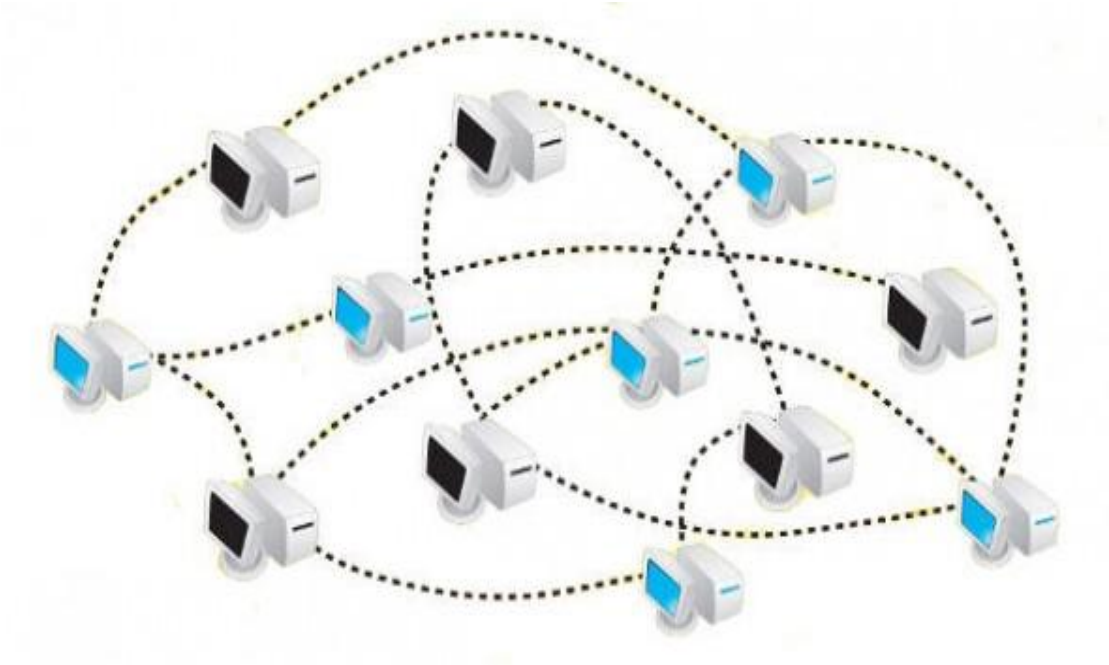
ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΗΠΕΙΡΟΥ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε.

Ανίχνευση και ανάλυση δικτυακής κίνησης με τη χρήση του εργαλείου Wireshark.

Περίπτωση μελέτης «δικτυακή κίνηση παραγόμενη από το Skype».

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ



Εισηγήτρια: Σολδάτου Μαρία 9134

Επιβλέπουσα: Μαργαρίτη Σπυριδούλα

Ανίχνευση και ανάλυση δικτυακής κίνησης με τη χρήση του εργαλείου wireshark.

Περίπτωση μελέτης «δικτυακή κίνηση παραγόμενη από το Skype».

ΣΟΛΔΑΤΟΥ ΜΑΡΙΑ

A.M. 9134, email: soldatou.maria@gmail.com

ΠΕΡΙΛΗΨΗ

Σκοπός της πτυχιακής εργασίας είναι να μελετήσουμε την κίνηση μέσα σε ένα δίκτυο ώστε να μπορέσουμε να πετύχουμε ορθότερη διαχείριση όσον αφορά την απόδοση και τη βελτιστοποίηση υπηρεσιών. Για να επιτευχθεί η σωστή διαχείριση θα πρέπει να έχουμε εικόνα για την κίνηση που υπάρχει στο δίκτυο και γι' αυτό θα χρησιμοποιηθούν εργαλεία για την παρακολούθηση και την ανίχνευση της κίνησης. Στην συγκεκριμένη περίπτωση θα χρησιμοποιηθεί το εργαλείο Wireshark. Στόχος αυτής της εργασίας είναι η ανίχνευση και η ανάλυση της δικτυακής κίνησης μιας εφαρμογής Voice over Internet Protocol (VoIP) που χρησιμοποιεί το διαδίκτυο για μεταφορά φωνής και βίντεο, της εφαρμογής Skype. Οι μετρούμενες παρατηρήσεις αξιολογούνται ως προς την ποιότητα υπηρεσιών, ώστε τελικά, να προταθούν βελτιώσεις και παρατηρήσεις σε έναν διαχειριστή με βάση την απόδοση και την ποιότητα των υπηρεσιών.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΕΝΟΤΗΤΑ 1

ΕΙΣΑΓΩΓΗ

1.1 Δίκτυο

Δίκτυο είναι ένα σύνολο ανεξάρτητων υπολογιστικών συστημάτων που συνδέονται μεταξύ τους και έχουν τη δυνατότητα να ανταλλάσουν πληροφορίες και να εκμεταλλεύονται πόρους υλικού και λογισμικού[12].

Η σύνδεση δύο ή περισσοτέρων αυτόνομων υπολογιστικών συστημάτων μεταξύ τους είναι ένα δίκτυο ηλεκτρονικών υπολογιστών, μέσω του οποίου οι χρήστες μπορούν να μοιράζονται ίδιους πόρους, να ανταλλάσουν μηνύματα, να χειρίζονται κοινές εφαρμογές και να έχουν ταυτόχρονη πρόσβαση σε ένα αρχείο δεδομένων[13].

Η σύνδεση των υπολογιστών μπορεί να γίνει είτε ενσύρματα, με τη χρήση ομοαξονικού καλωδίου (καλώδιο κεραίας τηλεόρασης) είτε με UTP-45 καλώδιο (καλώδιο τηλεφώνου) είτε μέσω οπτικών ινών είτε ασύρματα με τη χρήση πομποδεκτών ή δορυφορικών συστημάτων[13].

Γενικότερα, η τεχνολογία των δικτύων αναπτύσσεται με ραγδαίο ρυθμό. Αυτό βασίζεται κυρίως στην εξέλιξη που υπάρχει στον χώρο των τηλεπικοινωνιών και ανάλογα στην κατηγορία που ανήκει το κάθε δίκτυο, έχει και την ανάλογη εξέλιξη.

1.1.1 Διάκριση Δικτύων

Η διάκριση των δικτύων γίνεται ως προς τη φυσική τους έκταση, δηλαδή, ανάλογα την απόσταση την οποία μπορούνε να καλύψουνε. Τα δίκτυα διακρίνονται κυρίως σε LAN, MAN,WAN και Internet.

1.1.1.1 Τοπικά Δίκτυα (Local Area Networks – LAN)

Είναι ένα ηλεκτρονικό δίκτυο επικοινωνιών το οποίο το οποίο είναι υπεύθυνο για την σύνδεση ενός εξοπλισμού, όπως υπολογιστές, εκτυπωτές, Servers, modems, faxes κ.λ.π. Σκοπός του δικτύου είναι μοιράζονται οι κοινοί πόροι σε μια γεωγραφική περιοχή έως και 2km. Η ταχύτητα στα τοπικά δίκτυα περιορίζεται από τα 10Mbps ως τα 100Mbps[12].

1.1.1.2 Μητροπολιτικά Δίκτυα (Metropolitan Area Networks – MAN)

Τα Μητροπολιτικά δίκτυα καλύπτουν τα όρια μιας πόλης και μπορεί να είναι είτε ιδιωτικά είτε δημόσια. Τα κύριο χαρακτηριστικό τους είναι ότι χρησιμοποιούν ένα κοινό μέσο εκπομπής πάνω στο οποίο είναι συνδεδεμένοι όλοι οι υπολογιστές. Την απόσταση την οποία καλύπτουν αυτά τα δίκτυα

είναι έως και 10km[12].

1.1.1.3 Δίκτυα Ευρείας Περιοχής (Wide Area Networks – WAN)

Τα δίκτυα Ευρείας Περιοχής καλύπτουν μεγαλύτερες γεωγραφικά περιοχές, όπως για παράδειγμα μία χώρα ή μία ήπειρο. Αποτελούνται από τους hosts (μηχανές που τρέχουν εφαρμογές χρηστών) και από το υποδίκτυο επικοινωνίας (το δικτυακό υλικό που μεταφέρει την πληροφορία από host σε host). Την απόσταση την οποία καλύπτουν αυτά τα δίκτυα είναι από 100km έως 1000km[12].

1.1.1.4 Διαδίκτυο (Internet)

Το Διαδίκτυο είναι ένα σύνολο δικτύων που είναι συνδεδεμένα μεταξύ τους. Η απόσταση την οποία καλύπτει είναι από 10000km και πάνω[12].

1.2 Δικτυακή Κίνηση

Η δικτυακή κίνηση είναι η ανταλλαγή πληροφορίας από ένα σημείο του δικτύου σε ένα άλλο με τη μορφή πακέτων. Η πληροφορία που ανταλλάσσεται μπορεί να είναι αιτήσεις, αποκρίσεις ή δεδομένα ελέγχου. Κάθε πακέτο ξεχωριστά περιλαμβάνει την διεύθυνση του αποστολέα, τη διεύθυνση του παραλήπτη, το είδος της πληροφορίας που μεταφέρει, τον χρόνο ζωής του καθώς και έναν συγκεκριμένο σειριακό αριθμό[14].

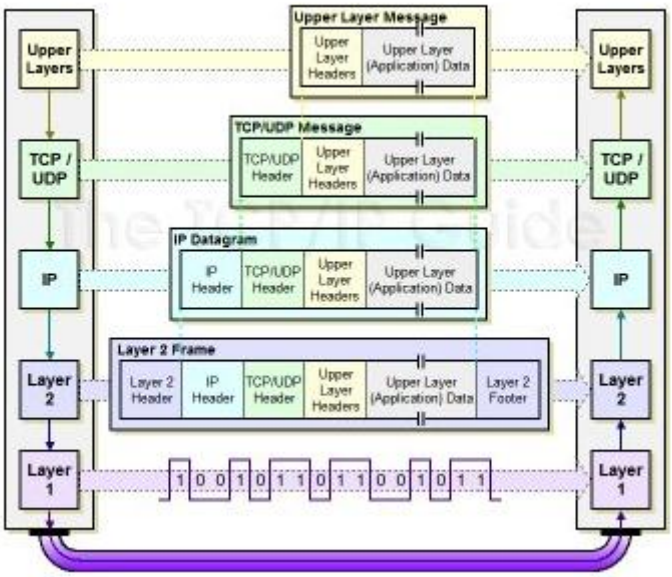
Κατά κανόνα, τα δεδομένα εμπεριέχονται σε TCP segments [1]τα οποία με τη σειρά τους, τοποθετούνται μέσα σε IP πακέτα. Κάθε TCP segment περιέχει πληροφορίες όπως: τα ports του αποστολέα και του παραλήπτη, τα sequence numbers, ένα σύνολο από flags, καθώς και το μέγεθος των δεδομένων[14].

Εξετάζοντας, τα IP πακέτα ή τα TCP segments,είναι δύσκολο να ληφθούν αποτελέσματα γιατί το σύνολο της πληροφορίας που μεταφέρεται στο Internet κατακερματίζεται σε ένα σύνολο από TCP segments (και IP πακέτα) ή και αρκετές φορές, σε UDP πακέτα[2], τα οποία περιέχουν κοινή πληροφορία και είναι αλληλένδετα μεταξύ τους. Κατά τη συλλογή των δεδομένων, στην ουσία, παρέχονται απεριόριστες δυνατότητες για την διεξαγωγή συμπερασμάτων μέσω μαθηματικών προτύπων αλλά μόνο στα πακέτα με IP πληροφορία και όχι στα επιμέρους. Ωστόσο, επειδή τα IP πακέτα και τα επιμέρους εξαρτώνται μεταξύ τους, η ανάλυση τους είναι αρκετά δύσκολη και δεν μπορεί να γίνει με μαθηματικούς τρόπους, αλλά θα πρέπει να γίνει μοντελοποίηση της κίνησης[14].

[1] Transmission Control Protocol-TCP είναι ένα από τα βασικότερα και αξιόπιστα πρωτόκολλα που χρησιμοποιείται για την μεταφορά δεδομένων στο διαδίκτυο. Τα πακέτα που μεταφέρει καλούνται ως TCP segments (τμήματα).
[2] User Datagram Protocol-UDP είναι ένα από τα βασικότερα πρωτόκολλα που χρησιμοποιείται για την ταχύτερη μεταφορά δεδομένων χωρίς εγγυημένη αξιοπιστία. Τα μηνύματα τα οποία μεταφέρει καλούνται ως datagram.

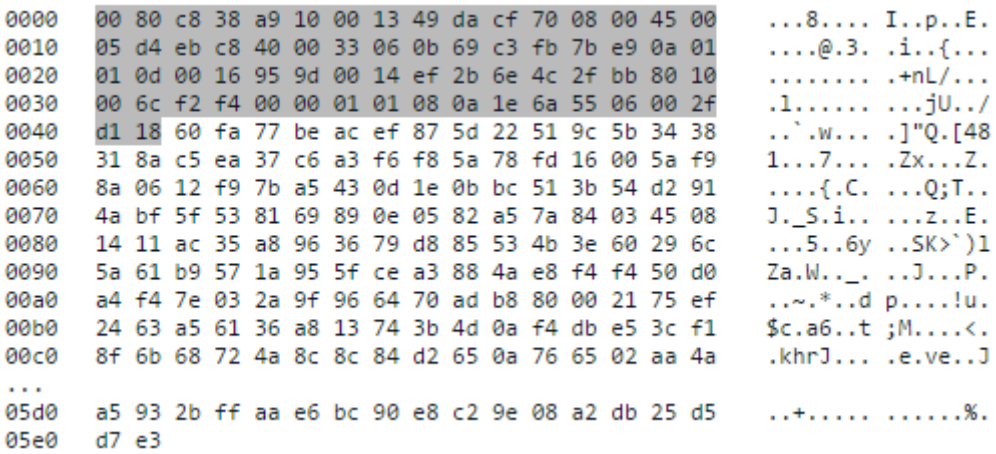
Έτσι, μελετώντας την δικτυακή κίνηση, τα συμπεράσματα που μπορούν να διεξαχθούν, αφορούν την κίνηση αυτή καθαυτή, το δίκτυο, τους χρήστες και το σύνολο της χρήσης δεδομένων. Αυτό έχει ως αποτέλεσμα, να είναι δυνατή η βελτιστοποίηση του δικτύου και των πόρων, σύμφωνα με τις ανάγκες που θα ζητηθούν. Επιπλέον, μπορεί να γίνει μοντελοποίηση της κίνησης και κατ' επέκταση, έλεγχος για θέματα νομιμότητας και ασφάλειας[14].

Ο τρόπος με τον οποίο η δικτυακή κίνηση πραγματοποιείται, είναι η διαδικασία της ενθυλάκωσης. Η διαδικασία αυτή είναι ο πιο αυστηρός τρόπος διαχωρισμού δεδομένων και μεταδεδομένων. Κατά αυτό τον τρόπο μπορεί να γίνει μια πλήρης μελέτη της δικτυακής κίνησης χωρίς να υπάρξει οποιοδήποτε πρόβλημα που να αφορά την παραβίαση του ιδιωτικού απορρήτου. Ωστόσο, το πρόβλημα το οποίο δημιουργείται είναι ότι η δικτυακή κίνηση, από τη μία, επιτρέπει την εξόρυξη μόνο των μεταδεδομένων χωρίς να δίνει την δυνατότητα παρακολούθησης των δεδομένων, και από την άλλη για τη σωστή μελέτη της, επειδή ο όγκος της πληροφορίας είναι τεράστιος, είναι απαραίτητο να υπάρχει ενημέρωση και για τα δεδομένα. Επομένως, αφού αυτό είναι πρακτικά αδύνατο, η καταγραφή και η μελέτη της δικτυακής κίνησης μέσω των δεδομένων, είναι δύσκολο να συμβεί[14].



Εικόνα 1: Διαδικασία Ενθυλάκωσης[14].

Παρακάτω εμφανίζεται ένα παράδειγμα δεδομένων ενός IP πακέτου, όπου τα πρώτα 66 bytes (το σκιαγραφημένο κομμάτι) είναι τα μεταδεδομένα. Από όλο το πακέτο αυτά έχουν όλες τις πληροφορίες που θα χρειάζεται ο χρήστης για να αναλύσει την δικτυακή κίνηση[14].



Εικόνα 2: Παράδειγμα Δεδομένων ενός IP πακέτου[14].

Οι δικτυακές συσκευές ασχολούνται κατά κύριο λόγο, μόνο με της πληροφορίες που παρέχουν τα μεταδεδομένα πακέτα. Πιο αναλυτικά, τα 66 bytes αναλύονται ως εξής:

Layer 3 Protocol :	IP
Version :	4
DiffServ Field :	0x00, No ECN
Total Length :	1492
ID :	0xebc8
Flags :	0x04 (Don't Fragment)
Fragment Offset :	0
Layer 4 Protocol :	TCP
Source IP :	195.251.123.233
Destination IP :	10.1.1.13
Source Port :	22
Destination Port :	38301
Sequence Number :	0x0014ef2b
Acknowledgment number :	0x6e4c2fbb
TCP Header Length :	32
Flags :	0x10 (ACK)
Window size :	108
Checksum :	0xf2f4

Εικόνα 3: Ανάλυση 66bytes[14].

1.2.1 Ανάλυση Δεδομένων Δικτύου

Στις μέρες μας, η τεχνολογία έχει αναπτυχθεί με ραγδαίο ρυθμό. Αυτό έχει ως αποτέλεσμα να δημιουργεί νέους τρόπους για τη συλλογή πληροφοριών και δεδομένων. Σε διάφορους τομείς ο όγκος των δεδομένων είναι τόσο μεγάλος που είναι φύσις αδύνατο να αποθηκευτεί ολόκληρος. Ακόμα και σε περιπτώσεις όπου υπάρχει δυνατότητα αποθήκευσης, ο όγκος των παραγόμενων δεδομένων είναι

αρκετά μεγάλος. Αυτό έχει ως αποτέλεσμα να είναι δύσκολη η επεξεργασία και η ανάλυση των δεδομένων.

Υπάρχουν δύο ειδών δεδομένα. Τα δεδομένα συνεχούς ροής και τα αποθηκευμένα δεδομένα. Στο μοντέλο συνεχούς ροής (Data Stream Model) σχεδόν όλα τα εισερχόμενα δεδομένα δεν είναι διαθέσιμα για προσπέλαση από κάποιο αποθηκευτικό μέσο, είτε μόνιμο, είτε προσωρινό, αλλά, καταφθάνουν ως συνεχόμενες ροές[14].

Τα δύο αυτά είδη δεδομένων διαφέρουν σε κάποια σημεία. Τα δεδομένα στη συνεχή ροή καταφθάνουν με on line τρόπο. Τα δεδομένα τα οποία εισέρχονται για επεξεργασία, δεν περνούν κάποιον έλεγχο όσον αφορά τη σειρά με την οποία θα εισέλθουν. Επιπλέον, τα δεδομένα ροής μπορεί να είναι υπερβολικά μεγάλα σε μέγεθος σε σχέση με τα υπόλοιπα δεδομένα. Τέλος, από τη στιγμή που κάποια δεδομένα ροής δεχθούν επεξεργασία, είτε καταστρέφονται είτε αρχειοθετούνται και είναι πολύ δύσκολο να ανακτηθούν στην μνήμη πάλι, γιατί η μνήμη, τυπικά, είναι πολύ μικρή[14].

1.3 Έλεγχος Ετοιμότητας Υποστήριξης Κίνησης (Δυναμικότητα Δικτύου)

Σκοπός του δικτύου είναι να μπορεί να υποστηρίξει εισερχόμενες εφαρμογές TCP,UDP και VoIP, καθώς και νέους χρήστες. Στην ουσία, η δυναμικότητά του, παίζει σημαντικό ρόλο στην υλοποίηση των μηχανισμών QoS (Quality Of Service).

Ο έλεγχος της δυναμικότητας του δικτύου γίνεται με την καταγραφή των επιπέδων κίνησης σε επίπεδο εφαρμογής, με τον έλεγχο της συμπεριφοράς των εφαρμογών και την προσομοίωση κίνησης εφαρμογών TCP, UDP, VoIP μεταξύ επιλεγμένων σημείων, με σκοπό να δοθούν αναφορές σχετικά με τις παραμέτρους ποιότητας του δικτύου (χρόνος απόκρισης, ρυθμοαπόδοση (throughput), διαθεσιμότητα, one way delay, packet loss,mean opinion score(για VoIP κίνηση)).

Τα αποτελέσματα που θα ληφθούν δίνουν συμπεράσματα σχετικά με τα όρια αντοχής του δικτύου, την κίνηση που μπορεί να υποστηρίξει, την συμπεριφορά της νέας εφαρμογής που θα εισέλθει, τις επιπτώσεις που μπορεί να έχει η νέα εφαρμογή σε σχέση με τις ήδη υπάρχουσες, την απόδοση του δικτυακού εξοπλισμού (Switches,Routers, Firewalls) καθώς και τη σωστή εφαρμογή πολιτικών QoS. Τα αποτελέσματα αυτά βοηθούν στην υλοποίηση αναβαθμίσεων και επεκτάσεων του δικτύου.

1.3.1 Παράγοντες Δικτυακής Κίνησης

Για τη σωστή ανάλυση και διαχείριση της δικτυακής κίνησης, είναι σημαντικό να είναι γνωστά ο συνολικός χρόνος παράδοσης ή χρόνος απόκρισης του πακέτου (response time), η ταχύτητα μετάδοσης των δεδομένων (transmission speed), καθώς και ο χρόνος μετάδοσης ενός μηνύματος μέχρι το τέλος της μετάδοσής του (transmission time).

