.



Εικόνα 22: Κεφαλίδα πακέτου ICMP

Το πεδίο **Type**, δηλώνει τον κωδικό του τύπου μηνύματος ICMP.

Το πεδίο **Code**, χρησιμοποιείται ως επέκταση του προηγούμενου. Για παράδειγμα εάν το πεδίο Type περιέχει την τιμή 3 (Destination Unreachable), τότε το πεδίο αυτό μπορεί να περιέχει έναν κωδικό από το 1 έως το 15 που να δίνει τον λόγο για τον οποίο ο υπολογιστής που ψάχνουμε είναι εκτός δικτύου.

Το πεδίο **Checksum**, χρησιμοποιείται για τον έλεγχο σφαλμάτων κατά την μετάδοση του πακέτου.

Το πεδίο **ID**, δηλώνει την τιμή ID του πακέτου, η οποία επιστρέφεται στον υπολογιστή που δημιούργησε το πακέτο στην περίπτωση που έχουμε απάντηση echo reply.

Το πεδίο **Sequence Number**, περιέχει την τιμή σειράς του πακέτου και επιστρέφεται στον υπολογιστή που δημιούργησε το πακέτο στην περίπτωση που έχουμε απάντηση echo reply.

3.2.2.2 Το πρωτόκολλο ARP

Το **Πρωτόκολλο Μετατροπής Διεύθυνσης-ARP** (Address Resolution Protocol), κάνει δυναμική μετατροπή των IP διευθύνσεων σε φυσικές (Ethernet) διευθύνσεις. Η μετατροπή αυτή είναι απαραίτητη για να μπορέσουν να επικοινωνήσουν μεταξύ τους, συστήματα που δεν γνωρίζουν το ένα τη φυσική σύνδεση του άλλου. Χρησιμοποιεί έναν ARP πίνακα, ο οποίος έχει για κάθε συσκευή του δικτύου μια γραμμή και δύο στήλες: την IP διεύθυνση και τη φυσική διεύθυνση της συσκευής. Οι εγγραφές του πίνακα, που δεν έχουν χρησιμοποιηθεί για ορισμένο χρονικό διάστημα διαγράφονται από τον πίνακα.

IP Διεύθυνση	Ethernet Διεύθυνση
223.1.2.1	08-00-39-00-2F-88
223.1.2.3	08-00-44-45-77-4D
223.1.2.4	08-00-10-BF-3E-33

Εικόνα 23: ARP Πίνακας

Πώς λειτουργεί το πρωτόκολλο ARP;

Μόλις το ARP πάρει μια IP διεύθυνση ψάχνει στον ARP πίνακα, για να ελέγξει αν υπάρχει εγγραφή που να αντιστοιχεί σε αυτή την IP διεύθυνση. Εάν υπάρχει εγγραφή, τότε επιστρέφει την αντίστοιχη φυσική διεύθυνση. Διαφορετικά, στέλνει ένα ειδικό μήνυμα που ονομάζεται ARP αίτηση σε όλες τις συσκευές του δικτύου. Εάν, μια συσκευή αναγνωρίσει στην IP διεύθυνση προορισμού της αίτησης τη δική της IP διεύθυνση, στέλνει μια ARP απάντηση με τη δική της φυσική διεύθυνση στη συσκευή που έστειλε την ARP αίτηση. Η συσκευή που δημιούργησε την ARP αίτηση, δημιουργεί μια νέα εγγραφή στον ARP πίνακα και βάζει εκεί τη διεύθυνση που έλαβε.

3.2.2.3 Το πρωτόκολλο RARP

Το ARP λύνει το πρόβλημα της ανεύρεσης διεύθυνσης Ethernet που αντιστοιχεί σε μια συγκεκριμένη διεύθυνση IP. Μερικές φορές πρέπει να λυθεί το αντίστροφο πρόβλημα: με δεδομένη ναι διεύθυνση Ethernet, ποια είναι η αντίστοιχη διεύθυνση IP; Συγκεκριμένα, το πρόβλημα αυτό εμφανίζεται όταν ξεκινά ένας σταθμός εργασίας χωρίς δίσκο. Μια τέτοια μηχανή συνήθως λαμβάνει τη δυαδική Εικόνα του λειτουργικού της συστήματος από έναν απομακρυσμένο διακομιστή αρχείων. Πώς όμως μαθαίνει την διεύθυνση IP της;

Η λύση που επινοήθηκε είναι η χρήση του **Αντίστροφου Πρωτοκόλλου Ανάλυσης Διευθύνσεων** - **RARP** (Reverse Address Resolution Protocol). Το RARP, κάνει την αντίστροφη δουλειά από το ARP. Βάζει δηλαδή, σε μια ερώτηση τη φυσική διεύθυνση της συσκευής και περιμένει σαν απάντηση την αντίστοιχη IP διεύθυνση. Παρ'όλο που οι ερωτήσεις του RARP, απευθύνονται σε όλες τις συσκευές του δικτύου, μπορούν να τις απαντήσουν μόνο ειδικές συσκευές που ονομάζονται RARP εξυπηρετητές.

3.2.2.4 Τα Πρωτόκολλα BOOTP και DHCP

Σε αντίθεση με το RARP, το BOOTP χρησιμοποιεί μηνύματα UDP, τα οποία προωθούνται μέσω των δρομολογητών. Επιπλέον, παρέχει στους σταθμούς εργασίας χωρίς δίσκο πρόσθετες πληροφορίες, στις οποίες περιλαμβάνεται η διεύθυνση IP του διακομιστή αρχείων που έχει την εικόνα μνήμης, η διεύθυνση IP του δρομολογητή και η μάσκα υποδικτύου που θα πρέπει να χρησιμοποιηθεί.

Ένα σοβαρό πρόβλημα με το BOOTP, είναι ότι απαιτεί χειρονακτική διευθέτηση πινάκων οι οποίοι αντιστοιχίζουν διευθύνσεις IP σε φυσικές διευθύνσεις. Όταν προστίθεται ένας νέος υπολογιστής υπηρεσίας σε ένα LAN, δεν μπορεί να χρησιμοποιήσει το BOOTP μέχρι κάποιος διαχειριστής να του εκχωρήσει μια διεύθυνση IP και να καταχωρήσει με το χέρι το ζεύγος (διεύθυνση Ethernet, διεύθυνση IP) στους πίνακες διευθέτησης του BOOTP. Για να εξαλειφθεί αυτό το επιρρεπές σε σφάλματα βήμα, το BOOTP επεκτάθηκε και πήρε νέο όνομα: **Πρωτόκολλο Δυναμικής Διευθέτησης Υπολογιστών Υπηρεσίας-DHCP** (Dynamic Host Configuration Protocol).

Το DHCP είναι ένα πρωτόκολλο πελάτη-εξυπηρετητή (client-server). Ένας πελάτης που μόλις έχει φτάσει σε ένα δίκτυο επιθυμεί να λάβει μια IP διεύθυνση. Στην περίπτωση αυτή το πρωτόκολλο DHCP, εκτελεί μια διαδικασία τεσσάρων βημάτων:

- **Ανακάλυψη Εξυπηρετητή DHCP (DHCP Discover)**: Η πρώτη εργασία ενός μόλις αφικνούμενου πελάτη είναι να βρει έναν εξυπηρετητή DHCP με τον οποίο θα αλληλεπιδράσει. Αυτό το επιτυγχάνει στέλνοντας ένα μήνυμα ανακάλυψης DHCP προς όλους τους υπολογιστές του δικτύου.
- **Προσφορά Εξυπηρετητή DHCP (DHCP Offer)**: Ένας DHCP εξυπηρετητής, που έχει λάβει το μήνυμα ανακάλυψης DHCP από τον πελάτη, του απαντά με ένα μήνυμα προσφοράς DHCP, το οποίο περιέχει μεταξύ άλλων πληροφοριών την προσφερόμενη IP διεύθυνση και το χρόνο για τον οποίο θα είναι έγκυρη. Δεδομένου ότι υπάρχει δυνατότητα το μήνυμα ανακάλυψης DHCP να έχει ληφθεί από περισσότερους του ενός DHCP εξυπηρετητές, ο πελάτης μπορεί να επιλέξει ανάμεσα σε πολλά μηνύματα προσφοράς DHCP.
- **Αίτηση DHCP (DHCP Request)**: Ο πελάτης επιλέγει μια προσφορά εξυπηρετητή DHCP και ενημερώνει τον αντίστοιχο εξυπηρετητή.
- **Βεβαίωση λήψης DHCP (DHCP ACK)**: Ο DHCP εξυπηρετητής απαντά στον πελάτη βεβαιώνοντας τις παραμέτρους της προσφοράς του προς εκείνον.

Όταν ο πελάτης λάβει τη βεβαίωση λήψης DHCP, η αλληλεπίδραση με τον DHCP εξυπηρετητή έχει ολοκληρωθεί και ο πελάτης μπορεί να χρησιμοποιήσει την IP διεύθυνση για όσο χρόνο είναι έγκυρη. Επειδή, ωστόσο ο πελάτης ενδέχεται να επιθυμεί τη χρήση της συγκεκριμένης διεύθυνσης περισσότερο χρόνο από όσο του έχει εκχωρηθεί, το πρωτόκολλο DHCP, παρέχει ένα μηχανισμό που του επιτρέπει να ανανεώσει το χρόνο της IP διεύθυνσης.

Αντιστοίχιση διευθύνσεων IP

Το DHCP υποστηρίζει τρεις μηχανισμούς για να αντιστοιχίζει διευθύνσεις. Αυτοί είναι:

- **Αυτόματη αντιστοίχηση** (με αντιστοίχηση μόνιμης διεύθυνσης).
- **Δυναμική αντιστοίχηση** (με διεύθυνση με ημερομηνία λήξης).
- **Χειροκίνητη αντιστοίχηση** (ο διαχειριστής κανονίζει ότι θεωρεί καλύτερο).

Δέσμευση διευθύνσεων δικτύου

Όπως προαναφέρθηκε, το DHCP έχει 3 μηχανισμούς για να δεσμεύει και να αντιστοιχίζει διευθύνσεις δικτύου. Ένα δίκτυο μπορεί να χρησιμοποιεί έναν ή περισσότερους μηχανισμούς ανάλογα με την απόφαση του διαχειριστή του. Η δυναμική αντιστοίχιση, είναι ο μόνος από τους 3 μηχανισμούς που επιτρέπει αυτόματη επαναχρησιμοποίηση μίας διεύθυνσης που δεν χρειάζεται πια από τον πελάτη στον οποίο δόθηκε. Έτσι, η δυναμική αντιστοίχηση είναι ιδιαιτέρως χρήσιμη για δίκτυα που αποτελούνται από πολλούς πελάτες που συνδέονται προσωρινά ή σε περιπτώσεις που παρατηρείται έλλειψη διευθύνσεων IP ανάμεσα σε μία ομάδα πελατών που δεν χρειάζονται μόνιμες διευθύνσεις. Ο βασικός μηχανισμός για τη δυναμική αντιστοίχηση των διευθύνσεων είναι απλός. Ο πελάτης ζητά τη χρήση μίας διεύθυνσης για ένα πεπερασμένο χρονικό διάστημα (lease). Ο μηχανισμός εγγυάται να μην αντιστοιχίσει τη διεύθυνση αλλού σε αυτό το διάστημα και προσπαθεί να επιστρέφει την ίδια διεύθυνση κάθε φορά που αυτός ο πελάτης ζητά διεύθυνση. Ο πελάτης μπορεί να:

- ζητήσει το lease με άλλες πληροφορίες.
- ρωτήσει αν είναι δυνατή η μόνιμη αντιστοίχιση με ένα αορίστου χρόνου lease.
- στείλει μήνυμα για να απελευθερώσει τη διεύθυνση πίσω στο διακομιστή όταν δεν τη χρειάζεται άλλο.

Στην χειροκίνητη αντιστοίχηση το DHCP απλά χειρίζεται τον έλεγχο λαθών που μπορεί να προκύψουν από την διαχείριση των διευθύνσεων. Στην αυτόματη αντιστοίχηση το DHCP μπορεί να δίνει μόνιμες διευθύνσεις στους hosts χωρίς ανθρώπινη παρέμβαση.

Σαν τελικό έλεγχο ο εξυπηρετητής ελέγχει αν η διεύθυνση που πάει να δώσει όντως δεν χρησιμοποιείται. Αυτό γίνεται με μία ICMP echo ενώ παράλληλα και ο πελάτης ελέγχει την διεύθυνση που έλαβε.

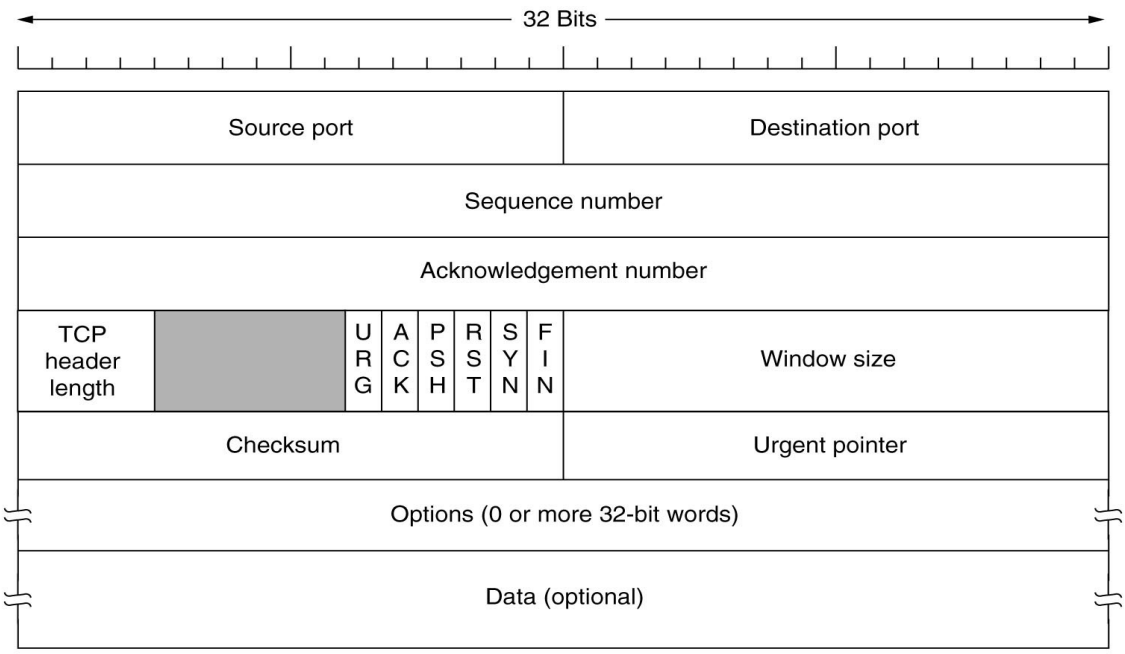
3.3 Το επίπεδο μεταφοράς - Transport layer στο Internet

3.3.1 Το πρωτόκολλο TCP

Το **Πρωτόκολλο Ελέγχου Μετάδοσης-TCP** (Transmission Control Protocol), αποτελεί το βασικό πρωτόκολλο που βρίσκεται στο επίπεδο μεταφοράς της τεχνολογίας TCP/IP και βρίσκεται πάνω από το IP Protocol (πρωτόκολλο διαδικτύου). Το πρωτόκολλο ελέγχου μεταφοράς είναι connection-oriented, δηλαδή η μεταφορά δεδομένων, γίνεται μέσω σύνδεσης, η οποία οριοθετείται από ένα σήμα έναρξης και ένα σήμα τέλους ή διακοπής. Σχεδιάστηκε ειδικά για την παροχή μιας απ' άκρου εις άκρο αξιόπιστης ροής δεδομένων μέσω ενός αναξιόπιστου διαδικτύου. Το διαδίκτυο διαφέρει από ένα μοναδικό δίκτυο, επειδή τα διάφορα μέρη του μπορεί να έχουν εντελώς διαφορετική τοπολογία, εύρος ζώνης, μέγεθος πακέτων και άλλες παραμέτρους. Το TCP σχεδιάστηκε για να προσαρμόζεται δυναμικά στις ιδιότητες ενός διαδικτύου και είναι ανθεκτικό σε πολλά είδη αστοχιών. Οι κύριοι στόχοι του πρωτοκόλλου TCP, είναι να επιβεβαιώνεται η αξιόπιστη αποστολή και λήψη δεδομένων, η μεταφορά των δεδομένων χωρίς λάθη μεταξύ του επιπέδου δικτύου (network layer) και του επιπέδου εφαρμογής (application layer) και φτάνοντας τα δεδομένα αυτά στο επίπεδο εφαρμογής να έχουν τη σωστή σειρά.

3.3.1.1 TCP Header

Τα πακέτα του πρωτοκόλλου TCP καλούνται segments (τμήματα). Ένα από τα κυριότερα μέρη ενός segment είναι η TCP επικεφαλίδα (TCP Header), η οποία παρέχει συγκεκριμένες πληροφορίες για το πρωτόκολλο TCP. Η Εικόνα 24 δείχνει τη μορφή της επικεφαλίδας του TCP. Παρακάτω, θα αναλύσουμε την επικεφαλίδα πεδίο προς πεδίο.



Εικόνα 24: Η επικεφαλίδα του TCP (TCP Header)

Τα πεδία **Source port** και **Destination port**, καθορίζουν τα τοπικά τερματικά σημεία της σύνδεσης και μαζί με τις IP διευθύνσεις ορίζουν μια TCP σύνδεση με μοναδικό τρόπο.

Το πεδίο **Sequence number** έχει διπλό ρόλο: Εάν υπάρχει η SYN flag, τότε είναι ο αρχικός αριθμός ακολουθίας (ISN-initial sequence number) και η πρώτη οκτάδα δεδομένων του πακέτου είναι ISN+1. Διαφορετικά, εάν δεν υπάρχει η SYN flag τότε η πρώτη οκτάδα δεδομένων είναι ο αριθμός ακολουθίας.

Στο πεδίο **Acknowledgment number**, όταν υπάρχει η ACK flag, η τιμή αυτού του πεδίου δείχνει τον επόμενο αριθμό ακολουθίας (sequence number), που αναμένει ο αποστολέας. Και τα δύο πεδία έχουν μήκος 32 bit, επειδή σε μια ροή TCP αριθμείται κάθε byte.

Το πεδίο **TCP Header length**, δείχνει πόσες λέξεις μεγέθους 32 bit περιέχει η επικεφαλίδα TCP. Αυτή η πληροφορία χρειάζεται επειδή το πεδίο options έχει μεταβλητό μήκος, άρα το ίδιο ισχύει και για την επικεφαλίδα. Από τεχνική άποψη, στην πραγματικότητα το πεδίο αυτό δείχνει την αρχή των δεδομένων μέσα στο τμήμα, μετρώντας λέξεις μεγέθους 32 bit , αλλά ο αριθμός αυτός είναι προφανώς ίσος με το μήκος της επικεφαλίδας σε λέξεις, οπότε το αποτέλεσμα είναι το ίδιο.

Στη συνέχεια ακολουθεί ένα πεδίο 6 bit "κρατημένων" (reserved), για μελλοντική χρήση. Η τιμή των bit πρέπει να είναι μηδέν.

Ακολουθεί το μεγέθους 6-bit πεδίο Flags, που χρησιμοποιείται για την ανταλλαγή πληροφοριών ελέγχου, μεταξύ των άκρων της επικοινωνίας:

- **URG (urgent):** Παίρνει την τιμή 1 αν είναι σε χρήση ο Δείκτης Επειγόντων (urgent pointer). Ο Δείκτης Επειγόντων χρησιμοποιείται για να προσδιορίσει την απόσταση σε byte από τον τρέχοντα αριθμό ακολουθίας στην οποία βρίσκονται τα επείγοντα δεδομένα. Αυτή η βοηθητική λειτουργία χρησιμοποιείται σε αντικατάσταση των μηνυμάτων διακοπών.
- **ACK (acknowledgment):** Παίρνει την τιμή 1 για να δείξει ότι ο αριθμός επιβεβαίωσης (acknowledgment number), είναι έγκυρος. Αν έχει τιμή 0 το τμήμα δεν περιέχει κάποια επιβεβαίωση, έτσι το πεδίο acknowledgment number παραβλέπεται.
- **PSH (push):** Υποδεικνύει δεδομένα, στα οποία χρησιμοποιήθηκε η λειτουργία ώθηση. Με αυτό το bit ζητείται από τον παραλήπτη να παραδώσει τα δεδομένα στην εφαρμογή κατά την άφιξή τους, αντί να τα αποθηκεύσει προσωρινά μέχρι να λάβει μια πλήρη περιοχή προσωρινής αποθήκευσης.
- **RST (reset):** Χρησιμοποιείται για την επαναφορά μιας σύνδεσης που έχει μπλεχτεί λόγω της κατάρρευσης ενός server ή εξαιτίας κάποιας άλλης αιτίας. Χρησιμοποιείται επίσης, για την απόρριψη ενός μη έγκυρου τμήματος ή για την άρνηση σε μια απόπειρα ανοίγματος σύνδεσης. Γενικά, αν λάβουμε ένα τμήμα με ενεργοποιημένο το RST έχουμε κάποιο πρόβλημα.
- **SYN (synchronize):** Χρησιμοποιείται για την εγκαθίδρυση των συνδέσεων.
- **FIN (finish):** Χρησιμοποιείται για τον τερματισμό μιας σύνδεσης. Καθορίζει ότι ο αποστολέας δεν έχει άλλα δεδομένα προς μετάδοση.

Το πεδίο **Window size**, δείχνει τον αριθμό από οκτάδες δεδομένων (bytes) που επιθυμεί να δεχτεί ο αποστολέας του πακέτου, αρχίζοντας από εκείνη που δείχνει το πεδίο επιβεβαίωσης (acknowledgment field, ACK).

Το πεδίο **Checksum**, χρησιμοποιείται για έλεγχο λαθών στην επικεφαλίδα και στα δεδομένα. Η ύπαρξη και η χρήση του είναι υποχρεωτικές. Η τιμή του, πρέπει να υπολογιστεί από τον αποστολέα και να επιβεβαιωθεί από τον παραλήπτη.

Το πεδίο **Options**, είναι η μεταβλητή η οποία καθορίζει ειδικές επιλεγόμενες ρυθμίσεις και μπορεί να καταλάβει χώρο στο τέλος της επικεφαλίδας TCP (TCP Header). Το μήκος τους είναι πολλαπλάσιο των 8 bit και το περιεχόμενο της επικεφαλίδας μετά την τελευταία επιλογή πρέπει να γεμίζει (πχ. με μηδενικά). Με αυτόν τον τρόπο το data offset θα δείχνει σωστά την αρχή των δεδομένων.

Στο πεδίο **Urgent pointer**, εάν ενεργοποιημένο το URG bit ελέγχου, τότε αυτό το πεδίο δείχνει τον αριθμό ακολουθίας (sequence number) της οκτάδας που βρίσκεται αμέσως μετά το τελευταίο byte από τα επείγοντα δεδομένα. Έτσι παρουσιάζει τη θέση του τελευταίου byte με επείγοντα δεδομένα.

Το πεδίο **Data**, είναι προαιρετικό, αφού η ύπαρξη δεδομένων στο TCP segment είναι προαιρετική.

3.3.1.2 Εγκαθίδρυση συνδέσεων στο TCP

Η ανταλλαγή δεδομένων στο TCP μπορεί να γίνει μετά την εγκαθίδρυση της σύνδεσης. Πριν να προσπαθήσει ένας client, να συνδεθεί με ένα server, ο sever πρέπει πρώτα να δεσμεύσει μια θύρα (port) και να την ανοίξει έτσι ώστε να δέχεται συνδέσεις: αυτό καλείται passive open. Όταν γίνει αυτό, ο client μπορεί να αρχίσει τη σύνδεση (active open). Η εγκαθίδρυση της σύνδεσης, γίνεται με τον αλγόριθμο της τριπλής χειραψίας (**three-way handshake**). Ο αλγόριθμος, περιλαμβάνει την ανταλλαγή τριών μηνυμάτων μεταξύ του client και του server. Η διαδικασία ξεκινά από τον client.

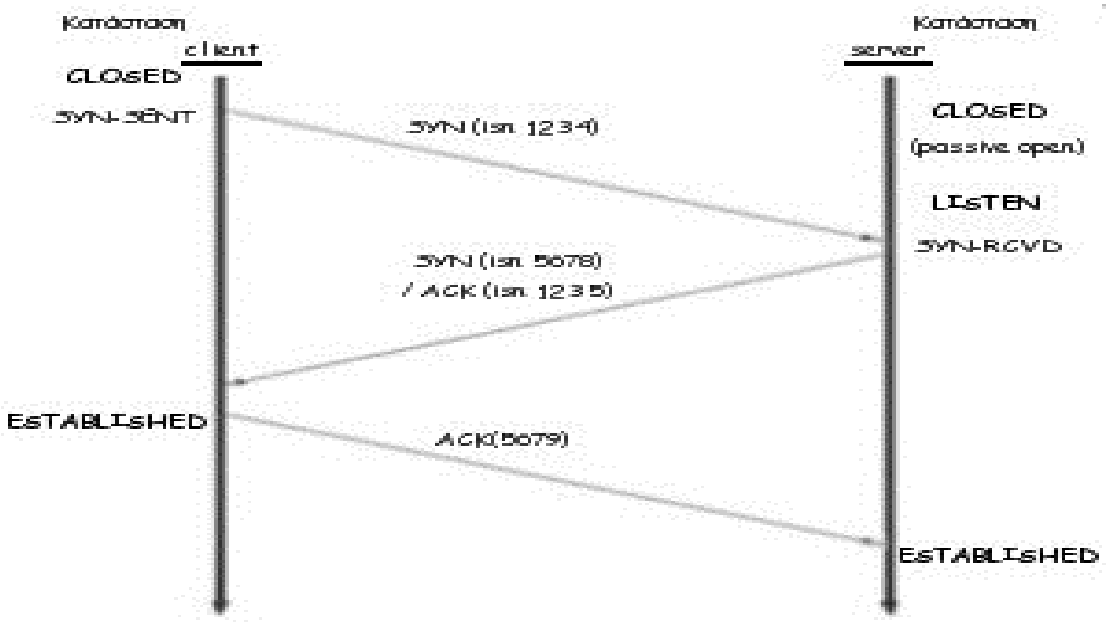
Αρχικά, αποστέλλεται ένα πακέτο με το SYN bit ενεργοποιημένο. Ο client θέτει το πεδίο αριθμού ακολουθίας (sequence number) στην TCP Header στον αρχικό αριθμό ακολουθίας του (ISN - initial sequence number).