Όταν γίνεται αγνόηση του χρόνου μετάδοσης (transmission time), ο χρόνος απόκρισης (response time) είναι το άθροισμα του χρόνου υπηρεσίας (service time) και του χρόνου αναμονής (wait time). Ο χρόνος υπηρεσίας είναι ο χρόνος που χρειάζεται για να ολοκληρωθεί μία εργασία, ενώ ο χρόνος αναμονής είναι το διάστημα που περιμένει ένα μήνυμα στην ουρά πριν εξυπηρετηθεί.

Γενικότερα, ο χρόνος απόκρισης (response time) βασίζεται στην ταχύτητα μετάδοσης (transmission speed). Στην αποστολή ενός πακέτου, το response time μπορεί να είναι σχετικά αργό, παρ' όλο που το transmission time μπορεί να είναι γρήγορο. Αυτό συμβαίνει γιατί το αίτημα μπαίνει στην ουρά και αναμένει για την παράδοση και εξυπηρέτησή του.

Ωστόσο, για τη σωστή ανάλυση της δικτυακής κίνησης, δεν παίζουν ρόλο μόνο η ταχύτητα και ο χρόνος, αλλά θα πρέπει να ληφθούν υπ' όψιν και κάποιοι άλλοι παράγοντες που επηρεάζουν την κίνηση του δικτύου.

1.4 Ανίχνευση – Μέτρηση Δικτυακής Κίνησης

Για την ανίχνευση και την μέτρηση της δικτυακής κίνησης, υπάρχουν τρεις τρόποι τους οποίος ο χρήστης θα πρέπει να λάβει υπ' όψη. Κάθε τρόπος παρέχει και διαφορετικές πληροφορίες.

1.4.1 Server Logs

Οι Server Logs είναι αρχεία τα οποία δημιουργούνται αυτόματα μέσα στον Server και παρέχουν έναν κατάλογο με τις ενέργειες τις οποίες έχει εκτελέσει. Οι πληροφορίες τις οποίες παρέχει, αφορούν κυρίως χαρακτηριστικά των αιτημάτων που έχουν σταλθεί (ημερομηνία, ώρα, IP διεύθυνση κ.τ.λ.) κατά την διάρκεια που εκτελεί μία ενέργεια ο Server. Ωστόσο, τα στοιχεία αυτά δεν είναι προσιτά σε όλους τους χρήστες. Οι ιδρυτές της κάθε σελίδας μπορούν να τα δουν αλλά δεν μπορούν να τα επεξεργαστούν. Γενικότερα, οι Server Logs χρησιμοποιούνται για τη λήψη στατιστικών που αφορούν τους πόρους που χρησιμοποιούνται ώστε να μπορέσουν να αναλυθούν τα αρχεία καταγραφής του Server.

1.4.2 Passive Measurement

Οι παθητικές μετρήσεις (Passive Measurement) αναφέρονται στις μετρήσεις του δικτύου χωρίς να έχει ξεκινήσει ή να έχει τροποποιηθεί η κίνηση του. Οι πληροφορίες τις οποίες παρέχουν, αναφέρονται κυρίως στα πρωτόκολλα που χρησιμοποιούνται για την δικτυακή κίνηση, των ακριβή αριθμό των bit και των πακέτων που διανέμονται, καθώς και τον χρόνο άφιξης των πακέτων. Επιπλέον, οι παθητικές μετρήσεις, παρέχουν τον εντοπισμό των σφαλμάτων που συμβαίνουν μέσα στο δίκτυο[19].

1.4.3 Active Measurement

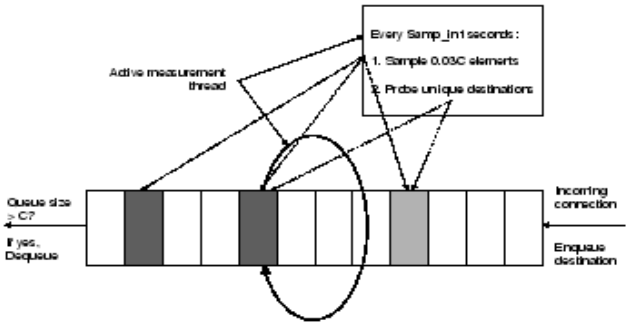
Οι ενεργές Μετρήσεις είναι παρόμοιες με τις παθητικές. Διαθέτουν έναν πίνακα κατακερματισμού της απόδοσης και υπολογίζουν τους υποψήφιους προορισμούς. Για να είναι τα αποτελέσματά τους πιο έγκυρα, χρησιμοποιούν δύο τεχνικές:

- **Frequency Counts**

Είναι ακριβώς ίδιος με τον παθητικό τρόπο, όπου μετριούνται ο αριθμός των αιτημάτων του πελάτη που κατευθύνονται προς τον τελικό προορισμό. Κάθε δευτερόλεπτο, οι ενεργοί μετρητές, ελέγχουν τους προορισμούς στους οποίους ο αριθμός των αιτημάτων υπερβαίνουν ένα συγκεκριμένο όριο[20].

- **Sliding Window**

Αυτό το σύστημα, περιέχει ένα παράθυρο C, το οποίο περιέχει τους πιο πρόσφατους προορισμούς στους οποίους υπήρχε πρόσβαση. Το παράθυρο λειτουργεί με την μέθοδο FIFO(First In First Out) όπου εισάγονται οι πιο πρόσφατοι προορισμοί στους οποίους έχουν γίνει οι συνδέσεις. Όταν ο αριθμός των στοιχείων υπερβεί το όριο, τότε το παράθυρο αφαιρείται. Κάθε δευτερόλεπτο, γίνονται μετρήσεις και επιλέγονται τυχαία τα στοιχεία. Οι διπλοί προορισμοί απορρίπτονται με αποτέλεσμα οι ενεργές μετρήσεις να μετρούν την απόδοση στους υπόλοιπους προορισμούς που παρέχονται[20].



Εικόνα 4: Έλεγχος απόδοσης[20].

1.4.4 Active Measurements vs Passive Measurements

Υπάρχουν διάφοροι τρόποι για την προσέγγιση της δικτυακής κίνησης. Οι πιο κοινοί είναι οι παθητικές και οι ενεργητικές μετρήσεις, τις οποίες για να μπορέσει να επέλθει ένα καλύτερο αποτέλεσμα, θα ήταν καλό να συνδυάζονται μεταξύ τους γιατί η μία συμπληρώνει την άλλη. Οι παθητικές μετρήσεις, κάνουν προεπισκόπηση της κίνησης του δικτύου ενώ οι ενεργητικές κάνουν καταμέτρηση των υπηρεσιών που εκτελούνται στο δίκτυο. Ένα πλεονέκτημα της παθητικής

προσέγγισης, είναι ότι δεν αυξάνει την κυκλοφορία του δικτύου για να μπορέσει να λάβει τις μετρήσεις, σε αντίθεση με την ενεργητική, η οποία στέλνει πακέτα για να μπορέσει να καταγράφει την κυκλοφορία. Ωστόσο, επειδή οι παθητικές μετρήσεις απαιτούν την προβολή όλων των πακέτων του δικτύου για να καταφέρουν να εξαλείψουν βλάβες και πιθανά λάθη, υπάρχει περίπτωση τα δεδομένα να μην μπορούν να ληφθούν γιατί τα προσωπικά δεδομένα προστατεύονται. Από την άλλη, οι ενεργειακές προσεγγίσεις κάνουν έλεγχο σε οτιδήποτε χρειάζεται και κυρίως στην ποιότητα των υπηρεσιών (QoS- Quality of Service) ή σε Συμφωνίες Επιπέδου Υπηρεσιών (SLA- Service Level Agreements) , κάτι που τις καθιστά πιο απλές και χρήσιμες[21].

Όπως προαναφέρθηκε, και οι δύο προσεγγίσεις συσχετίζονται. Αυτό σημαίνει ότι για να λειτουργήσει σωστά η μία χρειάζεται τις μετρήσεις της άλλης. Όταν η ενεργητικές μετρήσεις ολοκληρωθούν, τότε οι παθητικές συλλέγουν τις πληροφορίες και τις επεξεργάζονται. Με αυτόν τον τρόπο γίνεται επαλήθευση των δεδομένων και οι πιθανότητες λαθών μειώνονται[21].

1.5 Μετρητές Απόδοσης

Τα τελευταία χρόνια, η πλειοψηφία των χρηστών, χρησιμοποιεί την τεχνολογία των ασύρματων δικτύων, WiFi. Η αύξηση αυτή των χρηστών, έχει ως αποτέλεσμα τη μείωση της διαθεσιμότητας του εύρους ζώνης των δικτύων. Έτσι, κάθε φορά που κάποιος χρήστης θέλει να συνδεθεί σε ένα ασύρματο δίκτυο, αναρωτιέται πόσο καλή είναι η απόδοση του δικτύου, πως γίνεται να μειωθεί η συμφόρηση του δικτύου και πόσο εγγυημένη είναι η ποιότητα των υπηρεσιών (QoS-Quality of Services). Τις απαντήσεις αυτές, τις δίνουν οι μετρητές απόδοσης, οι οποίοι βοηθούν στο να διαχειριστεί και να βελτιωθεί η δικτυακή κίνηση[16].

1.5.1 Packet Loss

Το Packet Loss είναι η απώλεια των πακέτων που συμβαίνει όταν ένα ή περισσότερα πακέτα δεδομένων ταξιδεύουν σε ένα δίκτυο και αποτυγχάνουν να φτάσουν στον προορισμό τους. Η απώλεια πακέτων προκαλείται κυρίως από συμφόρηση του δικτύου. Το πρωτόκολλο το οποίο είναι υπεύθυνο για την ανίχνευση των πακέτων και για την αποφυγή της συμφόρησης του δικτύου, είναι το Transmission Control Protocol (TCP).

Όπως θα δούμε και παρακάτω, αρκετές φορές η απώλεια των πακέτων δεν είναι προφανής. Όταν συμβαίνει σε επίπεδο πελάτη με διακομιστή, κανένα πρόγραμμα δεν μπορεί να υπολογίσει την απώλεια των πακέτων. Το TCP όμως, καταλαβαίνει ότι κάτι δεν είναι σωστό, και κάθε φορά που το πακέτο δεν φτάνει ή φτάνει σε λάθος στιγμή, κάνει αναμετάδοση (retransmission) ή στέλνει Duplicate ACKs όσες φορές χρειαστεί. Ακόμα και αυτό είναι ένα είδος απώλειας πακέτων.

Γενικότερα, η απώλεια των πακέτων σε ένα δίκτυο θα πρέπει να είναι μικρότερη του 10%, διαφορετικά δεν υπάρχει διαδοχική σειρά στην αποστολή των πακέτων.

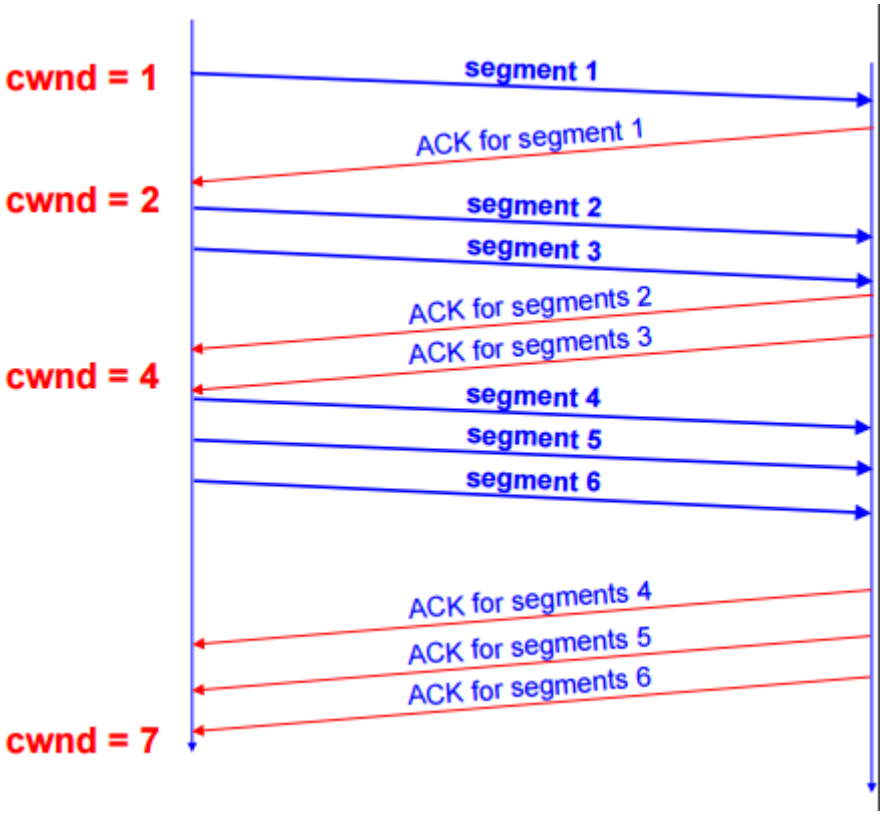
Αρκετές φορές τα πακέτα φτάνουν με διαφορετική σειρά από ότι έχουν σταλθεί. Αυτό συμβαίνει γιατί ένα δίκτυο έχει πολλαπλές διαδρομές ή ο εξοπλισμός του δεν είναι αρκετά καλός με αποτέλεσμα να προκαλεί καθυστερήσεις. Τα πακέτα τα οποία δεν φτάνουν στον προορισμό τους με την αρχική σειρά που έχουν σταλθεί, ονομάζονται out- of-order πακέτα. Το TCP για να αντιμετωπίσει αυτό το πρόβλημα, ελέγχει τα προβληματικά πακέτα και τους κάνει Fast Retransmit (γρήγορη επαναμετάδοση). Η λειτουργία αυτή μειώνει τον χρόνο αναμονής του αποστολέα πριν την αναμετάδοση του λανθασμένου πακέτου.

1.5.1.1 Λειτουργία Fast Retransmit

Ένας αποστολέας TCP χρησιμοποιεί ένα χρονόμετρο για να αναγνωρίζει τα χαμένα τμήματα των πακέτων. Αν η επιβεβαίωση παράδοσης τους δεν έχει ληφθεί στο συγκεκριμένο χρονικό όριο, ο αποστολέας θα λάβει το τμήμα το οποίο χάθηκε και θα το επαναμεταδώσει ξανά.

Η διπλή αναγνώριση των πακέτων, είναι η βάση του μηχανισμού γρήγορης αναμετάδοσης, ο οποίος λειτουργεί ως εξής: μόλις λάβει ένα πακέτο με π.χ. αύξοντα αριθμό 1, ο δέκτης στέλνει μία επιβεβαίωση προσθέτοντας 1 στον αριθμό ακολουθίας, δηλαδή ο αριθμός αναγνώρισης θα είναι 1. Αυτό σημαίνει ότι ο δέκτης λαμβάνει τον αριθμό 1 για το πακέτο και αναμένει από τον αποστολέα τον αριθμό πακέτων 2. Αν υποθέσουμε ότι τα επόμενα τρία πακέτα έχουν χαθεί, τότε ο δέκτης λαμβάνει τους αριθμούς 5 και 6 για τα πακέτα. Μετά την λήψη του πακέτου 5, ο δέκτης στέλνει μία επιβεβαίωση αλλά με αύξοντα αριθμό ίσον με 2. Όταν θα λάβει το πακέτο με αριθμό 6, θα στείλει πάλι μία επιβεβαίωση με αύξοντα αριθμό το 2. Επειδή ο αποστολέας λαμβάνει περισσότερες από μία αναγνωρίσεις με τον ίδιο αριθμό, αυτή η διαδικασία ονομάζεται διπλή αναγνώριση.

Ο μηχανισμός της γρήγορης αναμετάδοσης, στέλνει τα πακέτα που θεωρεί ότι χάθηκαν, χωρίς να περιμένει να λάβει κάποια επιβεβαίωση. Δηλαδή, αν ο αποστολέας TCP λάβει έναν συγκεκριμένο αριθμό από πακέτα, όπου αν λάβει τρεις διπλές επιβεβαιώσεις με τον ίδιο αριθμό, καταλαβαίνει ότι οι φορές που έχουν σταλθεί τα πακέτα είναι συνολικά τέσσερις, ο αποστολέας μπορεί να υποθέσει με βεβαιότητα ότι τα πακέτα χάθηκαν ή τέθηκαν εκτός λειτουργίας. Γι αυτό τον λόγο θα κάνει γρήγορη αναμετάδοση των πακέτων, χωρίς να περιμένει να ξεπεράσουν το χρονικό όριο ή να λάβει κάποια ενημέρωση.



Σχήμα 1: Διπλή αναγνώριση Πακέτων

1.5.2 Delay

Το Delay είναι ένα σημαντικό χαρακτηριστικό για την απόδοση του δικτύου, που καθορίζει τον χρόνο που χρειάζονται τα δεδομένα για να ταξιδέψουν στο δίκτυο. Μετριέται σε bit/sec. Ωστόσο, το Delay διαιρείται σε κάποιες υποκατηγορίες καθυστέρησης, οι οποίες πρέπει να ληφθούν υπ' όψιν για τη σωστή καταμέτρηση της καθυστέρησης.

1.5.2.1 Καθυστέρηση Επεξεργασίας (Processing Delay)

Είναι ο χρόνος που απαιτείται σε κάθε κόμβο του δικτύου για την ανάγνωση των πληροφοριών, την εκτέλεση των πρωτοκόλλων και την προετοιμασία των νέων πεδίων για την απόκριση[17].

1.5.2.2 Χρόνος Αναμονής (Queuing Delay)

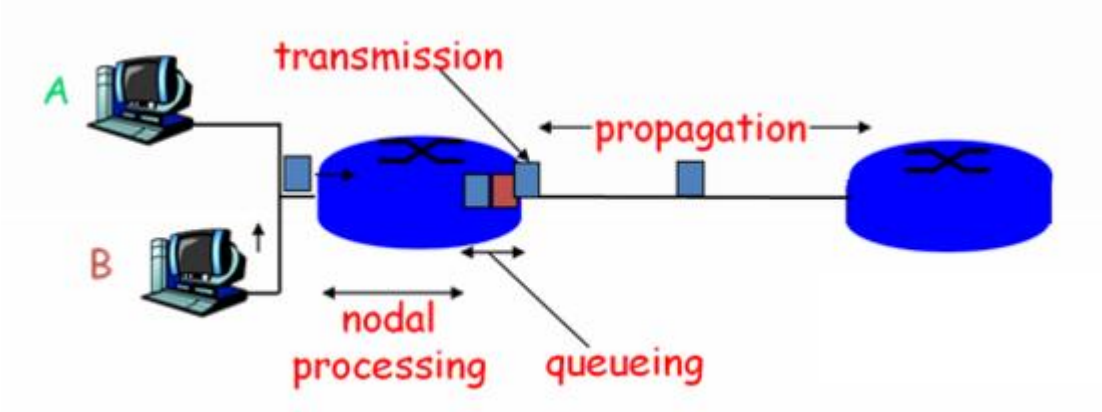
Είναι ο χρόνος που το πακέτο βρίσκεται στην ουρά περιμένοντας την μετάδοσή του στην επόμενη ζεύξη προς τον προορισμό του. Ο χρόνος αυτός είναι πολύ μικρός στα δίκτυα μεταγωγής πακέτων, αλλά στα δίκτυα πακέτων μπορεί να πάρει μεγάλες τιμές και να είναι η κύρια καθυστέρηση της μετάδοσης των πακέτων[17].

1.5.2.3 Χρόνος Μετάδοσης (Transmission Delay)

Είναι ο χρόνος που απαιτείται για να διαμορφωθεί ανάλογα ο πομπός όσες φορές χρειάζεται προκειμένου να μπορέσει να λάβει την πληροφορία που στέλνεται μέσω του δικτύου[17].

1.5.2.4 Καθυστέρηση Διάδοσης (Propagation Delay)

Είναι ο χρόνος που χρειάζεται για να ταξιδέψει το ηλεκτρομαγνητικό κύμα στο μέσο διάδοσης (οπτικό ή αέρα ή χαλκό) και είναι περίπου 5ns/m. Είναι μία σταθερά η οποία λαμβάνεται πάντα υπ' όψιν γιατί δεν υπάρχουν τεχνικά μέσα να την επηρεάσουν όπως συμβαίνει με άλλες συνιστώσες καθυστέρησης. Σε οποιοδήποτε μέσο διάδοσης και να μετρηθεί, η τιμή της δεν φέρει μεγάλες αλλαγές[17].



Σχήμα 2: Καθυστερήσεις Πακέτων

1.5.3 Throughput

Είναι ο αριθμός των μηνυμάτων που μεταδίδονται με επιτυχία ανά μονάδα χρόνου. Εξαρτάται από το διαθέσιμο εύρος ζώνης (bandwidth), από το υλικό και από τον θόρυβο που υπάρχει στο σήμα.

1.5.4 Availability

Είναι η ικανότητα ενός χρήστη να έχει πρόσβαση σε πόρους και πληροφορίες σε μια καθορισμένη θέση και με τη σωστή μορφή της πληροφορίας. Όταν δεν υπάρχει διαθεσιμότητα πληροφοριών ή τα δεδομένα δεν είναι ασφαλή, τότε επηρεάζεται η ασφάλεια των πληροφοριών καθώς και οι χρήστες. Επιπλέον, όταν σε ένα σύστημα πληροφοριών δεν παρέχονται πληροφορίες αποτελεσματικά, τότε η διαθεσιμότητα είναι σε κίνδυνο. Η διαθεσιμότητα των δεδομένων εξασφαλίζεται με την αποθήκευση, η οποία μπορεί να είναι είτε τοπική είτε σε κάποια άλλη εξωτερική εγκατάσταση[18].

1.6 Συμφόρηση Δικτύου

Ένα από τα πιο συχνά προβλήματα που αντιμετωπίζει ένα δίκτυο είναι η συμφόρηση. Κατά την συμφόρηση, ένα δίκτυο προσπαθεί να μεταφέρει περισσότερα πακέτα πληροφορίας απ' ότι είναι η δυνατότητά και η χωρητικότητά του[12].

Οι λόγοι για τους οποίους δημιουργείτε η συμφόρηση είναι κυρίως από πολλούς κινητούς κόμβους ή από μεγάλους πίνακες δρομολόγησης είτε από αυξημένο αριθμό μηνυμάτων ελέγχου. Σε περίπτωση συμφόρησης, το επίπεδο δικτύου των δρομολογητών, έχει την ικανότητα να τερματίσει τη ροή των πληροφοριών στο δίκτυο και έτσι είναι ικανό να κάνει διαχείριση της συμφόρησης[12].

Κατά κύριο λόγο, η διαχείριση της συμφόρησης μπορεί να αντιμετωπιστεί είτε με το να υπάρξει περιορισμός στην ποσότητα των πληροφοριών, οι οποίες εισάγονται και με αυτόν τον τρόπο ώστε να αποφεύγεται η συμφόρηση, είτε με το να διαγράφεται το επιπλέον φορτίο που περισσεύει και έτσι να ελέγχεται η συμφόρηση στο δίκτυο. Όσο πιο γρήγορα διαγράφεται το φορτίο που περισσεύει, τόσο πιο γρήγορα επανέρχεται το δίκτυο σε κανονικές συνθήκες λειτουργίας[12].

ΕΝΟΤΗΤΑ 2

VOICE OVER INTERNET PROTOCOL-VOIP

Η κίνηση μέσα στο δίκτυο, όπως προείπαμε, είναι η ανταλλαγή πληροφορίας με τη μορφή πακέτων. Τα πακέτα αυτά περιλαμβάνουν αιτήσεις, αποκρίσεις και δεδομένα ελέγχου. Τα στοιχεία των πακέτων μπορεί να προέρχονται από σύνδεση με κάποια web(html) σελίδα ή με κάποια σύνδεση VoIP εφαρμογής. Κάθε φορά που κάποιος χρήστης κάνει εισαγωγή σε ένα web site ή ξεκινά μία VoIP κλήση, στέλνονται αιτήσεις και αποκρίσεις κατά την μεταφορά των πακέτων. Την ίδια στιγμή γίνεται και έλεγχος δεδομένων μέσω του πρωτοκόλλου TCP/IP. Στην εργασία αυτή, εξετάζεται η περίπτωση των VoIP υπηρεσιών ώστε να παραχθεί καλύτερη απόδοση στην ποιότητα των υπηρεσιών.

2.1 Voice over IP (VoIP)

Το Voice over IP ή VoIP, είναι η τηλεφωνία μέσω διαδικτύου. Χαρακτηρίζεται αλλιώς και ως φωνή επί διαδικτυακού πρωτοκόλλου. Έχει τη δυνατότητα να προσφέρει φωνητική συνομιλία σε πραγματικό χρόνο με καλή ποιότητα φωνής και χωρίς κόστος. Οι συνομιλίες γίνονται μέσω ηλεκτρονικών υπολογιστών οι οποίοι είναι συνδεδεμένοι στο διαδίκτυο και διαθέτουν κατάλληλο εξοπλισμό (ακουστικά, μικρόφωνο). Στη συγκεκριμένη επικοινωνία δεν υπάρχει κάποια εταιρεία τηλεφωνίας (π.χ ΟΤΕ) που να μεσολαβεί και γι' αυτόν τον λόγο δεν υπάρχουν επιπλέον χρεώσεις. Επιπλέον, οι VoIP κλήσεις χρησιμοποιούν ένα πρότυπο για τα τηλεφωνικά κέντρα, το οποίο είναι το

SIP(Session Initiate Protocol), όπου όσα τηλεφωνικά κέντρα επικοινωνούν μεταξύ τους, δεν έχουν, επίσης, χρεώσεις.

Τα τελευταία χρόνια έχει παρατηρηθεί ότι γίνεται προώθηση κλήσεων VoIP και σε σταθερά δίκτυα τηλεπικοινωνιών με χαμηλό κόστος μέσω εναλλακτικών τηλεπικοινωνιακών φορέων. Επιπλέον, γίνεται προώθηση των κλήσεων από δίκτυα σταθερής ή κινητής τηλεφωνίας σε δίκτυα VoIP με πραγματικό αριθμό σταθερού ή κινητού τηλεφώνου. Έτσι, ο χρήστης κάνει εγκατάσταση ενός ειδικού λογισμικού VoIP στο κινητό του, στο Laptop του ή στο tablet του και ενώ ταξιδεύει σε όλον τον κόσμο, μπορεί να δέχεται διεθνής κλήσεις.

Ωστόσο, υπάρχουν κάποιες ειδικές τηλεφωνικές συσκευές USB VoIP, οι οποίες συνδέονται με ένα αντίστοιχο ανοιχτό λογισμικό, το οποίο είναι εγκατεστημένο στον ηλεκτρονικό υπολογιστή, και κάνουν τις δικτυακές κλήσεις πιο λειτουργικές. Παραδείγματα τέτοιων συσκευών είναι το δικτυακό τηλέφωνο Taichi, το Cyberphonek, η υπηρεσία FWD, το e-voice της HOL ή το Voice@net του OTEnet. Σε τέτοιες περιπτώσεις, ο χρήστης αγοράζει όσο χρόνο ομιλίας χρειάζεται μέσω πιστωτικής κάρτας και τον χρησιμοποιεί κατάλληλα.

Κατά την πάροδο του 2009, εμφανίστηκαν οι πρώτες ελληνικές εταιρίες που παρέχουν ελληνικά νούμερα για χρήση VoIP υπηρεσίες οι οποίες ναι μεν δέχονται εισερχόμενες κλήσεις, αλλά δέχονται και εξερχόμενες από όλους τους τηλεπικοινωνιακούς παρόχους. Παραδείγματα τέτοιων εταιριών είναι η Viva Services, η Yuboto, η Omnivoice, η Inter Telecom, η Modulus και η Future Solution.

2.1.1 Εφαρμογή VoIP Κλήσεων

Στην περίπτωση των VoIP κλήσεων, οι κλήσεις γίνονται μόνο από Η/Υ σε Η/Υ, όπου κάποιος υπολογιστής παίζει τον ρόλο του εξυπηρετητή (server) και οι υπόλοιποι υπολογιστές είναι οι πελάτες (client). Αυτές οι κλήσεις δεν περνάνε από τον Server κάποιου επίσημου φορέα αλλά από τον τοπικό Server. Γι' αυτόν τον λόγο, οι κλήσεις είναι δωρεάν και περιορίζονται στο τοπικό δίκτυο, δηλαδή, μεταξύ των ηλεκτρονικών υπολογιστών που συνδέονται στον Server. Επιπλέον, οι VoIP κλήσεις χρησιμοποιούνται από εταιρίες call center αλλά και από εταιρίες και ιδιώτες που βρίσκονται σε διαφορετικό γεωγραφικό μέρος, είτε στην Ελλάδα είτε στο εξωτερικό. Αυτό συμβαίνει επειδή το κόστος των χρεώσεων των VoIP κλήσεων είναι πολύ χαμηλό.

2.1.2 Λειτουργία VoIP

Το VoIP(Voice over IP) είναι μια τεχνολογία η οποία χρησιμοποιεί κατά κύριο λόγο το πρωτόκολλο IP, το οποίο αποτελείται από ένα σύνολο κανόνων οι οποίοι καθορίζουν τον τρόπο με τον οποίο τα πακέτα μεταδίδονται στο Διαδίκτυο. Στην ουσία, τυποποιεί την διαδικασία με την οποία τα πακέτα δρομολογούνται μέσω διαδικτύου ή σε οποιοδήποτε άλλο δίκτυο IP με βάση τις διευθύνεις IP. Το VoIP, εν τέλει, αξιοποιεί τις δυνατότητες που του προσφέρει το πρωτόκολλο IP για τη μετάδοση των πακέτων δεδομένων φωνής[8].

Το πρωτόκολλο IP όμως, έχει ένα μεγάλο μειονέκτημα. Αν και, καθορίζει τον τρόπο με τον οποίο θα μεταδοθούν τα πακέτα, δυστυχώς, δεν εγγυάται τη βέβαιη παράδοση τους. Έτσι, τον ρόλο αυτό τον αναλαμβάνει το πρωτόκολλο TCP(Transmission Control Protocol). Το πρωτόκολλο αυτό, εγγυάται αξιοπιστία σε μία μετάδοση πακέτων, όπου εξασφαλίζει ότι δεν υπάρχει καμία απώλεια πακέτων, τα πακέτα μεταδίδονται με τη σωστή σειρά, ότι μπορεί ναι μεν κάποιες φορές να υπάρχουν καθυστερήσεις αλλά ποτέ δεν ξεπερνούν το προκαθορισμένο όριο και επίσης, έχει την δυνατότητα να εξασφαλίζει ότι δεν υπάρχει επικάλυψη των πακέτων. Ο Στόχος του συγκεκριμένου πρωτοκόλλου είναι να διασφαλίζει ότι όλα τα δεδομένα έχουν ληφθεί με τη σωστή σειρά που στάλθηκαν έτσι ώστε να μην υπάρχουν προβλήματα και η φωνή να ακούγεται συνεχής και όχι διακεκομμένη[8].

Η λειτουργία των δύο πρωτοκόλλων (IP,TCP) συνδυάζεται. Το TCP λειτουργεί πάντα πριν το IP και δεσμεύει δεδομένα σε πακέτα TCP πριν τα στείλει στο IP, το οποίο στη συνέχεια τα λαμβάνει και τα συμπιέζει σε πακέτα IP. Ένα πακέτο IP είναι ένα πακέτο δεδομένων το οποίο αποτελείται από ένα φορτίο δεδομένων και μία κεφαλίδα IP(IP Header). Τα δεδομένα αυτά διαχωρίζονται σε bits, τοποθετούνται σε αυτά τα πακέτα και μεταδίδονται στο δίκτυο. Όταν τα πακέτα ολοκληρώσουν τη διαδρομή τους και φτάσουν στον προορισμό τους, τότε ανακατασκευάζονται στα αρχικά δεδομένα[8].

Στις μέρες μας, το πρωτόκολλο TCP/IP είναι ιδιαίτερα διαδεδομένο κυρίως σε εφαρμογές που έχουν ως στόχο τη μετάδοση της φωνητικής πληροφορίας. Αυτό συμβαίνει λόγω της βελτίωσης της ταχύτητας των συνδέσεων οι οποίες επιτρέπουν την πιο γρήγορη μετάδοση δεδομένων μεταξύ των δικτύων, το οποίο συμβάλλει στην βελτίωση της ποιότητας του ήχου που μεταδίδεται σε πραγματικό χρόνο. Μετά από έρευνες, έχει ανακαλυφθεί και αξίζει να σημειωθεί, πως η ανθρώπινη φωνή μπορεί να συμπιεστεί σε τέτοιο βαθμό, με αποτέλεσμα να παραμείνει αναλλοίωτη η ποιότητα και η χροιά της[8].

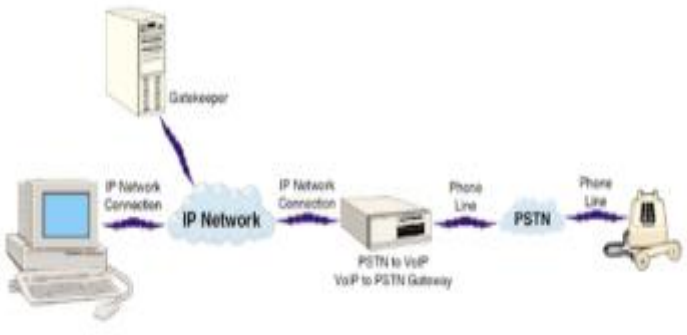
Έτσι, για να μπορέσει να πραγματοποιηθεί μια τηλεφωνική κλήση μέσω του δικτύου VoIP, θα πρέπει αν εκτελεσθούν κάποιες βασικές λειτουργίες. Οι κύριες είναι οι εξής:

1. Σηματοδοσία

Είναι η λειτουργία που παίζει τον βασικότερο ρόλο στα VoIP συστήματα. Η λειτουργία αυτή εκτελείται από έναν ειδικό μηχανισμό που λέγεται Gatekeeper, ο οποίος, ενεργοποιεί, διαχειρίζεται και συντονίζει όλο το δίκτυο που συμμετέχει σε μια τηλεφωνική συνομιλία.

2. Αριθμοδότηση

Πάντα, για να πραγματοποιηθεί μία κλήση, η πρώτη κίνηση που γίνεται είναι η πληκτρολόγηση ενός τηλεφωνικού αριθμού. Υπάρχουν δύο είδη δικτύων, τα PSTN και τα IP. Στα PSTN δίκτυα, υπάρχουν τηλεφωνικά νούμερα, ενώ στα IP δίκτυα υπάρχουν διευθύνσεις IP (IP address). Και τα δύο συνεργάζονται μεταξύ τους μέσω της μετάφρασης διευθύνσεων (address translation). Στις VoIP κλήσεις, κάθε αριθμός αντιστοιχίζεται με μία διεύθυνση IP. Όταν μία συσκευή πραγματοποιεί μια κλήση VoIP, η IP διεύθυνσή του μεταφράζεται σε αριθμό τηλεφώνου και μεταβιβάζεται στο δίκτυο PSTN. Ο μηχανισμός που χρησιμοποιείται για να συνδεθεί ένα IP δίκτυο με ένα τηλεφωνικό, ονομάζεται Gateway.



Σχήμα 3: Αντιστοίχιση τηλεφωνικού αριθμού PSTN σε IP διεύθυνση[8].

3. Διαχείριση Δρομολόγησης Κλήσεων

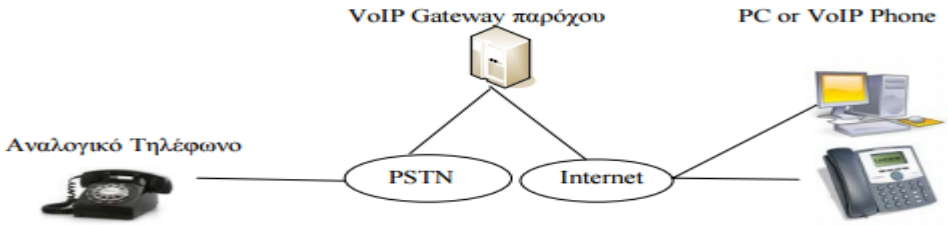
Ως δρομολόγηση κλήσης καλείται η διαδρομή μέσα στο δίκτυο για να αρχίσει, ν υλοποιηθεί και να τερματίσει μία τηλεφωνική συνομιλία. Σύμφωνα με τους κανόνες δρομολόγησης του Internet, τα πακέτα φωνής φτάνουν στον προορισμό τους ακολουθώντας πολλές εναλλακτικές διαδρομές. Μόλις οι χρήστες ξεκινήσουν να συνομιλούν, στο δίκτυο δεσμεύονται πόροι οι οποίοι μετά τον τερματισμό της κλήσης αποδεσμεύονται και είναι διαθέσιμοι για τους υπόλοιπους χρήστες του δικτύου που επιδιώκουν να συνομιλήσουν. Στις περιπτώσεις αυτές χρησιμοποιούνται τα πρωτόκολλα SIP,H.323,το IAX2 και το MGCP. Η δρομολόγηση μιας κλήσης μπορεί να γίνει με τρεις τρόπους:

-από χρήστη VoIP σε χρήστη VoIP (IP-IP)

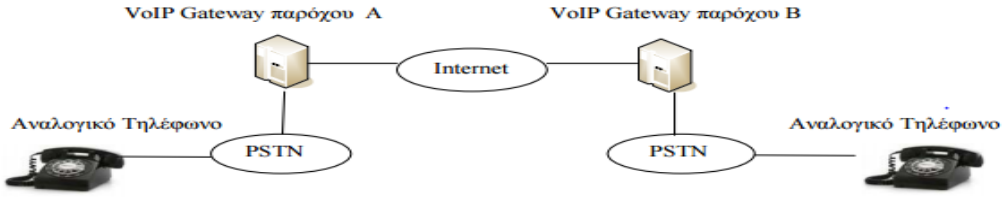
-από τηλέφωνο σε χρήστη VoIP (PSTN-IP)

-από τηλέφωνο σε τηλέφωνο (PSTN-PSTN)

Σχήμα 4: Από χρήστη VoIP σε χρήστη VoIP[8].



Σχήμα 5: Από τηλέφωνο σε χρήστη VoIP[8].

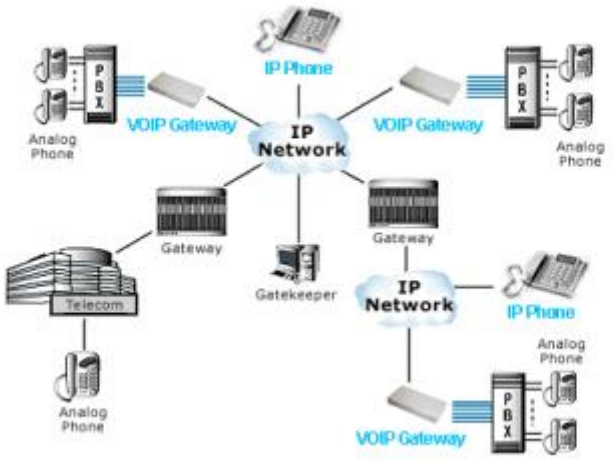


Σχήμα 6: Από τηλέφωνο σε τηλέφωνο[8].

4. Ψηφιοποίηση και Από-ψηφιοποίηση Φωνής

Στη λειτουργία αυτή, τα αναλογικά σήματα φωνής μετατρέπονται σε ψηφιακά ώστε να μεταδοθούν μέσα από το δίκτυο IP. Έπειτα, συμπιέζονται ώστε να γίνει οικονομία των πόρων μέσα στο δίκτυο. Η ασυμπίεστη φωνή απαιτεί μεγάλο εύρος ζώνης (bandwidth)

αρκετών Mbps για να ολοκληρωθεί μια τηλεφωνική κλήση. Αντίθετα, μόλις συμπιεστεί καταναλώνονται μόνο λίγα Kbps, εξασφαλίζοντας την ποιότητα και ότι η φωνή δεν θα είναι διακεκομμένη. Η πιο γνωστή τεχνική κωδικοποίησης είναι η Παλμοκωδική Διαμόρφωση (Pulse Code Modulation-PCM),η οποία μετατρέπει τη φωνή σε ψηφιακή μορφή με δειγματοληψία, 8000 δείγματα ανά δευτερόλεπτο. Για την ψηφιοποίηση και την συμπίεση της φωνής χρησιμοποιείται ένας μηχανισμός που ονομάζεται Coder. Έπειτα, ακολουθείται η αντίστροφη διαδικασία όπου, το σήμα αποκωδικοποιείται και από ψηφιακό γίνεται αναλογικό για να μπορέσει να ακουστεί στον επόμενο συνομιλητή. Αυτή η διαδικασία γίνεται με έναν άλλον μηχανισμό που ονομάζεται decoder. Και οι δύο μηχανισμοί (coder, decoder) ονομάζονται με μία λέξη Codec.



Σχήμα 7: Διάγραμμα VoIP δικτύου[8].

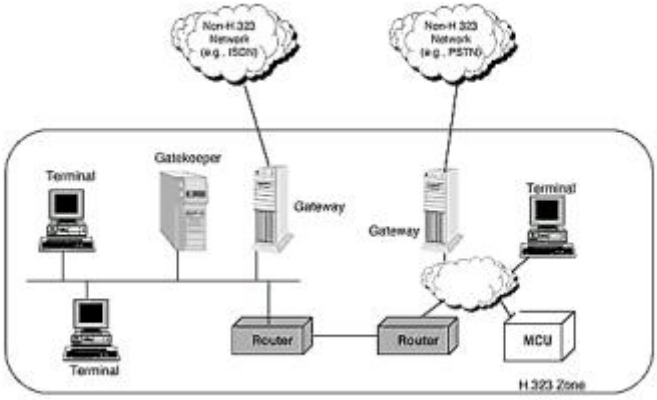
2.1.3 Πρωτόκολλα Σηματοδοσίας

Σε ένα δίκτυο VoIP, στην ψηφιοποίηση, στη συμπίεση και στη μετατροπή του αναλογικού σήματος σε πακέτα IP, μεγάλο ρόλο παίζουν τα πρωτόκολλα σηματοδοσίας. Ένα πρωτόκολλο σηματοδοσίας (signaling protocol) χρησιμοποιείται για να ξεκινήσει και να τερματίσει τις τηλεφωνικές κλήσεις, καθώς και να εντοπίζει τον άλλον χρήστη και να διαχειρίζεται τους πόρους ρου δικτύου. Όπως προαναφέραμε, τα συνηθέστερα πρωτόκολλα είναι το H.323, το SIP, το MGCP και το IAX2[8].