Ο server στο άλλο άκρο απαντάει:

- Είτε με SYN (για να στείλει και το δικό του ISN) και ACK (που έχει το ISN+1, του client) του πρώτου πακέτου του client για να αποδεχτεί τη σύνδεση
- ή SYN/RST για να ενημερώσει τον client ότι αρνείται τα σύνδεση και η διαδικασία σταματά

Όταν ο client λάβει ένα πακέτο SYN/ACK απαντάει, αυτή τη φορά, με ένα, πακέτο ACK. Σε αυτό το σημείο, τα δύο μέρη συνδέονται και μπορούν να στείλουν δεδομένα.

Στην Εικόνα 27 παρουσιάζεται με σχήμα, η εγκαθίδρυση σύνδεσης μέσω της τριπλής χειραψίας.



Εικόνα 27: Εγκαθίδρυση σύνδεσης με three-way-handshake

3.3.1.3 Αποδέσμευση συνδέσεων στο TCP

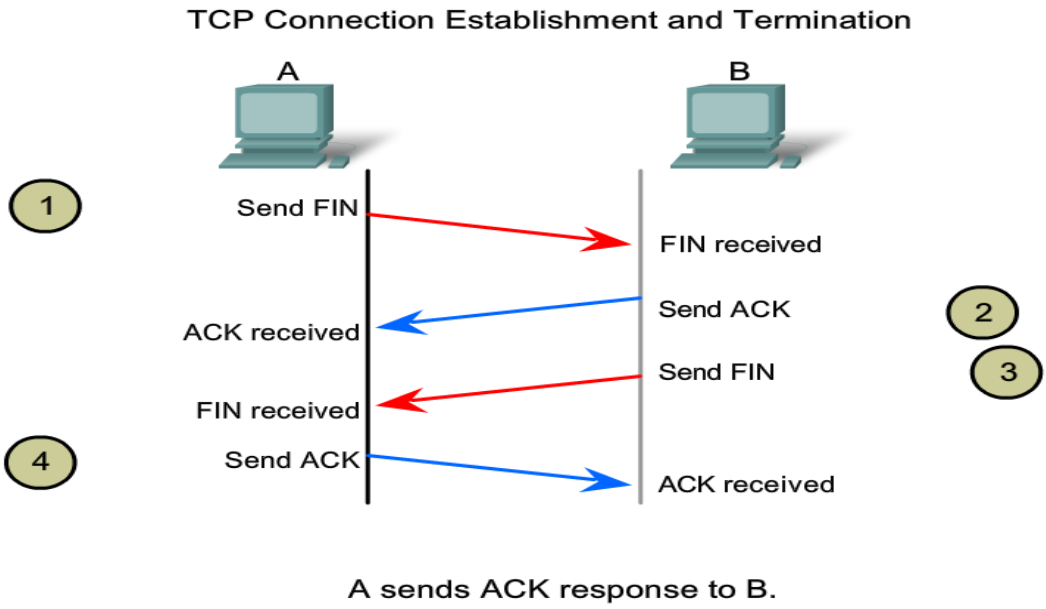
Η αποδέσμευση μιας σύνδεσης είναι ευκολότερη από την εγκαθίδρυση μιας σύνδεσης. Η σύνδεση τερματίζεται με ένα 4-way handshake, με την κάθε πλευρά να τερματίζει ανεξάρτητα:

- Όταν κάποιο άκρο επιθυμεί να τερματίσει τη σύνδεση από πλευράς του, στέλνει ένα πακέτο με το bit FIN ενεργοποιημένο.
- Το πακέτο αυτό επιβεβαιώνεται από το άλλο άκρο με την αποστολή ενός πακέτου ACK.
- Στη συνέχεια, στέλνει το ένα πακέτο FIN.
- Η πλευρά που ξεκίνησε τον τερματισμό της σύνδεσης, μπορεί να τον επιβεβαιώσει στέλνοντας ένα πακέτο ACK.

Για την αποδέσμευση μιας σύνδεσης, χρειάζεται ένα ζεύγος πακέτων FIN και ACK για κάθε άκρο στη σύνδεση TCP. Μία σύνδεση μπορεί να είναι “half open”, δηλαδή η μια πλευρά να έχει τερματίσει τη σύνδεση, όχι όμως και η άλλη. Η πλευρά που έχει τερματίσει δεν μπορεί να στείλει δεδομένα, ενώ η άλλη πλευρά μπορεί.

Τέλος, είναι δυνατό, αν και λιγότερο πιθανό, οι δύο πλευρές να στείλουν ταυτόχρονα ένα πακέτο FIN η μια στην άλλη. Στη συνέχεια η κάθε πλευρά επιβεβαιώνει το FIN που δέχτηκε με ένα πακέτο ACK. Στο σημείο αυτό και οι δύο διακόπτουν τη σύνδεση.

Στην Εικόνα 28 που ακολουθεί, παρουσιάζεται σχηματικά ο τρόπος αποδέσμευσης μιας σύνδεσης.



Εικόνα 28: Αποδέσμευση σύνδεσης στο TCP

Μεταφορά δεδομένων

Μόλις ανταλλαχθούν οι αρχικοί αριθμοί ακολουθίας (ISNs), οι εφαρμογές μπορούν να διαβιβάσουν δεδομένα η μια στην άλλη. Η ανάλυση του τρόπου με τον οποίο γίνεται η μεταφορά δεδομένων , απαιτεί εξέταση για **έλεγχο ροής (flow control)** και **τεχνικές ελέγχου συμφόρησης (congestion avoidance).**

Σε μια απλή υλοποίηση του TCP, χωρίς τους παραπάνω ελέγχους, η εφαρμογή θα στείλει πακέτα στο δίκτυο προς τον παραλήπτη, εφ' όσον υπάρχουν δεδομένα προς αποστολή και εφ' όσον ο αποστολέας δεν υπερβαίνει το window size που του έχει υποδείξει ο παραλήπτης. Όταν ο παραλήπτης δέχεται πακέτα TCP, στέλνει acknowledgments, δείχνοντας σε ποιο σημείο της ροής δεδομένων (byte stream) βρίσκεται. Αυτά τα acknowledgments, περιέχουν επίσης το επόμενο window size που καθορίζει πόσα byte επιθυμεί να δεχτεί στη συνέχεια ο παραλήπτης.

3.3.1.4 Έλεγχος ροής-flow control

Ο παραλήπτης κάθε σύνδεσης, έχει ένα προσωρινό χώρο αποθήκευσης (buffer), στον οποίο αποθηκεύει τα πακέτα τα οποία έχουν φτάσει και βρίσκονται στη σωστή σειρά. Η εφαρμογή που σχετίζεται με την σύνδεση αυτή, διαβάζει από αυτό τον αποθηκευτικό χώρο όποτε το θεωρήσει αυτή αναγκαίο και όχι με ένα σταθερό ρυθμό. Εάν ο ρυθμός αυτός είναι σχετικά αργός, τότε ο αποθηκευτικός χώρος θα γεμίσει σχετικά γρήγορα και τα πακέτα τα οποία θα φτάνουν από εκείνη την στιγμή και μετά θα ρίχνονται αναγκαστικά από τον παραλήπτη.

Το TCP για να αποφύγει αυτό το πρόβλημα παρέχει ένα μηχανισμό ελέγχου ροής, έτσι ώστε να εμποδίζει τον αποστολέα να στέλνει δεδομένα πιο γρήγορα από τον ρυθμό που ο παραλήπτης μπορεί να τα παραλαμβάνει. Για τον σκοπό αυτό, ο παραλήπτης διατηρεί ένα παράθυρο (window) το οποίο αντιπροσωπεύει τον ελεύθερο αποθηκευτικό χώρο που υπάρχει. Το μέγεθος αυτό, στέλνεται στον αποστολέα με κάθε επιβεβαίωση που στέλνεται για πακέτα που έχουν παραληφθεί. Ο αποστολέας χρησιμοποιεί το δεδομένο αυτό ως εξής : Ο αποστολέας γνωρίζει το μέγεθος των δεδομένων που έχει στείλει στον παραλήπτη καθώς και το ποσοστό των δεδομένων αυτών που έχουν επιβεβαιωθεί ότι έφτασαν κανονικά στον παραλήπτη. Ο αποστολέας τότε γνωρίζει πως τα νέα δεδομένα που θα στείλει προστιθέμενα στα δεδομένα που δεν έχουν ακόμα επιβεβαιωθεί, δεν πρέπει να ξεπερνούν συνολικά τον ελεύθερο διαθέσιμο αποθηκευτικό χώρο του παραλήπτη.

3.3.1.5 Έλεγχος συμφόρησης-congestion control

Όταν το προσφερόμενο φορτίο σε οποιοδήποτε δίκτυο είναι μεγαλύτερο από αυτό που μπορεί να αντιμετωπίσει το δίκτυο, παρουσιάζεται συμφόρηση. Θεωρητικά, η συμφόρηση μπορεί να αντιμετωπιστεί αν χρησιμοποιήσουμε μια αρχή δανεισμένη από τη φυσική: το νόμο της διατήρησης των πακέτων. Η ιδέα είναι να αποφεύγουμε να εισάγουμε νέο πακέτο στο δίκτυο μέχρι να φύγει (δηλαδή, να παραδοθεί) ένα παλιό πακέτο. Το TCP προσπαθεί να πετύχει το στόχο αυτόν εκτελώντας δυναμική διαχείριση του μεγέθους του παραθύρου. Όταν εγκαθιδρύεται μια σύνδεση, πρέπει να επιλεγεί ένα κατάλληλο μέγεθος παραθύρου. Ο παραλήπτης μπορεί να προσδιορίσει ένα παράθυρο το οποίο να βασίζεται στο μέγεθος της περιοχής προσωρινής αποθήκευσής του. Αν ο αποστολέας σεβαστεί αυτό το μέγεθος παραθύρου δεν θα εμφανιστούν προβλήματα λόγω υπερχείλισης των περιοχών προσωρινής αποθήκευσης στο άκρο του παραλήπτη, μπορεί όμως να εμφανιστούν προβλήματα λόγω εσωτερικής συμφόρησης μέσα στο δίκτυο.

Το πρωτόκολλο TCP, έχει τέσσερις αλγορίθμους που βοηθούν στην επίτευξη υψηλής απόδοσης και αποφυγής υπερφόρτωσης του δικτύου. Ο ρυθμός μετάδοσης δεδομένων ενός αποστολέα προσαρμόζεται από το TCP στις δυνατότητες του δικτύου αποφεύγοντας τη δημιουργία συμφόρησης. Οι αλγόριθμοι που χρησιμοποιούνται για την αποφυγή συμφόρησης είναι, ο αλγόριθμος της αργής εκκίνησης **(slow start)**, της αποφυγής συμφόρησης **(congestion avoidance)**, της γρήγορης αναμετάδοσης **(fast retransmit)** και της γρήγορης ανάκτησης **(fast recovery)**.

3.3.1.6 Χαρακτηριστικά TCP

Τα κυριότερα χαρακτηριστικά του TCP είναι τα εξής:

- Είναι connection protocol, δηλαδή, χρησιμοποιείται μόνο μεταξύ 2 υπολογιστών.
- Είναι αξιόπιστο. Το TCP του παραλήπτη ενημερώνει συνεχώς το TCP του αποστολέα, για το πιο είναι το επόμενο πακέτο που περιμένει, σύμφωνα με τον αύξοντα αριθμό των πακέτων που έχει ήδη λάβει και αν αντιληφθεί ότι κάποιο πακέτο χάθηκε στην πορεία, τότε επιβάλλει retransmission (αναμετάδοση). Αν το πακέτο δεν μπορεί να έρθει μετά από πολλαπλά retransmissions, τότε η σύνδεση διακόπτεται (timeout).
- Εγγυάται την σωστή σειρά άφιξης των δεδομένων στην εφαρμογή του παραλήπτη. Όταν τα δεδομένα έρθουν στην είσοδο του παραλήπτη με λάθος σειρά, τότε το TCP layer "κρατάει" αυτά τα δεδομένα μέχρι να έρθουν τα προηγούμενα τους. Αφού έρθουν τα διατάσσει στην σωστή σειρά και έπειτα τα παραδίδει στην εφαρμογή.
- Απόρριψη διπλών δεδομένων. Αποτρέπει την αποστολή διπλότυπων, δηλαδή δύο ακριβώς ίδιων δεδομένων.
- Προσφέρει αυτοματοποιημένο έλεγχο ροής δεδομένων (flow control) και έλεγχο συμφόρησης (congestion control), που είναι απαραίτητοι για τη σωστή λειτουργία ενός δικτύου.

3.3.1.7 Εφαρμογές που χρησιμοποιούν το TCP

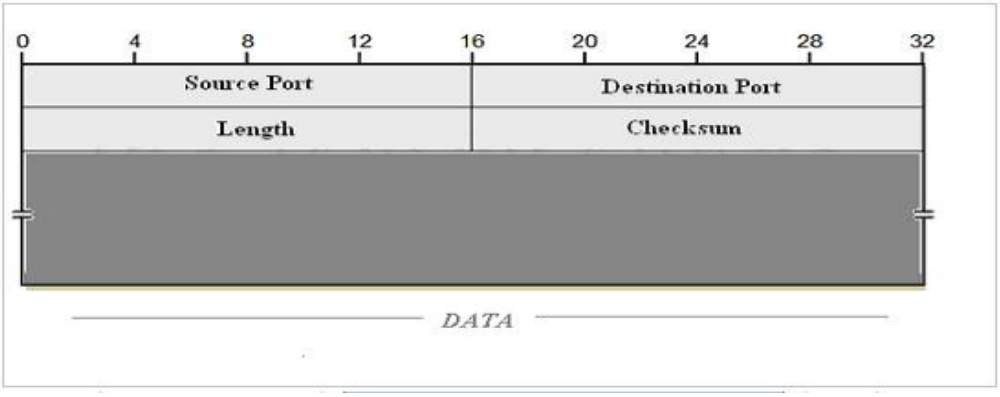
Εξαιτίας των παραπάνω χαρακτηριστικών του λοιπόν, το TCP χρησιμοποιείται και επιβάλλεται να χρησιμοποιείται , όπου η ακεραιότητα των δεδομένων είναι ύψιστης σημασίας. Δηλαδή σε εφαρμογές μεταφοράς αρχείων, σε αλληλεπιδραστικές εφαρμογές, υπηρεσίες όπως e-mail, web surfing και οποιαδήποτε άλλη μεταφορά data αρχείων ανάμεσα σε 2 υπολογιστές.

3.3.2 Το πρωτόκολλο UDP

Το **Πρωτόκολλο Αυτοδύναμων Πακέτων-UDP** (User Datagram Protocol), είναι ένα από τα βασικά πρωτόκολλα που χρησιμοποιούνται στο διαδίκτυο. Μία εναλλακτική ονομασία του πρωτοκόλλου είναι Universal Datagram Protocol. Διάφορα προγράμματα χρησιμοποιούν το πρωτόκολλο UDP για την αποστολή σύντομων μηνυμάτων (γνωστών και ως datagrams), από τον έναν υπολογιστή στον άλλον μέσα σε ένα δίκτυο υπολογιστών. Είναι πρωτόκολλο αυτοδύναμου πακέτου χωρίς σύνδεση δηλαδή η αποστολή ξεκινάει αμέσως, χωρίς να γίνει σύνδεση με την άλλη πλευρά και έτσι δεν υπάρχουν επιπλέον καθυστερήσεις. Δεν διαθέτει έλεγχο λαθών, δεν κάνει επαναμετάδοση δεδομένων και δεν κρατάει αντίγραφο των δεδομένων που στάλθηκαν για επιβεβαίωση. Επίσης, δεν εξασφαλίζει ότι τα τμήματα θα φτάσουν στον προορισμό τους με τη σωστή σειρά. Αν μια εφαρμογή που χρησιμοποιεί UDP χρειάζεται να εξασφαλίσει ότι τα δεδομένα της δεν έχουν επηρεαστεί από τα παραπάνω προβλήματα, τότε θα πρέπει να τα ελέγξει η ίδια. Μεταφέρεται δηλαδή, ο έλεγχος λαθών από το επίπεδο μεταφοράς στο επίπεδο εφαρμογής.

3.3.2.1 UDP Header

Κάθε πακέτο UDP έχει μια επικεφαλίδα που αναφέρει τα χαρακτηριστικά του. Η επικεφαλίδα, περιλαμβάνει τέσσερα πεδία, τα οποία είναι πολύ λίγα αν συγκριθούν με άλλα πρωτόκολλα, όπως το TCP. Δύο από τα τέσσερα πεδία είναι προαιρετικά. Στην π Εικόνα 29 βλέπουμε, την επικεφαλίδα του UDP και θα την αναλύσουμε πεδίο προς πεδίο.



Εικόνα 29: Η επικεφαλίδα του UDP (UDP Header)

Το πεδίο **Source port**, δείχνει τη θύρα του αποστολέα από την οποία προήλθε το πακέτο. Εάν ο παραλήπτης επιθυμεί να στείλει κάποια απάντηση, θα πρέπει να την στείλει

στην θύρα αυτήν. Το συγκεκριμένο πεδίο δεν είναι υποχρεωτικό και στις περιπτώσεις που δεν χρησιμοποιείται θα πρέπει να έχει την τιμή μηδέν.

Το πεδίο **Destination port**, δείχνει την θύρα του παραλήπτη στην οποία θα πρέπει να παραδοθεί το πακέτο.

Το πεδίο **Length,** έχει μέγεθος 16-bit και περιλαμβάνει το μέγεθος του πακέτου σε bytes. Το μικρότερο δυνατό μέγεθος είναι 8 bytes, αφού η κεφαλίδα αυτή καθ' αυτή καταλαμβάνει τόσο χώρο. Θεωρητικά, το μέγεθος του UDP πακέτου δεν μπορεί να ξεπερνάει τα 65,527 bytes, αλλά πρακτικά το όριο μειώνεται στα 65,507 bytes λόγω διαφόρων περιορισμών που εισάγει το πρωτόκολλο IPv4 στο επίπεδο δικτύου.

Το πεδίο **Checksum**, είναι ένα πεδίο 16-bit το οποίο χρησιμοποιείται για επαλήθευση της ορθότητας του πακέτου στο σύνολό του, δηλαδή τόσο της κεφαλίδας όσο και των δεδομένων. Το πεδίο αυτό είναι προαιρετικό.

3.3.2.2 Χαρακτηριστικά UDP

Τα κυριότερα χαρακτηριστικά του UDP είναι τα παρακάτω:

- Είναι αναξιόπιστο. Δεν μπορεί να εγγυηθεί την ακεραιότητα ή τη σωστή σειρά άφιξης των δεδομένων. Τα πακέτα (datagrams) μπορούν να φτάσουν με διαφορετική σειρά, να εμφανίζονται διπλά ή να μην έρθουν και καθόλου χωρίς καμία ειδοποίηση.
- Είναι γρήγορο. Αυτό το χαρακτηριστικό του εξασφαλίζει μικρό delay.
- Έχει πολλαπλή χρηστικότητα, δηλαδή, μπορεί να χρησιμοποιηθεί τόσο σε Unicast όσο και σε Multicast δίκτυα, καθώς δεν είναι connection protocol.
- Είναι "ελαφρύ", έτσι είναι λιγότερο απαιτητικό σε πόρους. Δεν δημιουργεί μεγάλο overhead στο δίκτυο, καθώς δεν ελέγχει αν όντως κάποιο πακέτο έφτασε ή όχι.
- Έχει μικρό Header. Το UDP έχει 8 bytes Header. Αυτό σημαίνει μικρότερο έξτρα overhead στο δίκτυο.

3.3.2.3 Εφαρμογές που χρησιμοποιούν το UDP

Οι εφαρμογές audio και video streaming χρησιμοποιούν κατά κόρον πακέτα UDP. Για τις εφαρμογές αυτές είναι πολύ σημαντικό τα πακέτα να παραδοθούν στον παραλήπτη σε σύντομο χρονικό διάστημα ούτως ώστε να μην υπάρχει διακοπή στην ροή του ήχου ή της εικόνας. Κατά συνέπεια προτιμάται το πρωτόκολλο UDP διότι είναι αρκετά γρήγορο, παρόλο που υπάρχει η πιθανότητα μερικά πακέτα UDP να χαθούν. Στην περίπτωση που

χαθεί κάποιο πακέτο, οι εφαρμογές αυτές διαθέτουν ειδικούς μηχανισμούς διόρθωσης και παρεμβολής ούτως ώστε ο τελικός χρήστης να μην παρατηρεί καμία αλλοίωση ή διακοπή στην ροή του ήχου και της εικόνας λόγω του χαμένου πακέτου. Σε αντίθεση με το πρωτόκολλο TCP, το UDP υποστηρίζει broadcasting, δηλαδή την αποστολή ενός πακέτου σε όλους τους υπολογιστές ενός δικτύου, και multicasting, δηλαδή την αποστολή ενός πακέτου σε κάποιους συγκεκριμένους υπολογιστές ενός δικτύου. Μερικές σημαντικές εφαρμογές που χρησιμοποιούν πακέτα UDP είναι οι εξής: Domain Name System (DNS), IPTV, Voice over IP (VoIP), Trivial File Transfer Protocol (TFTP), online games, Simple Network Management Protocol (SNMP) Dynamic Host Configuration Protocol (DHCP) και το Routing Information Protocol (RIP).

3.3.3 Το πρωτόκολλο RTP

Το πρωτόκολλο **Μεταφοράς Δεδομένων Πραγματικού Χρόνου-RTP** (Real-time Transport Protocol), είναι ένα δημοφιλές πρωτόκολλο για τη μεταφορά δεδομένων (εικόνας ή ήχου ή και των δύο), σε πραγματικό χρόνο μεταξύ τελικών συστημάτων πάνω σε ένα δίκτυο. Μπορεί να χρησιμοποιηθεί για μεταφορά κοινών αλλά και πιο εξειδικευμένων μορφών ήχου και video. Παραδείγματα κοινών μορφών ήχου είναι PCM, GCM και MP3, ενώ για video είναι MPEG και H.261. Είναι προϊόν επιστημονικής έρευνας της ομάδας εργασίας Audio Video Transmit (AVT), που δημιουργήθηκε στα πλαίσια της κοινότητας Internet Engineering Task Force (IETF), με σκοπό τον καθορισμό ενός πρωτοκόλλου για real-time μεταφορά δεδομένων ήχου και video πάνω από unicast ή multicast μετάδοση.

Το RTP, συνεργάζεται εξίσου αποτελεσματικά με υπηρεσίες μετάδοσης δεδομένων τύπου unicast (μόνο-εκπομπή) αλλά και τύπου multicast (πολύ-εκπομπή). Σε κάθε unicast μετάδοση δεδομένων ένα ξεχωριστό αντίγραφο δεδομένων στέλνεται από τον αποστολέα προς τον κάθε παραλήπτη. Δηλαδή, αν ο αποστολέας έχει να στείλει τα δεδομένα σε n παραλήπτες, τότε πρέπει να δημιουργηθούν n αντίγραφα των δεδομένων, ένα για κάθε unicast μετάδοση. Σε κάθε multicast μετάδοση δεδομένων ο αποστολέας εκπέμπει τα δεδομένα μόνο μια φορά και μετά είναι υπεύθυνο το δίκτυο να διοχετεύσει τα δεδομένα σε πολλαπλούς παραλήπτες. Επίσης, στη multicast μετάδοση οι παραλήπτες στέλνουν τις αναφορές τους πίσω προς όλα τα μέλη της ομάδας στην οποία γίνεται η επικοινωνία. Αυτό επιτρέπει σε όλους τους συμμετέχοντες να γνωρίζουν το εύρος ζώνης που απαιτείται για τη μεταφορά των δεδομένων και το φόρτο που προσθέτουν στον αποστολέα.

Το RTP, επιτρέπει στις εφαρμογές να αναγνωρίσουν τον τύπο των δεδομένων που μεταφέρονται (video ή ήχο), να εξακριβώσουν με ποια σειρά τα δεδομένα πρέπει να αναπαραχθούν και να συγχρονίσουν την αναπαραγωγή δεδομένων που προέρχονται από το ίδιο τερματικό σύστημα αλλά από διαφορετική πηγή.

Το RTP, δεν εγγυάται ότι τα δεδομένα που μεταδίδονται από ένα τερματικό σύστημα θα παραδοθούν στον παραλήπτη έγκαιρα και στη σειρά με την οποία μεταδόθηκαν. Δεν εγγυάται ποιότητα υπηρεσίας (QoS), ούτε δεσμεύει πόρους και δεν παρέχει κανένα μηχανισμό ελέγχου. Στην πραγματικότητα, δεν εγγυάται καθόλου την παράδοση των δεδομένων. Αξίζει να αναφερθεί ότι η ενσωμάτωση πακέτων RTP μέσα σε αυτά του UDP, γίνεται αντιληπτή μόνο στα τελικά συστήματα που παραλαμβάνουν τα δεδομένα.

Εκτός από τους συνηθισμένους ρόλους του αποστολέα και του παραλήπτη, το RTP εισάγει και δύο νέους ρόλους, του **μεταφραστή** (translator) και του **αναμείκτη** (mixer). Οι μεταφραστές και οι μείκτες βρίσκονται στο δίκτυο ανάμεσα στους αποστολείς και τους παραλήπτες και επεξεργάζονται RTP πακέτα που περνούν από αυτούς. Οι μεταφραστές απλώς μεταφράζουν μια μορφή ωφέλιμου φορτίου σε μια άλλη. Οι αναμείκτες, είναι παρόμοιοι με τους μεταφραστές αλλά, αντί να μεταφράζουν ξεχωριστά ρεύματα σε διαφορετικές μορφές, συνδυάζουν πολλαπλά ρεύματα σε ένα απλό ρεύμα διατηρώντας την αρχική τους μορφή.

3.3.3.1 Μεταφραστές και αναμείκτες

Το RTP υποστηρίζει την έννοια των αναμεταδοτών. Αναμεταδότες στο RTP, είναι συστήματα που λειτουργούν στο επίπεδο μεταφοράς και μπορούν να λαμβάνουν και να αποστέλλουν δεδομένα προς τα μέλη μια ς συνόδου. Χρησιμοποιούνται σε περιπτώσεις κατά τις οποίες ένα μέλος μια συνόδου αποστέλλει δεδομένα σε ένα άλλο μέλος, αλλά δεν μπορεί να το κάνει άμεσα είτε γιατί δεν χρησιμοποιεί καμία από τις κωδικοποιήσεις δεδομένων που χρησιμοποιεί ο συνομιλητής του, είτε γιατί το άλλο άκρο βρίσκεται πίσω από κάποιο firewall και δεν μπορεί να έχει άμεση επικοινωνία με κανέναν κόμβο στο Internet.

Μια κατηγορία αναμεταδότη είναι ο αναμείκτης (mixer), ο οποίος λαμβάνει δεδομένα από μια ή περισσότερες πηγές πληροφορίας τις συνδυάζει σε μια ροή και την στέλνει σε έναν ή περισσότερους παραλήπτες. Κατά την μείξη των διαφορετικών ροών

έχει τη δυνατότητα να αλλάζει και τη μέθοδο κωδικοποίησης και συμπίεσης δεδομένων. Κατά την ανάμειξη πληροφοριών, δεν είναι απαραίτητο όλες οι ροές να έχουν συγχρονισμένη χρονοσήμανση (timestamp). Ο αναμείκτης αναλαμβάνει να προσθέσει στην τελική ροή το δικό του χρονισμό και να προσθέσει τον εαυτό του σαν πηγή πληροφορίας.

Ο μεταφραστής, είναι ένας απλούστερος αναμεταδότης ο οποίος λαμβάνει ένα πακέτο κάθε φορά το επεξεργάζεται και το αποστέλλει. Αυτός μπορεί να αλλάξει την αρχική κωδικοποίηση της πληροφορίας, προκειμένου αυτή να γίνει αναγνωρίσιμη και επεξεργάσιμη από σταθμούς που δεν την υποστηρίζουν. Μπορεί επίσης να αυξήσει τη συμπίεση των δεδομένων, ώστε αυτά να διακινούνται και μέσω γραμμών χαμηλής χωρητικότητας, έστω και με χαμηλότερη ποιότητα.

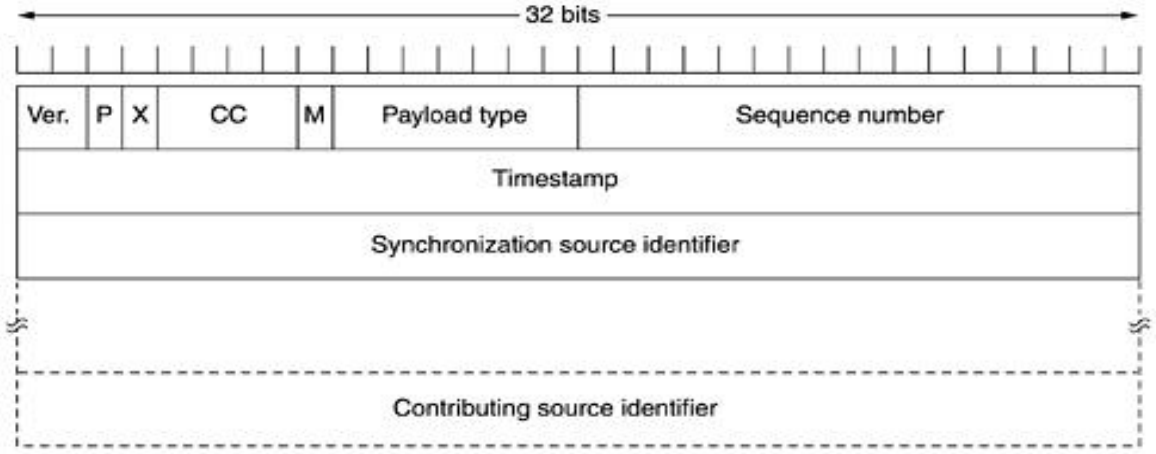
3.3.3.2 Τρόπος λειτουργίας RTP

Συνήθως το RTP βρίσκεται πάνω από το UDP στη στοίβα των πρωτοκόλλων. Το TCP και το UDP, είναι τα πρωτόκολλα που χρησιμοποιούνται πιο πολύ στο Internet για τη μετάδοση δεδομένων. Το TCP παρέχει connection-oriented και αξιόπιστη ροή δεδομένων ανάμεσα σε δύο υπολογιστές, ενώ το UDP παρέχει connectionless αλλά όχι αξιόπιστες υπηρεσίες. Το UDP επιλέγεται σαν το πρωτόκολλο μεταφοράς του RTP επειδή, το RTP είναι κυρίως σχεδιασμένο για multicast μεταδόσεις κάτι το οποίο δεν συμβαδίζει με το TCP που είναι συνδεσμοστρεφής πρωτόκολλο. Επίσης, επειδή για δεδομένα πραγματικού χρόνου, η αξιοπιστία δεν είναι τόσο σημαντική όσο η έγκαιρη μετάδοση. Η αξιόπιστη μετάδοση η οποία επιτυγχάνεται μέσω της επαναμετάδοσης των χαμένων πακέτων, μπορεί μα μην είναι επιθυμητή διαδικασία, αφού μπορεί να προκαλέσει υπερφόρτωση του δικτύου και προβλήματα στη συνεχή μετάδοση των δεδομένων.

Η εφαρμογή που τρέχει στην πλευρά του αποστολέα (εξυπηρετητή), δημιουργεί ένα πακέτο RTP στο οποίο έχει συμπεριλάβει τα προς μετάδοση δεδομένα και πληροφορίες που είναι απαραίτητες για τη σωστή λειτουργία του πρωτοκόλλου. Δηλαδή τα δεδομένα τα ενσωματώνει σε ένα πακέτο RTP με το να προσθέτει το RTP Header. Στη συνέχεια ενσωματώνει αυτό το πακέτο σε ένα ευρύτερο πακέτο του UDP με το να προσθέσει το UDP Header στο επίπεδο μεταφοράς. Τέλος, ότι έχει προκύψει το παραδίδει στο IP το οποίο προσθέτει το IP Header στο επίπεδο δικτύου.

3.3.3.3 Κεφαλίδα του RTP

Στην Εικόνα 30 που ακολουθεί παρουσιάζεται η κεφαλίδα του RTP η οποία αποτελείται από τρεις 32μπιτες λέξεις και θα την αναλύσουμε πεδίο προς πεδίο.



Εικόνα 30: Η κεφαλίδα του RTP

Το πεδίο **Version**, δείχνει την έκδοση του πρωτοκόλλου.

Το πεδίο **Padding** (P), δείχνει ότι το πακέτο έχει συμπληρωθεί, σε ένα πολλαπλάσιο των 4 byte. Το τελευταίο byte συμπλήρωσης δείχνει πόσα byte προστέθηκαν.

Το πεδίο **Extension** (X), δείχνει ότι υπάρχει μια κεφαλίδα επέκτασης. Η μορφή και η σημασία της κεφαλίδας επέκτασης δεν καθορίζονται. Το μόνο πράγμα που καθορίζεται είναι ότι η πρώτη λέξη της επέκτασης πρέπει να προσδιορίζει το μήκος της.

Το πεδίο **CC** (Contributing sources), δείχνει το πλήθος των CC αναγνωριστικών που ακολουθούν τη βασική κεφαλίδα.

Το πεδίο **Marker** (M), καθορίζεται από το προφίλ των δεδομένων. Αν είναι συμπληρωμένο, σημαίνει ότι τα τρέχοντα δεδομένα έχουν κάποια ειδική σχέση με την εφαρμογή.

Το πεδίο **Payload type**, δείχνει ποιος αλγόριθμος κωδικοποίησης έχει χρησιμοποιηθεί. Με αυτό το πεδίο ο αποστολέας γνωρίζει πώς να ερμηνεύσει και να αναπαράγει το φορτίο.

Το πεδίο **Sequence number**, είναι ένας μετρητής που αυξάνεται σε κάθε πακέτο RTP που στέλνεται. Χρησιμοποιείται για τον εντοπισμό των χαμένων πακέτων.

Το πεδίο **Timestamp**, αποτυπώνει τη χρονική στιγμή της δημιουργίας του πρώτου byte στο πακέτο. Η τιμή αυτή μπορεί να βοηθήσει στη μείωση της παραμόρφωσης χρονισμού στον παραλήπτη, επειδή ‘‘ αποσυνδέει’’ το χρόνο αναπαραγωγής από το χρόνο άφιξης του πακέτου.

Το πεδίο **Synchronization source identifier**, δείχνει σε ποια ροή ανήκει το πακέτο. Αυτή είναι η μέθοδος που χρησιμοποιείται για την πολύπλεξη και την αποπολύπλεξη πολλαπλών ροών δεδομένων σε μια μόνο ροή πακέτων UDP.

Τέλος, το πεδίο **Contributing source identifier**, χρησιμοποιείται όταν υπάρχουν αναμείκτες. Στην περίπτωση αυτή, η πηγή συγχρονισμού είναι ο αναμείκτης και στο πεδίο αυτό προσδιορίζονται οι ροές που χρησιμοποιούνται για τη μείξη.

3.3.3.4 Χαρακτηριστικά RTP

Το RTP παρέχει από άκρο εις άκρο υπηρεσίες, για δεδομένα με χαρακτηριστικά πραγματικού χρόνου, όπως το αλληλεπιδραστικό video. Οι εφαρμογές, κυρίως τρέχουν το RTP πάνω από το UDP για να κάνουν χρήση της πολυπλεξίας του και των υπηρεσιών για ανίχνευση λαθών. Παρόλα αυτά, έχουν γίνει προσπάθειες ώστε το RTP να γίνει ανεξάρτητο του επιπέδου μεταφοράς επομένως, θα μπορούσε να χρησιμοποιηθεί πάνω και από άλλα πρωτόκολλα.

Το RTP από μόνο του δεν μπορεί να παρέχει μηχανισμούς που να διασφαλίζουν την έγκαιρη παράδοση ή να εγγυώνται ποιότητα υπηρεσιών, αλλά βασίζεται στα πρωτόκολλα χαμηλότερων επιπέδων για αυτές τις υπηρεσίες. Επίσης, το RTP είναι μια υποδομή πρωτοκόλλου που είναι σκόπιμα μη ολοκληρωμένη. Ένας ολοκληρωμένος ορισμός για το RTP, για συγκεκριμένη εφαρμογή απαιτεί και άλλους ορισμούς όπως το format του φορτίου.

Το πρωτόκολλο RTP, δεν προϋποθέτει τίποτα για το υποκείμενο δίκτυο εκτός του ότι παρέχει πλαισίωση. Δεν γνωρίζει την έννοια της σύνδεσης και γι’ αυτό μπορεί να λειτουργεί είτε πάνω από προσανατολισμένα κατά σύνδεση δίκτυα είτε πάνω από χωρίς σύνδεση πρωτόκολλα χαμηλού επιπέδου. Ο πρωταρχικός σχεδιασμός του RTP σκόπευε στο να χρησιμοποιηθεί στο Internet, αλλά τείνει να γίνει ανεξάρτητο των πρωτοκόλλων και να τρέχει πάνω από ATM και IPv6.

3.4 Βιβλιογραφία & πηγές

Βιβλία

[1] Andrew S. Tanenbaum, 4η Αμερικάνικη Έκδοση <<Δίκτυα Υπολογιστών>>

[2] James Kurose & Keith Ross, 4η Έκδοση <<Δικτύωση Υπολογιστών- Προσέγγιση από Πάνω προς τα Κάτω>>

Links

[1] http://el.wikipedia.org/wiki/Transmission_Control_Protocol

[2] http://el.wikipedia.org/wiki/UDP

[3] http://el.wikipedia.org/wiki/Internet_Protocol

[4] http://en.wikipedia.org/wiki/Real-time_Transport_Protocol

[5] http://www.tcpipguide.com

[6] http://www.cs.uoi.gr/~epap/diktua/downloads/lect7.pdf

[7] http://www.freebsdworld.gr/diktia/theBookII.pdf

[8]http://www.teiser.gr/icd/staff/chilas/files/D_II/Transmission%20Control%20Protocol.pdf

ΚΕΦΑΛΑΙΟ 4: ΘΕΩΡΗΤΙΚΗ ΠΕΡΙΓΡΑΦΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ ΚΙΝΗΣΗΣ, ΤΩΝ ΣΗΜΑΝΤΙΚΟΤΕΡΩΝ ΔΙΑΔΙΚΤΥΑΚΩΝ ΕΦΑΡΜΟΓΩΝ

4.1 Voice over Internet Protocol (VoIP)

4.1.1 Τι είναι το VoIP;

Η τεχνολογία της Τηλεφωνίας πάνω από IP (Voice over Internet Protocol - VoIP) χρησιμοποιεί το Πρωτόκολλο Διαδικτύου (Internet Protocol - IP) ώστε να μεταδώσει φωνητικά σήματα σε μορφή πακέτων πάνω από το διαδίκτυο. Με αυτόν τον τρόπο, το VoIP μπορεί να επιτευχθεί σε οποιοδήποτε δίκτυο το οποίο χρησιμοποιεί IP, όπως το Internet, Intranet και τα Τοπικά Δίκτυα. Το φωνητικό σήμα σε αυτή τη τεχνολογία μετατρέπεται σε ψηφιακό συμπιέζεται, μετατρέπεται σε πακέτα IP και στη συνέχεια εκπέμπεται πάνω από το δίκτυο IP. Πρωτόκολλα σηματοδοσίας χρησιμοποιούνται για να εγκαταστήσουν και να τερματίσουν μια κλήση, να μεταφέρουν πληροφορίες ώστε να βρεθεί η θέση το χρήστη και να διαπραγματευτούν δυνατότητες του δικτύου. Ένα από τα σημαντικότερα πλεονεκτήματα της τεχνολογίας του VoIP είναι η πολύ χαμηλή χρέωση των κλήσεων. Άλλα πλεονεκτήματα είναι η κάλυψη των συνεχώς αυξανόμενων απαιτήσεων για επικοινωνίες πολυμέσων καθώς και των απαιτήσεων για ενοποίηση των δικτύων φωνής και δεδομένων (voice and data networks). Υπάρχουν τρεις διαφορετικές πτυχές της υπηρεσίας VoIP:

ATA (Analog Telephone Adaptor): ο οποίος είναι ένα μετατροπέας αναλογικού σήματος σε ψηφιακό (A/D converter). Λαμβάνει το αναλογικό σήμα από το κλασικό τηλέφωνο και το μετατρέπει σε ψηφιακά δεδομένα. Κυκλωματικά, παρεμβάλλεται ανάμεσα στην απλή τηλεφωνική συσκευή και στην πρίζα του τηλεφώνου.

IP Phones: τα οποία αντί για τους τυπικούς RJ - 11 connectors, έχουν έναν RJ - 45 Ethernet connector. Τα τηλέφωνα IP συνδέονται κατευθείαν σε έναν router και διαθέτουν το απαραίτητο hardware και software για τη διεκπεραίωση μιας κλήσης IP.

Computer - to - computer: το οποίο χρησιμοποιεί ένα software (πχ.Skype) που είναι εγκατεστημένο σε όλα τα τερματικά και αυτό μπορεί να τους παρέχει VoIP επικοινωνία.

4.1.2 Πρωτόκολλα σηματοδοσίας VoIP

Υπάρχει μια πληθώρα πρωτοκόλλων που χρησιμοποιούνται αυτή τη στιγμή για το VoIP. Τα πρωτόκολλα αυτά προσδιορίζουν τους τρόπους με τους οποίους συσκευές όπως οι codecs συνδέονται η μία με την άλλη και με το δίκτυο χρησιμοποιώντας το VoIP. Επίσης περιλαμβάνουν διευκρινίσεις (specifications) για audio codecs. Παρακάτω θα αναλύσουμε δύο από αυτά τα standards:

1. H.323
2. Session Initiation Protocol (SIP)

Στην Εικόνα 31 παρουσιάζεται μια σύντομη συγκριτική αναφορά των παραπάνω πρωτοκόλλων.

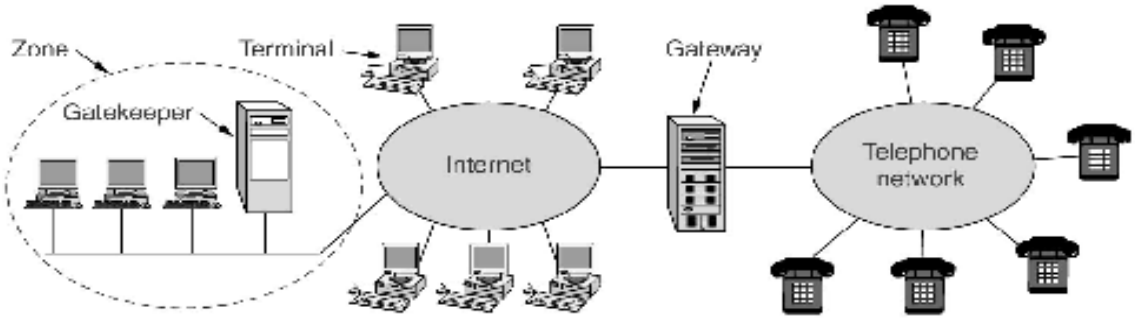
	H.323	SIP
Standardization	ITU-T	IETF
Architectural model	Peer-to-peer	Peer-to-peer
Media types	Voice, video, limited data	Voice, video, data
Call control	Gatekeeper	Proxy/Redirect Server
Endpoints	Gateway, terminal	User agent
Signaling transport	TCP or UDP	TCP or UDP
Network scope	Intranet, Extranet, Internet	Intranet, Extranet, Internet
Extensibility	Low	High
Scalability	Medium	High
Ease of deployment	Low	High

Εικόνα 31: Σύντομη συγκριτική αναφορά H.323 και SIP

H.323

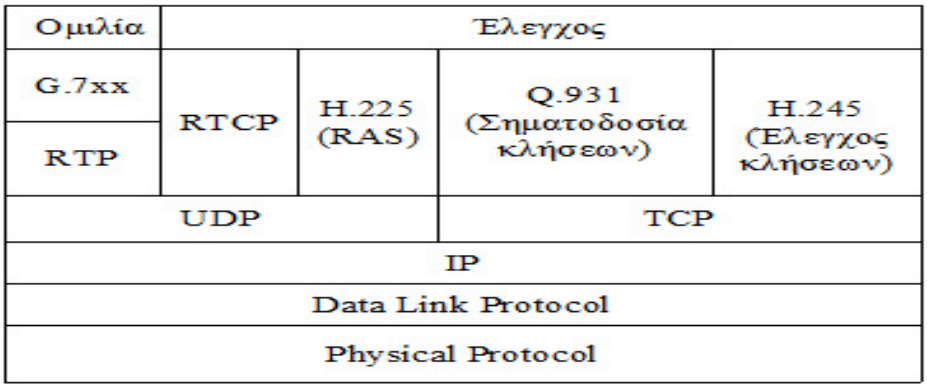
Το H.323 είναι μια πρόταση από την ITU που προσδιορίζει τα συστατικά, τα πρωτόκολλα και τις διαδικασίες που παρέχουν υπηρεσίες πολυμεσικών επικοινωνιών (real-time voice, video, chat, whiteboard, file sharing κλπ.) πάνω σε δίκτυα μετάδοσης πακέτων. Το H.323 είναι περισσότερο μια αρχιτεκτονική επισκόπηση της τηλεφωνίας Internet, παρά ένα συγκεκριμένο πρωτόκολλο. Αναφέρεται σε μεγάλο πλήθος συγκεκριμένων πρωτοκόλλων για κωδικοποίηση φωνής, εγκαθίδρυση κλήσεων,

σηματοδοσία, μεταφορά δεδομένων και άλλα θέματα, αντί να προδιαγράφει αυτό τα αντίστοιχα θέματα. Το γενικό μοντέλο απεικονίζεται στην Εικόνα 32. Στο κέντρο υπάρχει μια **πύλη δικτύου** (gateway) η οποία συνδέει το Internet με το τηλεφωνικό δίκτυο επικοινωνώντας με τα πρωτόκολλα της κάθε πλευράς. Οι συσκευές που επικοινωνούν ονομάζονται **τερματικά** (terminals). Ένα LAN μπορεί να έχει ένα **φρουρό πύλης** (gatekeeper) ο οποίος ελέγχει τα τερματικά σημεία που βρίσκονται στην δικαιοδοσία του, η οποία ονομάζεται **ζώνη** (zone).



Εικόνα 32: Το αρχιτεκτονικό μοντέλο του H.323 για την τηλεφωνία μέσω Internet

Ένα τηλεφωνικό δίκτυο χρειάζεται κάποια πρωτόκολλα. Καταρχήν, χρειάζεται ένα πρωτόκολλο για κωδικοποίηση και αποκωδικοποίηση ομιλίας και το οποίο ορίζεται στη σύσταση **G.711** της ITU. Δεν είναι όμως το μόνο πρωτόκολλο που υποστηρίζεται από το H.323 υποστηρίζονται και πολλά άλλα πρωτόκολλα συμπίεσης φωνής. Αφού επιτρέπονται διάφοροι αλγόριθμοι συμπίεσης, χρειάζεται ένα πρωτόκολλο που θα επιτρέπει στα τερματικά να διαπραγματεύονται ποιόν αλγόριθμο θα χρησιμοποιούν. Το πρωτόκολλο αυτό είναι το **H.245** το οποίο διαπραγματεύεται και το ρυθμό μετάδοσης bit. Το RTCP απαιτείται για τον έλεγχο των καναλιών RTP. Χρειάζεται επίσης ένα πρωτόκολλο για την εγκαθίδρυση και την αποδέσμευση συνδέσεων, παροχή τόνων επιλογής, παραγωγή κουδουνίσματος κλπ., το πρωτόκολλο που χρησιμοποιείται είναι το **Q.931**. Το κανάλι μεταξύ προσωπικού υπολογιστή και φρουρού πύλης το οποίο ελέγχεται από το πρωτόκολλο αυτό ονομάζεται κανάλι **Εγγραφής/Εισόδου/Κατάστασης** ή **RAS.** Το κανάλι αυτό επιτρέπει στα τερματικά να εισέρχονται και να αποχωρούν από τη ζώνη, να ζητούν και να επιστρέφουν εύρος ζώνης για την πραγματική μετάδοση των δεδομένων. Τέλος, χρειάζεται ένα πρωτόκολλο για την πραγματική μετάδοση των δεδομένων και γι αυτό το σκοπό χρησιμοποιείται το RTP. Ο έλεγχος γίνεται με το RTCP. Οι σχετικές θέσεις των πρωτοκόλλων φαίνεται στην Εικόνα 33.



Εικόνα 33: Η στοίβα πρωτοκόλλων του H.323

SIP – Το πρωτόκολλο έναρξης συνδιάλεξης

Η IETF σύστησε μια επιτροπή για να σχεδιάσει έναν απλούστερο και πιο αρθρωτό τρόπο για την υλοποίηση της φωνής μέσω IP. Έτσι αναπτύχθηκε το **Πρωτόκολλο Έναρξης Συνδιάλεξης** ή **SIP** (Session Initiation Protocol), το οποίο περιγράφεται στο RFC 3261. Το πρωτόκολλο αυτό περιγράφει πως εγκαθιδρύονται τηλεφωνικές κλήσεις, βίντεο-διασκέψεις και άλλες συνδέσεις πολυμέσων μέσω Internet. Σε αντίθεση με το H.323, το οποίο είναι ένα πλήρες πακέτο πρωτοκόλλων, το SIP είναι μία μόνο υπομονάδα, έχει όμως σχεδιαστεί για να παρέχει καλή διαλειτουργικότητα με τις υπάρχουσες εφαρμογές του Internet. Το SIP μπορεί να εγκαθιδρύσει συνδιαλέξεις δύο μερών, συνδιαλέξεις πολλών μερών και συνδιαλέξεις πολυδιανομής. Το SIP ασχολείται μόνο με την εγκαθίδρυση, τη διαχείριση και τον τερματισμό των συνδιαλέξεων. Άλλα πρωτόκολλα, όπως το RTP/RTCP, χρησιμοποιούνται για τη μεταφορά των δεδομένων. Το SIP είναι ένα πρωτόκολλο επιπέδου εφαρμογών και μπορεί να εκτελεστεί πάνω από το UDP ή το TCP.

Το SIP υποστηρίζει ποικίλες υπηρεσίες, στις οποίες περιλαμβάνεται ο εντοπισμός του καλούμενου και ο προσδιορισμός των δυνατοτήτων του, καθώς και η διαχείριση του μηχανισμού διευθέτησης και τερματισμού κλήσεων. Οι τηλεφωνικοί αριθμοί στο SIP αναπαριστάνονται σε μορφή URL και μπορούν να περιέχουν διευθύνσεις IPv4, IPv6 ή πραγματικούς τηλεφωνικούς αριθμούς

Το πρωτόκολλο SIP βασίζεται σε κείμενο και έχει ως μοντέλο το HTTP. Το ένα άκρο στέλνει ένα μήνυμα κειμένου ASCII, το οποίο αποτελείται από το όνομα μεθόδου στην πρώτη γραμμή και ακολουθείται από πρόσθετες γραμμές που περιέχουν κεφαλίδες για μεταβίβαση παραμέτρων. Πολλές από τις κεφαλίδες προέρχονται από το MIME, έτσι

ώστε να διευκολύνουν τη διαλειτουργικότητα του SIP με τις υπάρχουσες εφαρμογές του Internet. Οι έξι μέθοδοι που ορίζονται στις προδιαγραφές πυρήνα φαίνονται στην Εικόνα 34.