1. H.323: είναι ένα πρωτόκολλο που δημιουργήθηκε από τη Διεθνή Ένωση Τηλεπικοινωνιών (International Telecommunication Union-ITU), για την μετάδοση ήχου, βίντεο και δεδομένων σε πραγματικό χρόνο σε δίκτυα που βασίζονται στη μεταγωγή πακέτων (packet-based networks). Είναι ένα δυαδικό πρωτόκολλο το οποίο χρησιμοποιεί το TCP και το UDP. Με το TCP εξασφαλίζει

αξιοπιστία στη μεταφορά δεδομένων, καθώς και σωστή σειρά στην παράδοσή τους χωρίς να υπάρχει περίπτωση να χαθούν. Το UDP χρησιμοποιείται για την ροή των βίντεο και του ήχου, λόγω του ότι είναι ευαίσθητα στον παράγοντα του χρόνου. Τα βασικά συστατικά του H.323 είναι:

- **Terminal**: είναι το τελικό σημείο του χρήστη
- **Gateway**: είναι η συσκευή η οποία επιτρέπει την επικοινωνία μεταξύ H.323 δικτύων και δικτύων PSTN ή ISDN
- **Multipoint Control Unit (MCU)**: είναι υπεύθυνο για τη διασύνδεση περισσότερων από δύο τερματικών και αποτελείται από τις οντότητες Multipoint Controller (MC) και Multipoint Processor (MP)
- **Gatekeeper**: είναι προαιρετικό αλά παρέχει υπηρεσίες στο Terminal, στο Gateway και στο MCU. Παρέχει υπηρεσίες όπως, διευθυνσιοδότηση, έλεγχο αποδοχής, εξουσιοδότηση χρήστη, εύρος ζώνης κ.α.[8].

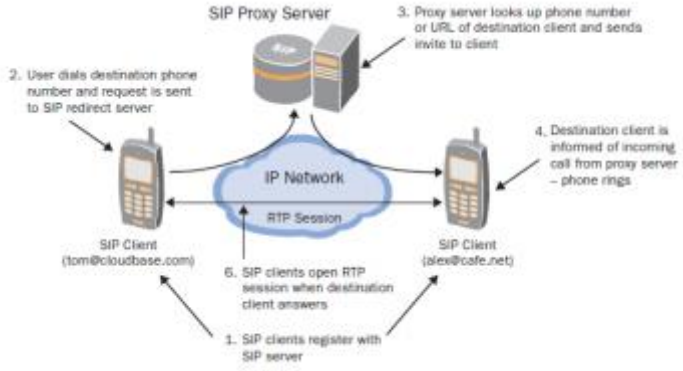


Σχήμα 8: Πρωτόκολλο H.323[8].

2. SIP: το SIP (Session Initiation Protocol) είναι ένα IETF (Internet Engineering Task Force) πρωτόκολλο επικοινωνίας, όπου, χρησιμοποιεί σηματοδοσία τύπου πελάτη- διακομιστή (client-server), για να κάνει την πραγματοποίηση, την τροποποίηση και τον τερματισμό των τηλεφωνικών κλήσεων VoIP. Επίσης, μπορεί να λειτουργήσει σε TCP ή UDP επίπεδα, σε επίπεδο HTTP (Hypertext Transfer Protocol) και σε επίπεδο SMTP (Simple Mail Transfer Protocol), λόγω της τεχνολογίας του text-based. Έχει την δυνατότητα να χρησιμοποιεί προσκλήσεις με στόχο να δημιουργήσει μηνύματα SDP (Session Description Protocol). Το SIP με βάση αυτόν τον τύπο (πελάτη- διακομιστή), υλοποιείται σε δύο μορφές: τον διακομιστή Proxy και τον διακομιστή Redirect[8].

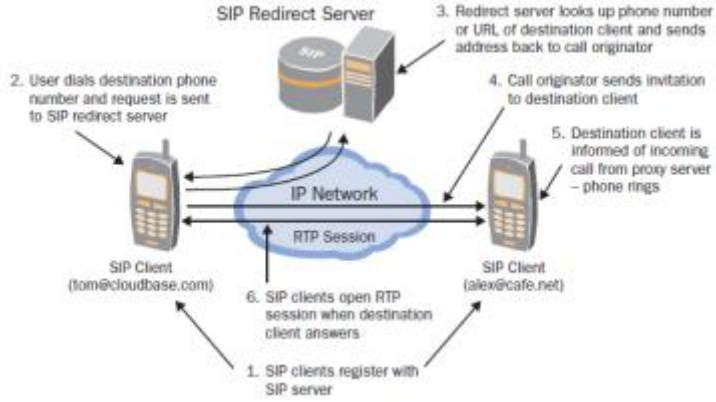
- ο **Proxy**, δέχεται αιτήματα από SIP πελάτες τα οποία, είτε τα απαντάει αυτός, είτε τα προωθεί σε άλλους διακομιστές. Επιπλέον, έχει τη δυνατότητα να αποκρύπτει τους

SIP χρήστες του και στους υπόλοιπους χρήστες μέσα στο δίκτυο VoIP, να εμφανίζεται ότι τις προσκλήσεις σηματοδοσίας τις στέλνει αυτός[8].



Εικόνα 5: SIP Proxy Server[8]

- Ο **Redirect**,δέχεται αιτήματα από SIP πελάτες και αναζητά την διεύθυνση που έχει ζητηθεί. Έπειτα, επιστρέφει την διεύθυνση και ξεκινάει μία επικοινωνία μεταξύ του πελάτη και του διακομιστή SIP[8].



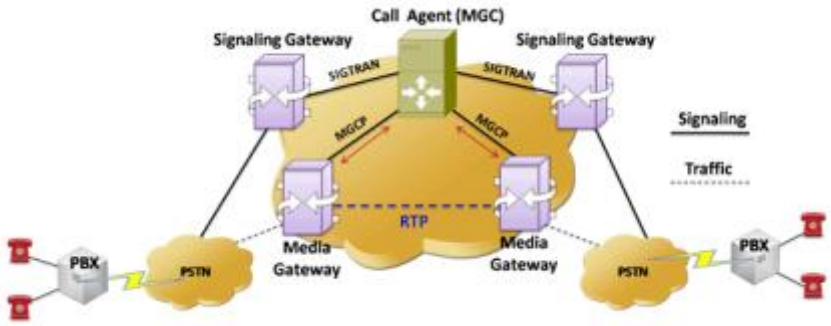
Εικόνα 6: SIP Redirect Server[8].

3. **MGCP**: Το MGCP (Media Gateway Control Protocol) είναι ένα πρωτόκολλο σηματοδοσίας και χρησιμοποιείται σε κλήσεις για VoIP συνδέσεις. Υποστηρίζει δύο βασικά πρωτόκολλα σηματοδοσίας το SIP και το H.323, ενώ για τη λειτουργία του χρησιμοποιεί το SGCP (Simple Gateway Control Protocol) και το πρωτόκολλο IP. Έχει την δυνατότητα να ελέγχει τις Media Gateways σε δίκτυα IP και PSTN. Αποτελείται από τρία μέρη:
   - Έναν Media Gateway Controller ή Call Agent, ο οποίος έχει την ικανότητα να ελέγχει και να διαχειρίζεται τις IP-based συνδέσεις επικοινωνίας μέσα σε ένα VoIP δίκτυο
   - Μία Media Gateway με την οποία κάνει μετατροπή των αναλογικών σημάτων σε

πακέτα δεδομένων που διακινούνται μέσω του Internet ή άλλων δικτύων.

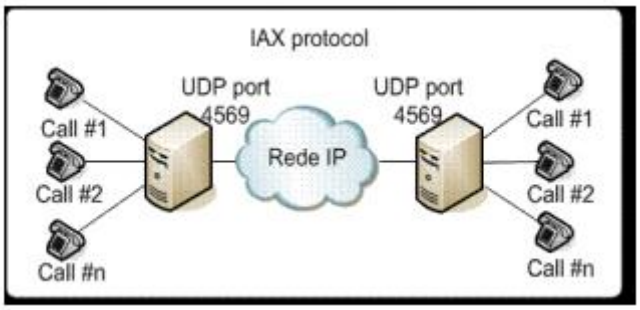
- Μία Signaling Gateway, η οποία χρησιμεύει όταν συνδέεται στο PSTN.

Γενικά, ο Media Gateway Controller δίνει την εντολή στην Media Gateway πότε να ξεκινήσει, να διακόψει ή να τερματίσει μία επικοινωνία[8].



Εικόνα 7: Πρωτόκολλο MGCP[8].

4. **IAX2**: Το IAX2 (Inter-Asterisk eXchange) δημιουργήθηκε από τον Mark Spencer για να ελέγχει και να μεταδίδει τα δεδομένα φωνής στους διακομιστές Asterisk. Είναι δυαδικό πρωτόκολλο και υποστηρίζεται από Softswitches και PBXs. Έχει την ικανότητα να προσφέρει σηματοδοσία και media. Επιπλέον, βοηθάει στην διευκόλυνση των VoIP συνδέσεων μεταξύ των διακομιστών που το χρησιμοποιούν. Ένα από τα βασικά χαρακτηριστικά του είναι ότι χρησιμοποιεί τη θύρα UDP 4569 και το κάνει πιο ασφαλές γιατί δουλεύει πίσω από το NAT (Network Address Translation). Ωστόσο, έχει ένα μεγάλο μειονέκτημα, το οποίο είναι ότι υπάρχουν λίγες τερματικές συσκευές που το υποστηρίζουν και γι' αυτό το λόγο χρησιμοποιείται κυρίως για τη διασύνδεση τηλεφωνικών κέντρων[8].



Εικόνα 8: Πρωτόκολλο IAX2[8].

2.1.4 Πλεονεκτήματα και Μειονεκτήματα VoIP Κλήσεων

Η υπηρεσία VoIP (Voice over IP) είναι μία υπηρεσία διαδικτυακής επικοινωνίας, όπως προείπαμε, η οποία παρέχει φωνητική συνομιλία με καλή ποιότητα φωνής και χωρίς κόστος. Ωστόσο, επειδή είναι μία σχετικά καινούργια υπηρεσία, ναι μεν έχει αρκετά πλεονεκτήματα αλλά έχει και μειονεκτήματα.

Η υπηρεσία αυτή παρέχει δωρεάν κλήσεις προς τηλέφωνα Internet χωρίς καμία απολύτως χρέωση. Επιτρέπει τις κλήσεις προς σταθερά και κινητά τηλέφωνα με πολύ χαμηλές χρεώσεις και αρκετές φορές, σύμφωνα με το συμβόλαιο του πελάτη- χρήστη, οι κλήσεις αυτές είναι δωρεάν. Η δρομολόγηση και η επαναδρομολόγηση των τηλεφωνικών κλήσεων μέσω των δικτύων δεδομένων είναι ευκολότερη και ταχύτερη χωρίς να χρειάζονται διαφορετικά δίκτυα κίνησης φωνής και κίνησης δεδομένων. Επιπλέον, ο χρήστης έχει το πλεονέκτημα να κάνει άμεση μεταφορά του VoIP τηλεφώνου του σε οποιαδήποτε θέση βρίσκεται, αρκεί στο συγκεκριμένο σημείο να του παρέχεται σύνδεση στο Internet. Επίσης, ο χρήστης μπορεί να πραγματοποιεί κλήσεις χωρίς κόστος με πολύ καλή ποιότητα ήχου και έχει τη δυνατότητα, ενώ βρίσκεται συνδεδεμένος στο Internet, να πραγματοποιεί κλήσεις ταυτόχρονα χωρίς κάποια διακοπή σύνδεσης. Οι κλήσεις είναι ασφαλείς γιατί χρησιμοποιούν τυποποιημένα πρωτόκολλα όπως το RTP(Real-Time Transport Protocol) και υπάρχει δυνατότητα, να μεταδίδονται περισσότερα από ένα τηλεφωνήματα σε μια μόνο ευρυζωνική σύνδεση[6][7][8].

Δυστυχώς όμως, όπως κάθε υπηρεσία έτσι και αυτή ναι μεν έχει κάποια πολύ σοβαρά πλεονεκτήματα, αλλά έχει και βασικά μειονεκτήματα. Κατά την διάρκεια των κλήσεων, υπάρχουν κάποιες καθυστερήσεις στη σύνδεση. Όταν ένας χρήστης είναι συνδεδεμένος με ένα σταθερό δίκτυο τηλεφωνίας, του παρέχεται μεγάλη αξιοπιστία στην πραγματοποίηση των κλήσεων του σε αντίθεση με τα VoIP τηλέφωνα, τα οποία δεν εξασφαλίζουν την ίδια αξιοπιστία σύνδεσης. Για παράδειγμα, σε κάποια διακοπή ρεύματος, τα VoIP τηλέφωνα σταματούν να λειτουργούν επειδή είναι συνδεδεμένα σε κάποιο modem και έτσι η σύνδεση τους στο Internet διακόπτεται. Επιπλέον, ένα ακόμα μειονέκτημα είναι η δυσκολία δρομολόγησης κλήσεων έκτακτης ανάγκης. Συνήθως, αυτές οι κλήσεις σπάνια καταλήγουν σε κάποιο κέντρο εξυπηρέτησης κλήσεων έκτακτης ανάγκης. Ωστόσο, με το πέρασμα του χρόνου, οι τεχνικοί προσπαθούν να το επιλύσουν αυτό το πρόβλημα. Έτσι, σε τέτοιες περιπτώσεις κλήσεων, επειδή δεν χρησιμοποιείται κρυπτογράφηση, δυστυχώς δεν υπάρχει ασφάλεια συνομιλίας με αποτέλεσμα, αρκετούς χρήστες να τους ενοχλεί αυτό. Ένα ακόμα μειονέκτημα είναι ότι για να πραγματοποιηθεί μια VoIP κλήση, χρειάζεται υψηλή ταχύτητα Internet και σε σχέση με τα παραδοσιακά τηλέφωνα, η ποιότητα της φωνής είναι χαμηλότερη. Επίσης, η υπηρεσία είναι πολύ επιρρεπής σε ιούς και σε κλοπές των φωνητικών δεδομένων που έχουν αποθηκευτεί, από Hackers[7][8][9].

2.2 Ποιότητα Υπηρεσιών (Quality of Service-QoS)

Το QoS(Quality of Service) είναι μία υπηρεσία η οποία ασχολείται με τεχνολογίες και τεχνικές δικτύωσης οι οποίες ελέγχουν τη διαθεσιμότητα των πόρων του δικτύου. Σκοπός τους είναι να επιτυγχάνουν τα επιθυμητά αποτελέσματα, μετρώντας τους ρυθμούς μετάδοσης και λαθών και διάφορα άλλα χαρακτηριστικά τα οποία καθορίζουν τον βαθμό απόδοσης του δικτύου, ώστε να πετύχουν τη βέλτιστη απόδοση και παράδοση πακέτων. Η υπηρεσία QoS, εκτός από το ότι μετράει τους ρυθμούς μετάδοσης και τους ρυθμούς λαθών, ελέγχει αν παραδόθηκαν όλα τα πακέτα που στάλθηκαν και αν η παράδοση τους έχει γίνει με τη σωστή σειρά με την οποία στάλθηκαν. Ωστόσο, υπάρχουν κάποιοι παράγοντες οι οποίοι επηρεάζουν την ποιότητα των υπηρεσιών και πολλές φορές μπορεί να υπάρχει καθυστέρηση κατά την μετάδοση των πακέτων και ένα μικρό ποσοστό μετάδοσης λανθασμένου πακέτου. Οι παράγοντες που επηρεάζουν την ποιότητα των υπηρεσιών, είναι κυρίως: η καθυστέρηση(delay) δηλαδή ο χρόνος μετάβασης ενός πακέτου από τον αποστολέα στον παραλήπτη, η διακύμανση (jitter) στην καθυστέρηση, το διαθέσιμο εύρος ζώνης(bandwidth), καθώς και η αξιοπιστία(reliability) του μέσου μετάδοσης[8][10].

Για να μπορέσει να επιτευχθεί η επιθυμητή απόδοση, υπάρχουν πρωτόκολλα τα οποία δείχνουν τον τρόπο με τον οποίο υποστηρίζονται οι υπηρεσίες πραγματικού χρόνου πάνω από το IP. Τα βασικότερα πρωτόκολλα είναι τα παρακάτω.

2.2.1 Πρωτόκολλο RTP

Το RTP (Real-time Transport Protocol) κατασκευάστηκε από την IETF και σκοπός της σχεδίασης του είναι η μεταγωγή real-time πακέτων που περιέχουν δεδομένα φωνής και βίντεο[8].

Το RTP για τη μετάδοση του ήχου και της εικόνας, χρησιμοποιεί τεχνολογίες multicast (πολλαπλών διαδρομών) και unicast (μία διαδρομή). Επίσης, χρησιμοποιεί το πρωτόκολλο UDP για τη μεταφορά δεδομένων καθώς, και κεφαλίδες (headers) που είναι σχεδόν ίδιες με το UDP και το IP[8].

Το RTP δεν είναι υπεύθυνο για τη διασφάλιση της επιθυμητής ποιότητας κλήσεων, αλλά, προσδιορίζει ανεπιθύμητα γεγονότα κατά την μεταφορά των πακέτων, όπως την καθυστέρηση της μετάδοσης των πακέτων (jitter), την παράδοση των πακέτων που είναι εκτός της σειράς που στάλθηκαν (out-of-order delivery) καθώς και αν υπάρχει κάποια απώλεια πακέτου (dropped packets)[8].

2.2.2 Πρωτόκολλο RTCP

Το RTCP (Real-time Transport Control Protocol) είναι συνδεδεμένο με το RTP και ο στόχος του είναι να ελέγχει τις συνεδρίες του RTP και είναι υπεύθυνο για τη μετάδοση των δεδομένων στους συνομιλητές. Τα πακέτα που μεταφέρονται κατατάσσονται σε τέσσερις κατηγορίες: τις αναφορές αποστολέα (SRs), τις αναφορές παραλήπτη (RRs), τα πακέτα περιγραφής της πηγής (SDEs) και τα πακέτα τερματισμού της συνόδου (BYE)[8].

Ο βασικότερος σκοπός του RTCP είναι η συλλογή στοιχείων για τον αριθμό των πακέτων που καταλήγουν στον προορισμό τους για να αποδειχθεί αν το δίκτυο χρησιμοποιεί με τον κατάλληλο τρόπο τις υπηρεσίες ποιότητας κλήσεων. Επιπλέον, το RTCP είναι υπεύθυνο για τον έλεγχο της κυκλοφορίας του δικτύου, γιατί, όσο αυξάνονται οι χρήστες που συμμετέχουν σε μια συνεδρία, τόσο αυξάνεται και ο αριθμός των πακέτων που αποστέλλονται. Γι' αυτόν το λόγο, το RTCP ελέγχει την κυκλοφορία ώστε να γίνει εξοικονόμηση πόρων στο δίκτυο και να καταφέρει εν τέλει, το RTP να εξυπηρετήσει πιο πολλούς χρήστες[8].

2.2.3 Πρωτόκολλο RTSP

Το RTSP (Real-Time Streaming Protocol) είναι ένα πρωτόκολλο σηματοδοσίας και ανήκει στο στρώμα εφαρμογής (application layer) του μοντέλου OSI. Ο βασικός του ρόλος είναι να συμπληρώνει το RTP και το RTCP. Σκοπός του είναι να ελέγχει τη ροή των δεδομένων που συγχρονίζονται και περιέχουν ήχο και εικόνα (πολυμέσα). Ασχολείται κυρίως με τον ήχο και την εικόνα που παράγονται τη συγκεκριμένη στιγμή και μεταφέρονται στο δίκτυο, που το πρωτόκολλο ελέγχει τη ροή. Οι τεχνολογίες μετάδοσης που χρησιμοποιεί είναι multicast και unicast. Ωστόσο, δεν είναι καθήκον του να κάνει μεταφορά πακέτων πληροφορίας πολυμέσων στο δίκτυο[8].

Το RTSP χρησιμοποιεί τα πρωτόκολλα μεταφοράς UDP και TCP και επίσης, έχει πολλά κοινά χαρακτηριστικά με το HTTP και παρέχει υπηρεσίες παρόμοιου επιπέδου για την μετάδοση των δεδομένων σε πραγματικό χρόνο (real-time)[8].

Σε μια συνεδρία RTSP, ο πελάτης (client) έχει το δικαίωμα να ξεκινάει και να τερματίζει αρκετές συνδέσεις ταυτοχρόνως, με σκοπό να καταφέρει να μεταβιβάσει τα αιτήματά του (requests) στον διακομιστή (server)[8].

2.2.4 Πρωτόκολλο RSVP

Το RSVP (Resource ReSerVation Protocol) έχει δημιουργηθεί από την IETF και είναι ένα πρωτόκολλο σηματοδοσίας που χρησιμοποιείται για τη δέσμευση πόρων. Χρησιμοποιείται κυρίως ως συμπλήρωμα του IP και η αρμοδιότητά του είναι να ελέγχει τη μετάδοση των πακέτων δεδομένων σε ένα IP δίκτυο. Σκοπός του είναι να επιτρέπει τη διανομή QoS αιτήσεων για μια ροή δεδομένων μιας

εφαρμογής. Πριν την έναρξη της εφαρμογής, δεσμεύεται ένα συγκεκριμένο εύρος ζώνης σε όλο το μήκος του μονοπατιού μεταξύ της πηγής και του προορισμού. Οι εξυπηρετητές και οι δρομολογητές χρησιμοποιούν το RSVP για να παραδίδονται οι QoS αιτήσεις που βρίσκονται στο συγκεκριμένο μονοπάτι[8][10].

Το RSVP αρχικά χρησιμοποιήθηκε σε multicast εφαρμογές, όπως η τηλεδιάσκεψη ήχου, βίντεο και το broadcasting, αλλά κατά την εξέλιξη του, φάνηκε ότι υπήρχε ενδιαφέρον για δέσμευση εύρους ζώνης (bandwidth) σε unicast εφαρμογές όπως NFS και VPN[10].