Μέθοδος	Περιγραφή
INVITE	Αίτηση έναρξης μια συνδιάλεξης
ACK	Επιβεβαίωση ότι η συνδιάλεξη έχει ξεκινήσει
BYE	Αίτηση τερματισμού μια συνδιάλεξης
OPTIONS	Ερώτημα σε έναν υπολογιστή υπηρεσίας για τις δυνατότητες του
CANCEL	Ακύρωση μιας εκκρεμούς αίτησης
REGISTER	Πληροφόρηση ενός διακομιστή ανακατεύθυνσης σχετικά με την τρέχουσα θέση του χρήστη

Εικόνα 34: Οι μέθοδοι του SIP που ορίζονται στις προδιαγραφές πυρήνα.

Για να εγκαθιδρυθεί μια συνδιάλεξη, ο καλών είτε δημιουργεί μια σύνδεση TCP με τον καλούμενο και του στέλνει μέσω αυτής ένα μήνυμα INVITE, είτε στέλνει το μήνυμα INVITE μέσα σε ένα πακέτο UDP. Και στις δύο περιπτώσεις, οι κεφαλίδες στη δεύτερη και στις επόμενες γραμμές περιγράφουν τη δομή του σώματος του μηνύματος, το οποίο περιέχει τις δυνατότητες του καλούντα, τους τύπους μέσων και τις μορφές τους. Αν ο καλούμενος αποδεχτεί την κλήση, απαντά με έναν κωδικό απάντησης τύπου HTTP. Μετά τη γραμμή κωδικού απάντησης, ο καλούμενος μπορεί επίσης να δώσει πληροφορίες για τις δυνατότητες του, τους τύπους μέσων και τις μορφές τους. Η σύνδεση πραγματοποιείται νε τριπλή χειραψία, έτσι ο καλούμενος απαντά με ένα μήνυμα ACK για να ολοκληρώσει το πρωτόκολλο και να επιβεβαιώσει τη λήψη του μηνύματος αποδοχής.

Οποιοδήποτε άκρο μπορεί να ζητήσει τερματισμό μιας συνδιάλεξης στέλνοντας ένα μήνυμα το οποίο περιέχει τη μέθοδο BYE. Όταν το άλλο επιβεβαιώσει το μήνυμα αυτό η συνδιάλεξη τερματίζεται.

Η μέθοδος OPTIONS χρησιμοποιείται για να ερωτηθεί μια μηχανή σχετικά με τις δυνατότητες της. Συνήθως χρησιμοποιείται πριν την έναρξη μιας σύνδεσης, για να εξεταστεί αν η μηχανή είναι ικανή να ξεκινήσει μια συνδιάλεξη.

Η μέθοδος REGISTER σχετίζεται με την ικανότητα του SIP να εντοπίζει και να συνδέεται με ένα χρήστη που δεν βρίσκεται στην οικιακή του θέση. Το μήνυμα αυτό στέλνεται σε ένα διακομιστή εντοπισμού του SIP, ο όποιος παρακολουθεί ποιος βρίσκεται

που. Ο διακομιστής αυτός μπορεί αργότερα να ερωτηθεί για να εντοπισθεί η τρέχουσα θέση του χρήστη. Η λειτουργία της ανακατεύθυνσης απεικονίζεται στην Εικόνα 35.

Εικόνα 35: Χρήση διακομιστή μεσολάβησης και υπηρεσίας εντοπισμού στο SIP

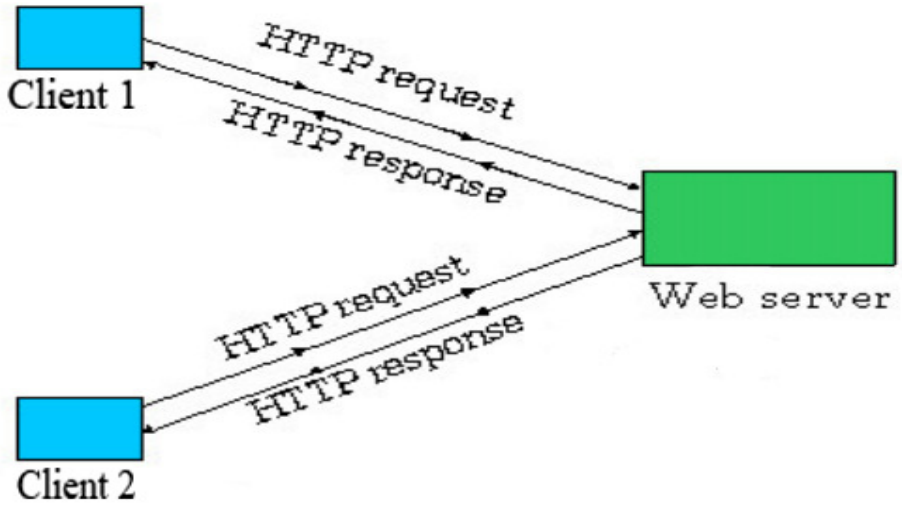
4.2 Browsing – Περιήγηση στο Διαδίκτυο

4.2.1 Το πρωτόκολλο HTTP

Το Hypertext Transfer Protocol (HTTP) αποτελεί το βασικό πρωτόκολλο για την ανταλλαγή πληροφορίας στο πλαίσιο του WWW. Είναι ένα ιδιαίτερα ευέλικτο πρωτόκολλο επιπέδου εφαρμογής (application level) που καθορίζει απλές δοσοληψίες μεταξύ του WWW browser και ενός HTTP server. Βασικός στόχος του HTTP είναι η επίτευξη χαμηλών χρόνων απόκρισης (response times). Προς αυτή την κατεύθυνση το HTTP αναπτύχθηκε σαν πρωτόκολλο χωρίς μνήμη (stateless protocol) δηλ. δεν διατηρεί καμία πληροφορία για μία σύνδεση μετά από την διεκπεραίωση μίας σχετικής αίτησης. Η διατήρηση πληροφορίας κατάστασης μπορεί να επιτευχθεί εκτός από τον ίδιο τον HTTP server μέσω εξωτερικών προγραμμάτων που ακολουθούν το πρωτόκολλο CGI ή βάσεων δεδομένων. Τέλος το HTTP χαρακτηρίζεται αντικειμενοστραφές (object oriented protocol). Μπορεί να εφαρμοστεί, με μικρές μετατροπές στις υποστηριζόμενες μεθόδους, σε name servers και κατανεμημένα συστήματα διαχείρισης αντικειμένων.

Τα μηνύματα του HTTP μοιάζουν σημαντικά με αυτά των πρωτοκόλλων FTP (File Transfer) και NNTP (Network News). Η βασική τους διαφορά είναι ο stateless χαρακτήρας του HTTP που δεν εντοπίζεται στα υπόλοιπα. Η απουσία μνήμης κρίνεται αποδοτική (efficient) για το πρωτόκολλο όταν ένας σύνδεσμος (link) από ένα αντικείμενο οδηγεί σε ένα αντικείμενο που βρίσκεται αποθηκευμένο σε άλλο server. Επίσης η ιδιότητα

αυτή κρίνεται κατάλληλη εφόσον ο client επιστρέφει πληροφορία στον χρήστη με βάση URIs και όχι παλαιότερες ενέργειες του.



Εικόνα 36: Βασική ιδέα του τρόπου λειτουργίας του HTTP

Λειτουργία

Το HTTP ακολουθεί το μοντέλο request/response. Ο client εγκαθιδρύει μία σύνδεση με τον server, κάνοντας χρήση του πρωτοκόλλου TCP, και αποστέλλει μία αίτηση προς αυτόν η οποία περιέχει:

- Την μέθοδο που πρόκειται να εφαρμοστεί σαν αποτέλεσμα της αίτησης (request method). Η χρήση του όρου μέθοδος οφείλεται στον αντικειμενοστρεφή προσανατολισμό του πρωτοκόλλου.
- Ένα Universal Resource Identifier (URI). Ο πόρος στον οποίο πρόκειται να εφαρμοστεί η παραπάνω μέθοδος.
- Την έκδοση του χρησιμοποιούμενου πρωτοκόλλου.
- Ένα μήνυμα που έχει την μορφή MIME (Multipurpose Internet Mail Extensions) και περιέχει πληροφορία σχετικά με τον client, πιθανά το σώμα του μηνύματος κα.

Ο server απαντάει με ένα μήνυμα που περιέχει:

- Μία γραμμή κατάστασης (Status line) που περιέχει την έκδοση του πρωτοκόλλου και κωδικό επιτυχίας/αποτυχίας (success/error code).
- Ένα μήνυμα που ακολουθεί την μορφή MIME και περιέχει πληροφορία σχετικά με τον server, μετά-πληροφορία σχετικά με το μεταφερόμενο αντικείμενο και πιθανά το σώμα του μηνύματος.

Η επικοινωνία HTTP γίνεται περισσότερο σύνθετη όταν μεταξύ του user agent και του origin server (request/response chain) παρεμβάλλονται ενδιάμεσοι (intermediaries). Αυτοί εμφανίζονται σε τρεις μορφές: proxy, gateway και tunnel. Ένας proxy ενδιάμεσος αποτελεί έναν πράκτορα προώθησης (forwarding agent) ο οποίος δέχεται αιτήσεις για κάποιο URI σε απόλυτη μορφή (absolute form), ανασκευάζει τα σχετικά μηνύματα μεταβάλλοντας όλα τα συστατικά τμήματα τους και τα προωθεί στον server ο οποίος προσδιορίζεται από το URI. Ένας gateway ενδιάμεσος αποτελεί ένα πράκτορα παραλαβής (receiving agent) ο οποίος τοποθετείται στο αμέσως υψηλότερο επίπεδο από ορισμένους servers και μεταφράζει τις αιτήσεις στο πρωτόκολλο που οι servers αυτοί αντιλαμβάνονται και μπορούν να ερμηνεύσουν. Ένας tunnel ενδιάμεσος λειτουργεί ως σημείο μεταγωγής (relay point) μεταξύ δύο συνδέσεων χωρίς να παρεμβαίνει στο περιεχόμενο των μηνυμάτων.

Όπως επισημάνθηκε παραπάνω η HTTP επικοινωνία βασίζεται σε συνδέσεις του πρωτοκόλλου TCP/IP. Η εξ' ορισμού TCP θύρα είναι η 80 αλλά δεν αποκλείεται η χρήση και άλλων. Επίσης δεν αποκλείεται η πραγματοποίηση της HTTP επικοινωνίας πάνω από άλλα πρωτόκολλα μεταφοράς στο Internet ή σε άλλα δίκτυα. Η μόνη προϋπόθεση που τίθεται από το HTTP για το πρωτόκολλο του δικτυακού υποστρώματος είναι η αξιόπιστη μεταφορά (reliable transport).

Γενικά, οι συνδέσεις εκκινούνται από τον client πριν από την αποστολή της αίτησης και τερματίζονται από τον server μετά την αποστολή της απάντησης.

Μέθοδοι Αιτήσεων

Στην 1.0 έκδοση του HTTP υποστηρίζονται οι μέθοδοι GET, HEAD και PUT με τα εξής χαρακτηριστικά:

GET: Η μέθοδος GET αφορά στην ανάκτηση της οποιασδήποτε πληροφορίας (αντικειμένου) καθορίζεται από το URI της αίτησης (Request URI). Εάν το URI της αίτησης υποδεικνύει μία διαδικασία επεξεργασίας δεδομένων θα πρέπει να επιστραφούν, ως απάντηση, τα δεδομένα όπως αυτά προέκυψαν από την σχετική διαδικασία. Μία αίτηση GET μπορεί να υποβληθεί υπό συγκεκριμένη συνθήκη (conditional GET). Στην περίπτωση αυτή, στην επικεφαλίδα της σχετικής αίτησης συμπεριλαμβάνεται το πεδίο If-modified-since. Το προσδιοριζόμενο αντικείμενο ανακτάται μόνο στην περίπτωση που η ημερομηνία της τελευταίας ενημέρωσης/ μεταβολής του είναι πιο πρόσφατη από την ημερομηνία που καθορίζεται από το πεδίο If-modified-since. Η δυνατότητα conditional

GET στοχεύει στην ελαχιστοποίηση του δικτυακού φόρτου επιτρέποντας την χρήση των cached αντιγράφων στους clients. Με τον μηχανισμό αυτό αποφεύγεται η ανταλλαγή περιττών δεδομένων στις περιπτώσεις αντικειμένων που δεν διακρίνονται για τις συχνές μεταβολές τους.

HEAD: Η μέθοδος αυτή είναι τελείως ανάλογη με την GET. Χρησιμοποιείται για τον έλεγχο συνδέσμων υπερκειμένου (hypertext links) σχετικά με την δυνατότητα πρόσβασης τους, την εγκυρότητα καθώς και ενδεχόμενες πρόσφατες μεταβολές τους. Δεν προβλέπεται η δυνατότητα conditional HEAD. Στην μέθοδο HEAD ο server δεν επιστρέφει, στην απάντηση του, το σώμα της προσδιοριζόμενης πληροφοριακής οντότητας (πεδίο Entity-body) παρά μόνο μετά-πληροφορία για αυτήν. Η επιστρεφόμενη μετά-πληροφορία είναι η ίδια με την περίπτωση της μεθόδου GET. Όπως επισημάνθηκε παραπάνω χρησιμοποιείται κατά κύριο λόγο από τους browsers που εφαρμόζουν caching για την ανάκτηση αντικειμένων με βάση το πεδίο επικεφαλίδας Last-modified-since. Εάν η ημερομηνία αυτή είναι νεότερη από αυτή του αντικειμένου της cache ζητείται το περισσότερο πρόσφατο αντικείμενο. Οι μέθοδοι GET και HEAD έχει επικρατήσει να χρησιμοποιούνται μόνο για την ανάκτηση πληροφορίας (retrieval) και όχι για άλλες λειτουργίες.

POST: Η μέθοδος αυτή υποδεικνύει στον server να δεχτεί την οντότητα που μεταφέρεται στην αίτηση σαν ένα νέο στιγμιότυπο (εγγραφή, καταχώρηση) του πόρου που προσδιορίζεται από το URI. Η μέθοδος POST σχεδιάστηκε για την αντιμετώπιση αναγκών όπως:

- Υποβολή ενός μηνύματος σε μία bulletin board, newsgroup, mailing list ή παρόμοια συλλογή άρθρων. Πέρασμα παραμέτρων σε μία διαδικασία επεξεργασίας δεδομένων σαν αποτέλεσμα υποβολής φόρμας (form submission).
- Επέκταση μίας βάσης δεδομένων με την προσθήκη εγγραφών κα.

Η πραγματική λειτουργία η οποία εκτελείται σαν αποτέλεσμα της POST αίτησης προσδιορίζεται από τον server και συχνά εξαρτάται από το URI της αίτησης. Η οντότητα που περιέχεται στην αίτηση καθίσταται για τον πόρο που προσδιορίζεται στο URI ότι ένα αρχείο για τον υπερκείμενο κατάλογο που το περιλαμβάνει ή μία εγγραφή για την βάση δεδομένων στην οποία ανήκει. Το αποτέλεσμα των POST αιτήσεων (αναφορικά με τους πόρους που ενδεχομένως διαμορφώθηκαν) περιγράφεται στα success/error codes τα οποία επιστρέφονται από τον server.

Πεδία επικεφαλίδας

Στην παράγραφο αυτή παρουσιάζονται τα σημαντικότερα από τα πεδία που συγκροτούν την επικεφαλίδα των HTTP μηνυμάτων.

Allow: Προσδιορίζει το σύνολο των μεθόδων που είναι εφαρμόσιμες στον πόρο που υποδεικνύεται από το URI της αίτησης. Δεν έχει δεσμευτικό χαρακτήρα για τον client.

Authorization: Επιστρέφει στον server πληροφορία authentication ύστερα από μήνυμα challenge.

Expires: Το πεδίο αυτό προσδιορίζει την ημερομηνία / ώρα ύστερα από την οποία η υποδεικνυόμενη οντότητα θα πρέπει να θεωρηθεί παρωχημένη (stale) και μη έγκυρη.

From: Το πεδίο αυτό περιέχει την διεύθυνση ηλεκτρονικού ταχυδρομείου (e-mail address) του χρήστη που ελέγχει τον αιτούμενο user agent. Από την πλευρά του server χρησιμοποιείται για την καταγραφή κίνησης χρηστών (user logging).

Last modified: Το πεδίο αυτό υποδεικνύει την ημέρα και ώρα στην οποία ο server πιστεύει ότι υπήρξε μεταβολή του περιεχομένου του πόρου.

Referrer: Επιτρέπει σε ένα client να προσδιορίσει το URI του πόρου από τον οποίο προήλθε το αιτούμενο URI (Request-URI).

Pragma: Μέσω του πεδίου αυτού μεταδίδονται οδηγίες προς τα μέλη της αλυσίδας request/response για την διεκπεραίωση συνδέσεων. Όταν μεταδίδεται η οδηγία "no-cache", σε μία αίτηση, η εφαρμογή θα πρέπει να την προωθήσει προς τον server ακόμα και αν διατηρεί ένα αντίγραφο του ζητούμενου URI. Οι οδηγίες θα πρέπει να περάσουν από ένα proxy ή gateway άσχετα από την σημασία που έχουν για τις εφαρμογές αυτές και να φτάσουν σε όλα τα μέλη της request/response αλυσίδας. Δεν είναι δυνατή η αποστολή οδηγιών προς ένα μόνο μέλος της αλυσίδας.

4.2.2 Το πρωτόκολλο HTTPS (Secure Hypertext Transfer Protocol)

Το πρωτόκολλο HTTPS αποτελεί μία επέκταση του πρωτοκόλλου HTTP. Παρέχει υπηρεσίες ασφαλείας που μπορούν να εφαρμοστούν μεμονωμένα με στόχο την εμπιστευτικότητα των δοσοληψιών (transaction confidentiality) καθώς και την αυθεντικότητα/ακεραιότητα (authenticity/integrity) της πηγής της μεταδιδόμενης πληροφορίας. Το πρωτόκολλο επιτρέπει την διαπραγμάτευση (σε επίπεδο δοσοληψίας) μεταξύ των επικοινωνούντων μερών των αλγορίθμων κρυπτογράφησης, διαχείρισης

κλειδιών καθώς και άλλων παραμέτρων ασφαλείας. Το HTTPS είναι συμβατό με το HTTP.

Στους client/servers που υποστηρίζουν το πρωτόκολλο HTTPS μπορούν να ενσωματωθούν πολλαπλά πρότυπα αναφορικά με την μορφή των κρυπτογραφημένων μηνυμάτων. Ιδιαίτερα δημοφιλή μεταξύ αυτών είναι τα PKCS-7 και PEM. Το πρωτόκολλο δεν απαιτεί public key certificate στην πλευρά του client. Έτσι, ορισμένες προσωπικές δοσοληψίες μπορούν να πραγματοποιηθούν χωρίς να απαιτείται από τους μεμονωμένους χρήστες να έχουν εξασφαλίσει κάποιο δημόσιο κλειδί. Οι ασφαλείς δοσοληψίες πραγματοποιούνται από άκρο σε άκρο (end-to-end) σε αντίθεση με το HTTP. Οι μηχανισμοί authorization του HTTP απαιτούσαν από τον client να επιχειρήσει την προσπάθεια πρόσβασης η οποία ενδεχομένως να απορρίπτονταν πριν να ενεργοποιηθεί κάποιος μηχανισμός διασφάλισης της επικοινωνίας. Στο HTTPS ο client με τον server μπορούν να διαπραγματευτούν τις παραμέτρους της ασφαλούς επικοινωνίας. Τα μηνύματα που ανταλλάσσονται μέσω του πρωτοκόλλου μπορούν να εξασφαλιστούν με: υπογραφή (signature), κρυπτογράφηση (encryption) και πιστοποίηση (authentication). Επίσης είναι δυνατός ο οποιοσδήποτε συνδυασμός των τριών.

4.3 Video Streaming

4.3.1 Η τεχνολογία streaming

Μέχρι πρόσφατα για να απολαύσουμε βίντεο στον υπολογιστή μας μέσω Internet, έπρεπε πρώτα να παραλειφθεί ολόκληρο το αρχείο και μετά να αρχίσει η αναπαραγωγή του. Το πλεονέκτημα αυτής της μεθόδου ήταν ότι μπορούσαμε να παρακολουθήσουμε βίντεο αρκετά καλής ποιότητας, ακόμα και από χαμηλής ταχύτητας συνδέσεις. Το σημαντικότερο μειονέκτημα, ωστόσο, ήταν ότι ο χρήστης θα έπρεπε να περιμένει για μεγάλο χρονικό διάστημα την παραλαβή ολόκληρου του αρχείου. Παράλληλα ετίθεντο και θέματα παραβίασης της πνευματικής ιδιοκτησίας, αφού καθίστατο δυνατή η αντιγραφή και διανομή του αρχείου αυτού.

Για την αντιμετώπιση των προβλημάτων αυτών, αναπτύχθηκε μία νέα τεχνολογία που επιτρέπει την αποστολή συμπιεσμένου ψηφιακού βίντεο μέσω δικτύων. Το video streaming όπως λέγεται αποτελεί μία από τις εντυπωσιακότερες και ταχύτατα αναπτυσσόμενες τεχνολογίες στο Internet. Έχει ήδη δημιουργήσει μια νέα αγορά, γνωστή σαν Internet broadcast ή intercast/webcast. Η εμπορική εκμετάλλευσή του δεν βασίστηκε

σε κάποιο ανοικτό στάνταρ, αλλά σε ιδιόκτητο κώδικα που αναπτύχθηκε από τις εταιρείες του χώρου. Οι λεπτομέρειες του streaming παραμένουν εν πολλοίς άγνωστες. Ακόμα και ο ορισμός του είναι στοιχειώδης και περιγραφικός. Σε γενικές γραμμές περιλαμβάνει την αποστολή υλικού (π.χ. ήχου και Εικόνας) από κάποιον server σε κάποιο τερματικό, μέσω ενός packet-based δικτύου, όπως το Internet, αν και αρκετά συχνά χρησιμοποιείται για να εκφράσει μια πιο συγκεκριμένη έννοια, όπως τις ταινίες που προβάλλονται σε υπολογιστές μέσω του Internet. Ο server τεμαχίζει το υλικό (media) σε πακέτα, τα οποία εκπέμπονται μέσω του δικτύου σε κάποιον καθορισμένο αποδέκτη. Κατά τη παραλαβή τους, τα πακέτα ανασυντίθενται και ξεκινά η αναπαραγωγή. Η αλληλουχία των πακέτων αυτών ονομάζεται ροή (stream) και η αναπαραγωγή του υλικού αρχίζει καθώς αυτό παραλαμβάνεται από τον υπολογιστή του χρήστη. Ενδέχεται μάλιστα ο τελικός αποδέκτης να μην παραλάβει ποτέ το συνολικό αρχείο, αλλά απλά να αναπαραγάγει τα πακέτα καθώς αυτά καταφθάνουν.

Για το χρήστη, η ουσία της όλης διαδικασίας εστιάζει στην προσδοκία ότι το υλικό που ζήτησε θα αναπαραχθεί στον υπολογιστή του άμεσα και χωρίς διακοπές. Αυτός είναι και ο σημαντικότερος στόχος του streaming και ο λόγος για τον οποίο αναπτύχθηκε η τεχνολογία αυτή. Ποιοι είναι, όμως, οι παράγοντες που διαμορφώνουν την τελική ποιότητα; Επειδή η διαδικασία δημιουργίας και διανομής streaming media αποτελείται από αρκετά στάδια, οι παράγοντες αυτοί ποικίλλουν και επηρεάζουν με διαφορετική κάθε φορά βαρύτητα το τελικό αποτέλεσμα. Το πρώτο βήμα, λοιπόν, είναι η καταγραφή ή η δημιουργία του υλικού, είτε σε απευθείας ψηφιακή μορφή είτε σε αναλογική και κατόπιν η ψηφιοποίηση της. Το επόμενο στάδιο αποτελείται από τη συμπίεση του υλικού, χρησιμοποιώντας τα κατάλληλα codecs που έχουν αναπτυχθεί. Αφού ολοκληρωθεί η επεξεργασία του υλικού, ακολουθεί η τοποθέτησή του σε κάποιον server και η αποστολή του προς τους τελικούς αποδέκτες μέσω των νέων streaming πρωτοκόλλων που έχουν αναπτυχθεί. Ο τρόπος με τον οποίο γίνεται η αποστολή, χωρίζει το streaming σε διάφορες μεθόδους και είδη τα οποία θα δούμε παρακάτω.

4.3.2 Μέθοδοι και είδη streaming

Σήμερα υπάρχουν δύο διαφορετικές προσεγγίσεις streaming που εξυπηρετούν διαφορετικές ανάγκες και απαιτούν διαφορετικό εξοπλισμό για τη λειτουργία τους. Η ουσιαστική διαφορά μεταξύ τους εστιάζεται στο συγχρονισμό ή μη μεταξύ του ρυθμού αποστολής και λήψης των on-line αρχείων.

Progressive streaming

Η μέθοδος progressive streaming είναι επίσης γνωστή και ως progressive download. Μέσω αυτής, το on-line υλικό αποστέλλεται στον υπολογιστή του χρήστη με το μέγιστο δυνατό ρυθμό, ανεξάρτητα από την ταχύτητα σύνδεσής του με το Internet. Καθώς τα πακέτα που αποτελούν το on-line αρχείο καταφθάνουν στον υπολογιστή μας, ανασυντίθενται και αποθηκεύονται σε αυτόν. Τα πακέτα που ακολουθούν προστίθενται στα προηγούμενα και σχηματίζουν σιγά σιγά το αρχικό υλικό. Αυτό σημαίνει ότι ανά πάσα στιγμή ο χρήστης διαθέτει αποθηκευμένο ένα μέρος του αρχείου, το οποίο συνεχώς μεγαλώνει έως ότου ολοκληρωθεί. Μπορούμε λοιπόν, να αναπαράγουμε το μέρος του αρχείου που έχει ήδη παραλειφθεί, αλλά δεν μπορούμε να μεταφερθούμε σε κάποιο σημείο πέραν αυτού. Αυτό είναι το βασικό χαρακτηριστικό της μεθόδου και η κύρια διαφοροποίησή της από το real-time streaming. Ο ρυθμός αποστολής του υλικού από τον server στον τελικό αποδέκτη είναι ανεξάρτητος από το ρυθμό που εκείνος το παραλαμβάνει. Σημαντικό πλεονέκτημα της συγκεκριμένης τεχνικής είναι ότι δεν απαιτεί την εγκατάσταση ειδικών server και πρωτοκόλλων. Το υλικό τοποθετείται σε απλούς HTTP ή FTP servers διευκολύνοντας τη διαχείρισή του, ενώ ταυτόχρονα δεν παρουσιάζονται ιδιαίτερα προβλήματα με την ύπαρξη firewalls. Στους servers αυτούς οφείλεται και ο χαρακτηρισμός HTTP streaming, ακόμα μία παραλλαγή της ονομασίας της μεθόδου. Το progressive download ταιριάζει ιδιαίτερα σε μικρού μήκους ταινίες και trailers που θέλουμε να παρακολουθήσουμε σε υψηλή ποιότητα. Η τεχνική αυτή εγγυάται την τελική ποιότητα του βίντεο, επειδή τα πακέτα που αποτελούν τη ροή του αρχείου (bitsream) δεν χάνονται ποτέ. Αντίθετα, προστίθενται συνεχώς στο ήδη αποθηκευμένο αρχείο καθώς καταφθάνουν στον υπολογιστή μας. Αυτό σημαίνει ότι το αρχικό υλικό μπορεί να είναι υψηλής ποιότητας και χαμηλής συμπίεσης. Παρόλο που η ταχύτητα σύνδεσής μας με το δίκτυο μπορεί να είναι μικρή και να μην επιτρέπει την αναπαραγωγή του υλικού ζωντανά (real time), το αρχείο θα αποθηκευτεί στον υπολογιστή με υψηλή ποιότητα και θα μπορέσουμε να το αναπαράγουμε αργότερα. Παρά τα πλεονεκτήματά του, το progressive streaming αποδεικνύεται ανεπαρκές για ένα πλήθος περιπτώσεων. Για παράδειγμα, η real time παρακολούθηση ταινιών είναι ουσιαστικά αδύνατη. Αυτό συμβαίνει γιατί με τη μέθοδο αυτή ο server δεν γνωρίζει το ρυθμό με τον οποίο παραλαμβάνεται το υλικό από τον αποδέκτη, αλλά ούτε μπορεί να αυξομειώσει κατάλληλα το ρυθμό με τον οποίο το αποστέλλει. Επομένως, σε περίπτωση που το δίκτυο είναι υπερφορτωμένο ή αντιμετωπίζει προβλήματα, τα πακέτα που αποτελούν το αρχείο

καθυστερούν να φθάσουν και ο χρήστης παρατηρεί ενοχλητικές διακοπές κατά την αναπαραγωγή μιας ταινίας.

Ένα επίσης σημαντικό πρόβλημα είναι η δυνατότητα αντιγραφής και διανομής του αρχείου που αποθηκεύεται στον υπολογιστή μας. Η πρακτική αυτή, που δεν αντιμετωπίζεται με το progressive download, συνιστά κατάφορη παραβίαση του νόμου περί πνευματικής ιδιοκτησίας. Ακόμα μεγαλύτερες δυσκολίες παρουσιάζει η περίπτωση κατά την οποία θέλουμε να αναζητούμε συγκεκριμένες πληροφορίες σε κάποιο υλικό (random-access), όπως σε διαλέξεις και παρουσιάσεις. Αν η πληροφορία βρίσκεται προς το τέλος, θα πρέπει να περιμένουμε μέχρι τη λήψη ολόκληρου του αρχείου, γεγονός που προκαλεί μεγάλη καθυστέρηση. Τέλος, η τεχνική αυτή δεν λειτουργεί για περιεχόμενο που πρέπει να μεταδοθεί ζωντανά και για το λόγο αυτό χαρακτηρίζεται on-demand.

Real-time streaming

Με τη μέθοδο αυτή ο ρυθμός αποστολής του on-line υλικού ελέγχεται, ώστε να προσεγγίζει το ρυθμό λήψης του από τον υπολογιστή του χρήστη. Αφού, λοιπόν, το υλικό αποστέλλεται με τον ίδιο ρυθμό που παραλαμβάνεται, μπορούμε να το παρακολουθήσουμε σε πραγματικό χρόνο. Όπως είναι φυσικό, η τεχνική αυτή είναι η πλέον κατάλληλη για τη μετάδοση real time περιεχομένου, όπως οι ζωντανές εκδηλώσεις και οι συναυλίες. Παράλληλα, παρέχει σημαντικά πλεονεκτήματα και για τις υπόλοιπες περιπτώσεις, αφού υποστηρίζει την τυχαία πρόσβαση (random access) στο on-line υλικό. Έτσι, ο χρήστης μπορεί να παραλείψει ολόκληρα τμήματα που δεν τον ενδιαφέρουν και να προχωρήσει στα επόμενα. Το χαρακτηριστικό αυτό αποδεικνύεται εξαιρετικά σημαντικό σε συνεντεύξεις ή ομιλίες, στις οποίες μπορούμε να αναζητήσουμε κάποια πληροφορία. Τέλος, μία πολύ σημαντική δυνατότητα είναι η ανάπτυξη μίας αγοράς που θα βασίζεται σε συνδρομητικές υπηρεσίες. Εφόσον ο χρήστης δεν παραλαμβάνει ποτέ ολόκληρο το αρχείο, δεν μπορεί να αντιγράψει την ταινία που παρακολουθεί ώστε να την παραχωρήσει και σε άλλους αργότερα. Για πρώτη φορά, λοιπόν, γίνεται δυνατή η δημιουργία on-line βίντεο κλαμπ που θα μας νοικιάζουν άμεσα ταινίες, τις οποίες θα μπορούμε να παρακολουθήσουμε από την άνεση του σπιτιού μας. Θεωρητικά, κατά τη real time μετάδοση streaming υλικού θα πρέπει να μην υπάρχουν διακοπές ούτε στην εικόνα αλλά ούτε και στον ήχο Στην πραγματικότητα, περιοδικές διακοπές συμβαίνουν και εξαρτώνται από το bandwidth, που παρέχει η σύνδεσή μας με το Internet. Όμως, το κυριότερο μειονέκτημα της μεθόδου εστιάζει στο ρυθμό αποστολής του αρχείου που καθορίζεται από

την ταχύτητα σύνδεσης. Επειδή οι σημερινές dial-up συνδέσεις προσφέρουν πολύ περιορισμένο bandwidth, ο ρυθμός αποστολής πρέπει να είναι αντίστοιχα μικρός, με αποτέλεσμα τη χαμηλή ποιότητα αναπαραγωγής. Η ποιότητα αυτή μειώνεται ακόμη περισσότερο, όταν το δίκτυο παρουσιάζει προβλήματα ή είναι υπερφορτωμένο. Στην περίπτωση αυτή, πολλά από τα πακέτα που αποτελούν τη ροή του αρχείου χάνονται και η μέθοδος δεν προβλέπει την εκ νέου αποστολή τους.

Τέλος, σε αντίθεση με το Progressive, το Real-time streaming απαιτεί νέα πρωτόκολλα και ειδικούς servers αφιερωμένους στη διαδικασία αποστολής του υλικού. Τέτοιοι servers είναι ο Quick Time Streaming Server, ο Real Server και ο Windows Media Server, οι οποίοι προσφέρουν καλύτερο έλεγχο επί της διαδικασίας, αλλά παρουσιάζουν περισσότερες δυσκολίες στη διαχείριση τους. Παράλληλα τα ειδικά πρωτόκολλα streaming, παρουσιάζουν πολλές φορές προβλήματα με τα firewalls. Για το λόγο αυτό ορισμένοι χρήστες ενδεχομένως να μην μπορούν να παρακολουθήσουν real-time streaming υλικό από ορισμένους υπολογιστές.

Τρόποι μετάδοσης streaming

Οι τρόποι μετάδοσης του βίντεο είναι δύο: On-Demand και Live. Στη πρώτη περίπτωση ζητάμε την αναπαραγωγή ενός ήδη καταγεγραμμένου και αποθηκευμένου βίντεο, ενώ στη δεύτερη η καταγραφή και μετατροπή σε streaming μορφή γίνεται σε πραγματικό χρόνο .Και στις δύο περιπτώσεις, η συνέχεια δεν έχει διαφορές. Η ροή του συμπιεσμένου βίντεο μετατρέπεται σε πακέτα και αποστέλλεται μέσω του Internet από τον streaming server. Στη πλευρά του χρήστη τα πακέτα ενώνονται και αποσυμπιέζονται για την αναπαραγωγή. Τα τρία μοντέλα streaming που έχουν αναπτυχθεί είναι τα παρακάτω:

Unicast

Στο μοντέλο αυτό κάθε χρήστης που απαιτεί το υλικό συνδέεται με τον server και παραλαμβάνει ξεχωριστή ροή δεδομένων. Το μειονέκτημα είναι ότι ο φόρτος του server αυξάνει ανάλογα με τον αριθμό των χρηστών που καλείται να εξυπηρετήσει. Όταν ο αριθμός αυτός ξεπεράσει κάποιο όριο, ο server υπερφορτώνεται και ουσιαστικά καταρρέει. Επίσης, η αποστολή της ίδιας ροής δεδομένων σε πολλούς χρήστες ταυτόχρονα είναι αναποτελεσματική, δημιουργεί υπερφόρτωση στο δίκτυο και μειώνει την ποιότητα εξυπηρέτησης. Ουσιαστικά, το μοντέλο αυτό επιτρέπει την αποστολή περιεχομένου "one-to-one", δηλαδή μια ροή δεδομένων για κάθε χρήστη. Αναφέρεται πολλές φορές και σαν

"Video-on-Demand" (VoD), επειδή κάθε χρήστης μπορεί να ζητήσει οποιαδήποτε ροή σε οποιαδήποτε στιγμή.

Multicast

Το μοντέλο αυτό παρέχει αρκετά πλεονεκτήματα έναντι του Unicast, που είναι εμφανή κυρίως στις ζωντανές μεταδόσεις. Στη περίπτωση αυτή είναι φυσικό ένας μεγάλος αριθμός χρηστών να απαιτήσουν τη σύνδεση και λήψη του ίδιου περιεχομένου ταυτόχρονα. Αντί λοιπόν να γίνει παράλληλη εκπομπή της ροή σε κάθε χρήστη ξεχωριστά, ο server στέλνει μία μόνο ροή που μεταδίδεται σε μία ή περισσότερες ομαδικές διευθύνσεις (group addresses). Ουσιαστικά αυτό που συμβαίνει είναι ότι μεταξύ του server και των clients παρεμβάλλονται multicast routers με τους οποίους συνδέονται οι χρήστες. Με τον τρόπο αυτό οι χρήστες ομαδοποιούνται και κάθε ομάδα παραλαμβάνει μία μόνο ροή δεδομένων. Με το αποκεντρωμένο αυτό μοντέλο, ο server αποσυνδέεται από τους τελικούς αποδέκτες και ο φόρτος του δεν αυξάνεται με κάθε νέα σύνδεση. Παρά όμως τα σαφή πλεονεκτήματα του Multicast, το μοντέλο χρησιμοποιείται μόνο από ένα μικρό ποσοστό οργανισμών και εταιρειών στο Internet, λόγω των πολύπλοκων τεχνικών δυσκολιών που παρουσιάζει η εγκατάσταση ενός τέτοιου συστήματος. Εκτός απ' αυτό η σημαντικότερη αιτία είναι ότι η πλειονότητα του streaming περιεχομένου που υπάρχει στο Internet είναι αποθηκευμένο και προσφέρεται στους χρήστες, ύστερα από αίτημά τους. Σε αυτές τις συνθήκες το μοντέλο αυτό δεν είναι αρκετά αποτελεσματικό, αφού οι αιτήσεις των χρηστών είναι τυχαίες και δεν μπορούν να συγκεντρωθούν σε ομαδικές διευθύνσεις για ταυτόχρονη μετάδοση. Σε αντίθεση λοιπόν με το Unicast, το Multicast επιτρέπει την αποστολή μίας ροής σε πολλούς πελάτες (one-to-many) και για το λόγο αυτό αναφέρεται και σαν "Near-Video-on-Demand (NVoD) αφού πολλοί χρήστες θα πρέπει να παρακολουθούν το ίδιο περιεχόμενο την ίδια στιγμή. Το μοντέλο αυτό παρουσιάζει ομοιότητες με την καλωδιακή τηλεόραση "pay-per-view" όπου ένα σύνολο χρηστών διαθέτει ταυτόχρονη πρόσβαση στο ίδιο πρόγραμμα. Ακόμα πιο εύκολο παράδειγμα είναι όταν θέλουμε να στείλουμε e-mail σε πολλαπλούς αλλά συγκεκριμένους αποδέκτες. Έτσι μέσω του προγράμματος που χρησιμοποιούμε (π.χ.Outlook Express) μπορούμε να ομαδοποιήσουμε τους φίλους μας και να στέλνουμε ένα e-mail στην ομάδα αυτή που περιέχει πολλούς παραλήπτες. Με το μοντέλο Unicast θα έπρεπε να το στείλουμε σε κάθε ένα φίλο μας ξεχωριστά.

Broadcast

Το μοντέλο αυτό είναι μία ιδιαίτερη περίπτωση του Multicasting που αποστέλλει μια ροή δεδομένων σε όλους του χρήστες. Η μέθοδος αυτή μπορεί να χρησιμοποιηθεί για ζωντανές μεταδόσεις παρουσιάσεων ή ανακοινώσεων προϊόντων σε όλους τους υπαλλήλους μίας εταιρείας παγκοσμίως. Όλοι οι χρήστες του δικτύου μπορούν να παρακολουθήσουν την εκπομπή, αρκεί να συνδεθούν την προκαθορισμένη ώρα μετάδοσης τους. Αν λοιπόν θέλετε να στείλετε μέσω broadcast ένα e-mail σε περιβάλλον γραφείου, θα το στέλνατε σε όλους τους υπαλλήλους είτε αυτοί το χρειάζονται είτε όχι.

4.3.3 Video codecs

Για την συμπίεση και αποσυμπίεση ήχου και βίντεο έχουν αναπτυχθεί διάφορες τεχνικές και αλγόριθμοι σε μορφή software και είναι γνωστοί σαν codecs (Compression/Decompression). Για τη συμπίεση βίντεο δύο είναι οι κυριότερες τεχνικές σε εφαρμογή σήμερα: οι interframe και intraframe. Η πρώτη εκμεταλλεύεται το γεγονός ότι οι περισσότερες πληροφορίες παραμένουν σταθερές από το ένα καρέ στο άλλο. Για παράδειγμα σε ένα βίντεο που απεικονίζει κάποιον ομιλητή, σχεδόν το σύνολο του φόντου παραμένει σταθερό, παρά τις διάφορες εκφράσεις του προσώπου του ομιλητή. Η δεύτερη αναλαμβάνει τη συμπίεση κάθε καρέ ξεχωριστά, με τρόπο παρόμοιο προς τη συμπίεση JPEG για εικόνες. Ο συνδυασμός των δύο τεχνικών μπορεί να επιτρέψει τη συμπίεση του αρχικού υλικού έως και 200:1. Οι codecs επίσης διαιρούνται σε συμμετρικούς και σε ασύμμετρους, ανάλογα με το αν η συμπίεση διαρκεί περισσότερο από την αποσυμπίεση. Οι ασύμμετροι codecs απαιτούν ισχυρούς υπολογιστές για την συμπίεση και χρησιμοποιούνται για υλικό που θα συμπιεστεί μία φορά και θα αναπαραχθεί πολλές. Οι συμμετρικοί codecs απ' την άλλη χρησιμοποιούνται σε real time εφαρμογές, όπως ζωντανές μεταδόσεις, όπου η συμπίεση πρέπει να γίνεται σε πραγματικό χρόνο. Επομένως κανένας codec δεν μπορεί να καλύψει όλες τις ανάγκες, αλλά αντίθετα απαιτείται ο κατάλληλος συνδυασμός τους για να πετύχουμε το καλύτερο αποτέλεσμα για τις περισσότερες περιπτώσεις.

Οι κυριότεροι codecs συμπίεσης/αποσυμπίεσης βίντεο που χρησιμοποιούνται είναι:

H.263

Ο codec αυτός αναπτύχθηκε από το I.T.U. το 1994 και αποτελεί εξέλιξη του H.261. Προορίζεται για βιντεοτηλέφωνα και διεξαγωγή τηλεδιασκέψεων μέσα από γραμμές ISDN

αλλά και modem, περιπτώσεις όπου η Εικόνα δεν έχει πολλή κίνηση. Κυριότερη βελτίωση έναντι του προκατόχου του είναι η υποστήριξη για ακόμα χαμηλότερα bit rates, ενώ περιλαμβάνεται και ένας μηχανισμός που επιτρέπει την καλύτερη αξιοποίηση του bandwidth. Ο μηχανισμός λειτουργεί ισορροπώντας μεταξύ της ποιότητας της Εικόνας και της κίνησης, με αποτέλεσμα οι εικόνες που περιλαμβάνουν έντονη κίνηση να είναι χαμηλότερης ποιότητας από τις στατικές.

JPEG και MJPEG

Τα αρχικά JPEG προέρχονται από τις λέξεις Join Photographic Experts Group. Πρόκειται για έναν φορέα που ανέλαβε την ανάπτυξη ενός αλγορίθμου συμπίεσης για 24-bit true color φωτογραφίες. Η συμπίεση οδηγεί σε απώλεια ποιότητας (lossy) και μπορεί να συμπιεστεί από 2 έως και 30 φορές το αρχικό υλικό, ανάλογα με τις ρυθμίσεις. Το MJPEG (Motion JPEG) είναι απλά μια ακολουθία JPEG εικόνων που αποτελούν το βίντεο.

MPEG

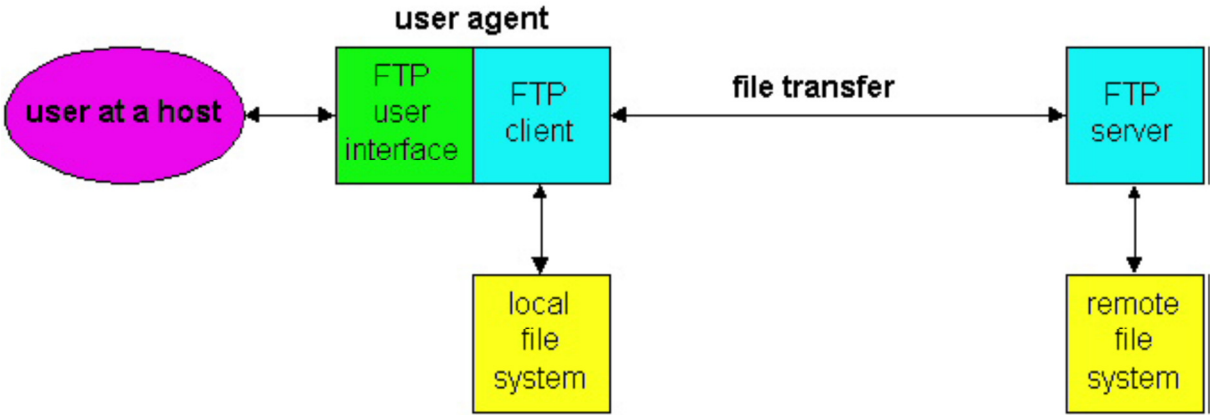
Ο International Standards Organization (ISO) έχει υιοθετήσει μια σειρά από πρότυπα για video codec που αναπτύχθηκαν από το Moving Pictures Experts Group (MPEG). Η σειρά περιλαμβάνει τους MPEG-1, MPEG-2 και MPEG-4, με σημαντικότερο τον τελευταίο. Το πρότυπο MPEG-4 σχεδιάστηκε για τη διανομή interactive multimedia υλικού μέσω δικτύων. Επομένως δεν πρόκειται για έναν απλό codec αλλά περιλαμβάνει προδιαγραφές για ήχο, βίντεο και δυνατότητες αλληλεπίδρασης (interactivity). Λειτουργεί αφαιρώντας πλεονάζουσες πληροφορίες μεταξύ των καρέ, αλλά και συμπιέζοντας ταυτόχρονα τα ίδια τα καρέ με μία τεχνική παρόμοια του JPEG. Υποστηρίζει δύο τρόπους κωδικοποίησης, με μεταβλητό ή σταθερό ρυθμό μετάδοσης, προσφέροντας υψηλής ποιότητας αναπαραγωγή και μικρό μέγεθος αρχείων.

4.4 File Sharing

4.4.1 Το πρωτόκολλο FTP

Το **FTP (File Transfer Protocol)** είναι ένα πρωτόκολλο που χρησιμοποιείται για την μεταφορά αρχείων από έναν υπολογιστή του Διαδικτύου σε κάποιον άλλον. Το FTP ξεκίνησε πειραματικά το 1971 αλλά παραμένει ως τις μέρες μας εξαιρετικά δημοφιλές.

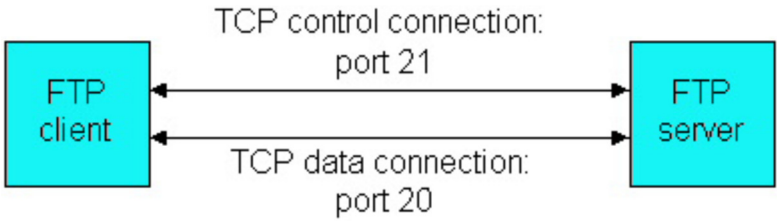
Ας υποθέσουμε ότι ένας χρήστης επιθυμεί να μεταφέρει ένα ή περισσότερα αρχεία από ή προς έναν άλλο απομακρυσμένο χρήστη. Για να μπορέσει ο χρήστης να έχει πρόσβαση στα αρχεία του απομακρυσμένου υπολογιστή, δηλαδή σε κάποιο λογαριασμό (account) του απομακρυσμένου υπολογιστή, πρέπει να δώσει ένα αναγνωριστικό όνομα χρήστη (user name) και έναν κωδικό (password). Μετά την παροχή των παραπάνω πληροφοριών πιστοποίησης (authentication), ο χρήστης μπορεί να μεταφέρει αρχεία από το σύστημα αρχείων του προς το απομακρυσμένο σύστημα αρχείων, και αντιστρόφως. Όπως φαίνεται και στην Εικόνα 37 ο χρήστης έρχεται σε επαφή με το FTP μέσω ενός αντιπροσώπου FTP.



Εικόνα 37: Τρόπος λειτουργίας FTP

Ο χρήστης πρώτα παρέχει το όνομα του απομακρυσμένου υπολογιστή (remote host name), με αποτέλεσμα η FTP διαδικασία πελάτη στον τοπικό υπολογιστή να εγκαθιστά μία σύνδεση TCP με τον εξυπηρετητή FTP στον απομακρυσμένο υπολογιστή. Τότε ο χρήστης παρέχει το user name και το password, τα οποία στέλνονται μέσω της σύνδεσης TCP ως μέρος εντολών FTP. Μετά την πιστοποίηση του χρήστη από τον εξυπηρετητή, ο χρήστης μπορεί να αντιγράψει ή να μετακινήσει ένα ή περισσότερα αρχεία από το τοπικό του σύστημα αρχείων προς το απομακρυσμένο σύστημα αρχείων, και αντιστρόφως. Το FTP χρησιμοποιεί δύο παράλληλες συνδέσεις TCP για την μεταφορά ενός αρχείου: μία σύνδεση ελέγχου (control connection) και μία σύνδεση δεδομένων (data connection). Η σύνδεση ελέγχου χρησιμοποιείται για την μεταφορά πληροφοριών ελέγχου μεταξύ των δύο υπολογιστών, πληροφορίες όπως το όνομα χρήστη (user name), τον κωδικό, για την αλλαγή του απομακρυσμένου καταλόγου και εντολές για την ανάκτηση (get) ή καταχώρηση (put) αρχείων. Η σύνδεση δεδομένων χρησιμοποιείται για την πραγματική μεταφορά του αρχείου. Εξαιτίας της ύπαρξης δύο TCP συνδέσεων, λέμε ότι το FTP

μεταφέρει την πληροφορία ελέγχου εκτός ζώνης (out-of-band). Αντίθετα στα πρωτόκολλα που χρησιμοποιούν μόνο μία σύνδεση λέμε ότι η πληροφορία ελέγχου μεταφέρεται εντός ζώνης (in-band). Στο παρακάτω σχήμα φαίνονται οι δύο ξεχωριστές TCP συνδέσεις που χρησιμοποιεί το FTP.



Εικόνα 38: Οι συνδέσει TCP που χρησιμοποιεί το FTP

Όταν ο χρήστης ξεκινά μία FTP σύνοδο με κάποιον απομακρυσμένο υπολογιστή, το FTP πρώτα εγκαθιστά μία TCP σύνδεση ελέγχου στην θύρα (port) 21 του FTP εξυπηρετητή. Ο FTP πελάτης στέλνει το αναγνωριστικό και τον κωδικό του χρήστη μέσω της σύνδεσης ελέγχου. Επίσης, μέσω της σύνδεσης ελέγχου ο FTP πελάτης στέλνει και εντολές για την αλλαγή του απομακρυσμένου καταλόγου. Όταν ο χρήστης ζητήσει μία μεταφορά αρχείου (από η προς τον απομακρυσμένο υπολογιστή) το FTP ανοίγει μία TCP σύνδεση δεδομένων στην θύρα 20 του FTP εξυπηρετητή. Μέσω αυτής της σύνδεσης δεδομένων στέλνεται μόνο ένα αρχείο και στη συνέχεια η σύνδεση δεδομένων κλείνει. Αν κατά τη διάρκεια αυτής της συνόδου ο χρήστης θέλει να μεταφέρει και άλλα αρχεία τότε ανοίγονται ξεχωριστές συνδέσεις δεδομένων, μία για κάθε αρχείο. Επομένως, στο FTP η σύνδεση ελέγχου παραμένει για όλη τη διάρκεια της συνόδου, ενώ χρησιμοποιείται μία ξεχωριστή σύνδεση δεδομένων για κάθε αρχείο που μεταφέρεται μεταξύ των δύο υπολογιστών.