Για την επίτευξη της επιθυμητής ποιότητας υπηρεσιών, χρησιμοποιούνται κάποιοι μηχανισμοί που ελέγχουν την κυκλοφορία:

- Admission Control: ελέγχει αν υπάρχουν οι απαραίτητοι πόροι για να ικανοποιηθεί το ζητούμενο QoS
- Policy Control: ελέγχει αν ο χρήστης έχει εξουσιοδοτηθεί για να αποδοθεί το ζητούμενο QoS
- Packet Scheduler: είναι υπεύθυνο για να αποφασίζει για την μετάδοση κάθε εξερχόμενου πακέτου σε μια διεπαφή, και,
- Packet Classifier: είναι υπεύθυνο για να καθορίζει τη δρομολόγηση κάθε εισερχόμενου πακέτου[10].

2.2.5 Πρωτόκολλο MPLS

Το MPLS (MultiProtocol Label Switching) είναι ένα πρωτόκολλο το ποίο κατασκευάστηκε από την IETF και έχει ως σκοπό να αυξήσει την ευελιξία και την απόδοση του παραδοσιακού IP και ταυτοχρόνως, να δώσει την δυνατότητα για την παροχή νέων υπηρεσιών στο διαδίκτυο. Το MPLS συνδυάζει την μεταγωγή με ετικέτα (label) και την παραδοσιακή δρομολόγηση του πρωτοκόλλου IP[10].

ΕΝΟΤΗΤΑ 3

ΕΡΓΑΛΕΙΑ ΑΝΙΧΝΕΥΣΗΣ ΚΑΙ ΑΝΑΛΥΣΗΣ ΔΙΚΤΥΑΚΗΣ ΚΙΝΗΣΗΣ

Στις μέρες μας, ο κλάδος της πληροφορικής και των τηλεπικοινωνιών, αναπτύσσεται με γρήγορο ρυθμό. Ένα από τα πολλά πλεονεκτήματα που παρέχει είναι να μπορεί κάθε χρήστης να κάνει βελτιστοποίηση του δικτύου του, μελετώντας και αναλύοντας την δικτυακή κίνηση. Υπάρχουν διάφορα προγράμματα και λογισμικά τα οποία δίνουν τη δυνατότητα στον χρήστη μα συλλέγει τις πληροφορίες του δικτύου και να τις επεξεργάζεται. Τα προγράμματα αυτά αναφέρονται ως network sniffer, δηλαδή, αναλυτές δικτύων, πρωτοκόλλων, Ethernet Sniffer, wireless sniffer κ.α. σκοπός τους είναι να ανιχνεύουν και να καταγράφουν τα δεδομένα σε ένα ψηφιακό δίκτυο. Καθώς τα ρεύματα δεδομένων (data streams) ταξιδεύουν μέσα στο δίκτυο, ο network sniffer συλλαμβάνει κάθε πακέτο, το αποκωδικοποιεί και αναλύει το περιεχόμενο του σύμφωνα με τον κατάλληλο RFC (Requests For Comments- έγγραφα οργάνωσης δικτύου) ή άλλες αντίστοιχες προδιαγραφές και μοντέλα.

Παρακάτω αναφέρονται κάποια εργαλεία και λογισμικά τα οποία παίζουν σημαντικό ρόλο στη διαχείριση και ανάλυση της δικτυακής κίνησης. Τα εργαλεία αυτά, ταξινομούνται σε τρεις κατηγορίες, ανάλογα με τις υπηρεσίες που παρέχουν. Υπάρχουν τα εργαλεία και τα λογισμικά τα οποία διερευνούν τις υπηρεσίες που τρέχουν στο τοπικό σύστημα (Local Systems), αυτά που διερευνούν τα απομακρυσμένα συστήματα (Remote End Systems), καθώς και τα εργαλεία και λογισμικά που διερευνούν τις υπηρεσίες που τρέχουν σε έναν δρομολογητή και του δίνουν τη δυνατότητα να συλλέγει πληροφορίες για την κυκλοφορία του δικτύου (Routers).

- Local Systems: NETSTAT, WIRESHARK, NMAP, TCPDUMP, NTOP
- Remote End Systems: MIB,SNMP,MRTG
- Routers: NETFLOW (CISCO)

3.1 Wireshark

Στα τέλη του 1990 ο Gerald Combs απόφοιτος του Πανεπιστημίου Missouri-Kansas City με ειδικότητα στην επιστήμη της πληροφορικής, εργαζόταν σε ένα μικρό ISP (Internet Service Provider), το οποίο είναι ένας οργανισμός που παρέχει υπηρεσίες για την πρόσβαση, τη χρήση και τη συμμετοχή ενός χρήστη στο Διαδίκτυο. Έτσι, ο Combs άρχισε να δημιουργεί το εργαλείο Ethereal το οποίο και κυκλοφόρησε το 1998.

Το 2006 ο Combs αποδέχθηκε μία δουλεία στην CACE Technologies και ταυτόχρονα είχε τα πνευματικά δικαιώματα για το Ethereal. Έτσι, έχοντας στην δικαιοδοσία του το εμπορικό σήμα του

Ethereal, το μετονόμασε σε Wireshark και το εξέλιξε. Το 2010 η εταιρία Riverbed Technology, αγόρασε την CACE και έτσι γίνεται και ο κύριος χορηγός του Wireshark.

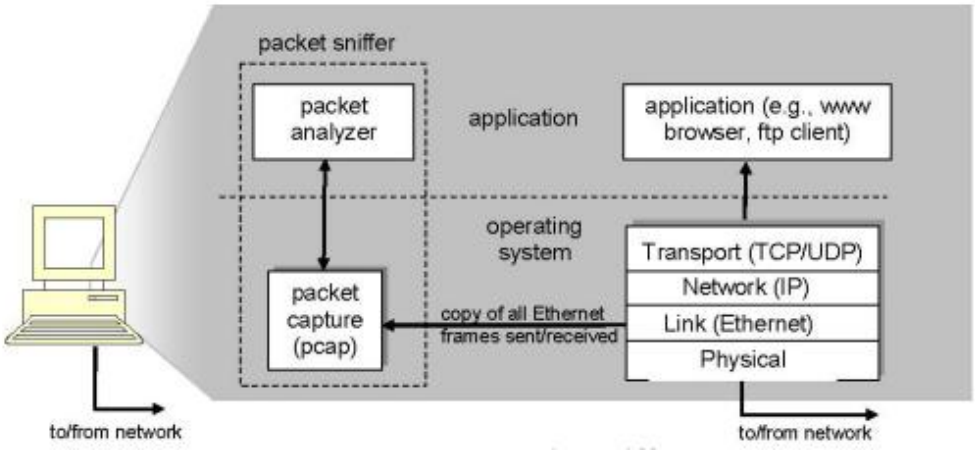
Το εργαλείο αυτό, με την πάροδο του χρόνου κέρδισε πολλά βραβείο βιομηχανίας κάποια εκ των οποίων είναι και τα eWeek, InfoWorld και βραβεία του περιοδικού PC Magazine. Το Wireshark, θεωρείται ότι είναι ένα από τα καλύτερα εργαλεία ασφάλειας δικτύου της Insecure.org καθώς και το SourceForge project του Αυγούστου του 2010. Τέλος, ο Combs εξακολουθεί να έχει τον πηγαίο κώδικα του Wireshark τον οποίο εξελίσσει και κάνει διανομές νέων εκδόσεων του λογισμικού.

Το Wireshark είναι ένα λογισμικό ανοιχτού κώδικα και ασχολείται με την ανάλυση πρωτοκόλλων δικτύου υπολογιστών. Η βασική του χρήση είναι για την ανάλυση και την παρακολούθηση του δικτύου, την αντιμετώπιση προβλημάτων στα δίκτυα, καθώς και για εκπαίδευση. Είναι διαθέσιμο για όλα τα λειτουργικά συστήματα όπως, Windows, Linux, Mac OS X, Solaris και BSD. Για το γραφικό του περιβάλλον χρησιμοποιεί το GTK+ και για την σύλληψη των πακέτων το Pcap. Έχει το πλεονέκτημα ότι διατίθεται δωρεάν από την GNU και είναι ελεύθερο λογισμικό.

3.1.1 Λειτουργία και Αποτελέσματα Εκτέλεσης Wireshark

Το Wireshark ή αλλιώς packet sniffer, είναι ένας αναλυτής πακέτων ο οποίος χρησιμοποιεί μια βιβλιοθήκη σύλληψης πακέτων στον υπολογιστή. Στην ουσία λαμβάνει μηνύματα (“sniffs”) τα οποία αποστέλλονται ή λαμβάνονται στον υπολογιστή, τα αποθηκεύει και τα απεικονίζει σε διάφορα πεδία πρωτοκόλλων που περιέχονται στα μηνύματα που λαμβάνονται. Οι βασικές του λειτουργίες είναι η καταγραφή – σύλληψη δεδομένων και η ανάλυση της δικτυακής κίνησης του υπολογιστή[5].

Ωστόσο, το Wireshark παρατηρεί τα μηνύματα που στέλνονται και λαμβάνονται από τις εφαρμογές, όπως επίσης και τα πρωτόκολλα που τρέχουν στον υπολογιστή αλλά δεν αποστέλλει ποτέ πακέτα ούτε λαμβάνει. Κάθε φορά που γίνεται κάποια ενέργεια, λαμβάνει αντίγραφο των πακέτων και των πρωτοκόλλων που εκτελούνται στον υπολογιστή[5].



Σχήμα 9: Δομή Packet Sniffer[5].

Στην παραπάνω εικόνα (Εικόνα 2), φαίνεται η δομή λειτουργίας του Wireshark (packet sniffer) όπου στη δεξιά πλευρά απεικονίζονται τα πρωτόκολλα του Διαδικτύου καθώς και οι εφαρμογές (π.χ. ένας web browser), τα οποία τρέχουν στον υπολογιστή την στιγμή που εκτελείται και ο packet sniffer. Το wireshark αποτελείται από δύο μέρη, τον packet capture όπου είναι η βιβλιοθήκη σύλληψης πακέτων και από τον packet analyzer, τον αναλυτή πακέτων[5].

Η βιβλιοθήκη λαμβάνει κάθε αντίγραφο που έρχεται από κάθε ενέργεια που γίνεται σε επίπεδο ζεύξης. Κάθε μήνυμα που αποστέλλεται ή λαμβάνεται μέσω των πρωτοκόλλων HTTP, FTP, TCP, UDP ή IP, όλα μαζί ενθυλακώνονται σε πλαίσια πεδίου ζεύξης τα οποία μεταδίδονται μέσω ενός καλωδίου Ethernet. Άρα, η βιβλιοθήκη σύλληψης πακέτων περιλαμβάνει όλα τα μηνύματα που ανταλλάσσονται από όλα τα πρωτόκολλα και τις εφαρμογές που εκτελούνται στον υπολογιστή[5].

Ο αναλυτής πακέτων (packet analyzer), απεικονίζει τα περιεχόμενα όλων των πεδίων μέσα στο μήνυμα ενός πρωτοκόλλου. Σκοπός του είναι να αντιλαμβάνεται τη δομή όλων των μηνυμάτων που ανταλλάσσονται από τα πρωτόκολλα.

3.1.2 Χαρακτηριστικά του Wireshark

Η χρήση του Wireshark καθημερινώς αυξάνεται. Αυτό συμβαίνει γιατί έχει αρκετά χαρακτηριστικά μέσω των οποίων οι χρήστες και οι προγραμματιστές μπορούν να κάνουν εύκολα τη δουλειά τους σε σχέση με άλλα εργαλεία. Είναι ένα από τα δημοφιλέστερα προγράμματα που χρησιμοποιούνται για την παροχή πληροφοριών πρωτοκόλλων και δεδομένων που διακινούνται μέσα σε ένα δίκτυο.

Ο κύριος λόγος που το κάνει τόσο δημοφιλές είναι ότι διατίθενται ελεύθερο και χωρίς κόστος στον

χρήστη και είναι αρκετά εύκολο στη χρήση του. Έχει την ικανότητα να υποστηρίζει μεγάλο πλήθος πρωτοκόλλων που ξεπερνούν τα 850, είτε αυτά είναι δικτυακά πρωτόκολλα (π.χ. IP, ARP, DHCP κ.α) είτε είναι εμπορικά (AppleTalk, Bit torent). Επιπλέον, υποστηρίζεται από όλα τα λειτουργικά συστήματα όπως, Windows, Linux, Mac OS X, Solaris και BSD. Τέλος, έχει αρκετά ευχάριστο και ωραίο γραφικό περιβάλλον και μπορεί να κάνει γραφική αναπαράσταση των δεδομένων.

3.2 NETSTAT

Το NETSTAT είναι ένα βοηθητικό πρόγραμμα το οποίο εμφανίζει διάφορες στατιστικές οι οποίες σχετίζονται με τα πρωτόκολλα IP, TCP, UDP και ICMP. Οι στατιστικές αυτές εμφανίζουν αριθμητικούς μετρητές για διάφορα στοιχεία όπως, τα datagram τα οποία έχουν σταλεί και έχουν ληφθεί, καθώς και μία λίστα από λάθη που θα μπορούσαν να συμβούν[15].

3.3 MIB

Το MIB (Management Information Base) είναι μία βάση δεδομένων που χρησιμοποιείται για την διαχείριση ενός δικτύου επικοινωνίας. Σχετίζεται κυρίως με το πρωτόκολλο διαχείρισης δικτύου (SNMP) και περιέχει πληροφορίες οι οποίες σχετίζονται με το δίκτυο.

3.4 SNMP

Το SNMP (Simple Network Management Protocol) δεν είναι πρόγραμμα αλλά ένα πρωτόκολλο που έχει δημιουργηθεί για να διαχειρίζεται και να παρακολουθεί απομακρυσμένες συσκευές σε ένα δίκτυο. Υποστηρίζει ένα σύστημα που επιτρέπει σε έναν διαχειριστή δικτύου να χρησιμοποιεί ένα σταθμό εργασίας από τον οποίο να διαχειρίζεται και να παρακολουθεί από μακριά υπολογιστές, δρομολογητές και άλλες συσκευές του δικτύου[15].

3.4.1 Αρχιτεκτονική SNMP

Τα βασικά χαρακτηριστικά της αρχιτεκτονικής του SNMP είναι:

- **Οθόνη Δικτύου:** είναι μία κονσόλα διαχείρισης που ονομάζεται διαχειριστής ή Network Management Console (NMS)και η οποία παρέχει μία κεντρική θέση για την διαχείριση των συσκευών σε ένα δίκτυο. Γενικότερα, είναι ένας υπολογιστής ο οποίος έχει ως λογισμικό διαχείρισης το SNMP.
- **Κόμβοι:** είναι οι συσκευές του δικτύου.
- **Κοινότητα:** είναι μία ομάδα από κόμβους που αποτελούν μια κοινή υποδομή διαχείρισης.

Η οθόνη του δικτύου χρησιμοποιεί τις παραμέτρους του Management Information Base (MIB) για να μπορέσει να πάρει τις πληροφορίες που χρειάζεται και να αλλάξει τις ρυθμίσεις διαμόρφωσης[15].

3.5 TCPDUMP

Το TCPDUMP είναι ένας αναλυτής πακέτων που τρέχει πίσω από κάθε γραμμή εντολών. Δίνει την δυνατότητα στον χρήστη να απεικονίσει TCP/IP και άλλα πακέτα που μεταδίδονται ή λαμβάνονται μέσω ενός δικτύου στο οποίο συνδέεται ο υπολογιστής.

Γενικότερα, είναι ένα ελεύθερο λογισμικό το οποίο δουλεύει σε λειτουργικά συστήματα όπως: Linux, Solaris, BSD, OS X, HP-UX και διαφόρων άλλων.

3.6 NTOP

Είναι ένα λογισμικό υπολογιστών που ερευνά ένα δίκτυο και δείχνει τη χρήση και τις ενέργειες του. Είναι διαθέσιμο για Unix λειτουργικά και για Windows 32 bit. Χρησιμοποιείται ως:

- Web interface
- Έχει περιορισμένη ρύθμιση και διαχείριση μέσω του web interface
- Μειωμένη χρήση της CPU και της μνήμης που χρησιμοποιεί (ανάλογα το μέγεθος του δικτύου).

3.7 NETFLOW (CISCO)

Είναι ένα χαρακτηριστικό το οποίο ανήκει στη CISCO για να δίνει την δυνατότητα στους δρομολογητές να συλλέγουν την κυκλοφορία των πακέτων σε ένα δίκτυο καθώς εισέρχεται ή εξέρχεται μία διεπαφή. Με την χρήση της ανάλυσης που γίνεται μέσω του NetFlow, ένας διαχειριστής μπορεί να μάθει για την προέλευση και τον προορισμό της κυκλοφορίας, την κατηγορία των υπηρεσιών, ακόμα και τους λόγους για τους οποίους μπορεί να υπάρξει κυκλοφοριακή συμφόρηση.

Η χρήση του NETFLOW αποτελείται από τρία κύρια μέρη:

- Εξαγωγέας Ροής (Flow Exporter): ασχολείται με αδρανή πακέτα που υπάρχουν στις ροές και με τις εξαγωγές των αρχείων προς έναν ή περισσότερους συλλέκτες ροής
- Συλλέκτης Ροής (Flow Collector): είναι υπεύθυνος για την παραλαβή, αποθήκευση και επεξεργασία των στοιχείων που λαμβάνει από τον flow exporter.
- Ανάλυση Εφαρμογής (Analysis Application): λαμβάνει τα δεδομένα της ροής και της ανίχνευσης εισβολέων.

3.8 MRTG

Το MRTG (Multi Router Traffic Grapher) είναι ένα ελεύθερο λογισμικό για την παρακολούθηση και τη μέτρηση του φόρτου της κυκλοφορίας που υπάρχει μέσα στο δίκτυο. Αναπτύχθηκε από τον Tobi

Oetiker και τον Dave Rand για να παρακολουθεί για την παρακολούθηση της κυκλοφορίας του δικτύου και πλέον έχει εξελιχθεί σε πρόγραμμα που εμφανίζει στατιστικές σε γραμμική μορφή. Είναι γραμμένο σε γλώσσα Perl και τρέχει σε Window, Linux, Unix, Mac OS και NetWare.

3.9 NMAP

Το Nmap (Network Mapper) είναι ένα ανοιχτό εργαλείο πηγής για την εξερεύνηση του δικτύου και τον έλεγχο της ασφάλειας. Λειτουργεί ως σαρωτής ασφάλειας και χρησιμοποιείται για να βρει κεντρικούς υπολογιστές, καθώς και τις υπηρεσίες που χρησιμοποιεί ένα δίκτυο.

Το Nmap είναι αρκετά ευέλικτο πρόγραμμα και έχει την δυνατότητα να υποστηρίζεται από αρκετά λογισμικά όπως, Linux, Microsoft Windows, HP-UX, BSD, AmigaOS, Mac OS X κ.α. Ωστόσο, είναι πιο διαδεδομένο στα Linux και έπειτα στα Windows.

3.9.1 Λειτουργία και Αποτελέσματα Εκτέλεσης Nmap

Το Nmap χρησιμοποιεί ακατέργαστα IP πακέτα, οποία καθορίζουν ποιοι είναι οι κεντρικοί υπολογιστές (hosts)και αν είναι ενεργοί, ποιες υπηρεσίες προσφέρουν οι hosts, τι λειτουργικά συστήματα τρέχουν, το είδος των πακέτων και φίλτρων/firewalls που χρησιμοποιούνται και διάφορα άλλα χαρακτηριστικά. Για να μπορέσει να επιτύχει τον σκοπό του, στέλνει ειδικά δημιουργημένα πακέτα στον υπολογιστή που είναι και ο προορισμός του και συνέχεια αναμένει να αναλύσει τις απαντήσεις που θα λάβει. Πριν στείλει τα πακέτα, παρακολουθεί τις συνθήκες του δικτύου, όσον αφορά, τις διακυμάνσεις της αδράνειας και τη συμφόρηση του δικτύου, για να μην επιβαρύνει και μεγαλώσει το πρόβλημα. Επιπλέον, έχει τη ικανότητα να καταλαβαίνει αν ένας κεντρικός υπολογιστής είναι σε λειτουργία ή όχι και ποια ports είναι ανοιχτά και ποια κλειστά. Μπορεί να καθορίσει το λειτουργικό σύστημα του προορισμού, καθώς και ονόματα και εκδόσεις των υπηρεσιών που χρησιμοποιεί, και αναγνωρίζει τν τύπο της συσκευής του προορισμού και αν υπάρχει παρουσία τείχους προστασίας.

Η έξοδος του Nmap είναι μία λίστα από σαρωμένους στόχους- προορισμούς, με πληροφορίες όπου η κάθε μία εξαρτάται από το τι ζητήθηκε. Ένα από τα βασικά στοιχεία που παρέχει, είναι ο πίνακας των ports (interesting ports table), ο οποίος παραθέτει τον αριθμό της θύρας και το πρωτόκολλο, το όνομα υπηρεσίας και την κατάσταση. Η κατάσταση είτε είναι ανοιχτή, είτε φιλτραρισμένη είτε κλειστή ή αφιλτράριστη. Όταν είναι ανοιχτή σημαίνει ότι μπορεί να εντοπίσει στον στόχο τις συνδέσεις και τα πακέτα της συγκεκριμένης θύρας. Όταν είναι φιλτραρισμένη, σημαίνει ότι ένα τείχος προστασίας ή κάποιο άλλο εμπόδιο στο δίκτυο, μπλοκάρει τη θύρα, έτσι ώστε το Nmap δεν μπορεί να καταλάβει αν είναι ανοιχτή ή κλειστή. Όταν είναι κλειστή σημαίνει ότι οι θύρες δεν έχουν εφαρμογή στο να εντοπίζονται συνδέσεις και πακέτα, ωστόσο, μπορούν να ανοίξουν οποιαδήποτε στιγμή. Αφιλτράριστες θεωρούνται οι θύρες όταν ανταποκρίνονται στους ανιχνευτές Nmap , αλλά το Nmap,

δεν μπορεί να τις προσδιορίσει αν είναι ανοιχτές ή κλειστές. Τέλος, τα αποτελέσματα του Nmap, εκτός από τους πίνακες των ports, μπορεί να παρέχει περαιτέρω πληροφορίες σχετικά με τους στόχους, όπου συμπεριλαμβάνονται και οι αντιστροφές των ονομάτων DNS, τα λειτουργικά συστήματα, τους τύπους των συσκευών καθώς και τις MAC διευθύνσεις.