Κατά την διάρκεια της συνόδου ο εξυπηρετητής κρατάει την κατάσταση (state) του χρήστη. Για κάθε σύνοδο έχουμε μία ξεχωριστή σύνδεση ελέγχου που συσχετίζεται με την λογαριασμό του χρήστη, και ο εξυπηρετητής κρατά το τρέχοντα κατάλογο του χρήστη στον λογαριασμό αυτό. Εξαιτίας της πληροφορίας για την κατάσταση των συνόδων των χρηστών έχουμε σημαντική μείωση στον αριθμό των χρηστών που μπορεί να εξυπηρετηθούν ταυτόχρονα, σε σχέση με άλλα πρωτόκολλα που δεν κρατάνε την κατάσταση του χρήστη, όπως το HTTP.

Τελειώνοντας την περιγραφή του FTP, θα αναφερθούμε στις εντολές (commands) και τις αποκρίσεις (replies) που χρησιμοποιεί. Οι εντολές από τον πελάτη προς τον

εξυπηρετητή και οι αποκρίσεις από τον εξυπηρετητή προς τον πελάτη στέλνονται μέσω της TCP σύνδεσης ελέγχου σε 7-bit ASCII κωδικοποίηση, και είναι αναγνώσιμες. Για τον διαχωρισμό των εντολών μεταξύ τους χρησιμοποιείται αλλαγή γραμμής και κάθε εντολή αποτελείται από τέσσερις κεφαλαίους ASCII χαρακτήρες και από κάποια προαιρετικά ορίσματα. Μερικές από τις πιο συχνά χρησιμοποιούμενες εντολές φαίνονται στην Εικόνα 39.

Εντολή	Ορίσματα	Χρήση
USER	*username*	Αποστολή user name στον εξυπηρετητή
PASS	*password*	Αποστολή password στον εξυπηρετητή
LIST	-	Αίτηση για αποστολή όλων των ονομάτων των αρχείων του τρέχοντα καταλόγου (τα οποία στέλνονται μέσω μίας νέας TCP σύνδεσης δεδομένων)
RETR	*filename*	Ανάκτηση του αρχείου filename από τον τρέχοντα κατάλογο του απομακρυσμένου υπολογιστή
STOR	*filename*	Τοποθέτηση του αρχείου filename στον τρέχοντα κατάλογο του απομακρυσμένου υπολογιστή

Εικόνα 39: Εντολές που χρησιμοποιούνται στο FTP

Τυπικά υπάρχει μία προς μία αντιστοιχία μεταξύ των εντολών που δίνει ο χρήστης και των εντολών FTP που στέλνονται μέσω της σύνδεσης ελέγχου. Κάθε εντολή ακολουθείται από μία απόκριση, η οποία αποτελείται από έναν τριψήφιο ακέραιο αριθμό και ένα προαιρετικό μήνυμα. Μερικές τυπικές αποκρίσεις φαίνονται στην Εικόνα 40.

Κωδικός απόκρισης	Προαιρετικό μήνυμα
331	User name OK, password required
125	Data connection already open; transfer starting
424	Can't open data connection
452	Error writing file

Εικόνα 40: Τυπικές αποκρίσεις που χρησιμοποιούνται στο FTP

4.5 Βιβλιογραφία & πηγές

Βιβλία

[1] Andrew S. Tanenbaum, 4η Αμερικάνικη Έκδοση <<Δίκτυα Υπολογιστών>>

[2] James Kurose & Keith Ross, 4η Έκδοση <<Δικτύωση Υπολογιστών- Προσέγγιση από Πάνω προς τα Κάτω>>

[3] Γεώργιος Β. Ξυλωμένος, Γεώργιος Κ. Πολύζος <<Τεχνολογία πολυμέσων και πολυμεσικές επικοινωνίες>>

Links

[1] http://el.wikipedia.org/wiki/VoIP

[2] http://en.wikipedia.org/wiki/H.323

[3] http://en.wikipedia.org/wiki/Session_Initiation_Protocol

[4] http://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol

[5] http://en.wikipedia.org/wiki/HTTP_Secure

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

[7] http://www.w3.org/Protocols/rfc2616/rfc2616.html

[8] http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_6-1/sip.html

[9] http://de.teikav.edu.gr/telematics/pdf/thlematikh_new2pdf

ΚΕΦΑΛΑΙΟ 5: Αναγνώριση κίνησης

5.1 Εισαγωγή

Στα πλαίσια της πειραματικής διαδικασίας, για την αναγνώριση της διαδικτυακής κίνησης που παράγεται από το τελικό χρήστη εξετάσαμε πέντε σενάρια κίνησης. Αυτό που κάναμε είναι να καταγράψουμε, με την βοήθεια ενός προγράμματος που δημιουργήσαμε με την γλώσσα προγραμματισμού Java, ξεχωριστά την κίνηση που παράγεται από τον εκάστοτε server στο τελικό χρήστη μετά από την αίτηση σύνδεσης του τελευταίου στο server. Τα σενάρια χωρίζονται στις παρακάτω κατηγορίες:

- Video Streaming, παρακολούθηση live video.
- Video on Demand, παρακολούθηση αποθηκευμένου video.
- Browsing, περιήγηση σε ιστοσελίδα.
- FTP, λήψη αρχείου από ftp server.
- VoIP, κλήση από το πρόγραμμα Skype η οποία χωρίζετε σε δύο κατηγορίες:
    - Voice call
    - Video call

Οι χρόνοι καταγραφής της κίνησης είναι δύο:

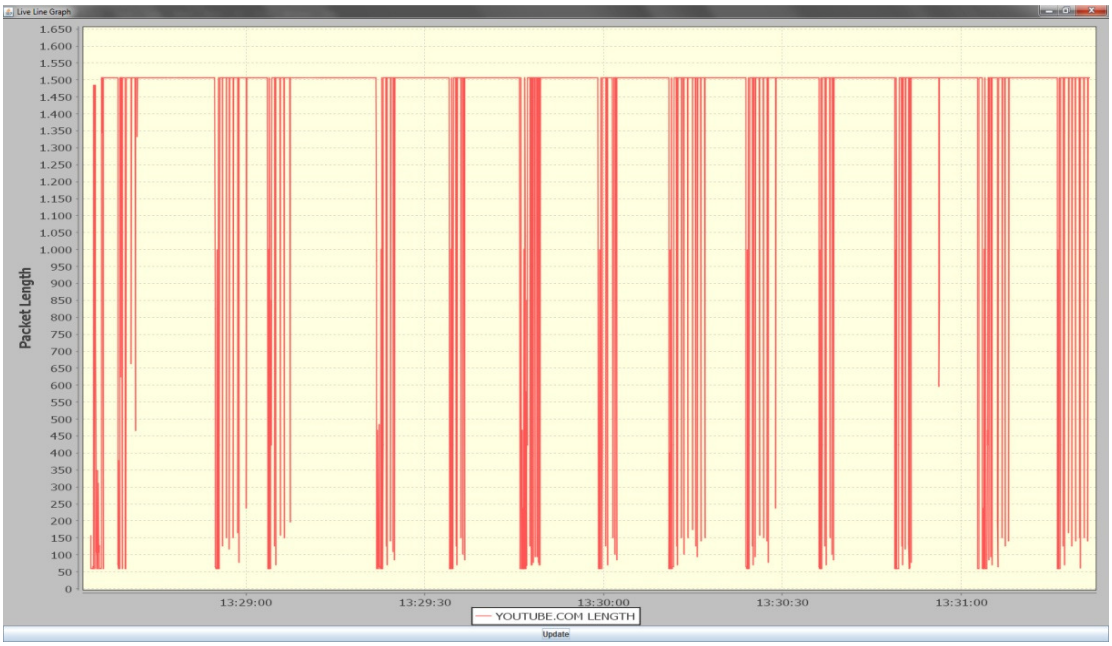
Το 1 λεπτό καταγραφής για τη κάθε κίνηση ξεχωριστά, σε αυτή την κατηγορία ανήκουν και όλα τα γραφήματα που θα δούμε παρακάτω σε αυτό το κεφάλαιο, επίσης έχει γίνει καταγραφή μίας κίνησης για κάθε ένα από τα πέντε σενάρια

Τα 2 λεπτά καταγραφής για τη κάθε κίνηση ξεχωριστά, σε αυτή την κατηγορία έχει γίνει καταγραφή κίνησης από τέσσερα site τα οποία παρέχουν live streaming video, από τρία site τα οποία παρέχουν Video on Demand κίνηση, από τέσσερα επιπλέον site τα οποία παράγουν κίνηση browsing και τέλος δύο εφαρμογές οι οποίες παρέχουν Video και Voice call για την καταγραφή της κίνησης VoIP.

Στην κίνηση FTP του τέταρτου σεναρίου δεν μας απασχόλησε ο χρόνος καταγραφής της κίνησης αλλά το μέγεθος των τριών αρχείων που κάναμε λήψη από τα τρία Ftp Site.

5.2 Σενάριο 1: Live Streaming, παρακολούθηση live video

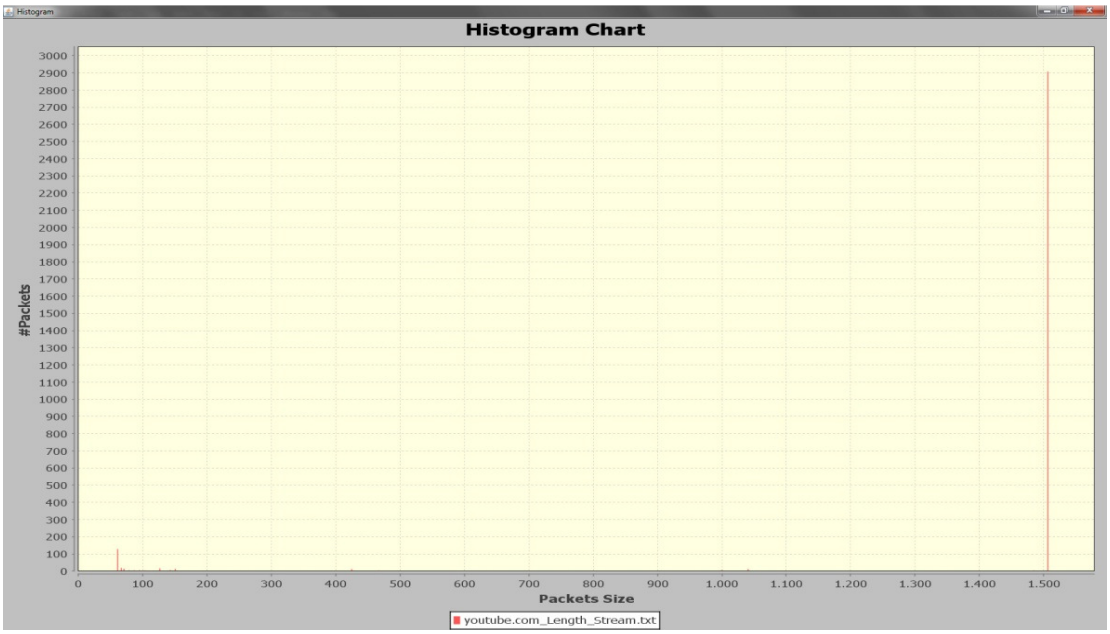
Στο 1ο σενάριο παρακολουθήσαμε live video streaming από τέσσερις ιστότοπους. Συγκεκριμένα, οι ιστότοποι αυτοί είναι: http://www.youtube.com, http://www.aljazeera.com, http://new.livestream.com και http://www.ustream.tv. Δημιουργήσαμε τέσσερα γραφήματα από το site του youtube τα οποία θα αναλύσουμε παρακάτω. Επίσης, παραθέτουμε και μερικά συνολικά στατιστικά στοιχεία που προέκυψαν από τις μετρήσεις, που θα μας βοηθήσουν στην ανάλυση και την κατανόηση της κίνησης.



Εικόνα 41: Packets Length from Streaming

Στην Εικόνα 41, βλέπουμε το μέγεθος των πακέτων, που έκανε λήψη η κάρτα δικτύου, όπως διαμορφώθηκε κατά τη διάρκεια της προσομοίωσης. Παρατηρώντας, τη γραφική παράσταση βλέπουμε ότι αρκετά πακέτα είναι της τάξεως των 1506 bytes, ωστόσο ανά τακτά χρονικά διαστήματα παρατηρούμε κάποια πλατώματα. Συγκεκριμένα, παρατηρούμε ότι τα πακέτα ξεκινούν από τα 60 bytes, πιθανόν να είναι κάποια acknowledgments που λάβαμε από το server, φτάνουν στα 1506 bytes και παραμένουν σταθερά σε αυτή τη τιμή για ένα χρονικό διάστημα περίπου πέντε δευτερολέπτων. Στη συνέχεια, υπάρχουν εναλλαγές στα μεγέθη των πακέτων με κάποια σκαμπανεβάσματα από τα 60 bytes για περίπου ένα διάστημα δύο δευτερολέπτων στα 1506 bytes. Από τις μετρήσεις που κάναμε, προέκυψε ότι σε πλήθος 3220 πακέτων, τα 2908 πακέτα έχουν

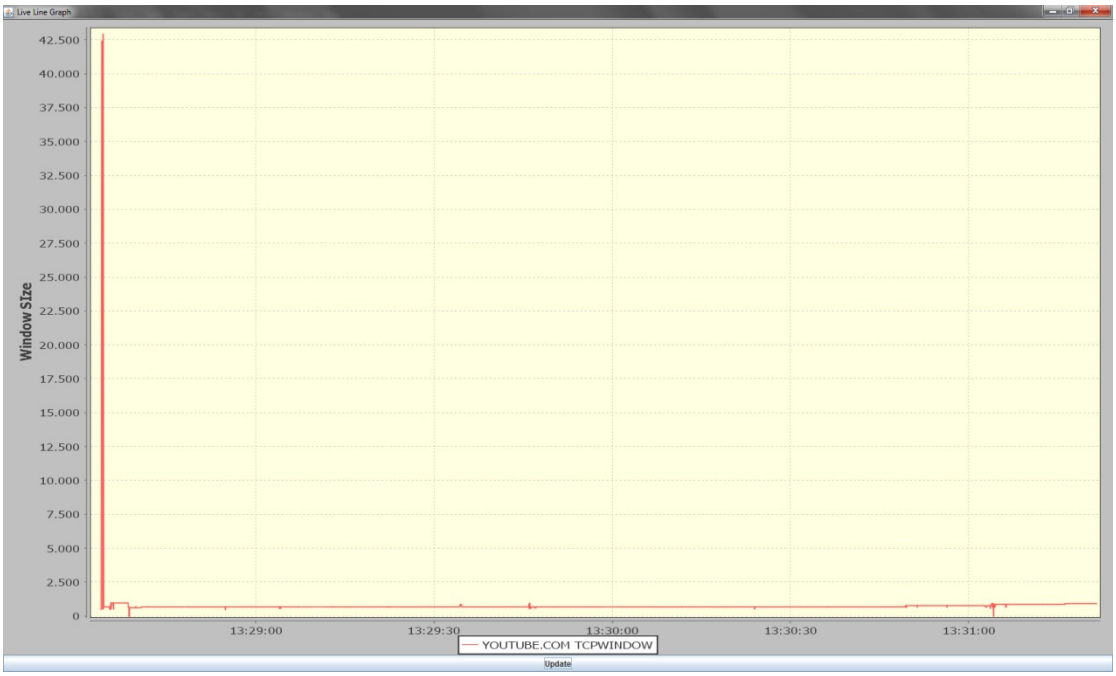
μέγεθος 1506 bytes, με ποσοστό 90,31%. Ένα σημαντικό στοιχείο που επιβεβαιώνει τα παραπάνω, είναι η τιμή της μέσης τιμής 1383 bytes, της διασποράς 150432 bytes και της τυπικής απόκλισης 387,86 bytes. Ιδιαίτερη σημασία έχει η τιμή της τυπικής απόκλισης, που δείχνει ότι η μέση τιμή αποτελεί αντιπροσωπευτικό στατιστικό μέτρο όσων είπαμε παραπάνω, αφού η τιμή της είναι σχετικά μικρή (387,86 bytes).



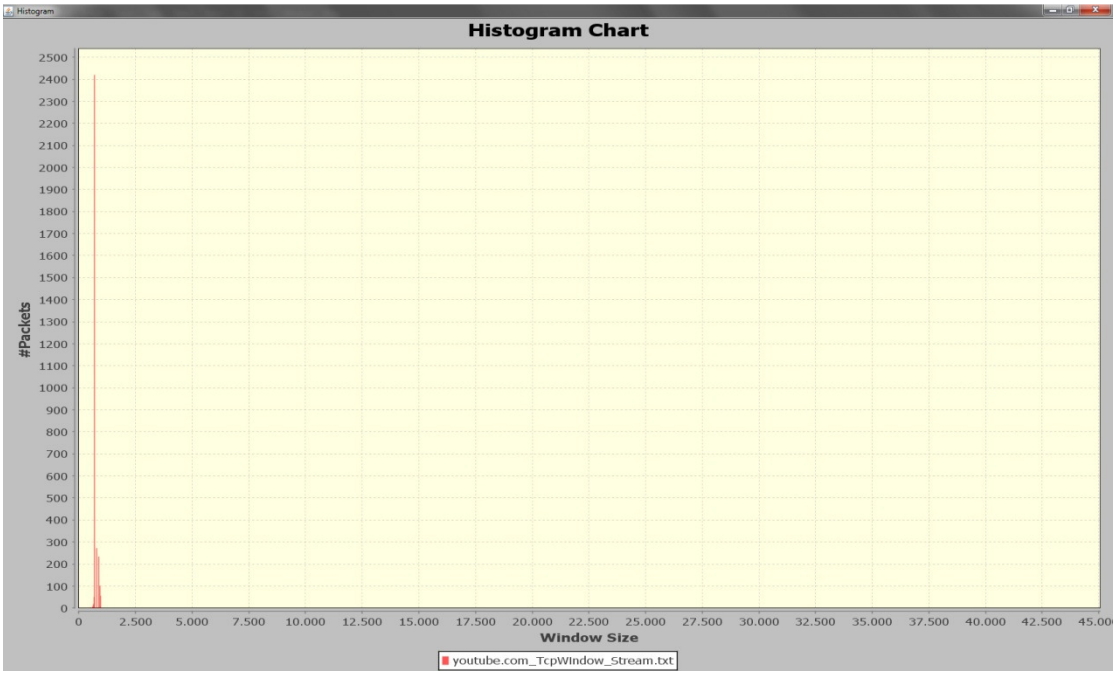
Εικόνα 42: Histogram of Packets Length from Streaming

Στην Εικόνα 42, απεικονίζεται το ιστόγραμμα με το πλήθος των πακέτων στον κάθετο άξονα και το μέγεθος τους στον οριζόντιο. Από το γράφημα αυτό γίνεται ευκολότερα αντιληπτό ότι 2908 πακέτα σε σύνολο 3220 πακέτων είναι της τάξεως των 1506 bytes.

Έχοντας καταγράψει όλη την κίνηση που παράχθηκε από όλα τα sites, ο Μ.Ο. που προκύπτει όσον αφορά το μέγεθος των πακέτων, δείχνει ότι το 91,92% των πακέτων έχει μέγεθος 1506 bytes. Επίσης, ο Μ.Ο. της μέσης τιμής είναι 1416,16 bytes, της διασποράς 106900 bytes,και της τυπικής απόκλισης 315,34 bytes. Οι τιμές αυτές λοιπόν, δείχνουν ότι υπάρχει μια σχετική σταθερότητα ως προς το μέγεθος των πακέτων και ότι υπάρχουν κάποιες αυξομειώσεις σε πακέτα μικρότερου μεγέθους, της τάξεως των 60 bytes.



Εικόνα 43: TCP Window Size from Streaming



Εικόνα 44: Histogram of TCP Window Size from Streaming

Στις Εικόνες 43 και 44 απεικονίζεται το μέγεθος του TCP Window όπως διαμορφώθηκε από την προσομοίωση για το youtube. Στην 43 στον κάθετο άξονα απεικονίζεται το μέγεθος του TCP Window και στην Εικόνα 44, το ιστόγραμμα, όπου στον κάθετο άξονα απεικονίζεται το πλήθος των πακέτων και στον οριζόντιο το μέγεθος

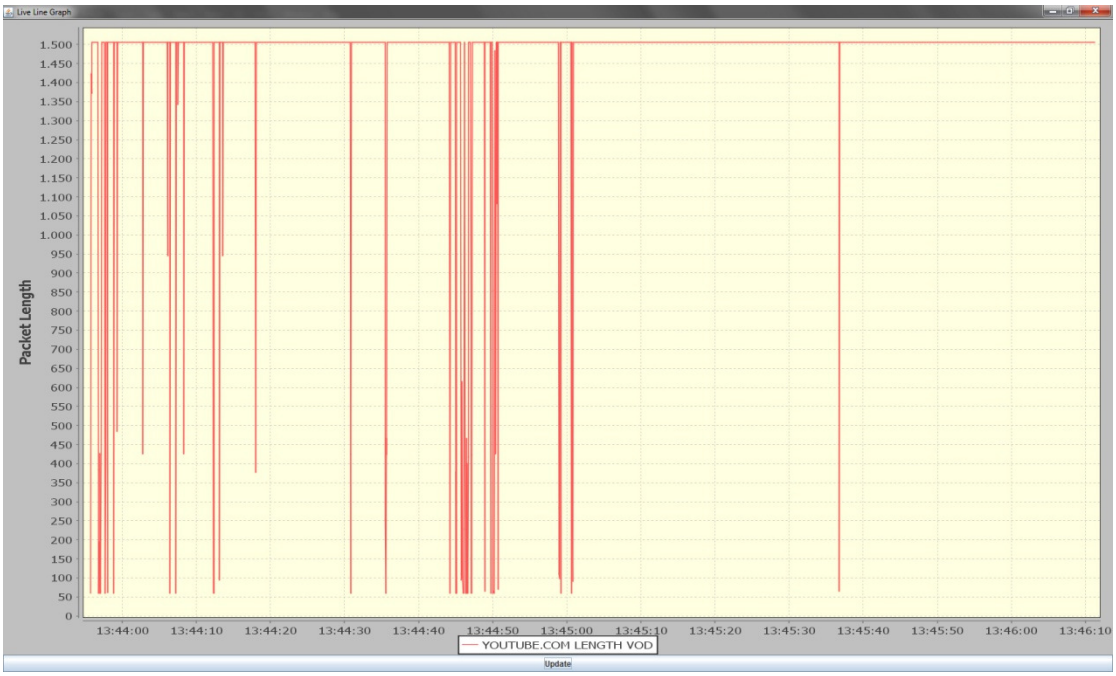
του TCP Window. Στην πρώτη γραφική παράσταση παρατηρούμε, ότι υπάρχει μια σταθερότητα στο μέγεθος του TCP Window. Αυτό οφείλεται στο τρόπο με τον οποίο λειτουργεί το live streaming. Ο ρυθμός αποστολής του on-line υλικού ελέγχεται ώστε να προσεγγίζει το ρυθμό λήψης από τον υπολογιστή του τελικού χρήστη και έτσι δεν χρειάζεται να μεσολαβήσει κάποιο μεγάλο χρονικό διάστημα για τη λήψη των πακέτων. Έτσι, το μέγεθος του TCP Window μπορεί να χαρακτηριστεί σταθερό.

Τα όσα αναφέραμε παραπάνω, γίνονται καλύτερα αντιληπτά στην Εικόνα 44, όπου παρατηρούμε μια ομοιομορφία ως προς το μέγεθος του TCP Window σε σχέση με το πλήθος των πακέτων. Και από τα αποτελέσματα των μετρήσεων, συμπεραίνουμε ότι σε ποσοστό 75% το μέγεθος του TCP Window δεν αλλάζει. Έχοντας καταγράψει, την live steaming κίνηση και από τις υπόλοιπες ιστοσελίδες μπορούμε να πούμε ότι δεν παρατηρήσαμε σημαντικές αλλαγές στο μέγεθος του TCP Window και σε ποσοστό περίπου 61% αυτό δεν παρουσιάζει ιδιαίτερες μεταβολές. Το ποσοστό αυτό, έχει μεγάλη διαφορά με το προηγούμενο και έτσι δεν μπορούμε να βγάλουμε κάποιο αξιόπιστο αποτέλεσμα.

Παρατηρώντας παρόμοια γραφήματα με αυτά των εικόνων 41, 42 και έχοντας υπόψη και τα αντίστοιχα αποτελέσματα αυτών, μπορούμε να πούμε ότι ο τελικός χρήστης παρακολουθεί κάποιο video με τη μορφή live streaming κατά ένα ποσοστό της τάξεως του 90% . Από τα στοιχεία για το TCP Window, δεν μπορούμε να βγάλουμε κάποιο αξιόπιστο αποτέλεσμα, αφού το 61% σαν ποσοστό είναι μικρό.

5.3 Σενάριο 2: Video on Demand (VoD), παρακολούθηση αποθηκευμένου video

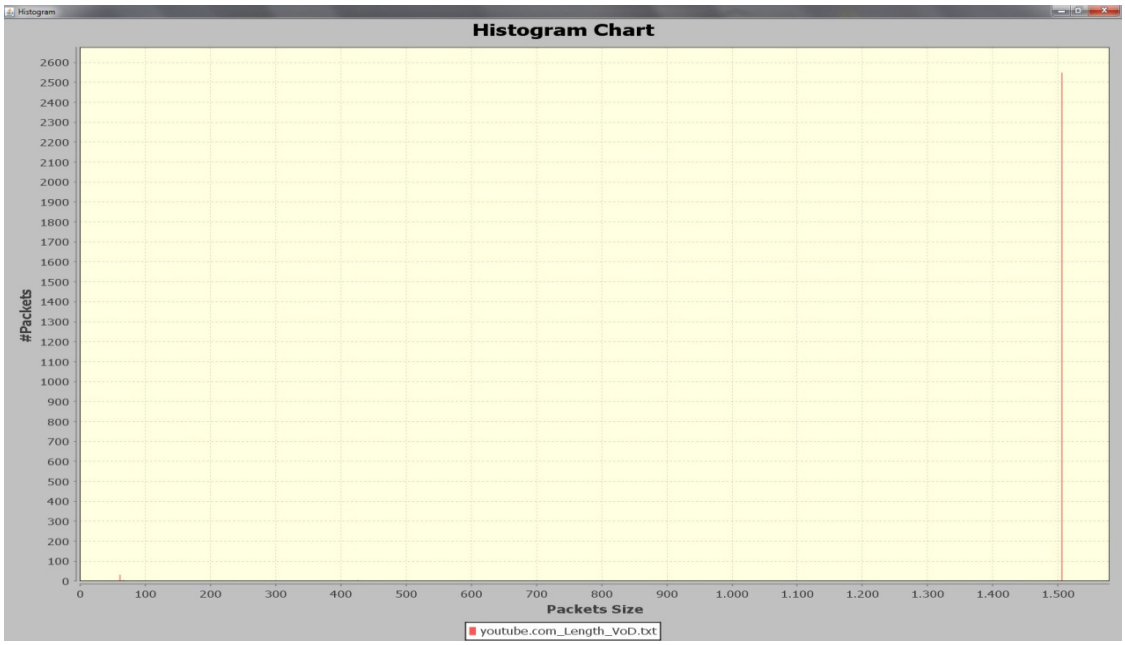
Σε αυτό το σενάριο, παρακολουθήσαμε πέντε video από τρεις ιστότοπους. Συγκεκριμένα, οι ιστότοποι αυτοί είναι: http://www.youtube.com, http://www.dailymotion.com και http:// www.veoh.com. Δημιουργήσαμε τέσσερα γραφήματα, από το site του youtube τα οποία θα αναλύσουμε παρακάτω. Επιπλέον, παραθέτουμε και μερικά συνολικά στατιστικά στοιχεία που προέκυψαν από τις μετρήσεις που μας βοηθούν στην κατανόηση της κίνησης.



Εικόνα 45: Packets Length from VoD

Στην Εικόνα 45 απεικονίζεται το μέγεθος των πακέτων που έπιασε η κάρτα δικτύου κατά τη διάρκεια της προσομοίωσης. Παρατηρώντας το γράφημα, βλέπουμε μια σταθερότητα στην κίνηση. Αρχικά, βλέπουμε ότι υπάρχουν μερικά πακέτα της τάξεως των 60 bytes και στη συνέχεια βλέπουμε ότι τα περισσότερα πακέτα έχουν μέγεθος 1506 bytes και παραμένουν σταθερά σε αυτό για μεγάλο χρονικό διάστημα. Επίσης, παρατηρούμε ότι στο μέσο περίπου της γραφικής παράστασης υπάρχει ένα βύθισμα για ένα μικρό διάστημα και έπειτα η κίνηση ξαναγίνεται σταθερή με τα πακέτα να κυμαίνονται και πάλι στα 1506 bytes, όπου και παραμένουν μέχρι το τέλος. Αυτό, ίσως να οφείλεται στον τρόπο με τον οποίο τοποθετούνται τα πακέτα στο buffer και την αποθήκευση τους στον υπολογιστή. Δηλαδή, από την αρχή μέχρι το μέσο του γραφήματος έχει γίνει αποθήκευση ενός μέρους του video και ύστερα από το βύθισμα που υπάρχει, συνεχίζεται η διαδικασία αποθήκευσης του υπόλοιπου video. Από τις μετρήσεις προέκυψε ότι σε σύνολο 2632 πακέτων τα 2549 πακέτα έχουν μέγεθος 1506 bytes με ποσοστό 96,85%. Σύμφωνα λοιπόν με αυτό το στοιχείο, θα μπορούσαμε να πούμε ότι το γράφημα, παρουσιάζει μια κανονικότητα ως προς την κίνηση και τη σταθερότητα στο μέγεθος των πακέτων. Κάποιες αυξομειώσεις που υπάρχουν, δεν είναι σημαντικές, αφού το παραπάνω ποσοστό είναι τεράστιο. Ένα επίσης σημαντικό στοιχείο που προέκυψε από τις μετρήσεις, είναι η τιμή της μέσης τιμής 1468 bytes, της διασποράς 47673 bytes και της τυπικής απόκλισης 218,34 bytes που

επιβεβαιώνουν όσα αναφέραμε παραπάνω ως προς τη σταθερότητα της κίνησης και το μέγεθος που έχουν τα πακέτα στο πλήθος τους.



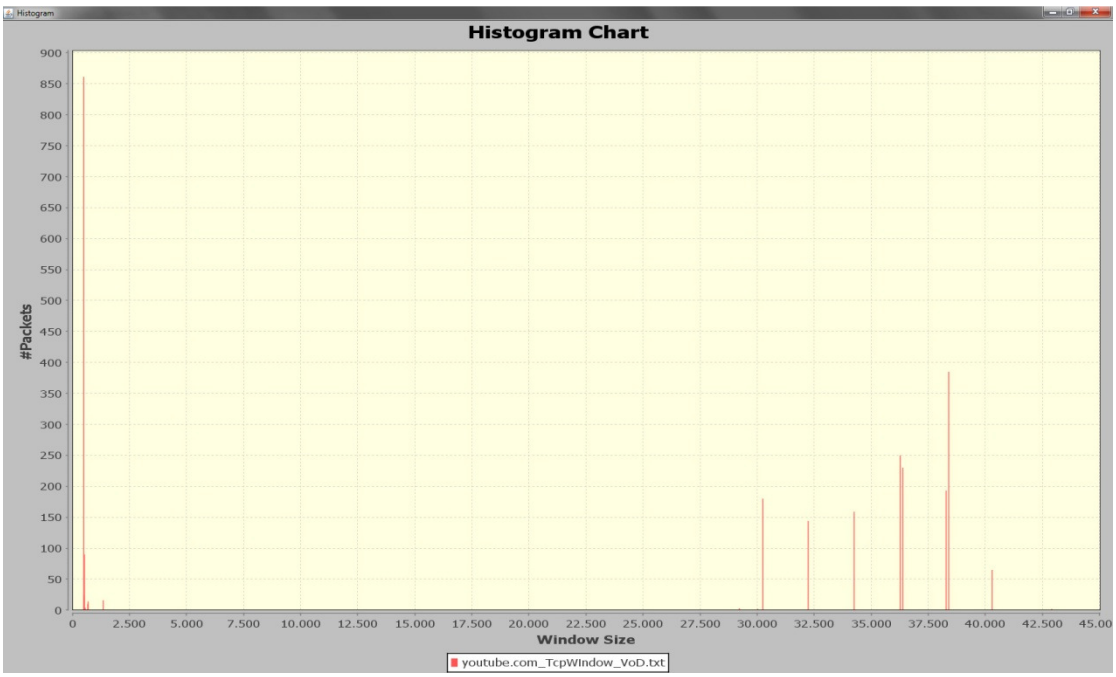
Εικόνα 46: Histogram of Packets Length from VoD

Στην Εικόνα 46, απεικονίζεται το ιστόγραμμα όπου στον κάθετο άξονα έχουμε το πλήθος των πακέτων και στον οριζόντιο το μέγεθος των πακέτων. Από το ιστόγραμμα, φαίνεται με ακρίβεια ότι 2549 πακέτα σε σύνολο 2632 έχουν μέγεθος 1506 bytes, πράγμα που δείχνει ότι η κίνηση είναι ως επί το πλείστον σταθερή, όπως είπαμε και παραπάνω.

Έχοντας καταγράψει την κίνηση από όλα τα sites, προέκυψαν τα ακόλουθα στοιχεία. Ο Μ.Ο. όσον αφορά το μέγεθος των πακέτων, δείχνει ότι το 95,75% των πακέτων έχει μέγεθος 1506 bytes. Αυτό το στοιχείο, επαληθεύει τα όσα αναφέρθηκαν παραπάνω ως προς τη σταθερότητα της κίνησης, αφού το ποσοστό είναι ιδιαίτερα υψηλό. Επίσης, ο Μ.Ο. για τη μέση τιμή είναι 1458,83 bytes, της διασποράς 571,95 bytes και της τυπικής απόκλισης 237,08 bytes.

Εικόνα 47: TCP Window Size from VoD

Στην Εικόνα 47, βλέπουμε το μέγεθος του TCP Window όπως διαμορφώθηκε κατά τη διάρκεια της προσομοίωσης. Παρατηρώντας τη γραφική παράσταση, μπορούμε να πούμε ότι TCP Window παρουσιάζει αρκετές διακυμάνσεις και αυξομειώσεις. Από αυτό το γράφημα θα χαρακτηρίζαμε ότι η κίνηση παρουσιάζει μια ανομοιομορφία. Στο ιστόγραμμα της Εικόνας 48 που ακολουθεί, μπορούμε να δούμε καλύτερα τα παραπάνω.



Εικόνα 48: Histogram of TCP Window Size from VoD

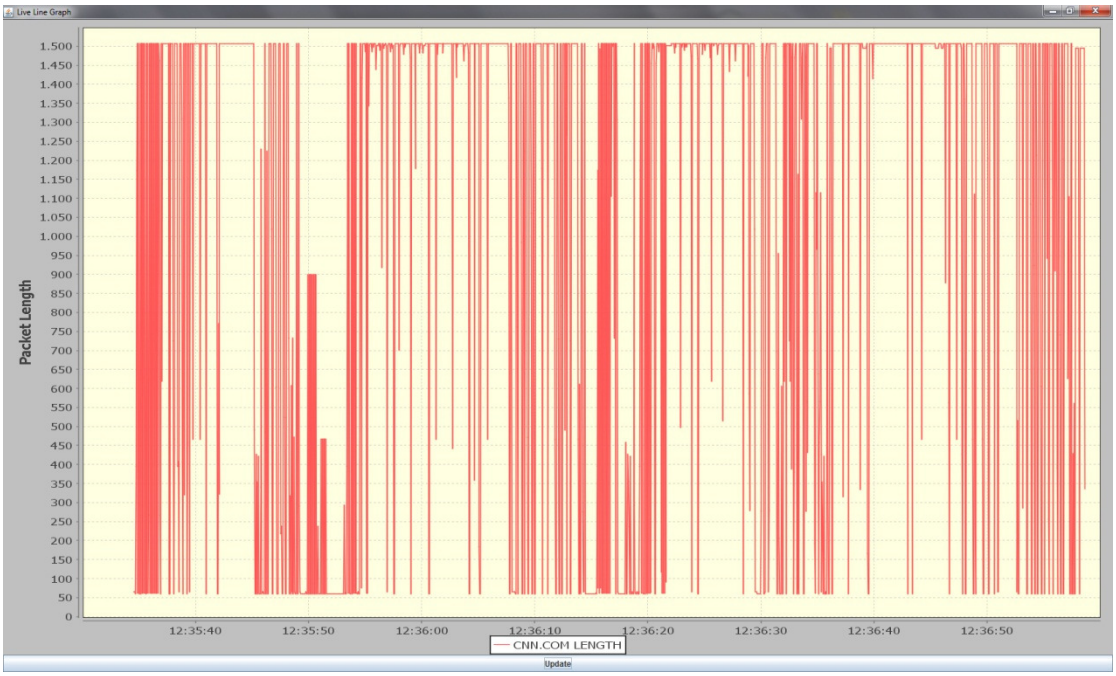
Στο ιστόγραμμα της Εικόνας 48, φαίνονται χαρακτηριστικά οι διακυμάνσεις του TCP Window σε σχέση με το πλήθος των πακέτων. Όπως προκύπτει από το γράφημα, βλέπουμε ότι υπάρχουν αρκετές εναλλαγές στο μέγεθος του TCP Window σε σχέση με το πλήθος των πακέτων. Από τις μετρήσεις, είδαμε ότι μόλις το 32,45% έχει σταθερό το TCP Window με την τιμή αυτού να είναι 488 bytes.

Από τις δοκιμές που κάναμε και στις υπόλοιπες ιστοσελίδες, παρατηρήσαμε, ότι σε ποσοστό 53%, το TCP Window παραμένει σταθερό, στοιχείο που δείχνει ότι υπάρχουν πολλές διακυμάνσεις αλλά δεν μας επιτρέπει να κάνουμε παραπάνω εκτιμήσεις αφού είναι μικρό.

Και σε αυτό το σενάριο, μπορούμε να καταλάβουμε ότι ο χρήστης παρακολουθεί κάποιο video λαμβάνοντας υπόψη τα δύο πρώτα γραφήματα και τα αποτελέσματα των μετρήσεων που αναφέρονται σε αυτά, καθώς τα ποσοστό που προέκυψε είναι ιδιαίτερα υψηλό, 96,85%.

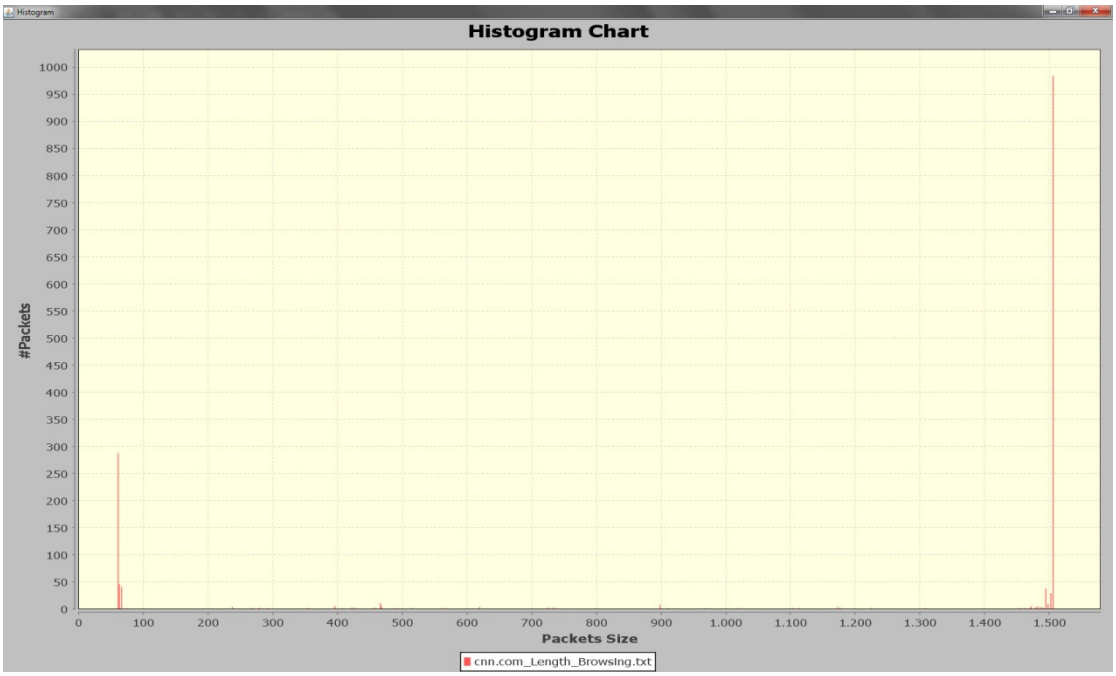
5.3 Σενάριο 3^{ο} Browsing, περιήγηση σε ιστοσελίδα

Στο 3ο σενάριο, γίνεται λήψη πακέτων από web sites. Συγκεκριμένα έγινε λήψη από πέντε ιστότοπους και αυτοί είναι http://www.cnn.com, http://www.contra.gr, http://www.gazzetta.gr, http://www.in.gr, http://www.tesyd.teimes.gr. Έχουμε δημιουργήσει τρία γραφήματα από την κίνηση πού παράχθηκε από το server του cnn.com, και στα οποία βλέπουμε το μέγεθος πακέτου ανά πακέτο, το πλήθος των πακέτων ανά μέγεθος πακέτου και το μέγεθος του TCP Window ανά πακέτο. Στην Εικόνα 49 βλέπουμε το μέγεθος κάθε πακέτου που έγινε λήψη από την κάρτα δικτύου. Παρατηρούμε ότι υπάρχουν πολλές εναλλαγές από τα 60 bytes στα 1500 bytes. Αυτό συμβαίνει, λόγω των επιβεβαιώσεων που στέλνονται για την σωστή ή τη λάθος λήψη του πακέτου από το Server.



Εικόνα 49: Packets Length from Browsing

Τις εναλλαγές αυτές, μπορούμε να τις αντιληφθούμε καλύτερα στην Εικόνα 50, το οποίο δείχνει ένα ιστόγραμμα του πλήθους των πακέτων ανά μέγεθος πακέτου. Σε αυτό βλέπουμε ότι από τα 1649 πακέτα που έγιναν λήψη τα 984 σχεδόν είναι μεγέθους 1506 bytes, το όποιο αντιστοιχεί στο 59.67% των πακέτων, και 288 πακέτα τα οποία είναι μεγέθους 60 bytes, δηλαδή 17.46% της κίνησης. Έχοντας κάνει καταγραφή και των άλλων τεσσάρων Site παρατηρούμε ότι κατά μέσο όρο 75% τις παραγόμενης browsing κίνησης αποτελείται από πακέτα 60 bytes και 1506 bytes. Από αυτό όμως δεν μπορούμε να βγάλουμε κάποιο απόλυτο συμπέρασμα γιατί πχ στο site contra.gr τα ποσοστά είναι 38.54% για τα πακέτα με μέγεθος 1506 bytes και 33.27% για τα πακέτα με μέγεθος 60 bytes, άρα η εναλλαγές ανάμεσα στα πακέτα εδώ είναι μεγαλύτερες. Επίσης αυτό που δείχνει τη μη ομοιόμορφη κίνηση με τα πολλά βυθίσματα που βλέπουμε στην Εικόνα 49 είναι η μέτρηση της τυπικής απόκλισης η οποία είναι ίση με 625.47 bytes για το cnn.com και 606.32 bytes κατά Μ.Ο για όλα τα site μαζί. Έτσι βλέπουμε ότι υπάρχουν μεγάλες διαφορές στο μέγεθος ανάμεσα στα πακέτα που αποστέλλονται.



Εικόνα 50: Histogram of Packets Length from Browsing

Στην Εικόνα 51, βλέπουμε το μέγεθος του TCP Window σε κάθε πακέτο που λαμβάνεται. Παρατηρούμε ότι TCP Window αλλάζει συνέχεια και δεν είναι σχεδόν ποτέ σταθερό. Αυτό μπορεί να συμβαίνει λόγου της μεγάλης επισκεψιμότητας που μπορεί να έχει ο web server του cnn.com και έτσι να μην μπορεί να λαμβάνει τον ίδιο αριθμό πακέτων κάθε χρονική στιγμή. Επίσης μπορεί να συμβαίνει γιατί η κίνηση δεν είναι συνεχόμενη, λόγω των εναλλαγών που γίνονται στις σελίδες του ιστότοπου για να υπάρξει κίνηση κατά το ένα λεπτό της προσομοίωσης του σεναρίου. Ακόμα και οι τιμές που υπολογίσαμε για κάθε site για την μέση τιμή δεν είχαν κάποια ομοιομορφία. Για το cnn.com η μέση τιμή είναι 4709 bytes, για το contra.gr είναι 11887 bytes, για το gazzetta.gr είναι 26147 bytes, για το in.gr είναι 19191 bytes και για το tesyd.teimes.gr είναι 31725 bytes. Με την ίδια σειρά υπολογίσαμε και τις τυπικές αποκλίσεις οι οποίες είναι 1141.18, 1384.94, 1497.21, 1045.67 και 1257.98 bytes. Στις τυπικές αποκλίσεις μπορούμε να πούμε ότι υπάρχει μία κανονικότητα, στο ότι δεν έχουν μεγάλες διαφορές μεταξύ τους και αυτό φαίνεται και στο Μ.Ο των τυπικών αποκλίσεων που είναι 1265,39.

Εικόνα 51: TCP Window Size from Browsing

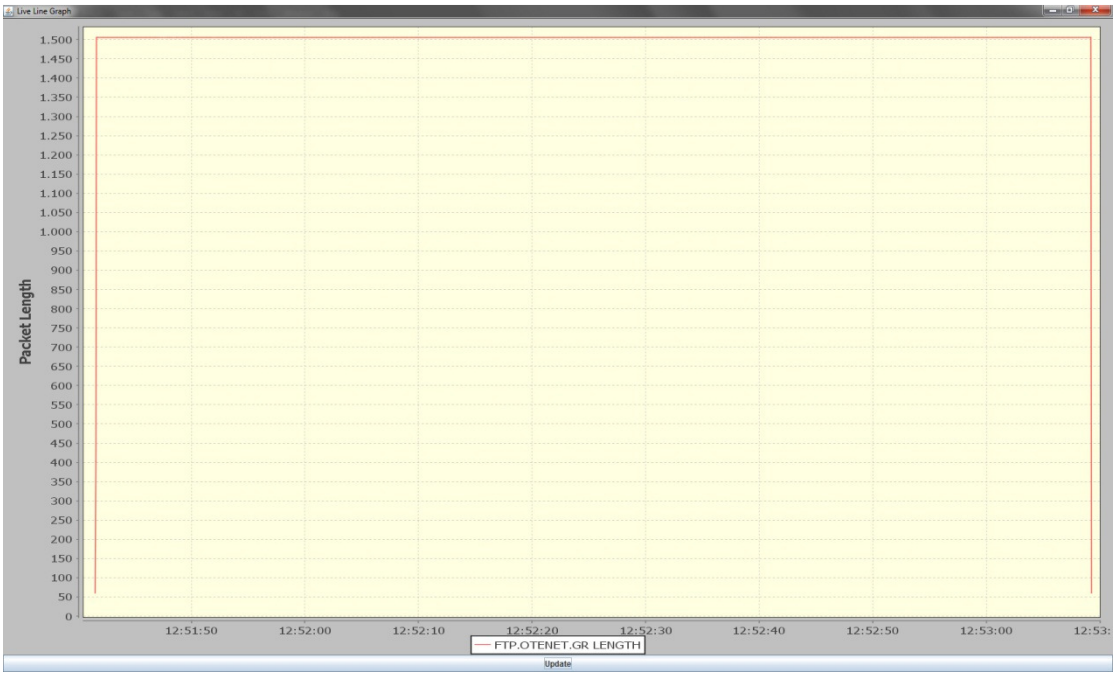
Στην κίνηση browsing του πρώτου σεναρίου αυτό που παρατηρήσαμε είναι ότι τα περισσότερα πακέτα χωρίζονται σε δύο ομάδες μεγεθών, από 50 bytes έως 100 bytes και από 1300 bytes έως 1550 bytes και ότι το TCP Window δεν παραμένει σχεδόν ποτέ σταθερό και γενικά η κίνηση είναι μη ομοιόμορφη. Αυτό λογικά συμβαίνει λόγω του ότι για να υπάρχει συνεχόμενη κίνηση για το 1 λεπτό ή των 2 λεπτών καταγραφής της κίνησης έπρεπε να κάνουμε συχνά ανανέωση ή εναλλαγή στις σελίδες του κάθε site.

Γενικά, πάντως δεν μπορούμε να βγάλουμε κάποιο αξιόπιστο συμπέρασμα από τις μετρήσεις γιατί το 75% σαν ποσοστό είναι μικρό και δεν είναι και αντιπροσωπευτικό για όλα τα site.

5.4 Σενάριο 4ο FTP, λήψη αρχείου από ftp server

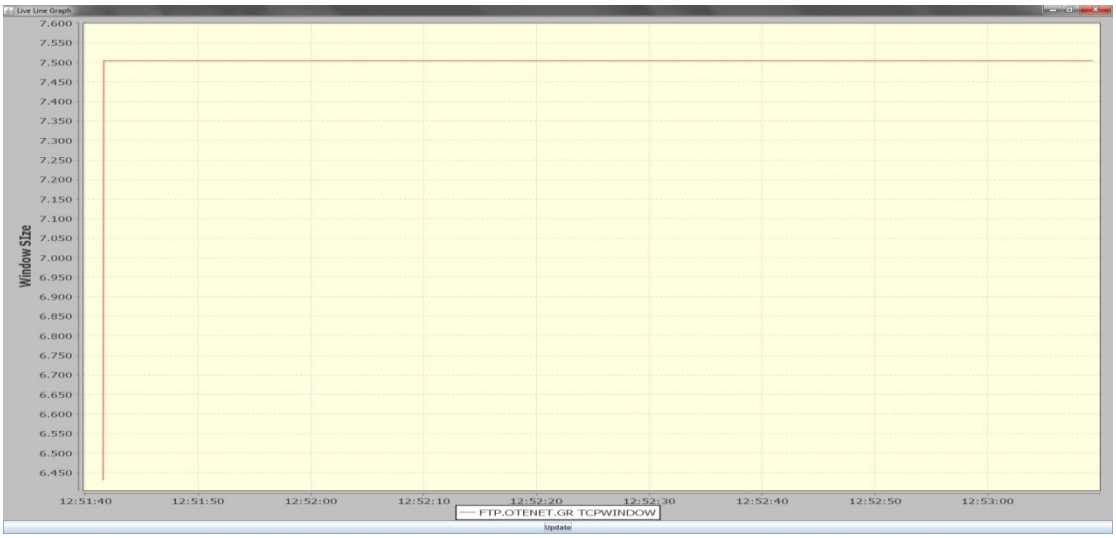
Στο 4ο σενάριο γίνεται λήψη τεσσάρων αρχείων από τρείς διαφορετικού FTP Server. Πιο συγκεκριμένα από το server http://ftp.ne.jp έγινε λήψη ενός αρχείου 35MB, από το http://ftp.otenet.gr έγινε λήψη δύο αρχείων μεγέθους 15MB και 35MB, και από το http://ftp.ntua.gr έγινε λήψη ενός αρχείου 35MB. Από καταγραφή της κίνησης που δημιουργήθηκε από το ftp.otenet.gr για το αρχείο των 15MB δημιουργούμε τα ίδια γραφήματα με το προηγούμενο σενάριο. Στην Εικόνα 52 παρατηρούμε ότι εκτός του πρώτου και του τελευταίου πακέτου που είναι 60 bytes, όλα τα άλλα πακέτα είναι 1506

bytes, το οποί αντιστοιχεί στο 99,82% της συνολικής κίνησης, και έτσι η κίνηση είναι σταθερή. Το ιστόγραμμα του FTP δεν το εμφανίζουμε, γιατί η κίνηση ως προς το μέγεθος των πακέτων είναι ξεκάθαρη στο γράφημα 52.