Το πρόγραμμα το οποίο χρησιμοποιείτε στην συγκεκριμένη εργασία για την ανίχνευση και την ανάλυση της δικτυακής κίνησης, είναι το Wireshark. Γενικότερα, υπάρχουν και διάφορα άλλα εργαλεία, όπως προείπαμε, τα οποία βοηθούν στο να γίνει ανίχνευση της δικτυακής κίνησης. Κάποια από αυτά διανέμονται δωρεάν και κάποια άλλα χρειάζονται κάποια συνδρομή. Η επιλογή του Wireshark για την ανάλυση της κίνησης, έγινε γιατί το πρόγραμμα αυτό έχει την ικανότητα να υποστηρίζει μεγάλο αριθμό πρωτοκόλλων, τρέχει σε Windows και είναι αρκετά εύκολο στη χρήση του.

ΕΝΟΤΗΤΑ 4

SKYPE ΜΕΣΩ VOIP ΥΠΗΡΕΣΙΩΝ

Τα τελευταία χρόνια, η τεχνολογία έχει εξελιχθεί αρκετά με αποτέλεσμα να υπάρχουν αρκετές εφαρμογές που χρησιμοποιούν VoIP υπηρεσίες. Η πιο διαδεδομένη είναι η εφαρμογή Skype η οποία χρησιμοποιείται για μεταφορά φωνής και βίντεο μέσω διαδικτύου. Στόχος της εργασίας αυτής, είναι η παρακολούθηση και η ανίχνευση της δικτυακής κίνησης μιας εφαρμογής Voice over Internet Protocol (VoIP), της εφαρμογής Skype, μέσω του εργαλείου Wireshark.

4.1 Εφαρμογές VoIP Υπηρεσιών

Το Skype είναι μία εφαρμογή η οποία επιτρέπει την πραγματοποίηση των φωνητικών κλήσεων μέσω διαδικτύου. Οι κλήσεις μέσω Skype προς άλλους χρήστες, είναι δωρεάν. Η εφαρμογή αυτή δίνει τη δυνατότητα στους χρήστες να κάνουν ανταλλαγή άμεσων μηνυμάτων, αποστολή αρχείων και παρέχει την δυνατότητα χρήσης των υπηρεσιών συνδιάσκεψης. Η τεχνολογία που χρησιμοποιεί είναι το P2P(Peer-to-Peer)[8]

Επιπλέον, μία ακόμα εφαρμογή είναι το Msn Messenger. Η εφαρμογή αυτή παρέχει υπηρεσίες συνδιάσκεψης με βίντεο και φωνή σε πολλούς χρήστες ταυτόχρονα. Το βασικό της χαρακτηριστικό είναι ότι στηρίζεται στο πρωτόκολλο SIP[8].

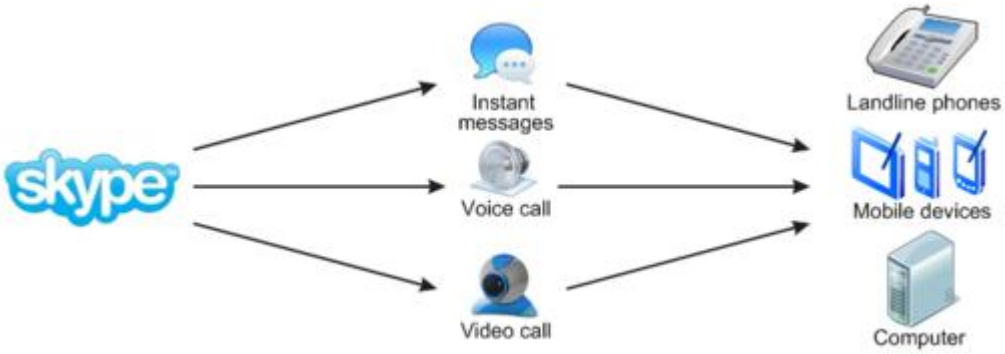
Τέλος, υπάρχουν και άλλες πολλές παρόμοιες εφαρμογές που χρησιμοποιούν την υπηρεσία VoIP. Κάποιες από αυτές είναι οι εξής: Asterisk, Yahoo Business Messenger, ICQ, VoipBuster, NetMeeting, Net2Phone, Firefly και Gnome-o-phone[8].

4.1.1 Peer-to-Peer(P2P)

Ένα δίκτυο υπολογιστών peer-to-peer(P2P) είναι ένα δίκτυο που επιτρέπει σε δύο ή περισσότερους υπολογιστές να μοιράζονται πόρους ισοδύναμα. Το δίκτυο αυτό χρησιμοποιεί την επεξεργαστική ισχύ, τον αποθηκευτικό χώρο και το εύρος ζώνης (bandwidth). Όλοι οι κόμβοι του δικτύου έχουν ίσα δικαιώματα, δηλαδή, πληροφορίες που υπάρχουν σε έναν κόμβο, ανάλογα με τα δικαιώματα που καθορίζονται, μπορούν να διαβαστούν από όλους τους άλλους και αντίστροφα[8].

Γενικά, η χρήση τέτοιων δικτύων ενώνει χρήστες από όλον τον κόσμο, λειτουργώντας χωρίς λογοκρισία, ελέγχους ή φραγμούς, προάγοντας τη βασική ιδέα του παγκόσμιου ιστού που δεν είναι άλλη από την ελευθερία ιδεών και τη δωρεάν παροχή υπηρεσιών και πληροφοριών. Η δομή αυτών των δικτύων είναι απλή και έχουν μηδαμινό κόστος. Αυτά τα δύο στοιχεία καθιστούν τη λειτουργία των P2P δικτύων μοναδική.

Επιπλέον, αυτά τα δίκτυα δίνουν την δυνατότητα της αντιγραφής και διανομής στοιχείων μεταξύ χρηστών, τα οποία προστατεύονται από πνευματικά δικαιώματα, όπως τραγούδια, ταινίες και λογισμικά, χωρίς τη συναίνεση του κατόχου των πνευματικών δικαιωμάτων. Γι αυτούς τους λόγους είναι επιθυμητά από εφαρμογές VoIP υπηρεσιών.



Σχήμα 10: Skype μέσω VoIP υπηρεσιών

4.2 Skype

Το Skype είναι μια εφαρμογή η οποία κυκλοφόρησε για πρώτη φορά το 2003. Σχεδιάστηκε από Εσθονούς προγραμματιστές τους Ahti Heinla, Pritt Kasesalu και Jaan Tallinn ο οποίος δημιούργησε το Kazaa, ένα πρόγραμμα ανταλλαγής αρχείων μεταξύ χρηστών[1].

Το Skype χρησιμοποιήθηκε από περισσότερους από 600 εκατομμύρια χρήστες και το 2011 αγοράσθηκε από τη Microsoft για 8,5 δισεκατομμύρια δολάρια και έχει την έδρα του στο Λουξεμβούργο. Ωστόσο, η Microsoft περνώντας τα χρόνια εξέλιξε τόσο πολύ την εφαρμογή ώστε

έγινε απαραίτητη από πολλούς χρήστες είτε για την ανταλλαγή πληροφοριών και αρχείων, είτε εν ώρα εργασίας για να μπορούν να επικοινωνήσουν μεταξύ τους[1].

Έτσι, δημιούργησε μια νέα ειδική έκδοση του Skype για επαγγελματίες (Skype for Business), η οποία θα είναι διαθέσιμη μέχρι το τέλος του Μαϊου 2015. Το γραφικό περιβάλλον του Skype θα είναι ακριβώς το ίδιο, με τη μόνη διαφορά ότι θα έχει ενσωματωμένο το Microsoft Office για την καλύτερη ενίσχυση και απόδοση του κάθε επαγγελματία. Με αυτόν τον τρόπο θα μπορεί ο χρήστης να εργάζεται και ταυτοχρόνως να μπορεί να πραγματοποιήσει κάποια βιντεοκλήση ακόμα και να γίνονται ομαδικές συσκέψεις[2].

Εικόνα 9: Λογότυπο Skype

4.3 Δυνατότητες και Χρήσεις Skype

Το Skype δίνει τη δυνατότητα στους χρήστες να επικοινωνούν με μέλη είτε από τον χώρο εργασίας τους είτε από τον φιλικό τους χώρο με τη χρήση ενός μικροφώνου και μίας κάμερα. Επιπλέον, μπορούν να ανταλλάσουν άμεσα γραπτά μηνύματα και να κάνουν ανταλλαγή αρχείων μέσω του Διαδικτύου[1].

Το Skype είναι μια από τις δημοφιλέστερες εφαρμογές VoIP (Voice over IP) που τη χρησιμοποιούν εκατομμύρια χρήστες σε όλον τον κόσμο. Ξεκίνησε έχοντας ως χρήση την επικοινωνία μεταξύ δύο ηλεκτρονικών υπολογιστών. Πλέον, οι δυνατότητες του Skype έχουν εξελιχθεί και δεν είναι μόνο ανταλλαγή μηνυμάτων αρχείων και κλήσεων, αλλά:

- Όσον αφορά τις κλήσεις:
  - Δωρεάν κλήσεις από χρήστες Skype, σε χρήστες παγκοσμίως
  - Κλήσεις προς σταθερά και κινητά με χαμηλές χρεώσεις
  - Ομαδικές κλήσεις

- Κλήσεις σε έναν αριθμό και απάντηση μέσω Skype οπουδήποτε στον κόσμο
- Προώθηση κλήσεων
- Αναγνώριση κλήσεως
- Διεθνείς κλήσεις με χαμηλές χρεώσεις

- Όσον αφορά τα βίντεο:
  - Βιντεοκλήσεις μεταξύ χρηστών
  - Ομαδικές βιντεοκλήσεις
- Όσον αφορά τα μηνύματα:
  - Βιντεομηνύματα
  - Αποστολή άμεσων μηνυμάτων
  - Αποστολή μηνυμάτων μέσω κινητού τηλεφώνου
  - Φωνητικά μηνύματα
  - Ομαδικά μηνύματα
- Όσον αφορά την κοινή χρήση μεταξύ μελών:
  - Ανταλλαγή αρχείων, φωτογραφιών
  - Κοινή χρήση οθόνης
  - Ομαδική κοινή χρήση οθόνης
  - Αποστολή επαφών[3].

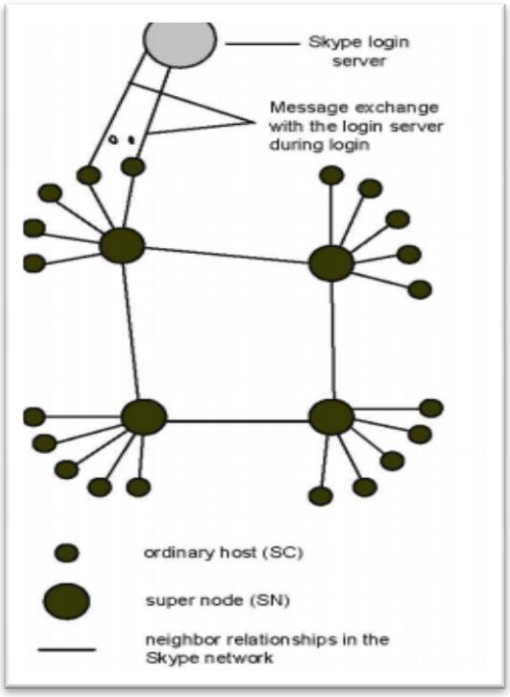
4.4 Διαδικασία Σύνδεσης Skype

Το Skype είναι ένας Peer-to-Peer client (P2P) υπηρεσίας VoIP το οποίο δημιουργήθηκε από το Kazaa, όπως προείπαμε. Όπως και το Kazaa που είναι και αυτό ένα πρόγραμμα P2P (μοιράσματος αρχείων), έτσι και το Skype χρησιμοποιεί ένα δικό του δίκτυο Peer-to-peer. Αυτό σημαίνει πως έχει δύο τύπους κόμβων, τους απλούς (SC) και τους υπερκόμβους (SN) [4].

Οι απλοί κόμβοι θεωρούνται ως μία εφαρμογή του Skype, η οποία τρέχει σε κάθε τερματικό του ηλεκτρονικού υπολογιστή με στόχο την προσφορά φωνητικών κλήσεων και αποστολή γραπτών μηνυμάτων σε χρήστες του ίδιου client[4].

Ωστόσο, κάθε κόμβος που έχει τη δυνατότητα να έχει δημόσια IP, δύναμη επεξεργασίας CPU, μνήμης και διεκπεραιότητας δικτύου, είναι ένας υπερκόμβος. Για να υπάρξει σύνδεση, θα πρέπει ο απλός κόμβος να έρθει σε επαφή με τον υπερκόμβο και να περάσουν από τον έλεγχο του Skype server[4].

Όμως, πέρα από τους κόμβους, υπάρχει και ο Skype Login Server στον οποίο αποθηκεύονται όλα τα ονόματα των χρηστών του Skype, με σκοπό τη σύνδεσή του με τους απλούς κόμβους (SC) και τους υπερκόμβους (SN)[4].



Εικόνα 10: Δίκτυο Skype. Υπερκόμβοι, απλοί κόμβοι και login servers[4].

Το δίκτυο του Skype είναι ένα εικονικό δίκτυο και γι' αυτό τον λόγο κάθε client θα πρέπει να δημιουργεί ανά τακτά χρονικά διαστήματα έναν πίνακα (Host Cache (HC)) με τους κόμβους με τους οποίους συνδέεται για λόγους ασφαλείας. Επίσης, χρησιμοποιεί πολλούς κωδικοποιητές (iLBC, iSAC, iPCM) οι οποίοι προσφέρουν καλή διατήρηση ποιότητας κλήσεων και λειτουργούν με εύρος 32 kb/sec[4].

Επιπρόσθετα, το Skype χρησιμοποιεί τα πρωτόκολλα TCP και UDP. Το TCP το χρησιμοποιεί για εύρεση σήματος και όταν χρειάζεται να κάνει μεταφορά δεδομένων, χρησιμοποιεί και το TCP και το UDP. Ωστόσο, ένας client Skype, ανοίγει μία πόρτα TCP και μία UDP για οποιονδήποτε εισερχόμενο αριθμό. Η επιλογή του αριθμού της πόρτας, γίνεται τυχαία κατά τη διαδικασία της εγκατάστασης. Συνήθως, για το TCP ανοίγει τις port 80 και port 443, των οποίων η χρήση είναι για αιτήσεις από HTTP και HTTP-over-TLS[4].

4.4.1 Πρωτόκολλο UDP

Το UDP (User Datagram Protocol) είναι ένα από τα βασικότερα πρωτόκολλα που χρησιμοποιεί το Διαδίκτυο. Χρησιμοποιείται για την αποστολή μηνυμάτων από έναν υπολογιστή σε έναν άλλον. Ένα από τα χαρακτηριστικά του είναι ότι δεν παρέχει αξιοπιστία στην επικοινωνία του. Κατά την αποστολή των πακέτων, ο παραλήπτης μπορεί να λάβει τα πακέτα είτε με λάθος σειρά ή διπλά ή αρκετές φορές να μην φτάσουν και καθόλου όταν το δίκτυο είναι υπερφορτωμένο[12].

Κατά κύριο λόγο χρησιμοποιείται από εφαρμογές που δεν τους ενδιαφέρει τόσο η αξιοπιστία, όσο το να μην υπάρχει διακοπή στη ροή ήχου και εικόνας. Είναι ένα αρκετά γρήγορο πρωτόκολλο παρ' όλο που υπάρχει πιθανότητα να χαθούν πακέτα. Ωστόσο, οι εφαρμογές αυτές, διαθέτουν μηχανισμούς διόρθωσης και αποκατάστασης των πακέτων, ώστε ο παραλήπτης να μην παρατηρεί καμία αλλοίωση[12].

4.4.2 Πρωτόκολλο TCP

Το TCP (Transmission Control Protocol) είναι ένα πρωτόκολλο ελέγχου Μεταφοράς το οποίο βρίσκεται πάνω από το IP πρωτόκολλο. Στόχος του είναι να επιβεβαιώνει την αξιοπιστία της αποστολής και λήψης πακέτων, τα οποία θα πρέπει να μεταφέρονται σωστά χωρίς λάθη και με σωστή σειρά.

Το πρωτόκολλο TCP παίζει σημαντικό ρόλο στην διαχείριση της δικτυακής κίνησης. Γι αυτό τον λόγο, είναι υπεύθυνο για τις παρακάτω ενέργειες:

- Διαίρεση των μηνυμάτων σε διαχειρίσιμα τμήματα δεδομένων, που θα μπορούν να περάσουν με αποτελεσματικό τρόπο από το υλικό μετάδοσης του δικτύου.
- Διασύνδεση με το υλικό του προσαρμογέα δικτύου.
- Διευθυνσιοδότηση: ο υπολογιστής αποστολής πρέπει να είναι ικανός να κατευθύνει τα δεδομένα σε έναν υπολογιστή λήψης. Ο υπολογιστής λήψης θα πρέπει να είναι ικανός να αναγνωρίσει ένα τμήμα που λαμβάνει.
- Δρομολόγηση των δεδομένων στο υποδίκτυο προορισμού, ακόμα και αν το υποδίκτυο προέλευσης και το υποδίκτυο προορισμού είναι ανόμοια δίκτυα.
- Εκτελεί έλεγχο λαθών, έλεγχο ροής και γνωστοποίηση: για να υπάρχει αξιόπιστη επικοινωνία, οι υπολογιστές αποστολής και λήψης θα πρέπει να μπορούν να προσδιορίζουν και να διορθώνουν λανθασμένες μεταδόσεις και να ελέγχουν τη ροή των δεδομένων.
- Αποδοχή δεδομένων από μια εφαρμογή και πέρασμά τους στο δίκτυο.
- Λήψη δεδομένων από το δίκτυο και πέρασμά τους σε μια εφαρμογή[15].

4.4.3 NAT και Firewall

Το NAT (Network Address Translation) είναι η διαδικασία κατά την οποία μία συσκευή δικτύου δίνει μία δημόσια διεύθυνση σε έναν υπολογιστή μέσα σε ένα ιδιωτικό δίκτυο. Η βασική του χρήση είναι ο περιορισμός των δημοσίων διευθύνσεων IP που πρέπει να χρησιμοποιούνται για λόγους οικονομίας και ασφάλειας[13].

Ένα ιδιωτικό δίκτυο χρησιμοποιεί διευθύνσεις από το εύρος 10.0.0.0 εώς 10.255.255.255, 172.16.0.0 εώς 172.31.255.255 ή από 192.168.0.0 εώς 192.168.255.255. Οι ιδιωτικές αυτές διευθύνσεις λειτουργούν καλά για τους υπολογιστές που έχουν πρόσβαση σε πόρους εντός του δικτύου. Για πόρους εκτός δικτύου, οι υπολογιστές θα πρέπει να έχουν μία δημόσια διεύθυνση προκειμένου να μπορούν να απαντήσουν σε αιτήσεις και να τις επιστρέψουν. Σε αυτό το σημείο βοηθάει το NAT[13].

Οι συσκευές NAT γενικά αντιστοιχούν IP διευθύνσεις από αυτό τα ιδιωτικό εύρος. Για να καταφέρει ένας χρήστης να φτάσει στον υπολογιστή ενός πελάτη NAT, θα πρέπει να το κάνει μέσω της διαδικασίας μετάφρασης διευθύνσεων. Η διαμόρφωση λιγότερων διευθύνσεων Internet, μαζί με την ασφάλεια ενός ιδιωτικού δικτύου, κάνουν τις συσκευές NAT να είναι πολύ δημοφιλείς σε οικιακά και εταιρικά δίκτυα[15].

Ωστόσο, πολλές φορές δεν είναι αυτό που φαίνεται. Ακόμα και οι πολύ ασφαλείς συσκευές μπορούν να παραβιαστούν. Οι συσκευές NAT έχουν μερικές φορές, ειδικές λειτουργίες για να παρέχουν πρόσβαση διαχειριστή από το Internet και αυτές οι λειτουργίες παρουσιάζονται όταν δεν είναι κλειδωμένες. Ένας συνηθισμένος τρόπος για να μπαίνουν εισβολείς μέσα σε ένα ιδιωτικό δίκτυο, είναι να κάνουν τον πελάτη να τους προσκαλέσει. Οι σύγχρονοι εισβολείς στέλνουν συνδέσεις σε ψεύτικες ιστοσελίδες και στήνουν παγίδες για να προσελκύσουν το χρήστη ώστε να ξεκινήσει μία σύνδεση σε ένα συνωμοτικό διακομιστή[15].