Εικόνα 52: Packets Length from FTP

Παρόμοια είναι και η γραφική παράσταση που βλέπουμε στο γράφημα 53, η οποία απεικονίζει το μέγεθος του TCP Window. Και εδώ το μέγεθος είναι σταθερό εκτός από το πρώτο πακέτο, αυτό που βλέπουμε είναι ότι όλα τα πακέτα που λαμβάνονται, εκτός από το 1^{ο} και το τελευταίο, έχουν το ίδιο TCP Window Size και σε ποσοστό αντιστοιχεί στο 99,88%. Σε άλλες δοκιμές ίδιας κίνησης, οι γραφικές παραστάσεις ήταν παρόμοιες, με την μόνη διαφορά το μέγεθος του TCP Window που ήταν μεγαλύτερο ή μικρότερο.



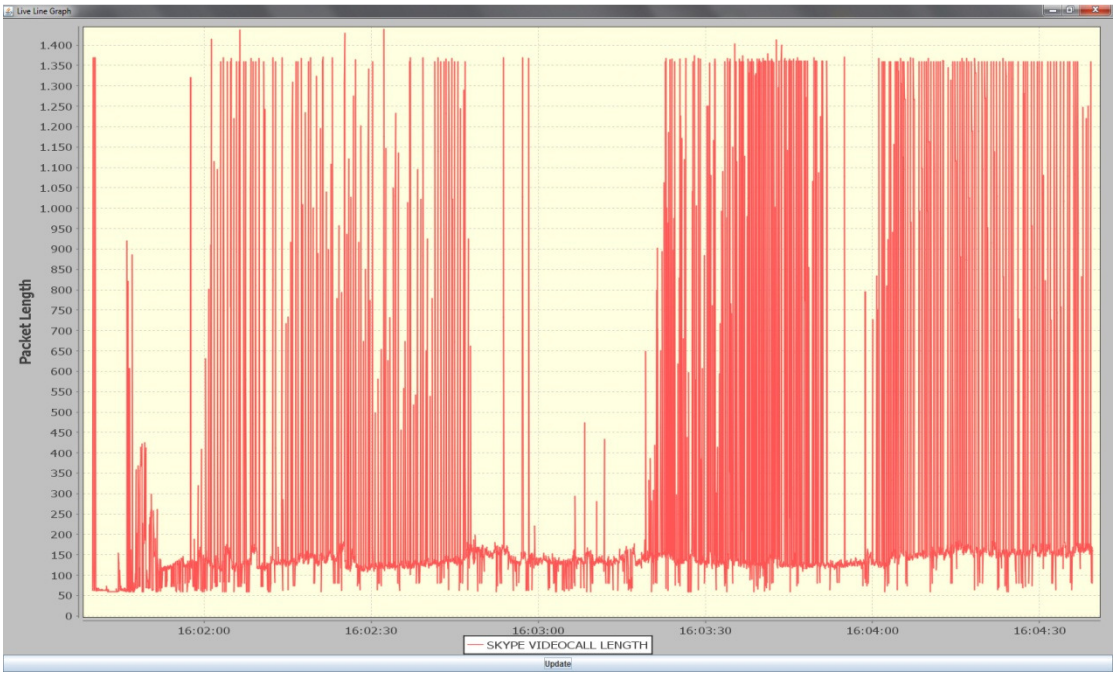
Εικόνα 53: TCP Window Size from FTP

Στην FTP κίνηση παρατηρούμε ότι η κίνηση που παράγεται είναι σταθερή όσο αναφορά το μέγεθος των πακέτων και το μέγεθος του παραθύρου. Έχοντας υπόψη και τα άλλα τρία αρχεία που έγιναν λήψη, η κίνηση που καταγράφηκε από όλους τους Servers, σε ποσοστό 99,94%, ήταν μεγέθους 1506 bytes το πακέτο. Επίσης το μέγεθος του TCP Window ήταν ίδιο σε όλη τη διάρκεια κάθε λήψης, με ποσοστό 99,97%. Βλέποντας τις γραφικές παραστάσεις ή τα στοιχεία των πακέτων μπορεί κατευθείαν να αναγνωριστεί η κίνηση η οποία έχει ληφθεί.

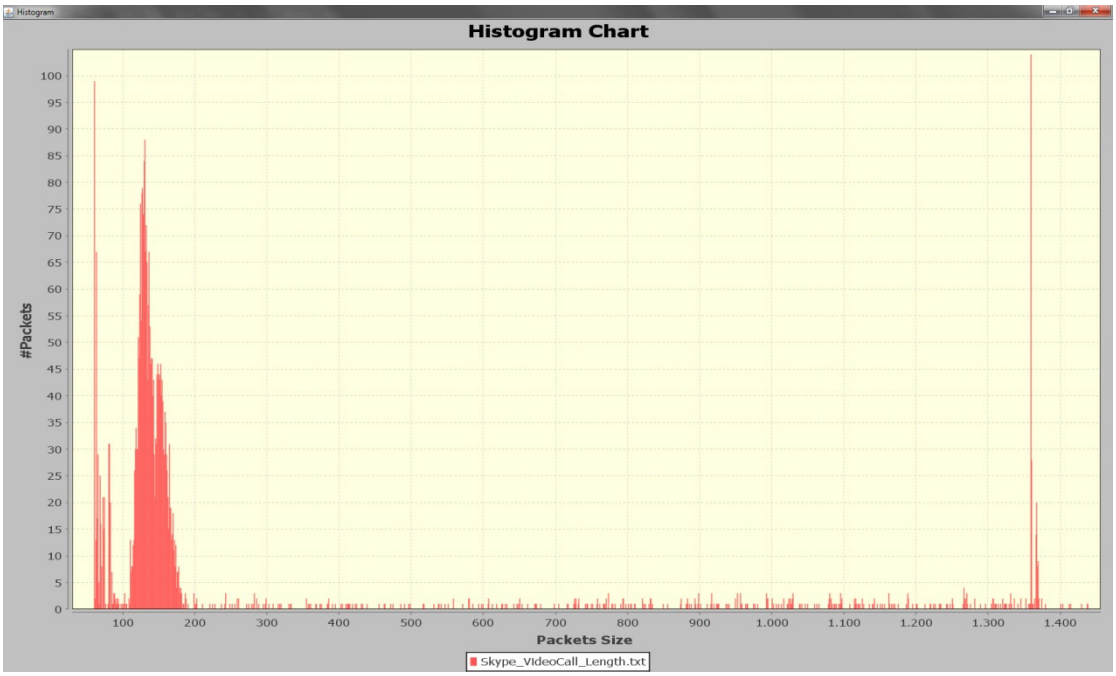
5.5 Σενάριο 5ο VoIP, κλήση από το πρόγραμμα Skype

Στο $5^{ο}$ σενάριο, πραγματοποιούνται έξι κλήσεις με την χρήση των προγραμμάτων Skype και ooVoo για να παρατηρήσουμε την κίνηση που παράγεται μέσω VoIP. Η $1^{η}$ και η $2^{η}$ κλήση είναι τύπου Voice Call από το Skype και είναι μεταξύ δύο τοπικών συσκευών, είναι κλήσεις 1 και 2 λεπτών αντίστοιχα. Η $3^{η}$ και η $4^{η}$ κλήση είναι τύπου Video Call και είναι και αυτή ανάμεσα σε δύο τοπικές συσκευές και η καταγραφή γίνεται για ένα 1 και 2 λεπτά. Η $5^{η}$ κλήση είναι τύπου Voice Call και είναι μεταξύ ενός τοπικού υπολογιστή και του Test Service της εφαρμογής και είναι διάρκειας ενός λεπτού. Η $6^{η}$ και τελευταία κλήση γίνεται μέσω του προγράμματος ooVoo και είναι τύπου Voice Call, διάρκειας ενός λεπτού. Σε αυτό το σενάριο έχουμε δημιουργήσει γραφήματα για την $1^{η}$ και την $3^{η}$ κλήση και τα οποία απεικονίζουν το μέγεθος του κάθε πακέτου ανά πακέτο, το πλήθος των πακέτων ανά μέγεθος και το πλήθος των πακέτων ανά τύπο πρωτοκόλλου.

Η Εικόνα 54 αφορά τη 3η κλήση, η οποία είναι Video, και βλέπουμε το μέγεθος των πακέτων ανά πακέτο που έχει ληφθεί. Παρατηρούμε ότι υπάρχει πολύ μεγαλύτερος αριθμός πακέτων σε σχέση με τα προηγούμενα δύο σενάρια. Τα πακέτα μεγέθους από 60 bytes έως 200 bytes είναι τα 2940 από τα 3516, το όποιο αντιστοιχεί στο 83,61% και 264 πακέτα μεγέθους 1200 bytes έως 1600 bytes, με ποσοστό 7,5%. Παρατηρώντας και τα στοιχεία που πήραμε και από την 4^{η} κλήση, που είναι Video Call διάρκειας 2 λεπτών, βλέπουμε ότι το εύρος των πακέτων με μέγεθος 60 bytes έως 200 bytes είναι της τάξεως 60% και το εύρος 1200 bytes έως 1600 bytes είναι 26,12%. Αν προσθέσουμε τα 2 εύρη και των δύο κλήσεων και μετά βγάλουμε το Μ.Ο τους βλέπουμε ότι το 88,65% των πακέτων ανήκουν σε αυτά τα μεγέθη. Ότι τα περισσότερα πακέτα κυμαίνονται στο παραπάνω εύρος μπορεί να παρατηρηθεί καλύτερα στην Εικόνα 55, η οποία αναπαριστά ένα ιστόγραμμα του πλήθους των πακέτων ανά μέγεθος, για την video κλήση.

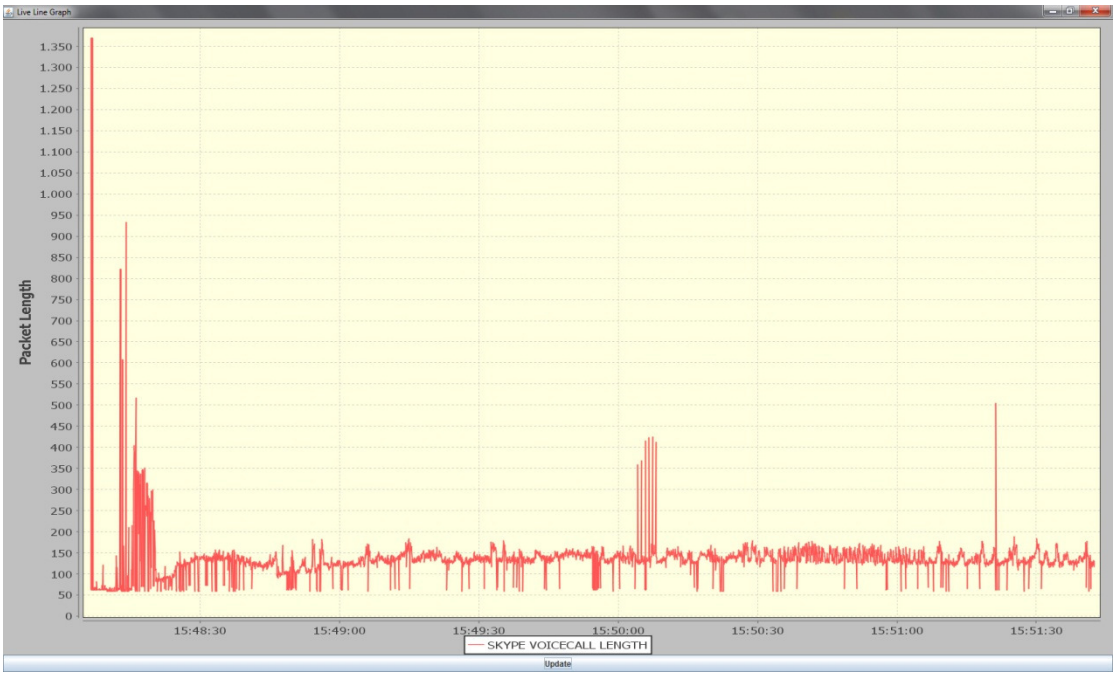


Εικόνα 54: Packets Length from VoIP (Skype Video Call)

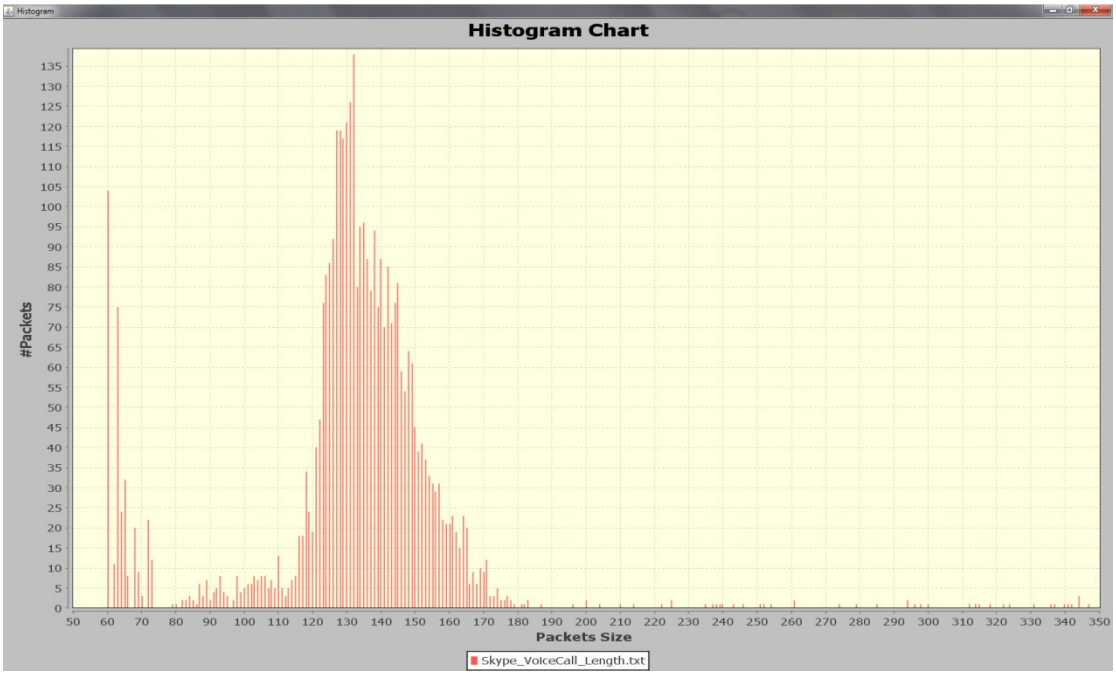


Εικόνα 55: Histogram of Packet Length from VoIP (Skype Video Call)

Αντίστοιχα, στην Εικόνα 56 και 57 βλέπουμε την κίνηση που παράγεται από την 1η κλήση, η οποία είναι Skype Voice Call διάρκειας ενός λεπτού, και παρατηρούμε ότι το μέγεθος των πακέτων που κυμαίνεται από 60 έως 200 bytes, είναι 3616 από τα 3679, το οποίο αντιστοιχεί στο 98,28% της κίνησης που παράχθηκε από την κλήση. Παρόμοια ποσοστά συναντήσαμε σε όλες τις Voice κλήσεις που έγιναν και στο Skype και στο ooVoo με το Μ.Ο των ποσοστών αυτών να είναι 95,3%. Βλέποντας επίσης την μέση τιμή των πακέτων που είναι 150 bytes και την τυπική απόκλιση η οποία είναι 119,94 bytes βλέπουμε ότι οι διαφορές στο μέγεθος ανάμεσα στα πακέτα είναι μικρές



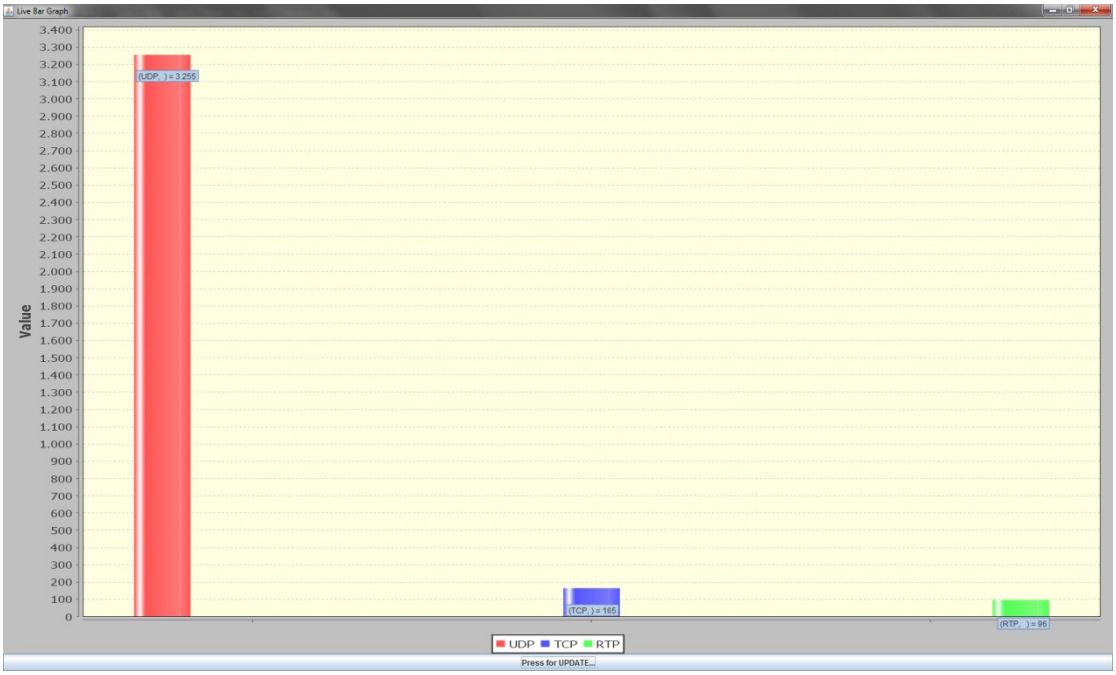
Εικόνα 56: Packets Length from VoIP (Skype Voice Call)



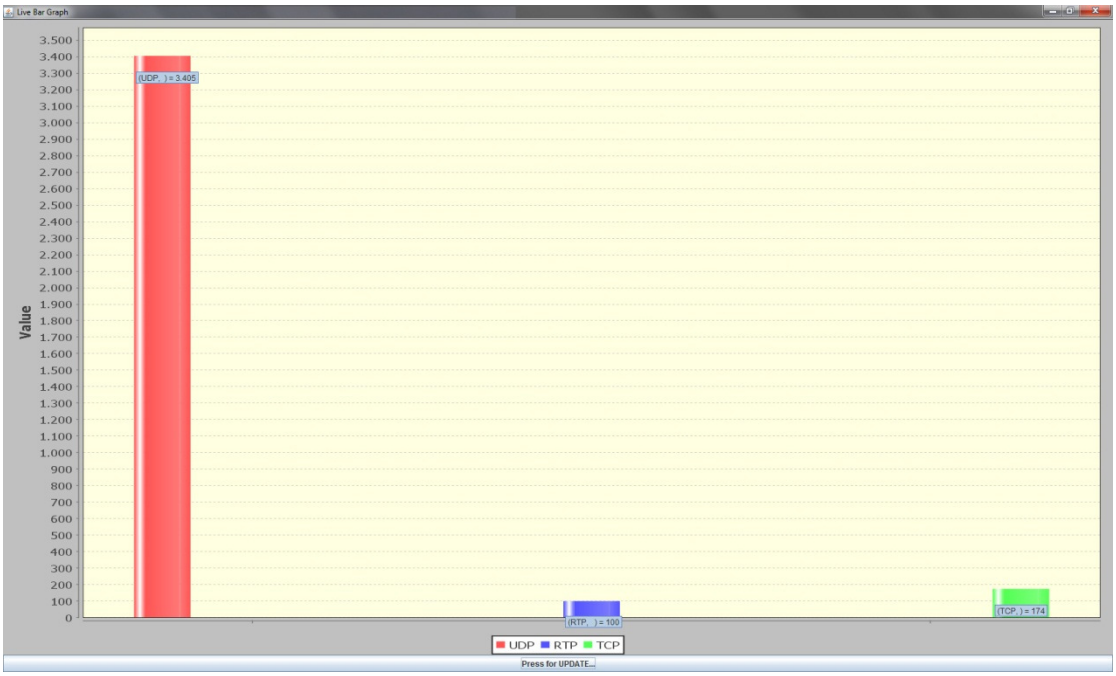
Εικόνα 57: Histogram of Packet Length from VoIP (Skype Voice Call)

Στις επόμενες δύο εικόνες (Εικόνα 58 και Εικόνα 59), βλέπουμε τους τύπους πρωτοκόλλων που χρησιμοποιούνται στις δύο κλήσεις, καθώς και τον αριθμό πακέτων σε κάθε πρωτόκολλο. Αυτές οι εικόνες μπορούν να χρησιμοποιηθούν, μαζί με τα παραπάνω ποσοστά και εικόνες, για εξακριβωθεί με μεγαλύτερη ακρίβεια ότι η κίνηση αυτή είναι

VoIP λόγω του ότι η κίνηση χρησιμοποιεί τα πρωτόκολλα UDP και RTP ενώ τα άλλα σενάρια χρησιμοποιούν μόνο TCP στο μεγαλύτερο ποσοστό τους. Η κίνηση VoIP βλέποντας ένα γράφημα ιστογράμματος και την κατανομή των τιμών μπορεί να αναγνωριστεί με αξιοπιστία και με ένα ποσοστό πάνω από 90%.



Εικόνα 58: Protocol Types for Video Call



Εικόνα 59: Protocol Types for Voice Call

5.6 Περιορισμοί και μελλοντική επέκταση

5.6.1 Περιορισμοί

Με την ολοκλήρωση της εργασίας θα θέλαμε να αναφέρουμε μερικούς σημαντικούς περιορισμούς που έχει η εφαρμογή που δημιουργήσαμε σε σχέση με την καταγραφή της κίνησης και το γραφικό περιβάλλον. Αυτοί οι περιορισμοί είναι:

- Η εφαρμογή δεν μπορεί να κάνει καταγραφή πακέτων όταν αυτά προέρχονται από servers οι οποίοι χρησιμοποιούν κρυπτογραφημένα πρωτόκολλα όπως το HTTPS και το FTPS. Σε αυτές τις περιπτώσεις το μόνο που κάνει είναι να λαμβάνει μόνο πακέτα τα οποία περιέχουν μόνο τις βασικές πληροφορίες οι οποίες ενθυλακώνονται από τα επίπεδα συνδέσεων δεδομένων, δικτύου και μεταφοράς χωρίς όμως να βλέπουμε το μέγεθος των πακέτων που περιέχουν τα δεδομένα.
- Δεν μπορεί να διαχωρίσει εφαρμογές που έχουν εγκατασταθεί στον υπολογιστή και οι οποίες μπορεί να χρησιμοποιούν τη σύνδεση του internet για να παρέχουν τις υπηρεσίες τους (πχ skype, torrent, antivirus, κα.).
- Επίσης, στις γραφικές παραστάσεις δεν εμφανίζει την χρονική στιγμή που έγινε η λήψη και η καταγραφή του πακέτου αλλά την χρονική στιγμή που γίνεται η εμφάνιση του πακέτου στο εκάστοτε γράφημα.
- Τέλος, ένας ακόμα περιορισμός της εφαρμογής όσο αναφορά το γραφικό περιβάλλον είναι ότι δεν παρέχει κάποια επιλογή αποθήκευσης των αρχείων και γραφημάτων που δημιουργούνται.

5.6.2 Μελλοντική επέκταση

Η εφαρμογή μας, όπως εξάλλου και κάθε άλλο υπαρκτό πρόγραμμα, επιδέχεται μια σειρά βελτιώσεων οι οποίες θα μπορούσαν να γίνουν σε μια μελλοντική επέκταση της. Θα χωρίζαμε αυτήν την μελλοντική επέκταση σε δύο κατηγορίες:

- **Εσωτερικές Λειτουργίες**
- **Χρηστικό Περιβάλλον**

Όσον άφορα τις εσωτερικές λειτουργίες, θα μπορούσε να κάνει καταγραφή και των κρυπτογραφημένων πακέτων, να μπορεί επίσης να αναγνωρίσει περισσότερα πρωτόκολλα και να δίνει περισσότερες πληροφορίες σχετικά με αυτά όταν αυτό ζητάτε από το χρήστη.

Επιπλέον, θα μπορούσε να κάνει αναγνώριση και διαχωρισμό των εγκατεστημένων εφαρμογών, ανάλογα με το είδος τις κίνησης που παράγουν.

Όσον αφορά το χρηστικό περιβάλλον, θα μπορούσε η εφαρμογή να παράγει περισσότερα είδη γραφικών παραστάσεων και επίσης να δίνει στο χρήστη την επιλογή να επιλέξει ποιες πληροφορίες θέλει να απεικονίσει γραφικά. Τέλος να μπορεί να αποθηκεύσει όλα όσα δημιουργήθηκαν όσο έτρεχε η εφαρμογή.