Ένας σταθμός εργασίας μέσα σε ένα δίκτυο στέλνει μία αίτηση σε έναν υπολογιστή στο Internet, οι δρομολογητές εντός του δικτύου αναγνωρίζουν ότι η αίτηση είναι εκτός δικτύου και στέλνεται αίτημα για τείχος προστασίας. Το firewall βλέπει το αίτημα από τον υπολογιστή με την εσωτερική IP. Έπειτα, κάνει το ίδιο αίτημα στο Internet χρησιμοποιώντας την δική της δημόσια διεύθυνση και έρχεται απάντηση από τον πόρο του διαδικτύου στον υπολογιστή μέσα στο ιδιωτικό δίκτυο. Από την πλευρά του πόρου στο διαδίκτυο, φαίνεται ότι αυτό στέλνει πληροφορίες στη διεύθυνση του τείχους προστασίας. Από την πλευρά όμως του σταθμού εργασίας, φαίνεται ότι η επικοινωνία με την ιστοσελίδα στο διαδίκτυο, είναι άμεση[13].

Τα περισσότερα Firewalls ρυθμίζουν τη σύνδεση της εσωτερικής εργασίας και του διαδικτύου. Έτσι, γίνεται εύκολα να παρακολουθούνται τα ports, τα πακέτα καθώς και οι IP διευθύνσεις που χρησιμοποιούνται. Κατά τον τερματισμό του τείχους προστασίας, όλες οι πληροφορίες σχετικά με τη

σύνδεση, απορρίπτονται[13].

Τα προσωπικά Firewall και άλλα μικρής κλίμακας εργαλεία βασισμένα σε γραφικό περιβάλλον, επιτρέπουν να οριστούν τα χαρακτηριστικά φιλτραρίσματος του firewall, επιλέγοντας συνήθως διάφορα πλαίσια ελέγχου. Ωστόσο, τα επαγγελματικά firewall δίνουν την δυνατότητα να μπορεί να δημιουργηθεί ένα αρχείο διαμόρφωσης όπου θα υπάρχουν εντολές ή κανόνες που ορίζουν την συμπεριφορά του τείχους προστασίας[15].

Κάθε τείχος προστασίας χρησιμοποιεί διαφορετικές εντολές και σύνταξη αλλά οι κανόνες επιτρέπουν στους διαχειριστές, ανεξάρτητα από το τι τείχος προστασίας υπάρχει, να δημιουργούν συσχετίσεις που αποτελούνται από μία διεύθυνση προέλευσης ή ένα εύρος διευθύνσεων, ένα εύρος διευθύνσεων προορισμού, μια υπηρεσία και μία ενέργεια. Οι παράμετροι αυτοί παρέχουν ένα μεγάλο εύρος επιλογών. Έτσι, μπορεί να γίνει απόκλιση της κίνησης από ή προς συγκεκριμένο εύρος διευθύνσεων, μπορεί να γίνει απόκλιση μίας συγκεκριμένης υπηρεσίας, όπως το Telnet ή το FTP, η οποία έρχεται από μία συγκεκριμένη διεύθυνση. Επίσης, μπορεί να γίνει απόκλιση μιας υπηρεσίας που έρχεται από όλες τις διευθύνσεις[15].

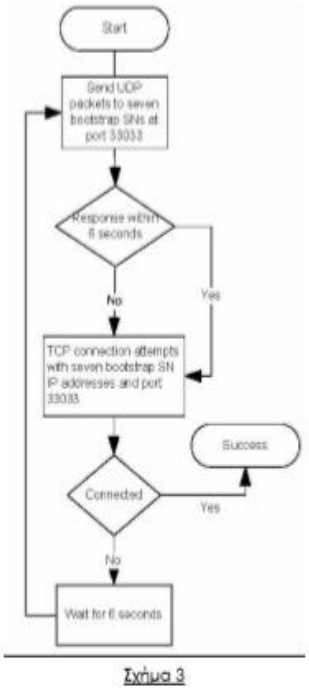
Αρκετές φορές οι κανόνες που λαμβάνει ένα τείχος προστασίας μπορεί να αφορά κάποια επέκτασή του, ή κάποιο script, ή μπορεί να είναι μία προειδοποίηση που στέλνει σελίδες ή μηνύματα ηλεκτρονικού ταχυδρομείου στον διαχειριστή του firewall, σε περίπτωση προβλήματος[15].

4.5 Σύνδεση Skype

Κατά τη διάρκεια της σύνδεσης, το Skype κάνει αυθεντικοποίηση του ονόματος του χρήστη και του κωδικού μέσα στο login server. Επιπλέον, προσδιορίζει το NAT (Network Address Translation) και το Firewall, ψάχνει για κόμβους που είναι συνδεδεμένοι με δημόσιες IP διευθύνεις και ελέγχει τη διαθεσιμότητα ροής τελευταίας έκδοσης του Skype[4].

Παρακάτω, έχουμε ένα πείραμα διαδικασίας σύνδεσης του Skype, όπου ο client στέλνει ένα πακέτο μήκους 18 bytes σε κάθε εναλλακτική IP διεύθυνση που βρήκε στην πόρτα 33033. Αν

δεν πάρει απάντηση μέσα σε 5 δευτερόλεπτα, τότε προσπαθεί να κάνει σύνδεση TCP σε κάθε μία από αυτές τις IP διευθύνσεις στην ίδια πόρτα. Αν υπάρχει αποτυχία σύνδεσης, τότε ξαναπροσπαθεί μετά από 6 δευτερόλεπτα[4].



Εικόνα 11: Πείραμα Διαδικασίας Σύνδεσης στο Skype[4].

ΕΝΟΤΗΤΑ 5

ΑΝΑΛΥΣΗ ΔΙΚΤΥΑΚΗΣ ΚΙΝΗΣΗΣ SKYPE

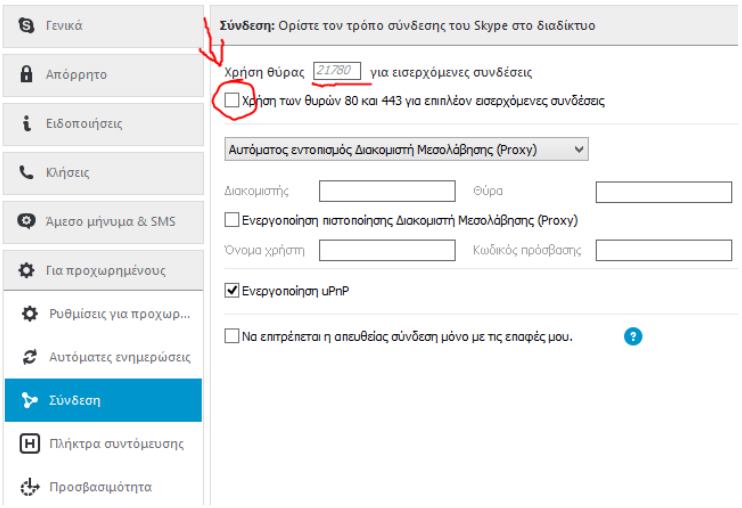
Στην ενότητα αυτή γίνεται ανάλυση της δικτυακής κίνησης της εφαρμογής Skype μέσω του εργαλείου Wireshark. Μέσω των αποτελεσμάτων που θα πάρουμε, θα κάνουμε ανάλυση των παραγόντων που επηρεάζουν την απόδοση της ποιότητας των υπηρεσιών και συμβάλλουν στην καλή λειτουργία των VoIP κλήσεων.

5.1 Σύνδεση Skype με Wireshark

Πρώτα από όλα θα πρέπει να εγκαταστήσουμε στον υπολογιστή μας τα δύο αυτά προγράμματα. Μέσω της διεύθυνσης www.skype.com και κάνοντας λήψη, κάνουμε εγκατάσταση του εργαλείου Skype στον υπολογιστή μας. Η εγκατάστασή του είναι αρκετά εύκολη. Έπειτα, από την διεύθυνση www.wireshark.com εγκαθιστούμε το εργαλείο wireshark.

Μόλις εγκαταστήσουμε το Skype, θα πρέπει να κάνουμε μία ρύθμιση. Πατάμε εργαλεία → Επιλογές → για προχωρημένους → σύνδεση, ξετσεκάρουμε την επιλογή «Χρήση των θυρών 80 και 443 για επιπλέον εισερχόμενες συνδέσεις και σημειώνουμε τον αριθμό της θύρας που υπάρχει ακριβώς από

πάνω. Έπειτα κάνουμε επανεκκίνηση του Skype[11].

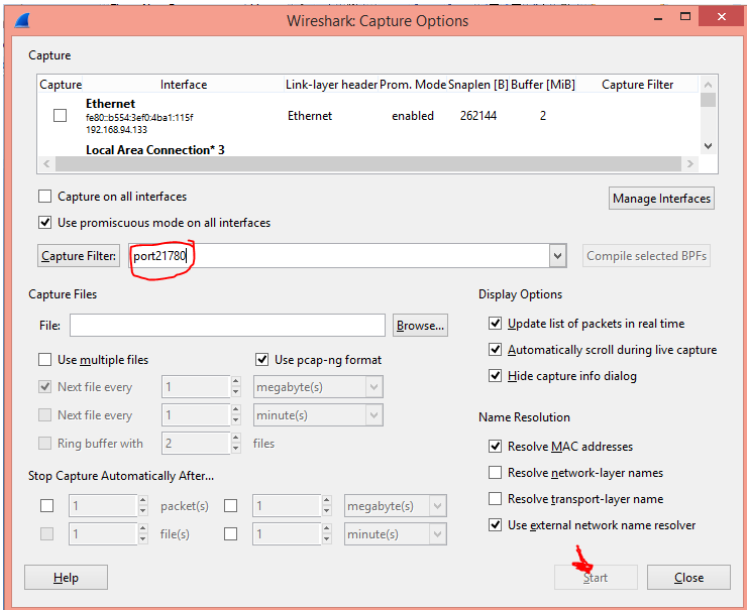


Εικόνα 12: Ρύθμιση Θυρών στο Skype

Η συγκεκριμένη ρύθμιση γίνεται στην περίπτωση που υπάρχει τείχος προστασίας (firewall) μεταξύ του υπολογιστή και του διαδικτύου και δεν επιτρέπει τη σύνδεση θυρών παρά μόνο μεταξύ ενός συγκεκριμένου εύρους[11].

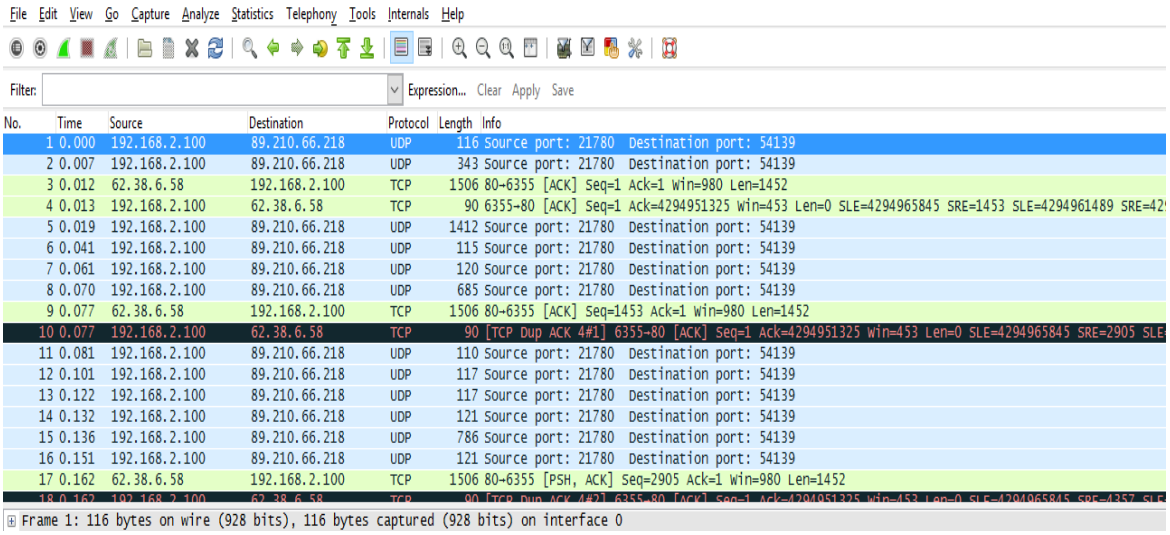
Έχοντας ήδη σημειώσει τον αριθμό της θύρας, μέσω του command window και πληκτρολογώντας την εντολή ipconfig, εμφανίζεται η IP address του υπολογιστή η οποία επίσης πρέπει να σημειωθεί.

Στην πορεία ανοίγοντας το wireshark για να εμφανίζεται μόνο η δικτυακή κίνηση του skype, πρέπει στο Capture Options να εισαχθεί ένα capture filter, το οποίο είναι ο αριθμός της θύρας που σημειώθηκε, και η σύνδεση δικτύου και πατάμε Start[11].



Εικόνα 13: Ρύθμιση Capture Filter.

Μόλις το Wireshark ξεκινήσει να εκτελείτε, έκανα μία κλήση σε άλλον χρήστη του Skype για 40sec και αυτό άρχισε να καταγράφει τα δεδομένα της κλήσης. Έχοντας IP: 192.168.2.100 και port: 21780 και ο άλλος χρήστης με IP: 192.168.1.5 και port: 54139, πήραμε τα παρακάτω αποτελέσματα.

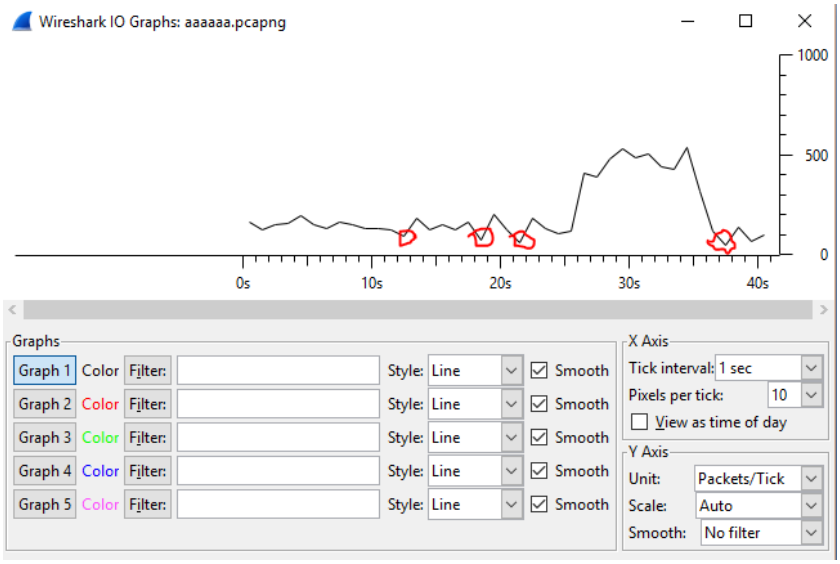


Εικόνα 14: Αποτελέσματα εκτέλεσης Wireshark.

5.2 Ανάλυση Αποτελεσμάτων Εκτέλεσης Wireshark

Μέσω των παραπάνω αποτελεσμάτων, θα πρέπει να αναλυθούν: το Latency(αδράνεια), το Jitter(διακύμανση) καθώς και το Packet Loss(Απώλεια Πακέτων), που επηρεάζουν την καθυστέρηση

και την ποιότητα των υπηρεσιών. Για την καλύτερη ανάλυση των στοιχείων δημιουργήσαμε το παρακάτω γράφημα ακολουθώντας τα παρακάτω βήματα: Statistics → IO Graph



Σχήμα 11: Αποτελέσματα Wireshark σε γράφημα.

Στο παραπάνω γράφημα εμφανίζεται η ροή των πακέτων σε συναρτήσει με τον χρόνο. Οι κόκκινοι κύκλοι εμφανίζουν τα προβλήματα τα οποία δημιουργούνται τις συγκεκριμένες χρονικές στιγμές κατά την μετάδοση των πακέτων.

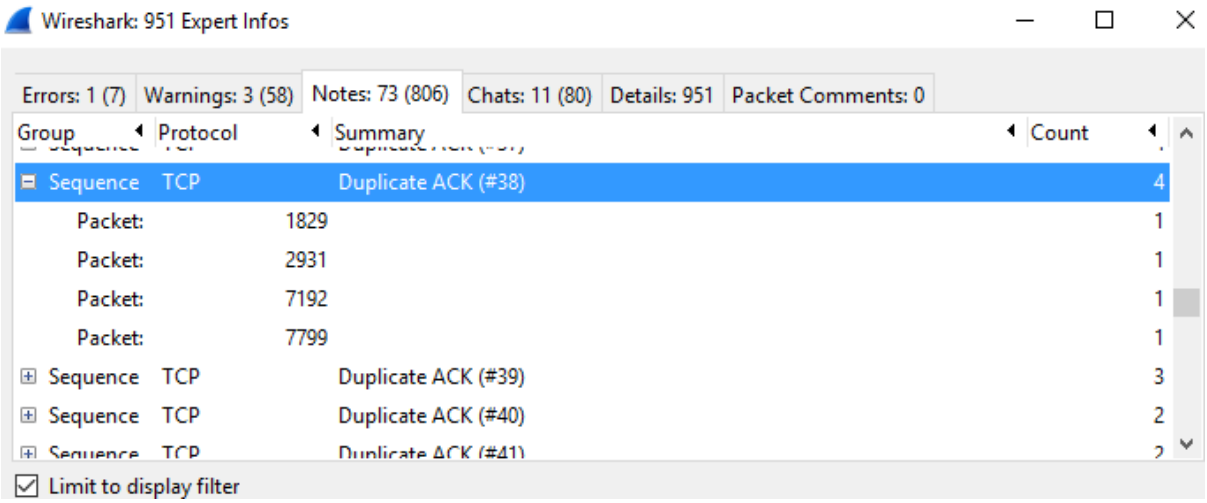
Όταν ένα δίκτυο είναι αργό ή υπάρχει πρόβλημα στη σύνδεση, η επικοινωνία μεταξύ των χρηστών έχει υψηλά ποσοστά αδράνειας (high Latency), αν η σύνδεση είναι γρήγορη τότε τα ποσοστά αδράνειας είναι μικρά (low Latency), όπου είναι και το ζητούμενο. Όταν η αδράνεια είναι μεγάλη, τότε υπάρχει μεγάλη καθυστέρηση παράδοσης πακέτων και αρκετές φορές υπάρχουν και απώλειες πακέτων (Packet Loss). Αυτό συμβαίνει είτε εξαιτίας το router που είναι συνδεδεμένο γιατί μπορεί να έχει μεγάλο όγκο δεδομένων, είτε γιατί γίνεται διακοπή υπηρεσιών.

Όταν συμβαίνει κάποιο από τα παραπάνω, το TCP ανιχνεύει το πρόβλημα και προχωρά στην επίλυση του. Ξεκινά κάνοντας αναμετάδοση των πακέτων κρίνοντας αυτό αν χρειάζεται με βάση το χρονικό όριο αναμετάδοσης (RTO) που λαμβάνει. Αν για κάθε πακέτο που θα σταλθεί, δεν ληφθεί ένα ACK,μέσα στο χρονικό όριο που πρέπει να αναμεταδοθεί, τότε το TCP προχωρά στην αναμετάδοση του πακέτου. Ο χρόνος μεταξύ των δύο πακέτων ονομάζεται round-trip time (RTT). Κάθε φορά που συμβαίνει μια αναμετάδοση, το χρονικό όριο(RTO), διπλασιάζεται με αποτέλεσμα το TCP να προχωρά σε αποστολή Duplicate ACKs.

Όλες οι συνδέσεις TCP ξεκινούν με έναν αριθμό ακολουθίας ISN. Για παράδειγμα, όταν ο υπολογιστής μου έχει αρχικό ISN=1000 και εγώ θα στείλω ένα πακέτο 200byte, η αναγνώριση που θα πρέπει να γίνει είναι ISN=1200 κ.ο.κ. Έτσι, όταν το νέο μου ISN είναι 1200, αλλά ο υπολογιστής

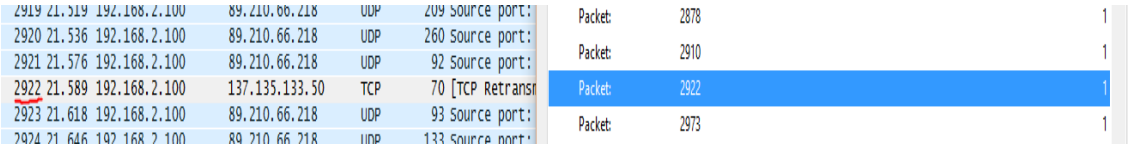
πηδά και στέλνει ένα πακέτο με ISN=1400, ο προορισμός καταλαβαίνει ότι κάτι είναι λάθος και στέλνει πίσω ένα duplicate ACK για το πακέτο με ISN=1200. Την διαδικασία αυτήν, θα την επαναλάβει όσες φορές χρειαστεί μέχρι να ληφθεί το σωστό πακέτο.

Στο γράφημα, είναι κυκλωμένες οι χρονικές στιγμές κατά τις οποίες το TCP κάνει αναμετάδοση(retransmission) ή αποστολή duplicate ACKs. Για παράδειγμα, την χρονική στιγμή 13sec περίπου, το TCP στέλνει Duplicated ACKs. Χρειάστηκε να γίνει 4 φορές ώστε να παραδοθούν τα δεδομένα σωστά μέσω των πακέτων 1829, 2931, 7192 και 7799.



Εικόνα 15: Duplicated ACKs

Επιπλέον, με βάση το γράφημα θα δούμε ότι την χρονική στιγμή των 22sec περίπου, υπάρχει πάλι πρόβλημα. Το TCP βρίσκει πρόβλημα στο πακέτο 2922 και κάνει αναμετάδοση του. Οι φορές που χρειάστηκαν για να αναμεταδοθεί σωστά είναι μία.



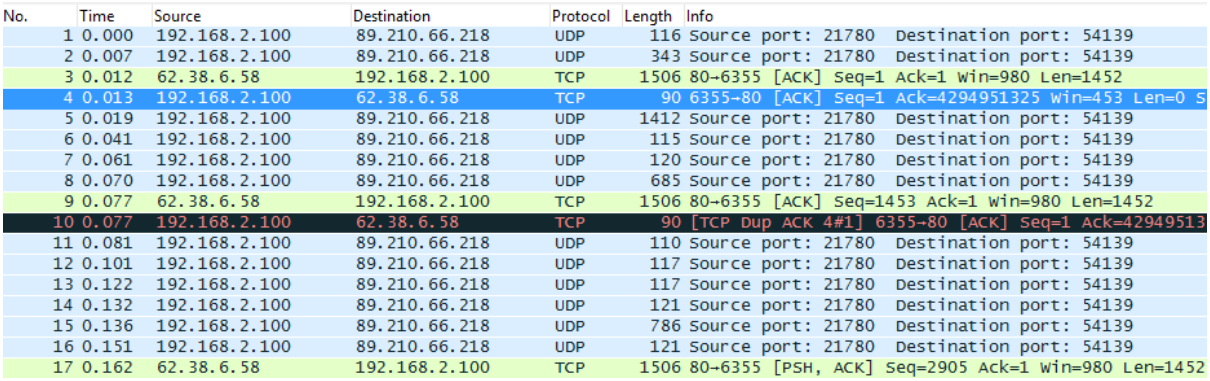
Εικόνα 16: Retransmission (Αναμετάδοση Πακέτων).

Όπως προείπαμε, τα τρία βασικά στοιχεία που παίζουν ρόλο στην ποιότητα των υπηρεσιών και στην καθυστέρηση των πακέτων, είναι η αδράνεια, η διακύμανση και η απώλεια πακέτων. Κοιτάζοντας τα αποτελέσματα του Wireshark μετά την κλήση στο Skype, διαπιστώνουμε ότι το πρώτο TCP πακέτο είναι το πακέτο με αριθμό 3. Για να καταλάβουμε καλύτερα τον χρόνο που μας δείχνει, επιλέγουμε View → Time Display Format → Milliseconds 0,123.

Έτσι, μπορούμε να διαπιστώσουμε ότι ο χρόνος για το πακέτο 3 ως το πακέτο 4, όπου είναι το round-trip time (RTT), είναι 13msec. Το RTT είναι ίσο με το Latency (αδράνεια). Άρα το Latency είναι

13msec.

Γενικότερα, το Latency είναι ο τρόπος για να καταλάβουμε αν μία VoIp κλήση, αλληλεπιδρά με την άλλη. Ουσιαστικά, είναι η καθυστέρηση ενός πακέτου, δηλαδή, πόσο χρόνο θα κάνει το πακέτο από την είσοδο του μέχρι το καθορισμένο σημείο. Στις συνδέσεις, όταν το Latency είναι λιγότερο από 100msec, τότε θεωρούνται αδρανείς ή τυπικές, όταν είναι λιγότερο από 25msec, τότε έχουμε το επιθυμητό αποτέλεσμα. Στο παράδειγμα μας, το Latency είναι 13 msec. Επομένως, η καθυστέρηση των πακέτων είναι αρκετά μικρή.



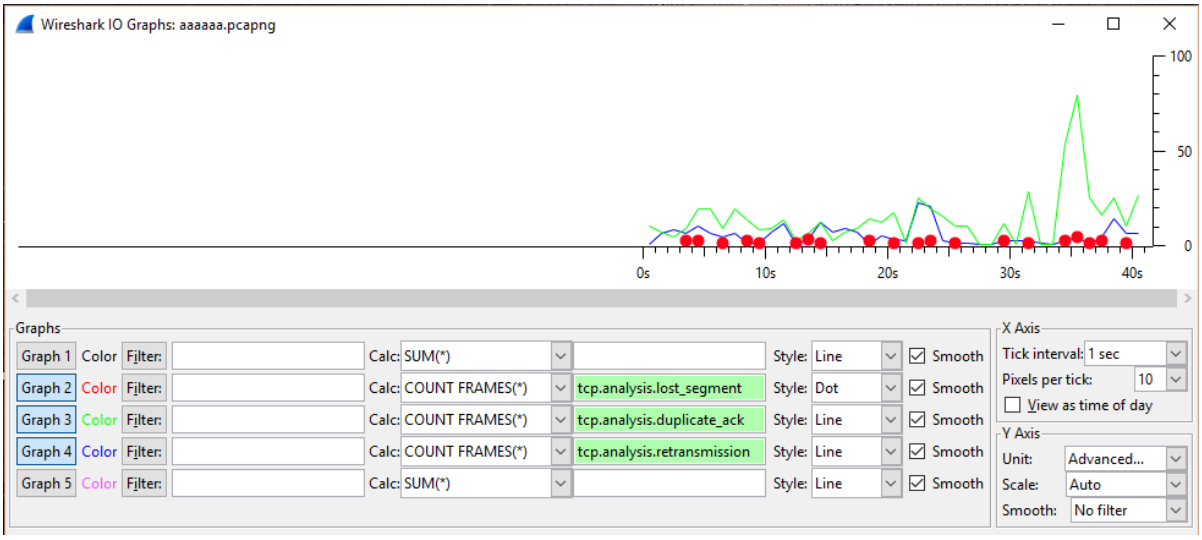
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000	192.168.2.100	89.210.66.218	UDP	116	Source port: 21780 Destination port: 54139
2	0.007	192.168.2.100	89.210.66.218	UDP	343	Source port: 21780 Destination port: 54139
3	0.012	62.38.6.58	192.168.2.100	TCP	1506	80→6355 [ACK] Seq=1 Ack=1 Win=980 Len=1452
4	0.013	192.168.2.100	62.38.6.58	TCP	90	6355→80 [ACK] Seq=1 Ack=4294951325 Win=453 Len=0 S
5	0.019	192.168.2.100	89.210.66.218	UDP	1412	Source port: 21780 Destination port: 54139
6	0.041	192.168.2.100	89.210.66.218	UDP	115	Source port: 21780 Destination port: 54139
7	0.061	192.168.2.100	89.210.66.218	UDP	120	Source port: 21780 Destination port: 54139
8	0.070	192.168.2.100	89.210.66.218	UDP	685	Source port: 21780 Destination port: 54139
9	0.077	62.38.6.58	192.168.2.100	TCP	1506	80→6355 [ACK] Seq=1453 Ack=1 Win=980 Len=1452
10	0.077	192.168.2.100	62.38.6.58	TCP	90	[TCP Dup ACK 4#1] 6355→80 [ACK] Seq=1 Ack=42949513
11	0.081	192.168.2.100	89.210.66.218	UDP	110	Source port: 21780 Destination port: 54139
12	0.101	192.168.2.100	89.210.66.218	UDP	117	Source port: 21780 Destination port: 54139
13	0.122	192.168.2.100	89.210.66.218	UDP	117	Source port: 21780 Destination port: 54139
14	0.132	192.168.2.100	89.210.66.218	UDP	121	Source port: 21780 Destination port: 54139
15	0.136	192.168.2.100	89.210.66.218	UDP	786	Source port: 21780 Destination port: 54139
16	0.151	192.168.2.100	89.210.66.218	UDP	121	Source port: 21780 Destination port: 54139
17	0.162	62.38.6.58	192.168.2.100	TCP	1506	80→6355 [PSH, ACK] Seq=2905 Ack=1 Win=980 Len=1452

Εικόνα 17: Καθυστέρηση Πακέτων (Latency)

Ωστόσο, στη συνέχεια καταγραφής των πακέτων στο Wireshark κατά την διάρκεια της κλήσης, η τιμή του Latency αυξήθηκε χωρίς όμως να ξεπερνάει τα 100msec. Η τιμή του κυμαινόταν από 25 ως 40msec. Αυτό συνέβαινε γιατί η σύνδεση του δικτύου δεν ήταν αρκετά καλή.

Ένας ακόμα λόγος που επηρεάζει την ποιότητα των υπηρεσιών, όπως προείπαμε, είναι η απώλεια πακέτων (packet loss). Η απώλεια πακέτων, συμβαίνει συνήθως όταν ο δρομολογητής λαμβάνει περισσότερα πακέτα από αυτά που μπορεί να μεταδώσει ή επειδή το λογισμικό είναι ελαττωματικό και ¨ξεχνάει¨ να αποστείλει πακέτα.

Στο Wireshark υπάρχουν φίλτρα τα οποία μας επιτρέπουν να δούμε την απώλεια των πακέτων, τις αναμεταδόσεις καθώς και τα duplicate Acks. Για να δούμε τις αναμεταδόσεις, χρησιμοποιούμε το φίλτρο tcp.analysis.retransmission, για τα duplicated Acks το tcp.analysis.duplicate_ack και για τα πακέτα που χάθηκαν, το φίλτρο tcp.analysis.lost_segment.

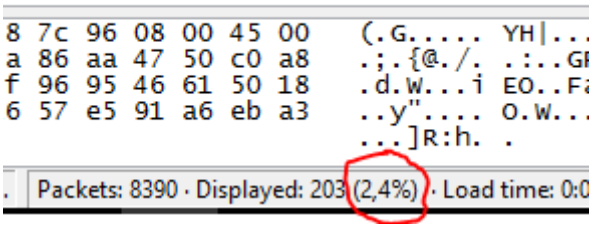


Σχήμα 12: Γράφημα για απώλεια πακέτων

Στο παραπάνω γράφημα, τοποθετήσαμε τα φίλτρα που προαναφέραμε και πήραμε τα αποτελέσματα. Με τις κόκκινες κουκίδες παρουσιάζεται η απώλεια των πακέτων, με την πράσινη γραμμή τα Duplicate Acks και με την μπλε γραμμή οι αναμεταδόσεις. Όπως φαίνεται και στο σχήμα, οι απώλειες πακέτων είναι σχεδόν μηδέν. Αυτό συμβαίνει γιατί οι απώλειες παρουσιάστηκαν μεταξύ πελάτη και διακομιστή με αποτέλεσμα να μην μπορούμε να τις υπολογίσουμε. Αν λάβουμε τα πακέτα του αποστολέα, τότε θα δούμε τα αρχικά πακέτα καθώς και τις αναμεταδόσεις που έγιναν. Αν λάβουμε τα πακέτα του παραλήπτη, δεν θα δούμε τα πακέτα που χάθηκαν αρχικά, αλλά μόνο τις αναμεταδόσεις των πακέτων.

Γενικότερα, η απώλεια των πακέτων θα πρέπει να είναι μικρότερη από 10%, διαφορετικά τα πακέτα δεν παραδίδονται διαδοχικά, με αποτέλεσμα να έχουμε κακή σύνδεση.

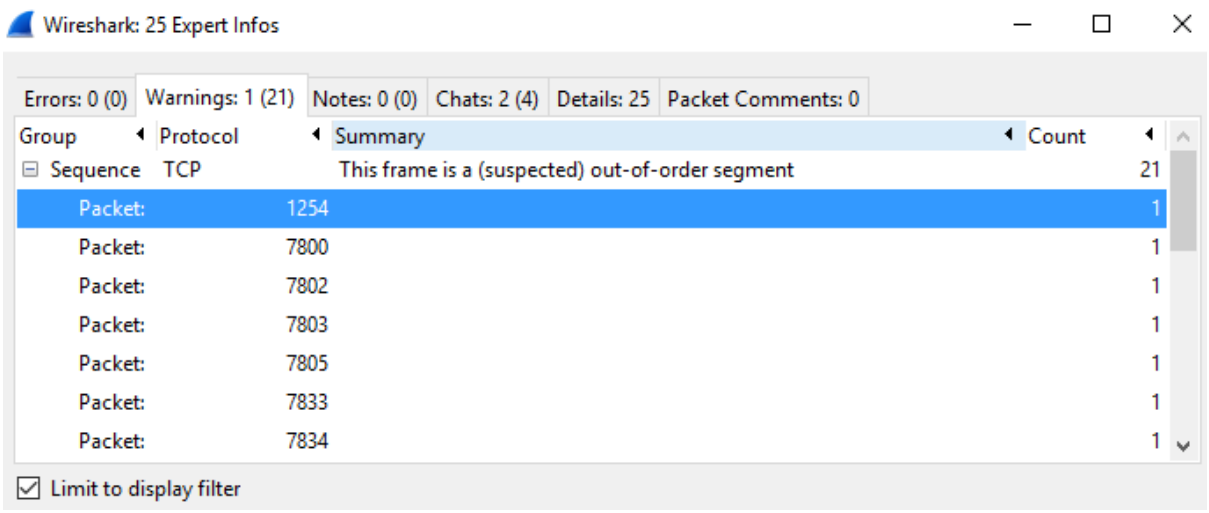
Στην συγκεκριμένη περίπτωση η απώλεια πακέτων είναι 0% και τα ποσοστά των αναμεταδόσεων και των Duplicate Acks είναι 2.4%. Αυτό σημαίνει ότι η σύνδεση είναι καλή, όπως και η ποιότητα των υπηρεσιών.



Εικόνα 18: Ποσοστά αναμετάδοσης και Duplicate Acks

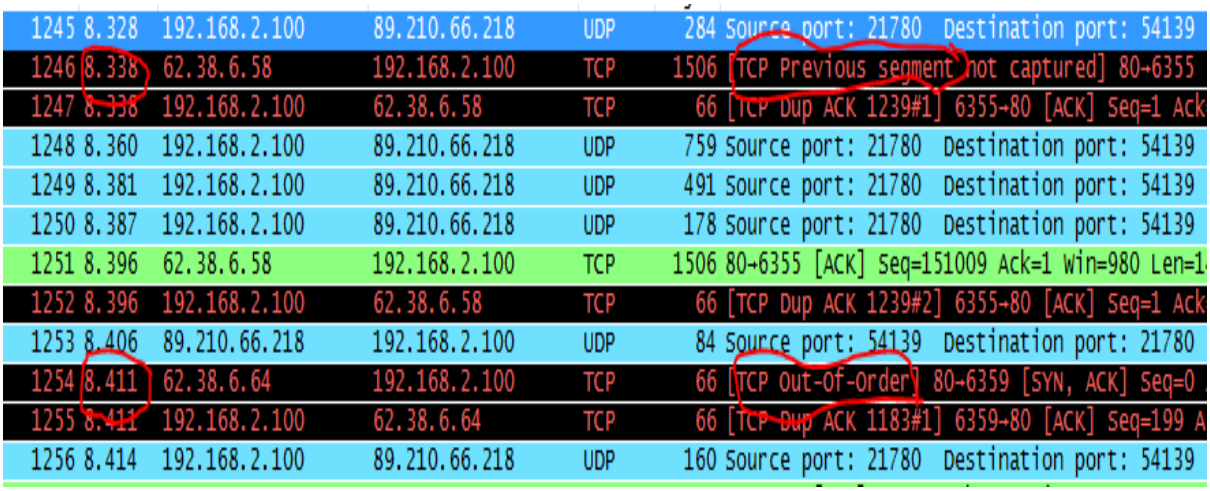
Ωστόσο, εκτός από τις αναμεταδόσεις και τα Duplicate Acks, υπάρχουν και τα πακέτα out-of order τα

οποία δηλώνουν ότι υπάρχει απώλεια πακέτων. Στην κατηγορία αυτή, κατατάσσονται τα πακέτα τα οποία παραδίδονται με διαφορετική σειρά από αυτή που στάλθηκαν. Το TCP πρέπει να τα αναγνωρίσει και να κάνει επίλυση του προβλήματος, είτε με την αντικατάστασή τους είτε να αποτρέψει την παράδοση τους. Για να μην υπάρξει απώλεια πακέτων, τα πακέτα αυτά θα πρέπει να αντικατασταθούν και να επαναμεταδοθούν μέσα σε 3ms. Για να βρούμε τα πακέτα αυτά, βάζουμε ως φίλτρο το tcp.analysis.out_of_order. Μέσω του expert Infos λαμβάνουμε τα παρακάτω αποτελέσματα:



Εικόνα 19: Out-of-Order Packets

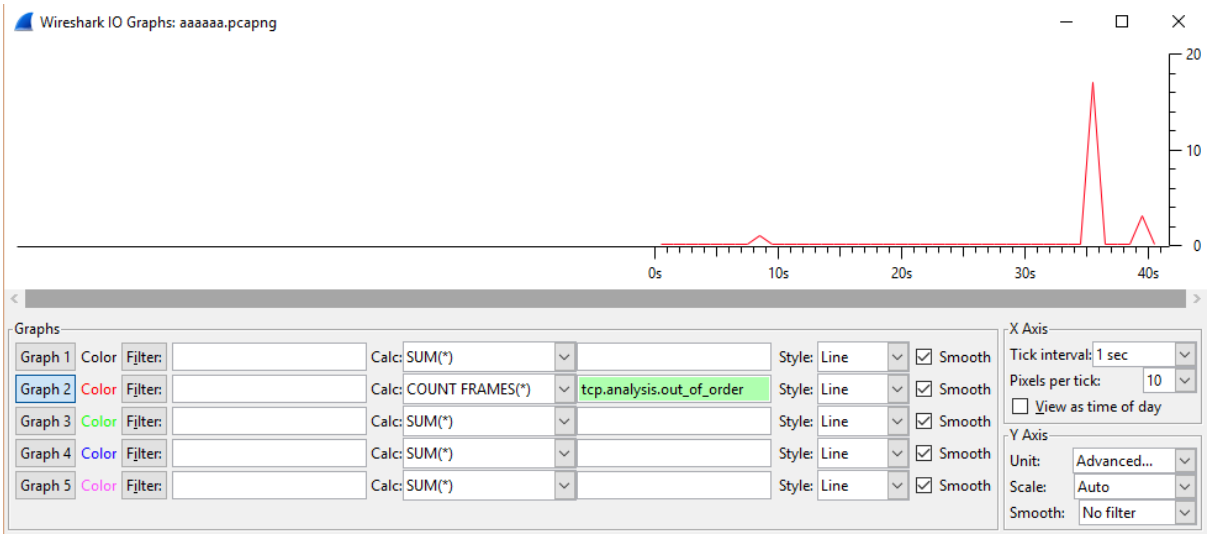
Από τη λίστα επιλέγουμε το πακέτο με αριθμό 1254.



Εικόνα 20: Παράδειγμα Out-Of-Order Packet

Όπως θα παρατηρήσουμε, το προηγούμενο πακέτο από το 1254 είναι το 1246. Ο χρόνος μεταξύ τους ανέρχεται στα 73microseconds. Αυτό σημαίνει ότι είναι μέσα στο χρονικό όριο των 3ms,επομένως, δεν έχουμε απώλεια πακέτων αλλά επίλυση του προβλήματος. Όπως φαίνεται και στο παρακάτω

γράφημα, οι περιπτώσεις των Out-Of-Order πακέτων είναι ελάχιστες και το TCP αντικαθιστά το πρόβλημα άμεσα.



Σχήμα 13: Γράφημα για Out-Of-Order Πακέτα

Το τρίτο και βασικό στοιχείο που επηρεάζει την καθυστέρηση και την ποιότητα των κλήσεων είναι το Jitter (Διακύμανση). Αυτό δημιουργείτε όταν τα πακέτα που αποστέλλονται δεν φτάνουν με σταθερό ρυθμό στον προορισμό τους, με αποτέλεσμα, όσο μεγαλύτερη διακύμανση υπάρχει, τόσο αυξάνεται και η αδράνεια του δικτύου. Αυτό σημαίνει ότι επηρεάζει αρνητικά την ποιότητα των υπηρεσιών.

Όταν για παράδειγμα κάθε πακέτο φτάνει ανά 10ms τότε ο ρυθμός είναι σταθερός και η σύνδεση δεν βιώνει διακυμάνσεις. Επιπλέον, αν ένα πακέτο φτάσει σε 20ms και το επόμενο στα 60ms, η καθυστέρηση και πάλι είναι πολύ μικρή με αποτέλεσμα να μην γίνεται και αντιληπτή.

Γενικά, το Jitter είναι ο χρόνος που χρειάζεται ένα πακέτο για να φτάσει από τον Α προορισμό στον Β. Αν για παράδειγμα, ο Α στέλνει πακέτα ανά 10ms και ο Β είναι απασχολημένος , αυτό σημαίνει ότι ο Β δεν θα λαμβάνει τα πακέτα ανά τακτά διαστήματα. Μπορεί να λάβει πακέτο στα 40ms, την επόμενη φορά, το πακέτο να το λάβει στα 20ms, την επόμενη στα 50ms και στο τέλος να λαμβάνει πολλά πακέτα μαζί. Αυτό είναι Jitter γιατί τα πακέτα δεν φτάνουν στον προορισμό τους με σταθερό ρυθμό με αποτέλεσμα να δημιουργούν προβλήματα καθυστέρησης και συμφόρησης πακέτων στο δίκτυο.

Συνήθως, όταν τα πακέτα αποστέλλονται πάντα υπάρχει μια μικρή καθυστέρηση που δεν τους δίνει τη δυνατότητα να μεταδίδονται σε ακριβή χρόνο. Στις μετρήσεις της εργασίας ο χρόνος που τα πακέτα φτάνουν στον προορισμό τους δεν είναι σταθερός. Παίρνοντας ένα δείγμα μετρήσεων ανά 5sec θα παρατηρήσουμε ότι, ο χρόνος παράδοσης των πακέτων R,αυξάνεται και όχι με σταθερό ρυθμό. Ωστόσο, αυτό μας απασχολεί κυρίως, είναι τοJitter να μην έχει μεγάλες αυξομειώσεις. Όταν

οι αλλαγές είναι μικρές δεν προκαλεί προβλήματα στην ποιότητα των κλήσεων.

Για τον υπολογισμό της διακύμανσης, θα χρησιμοποιήσουμε τους εξής τύπους:

$$D(i, j) = (R_j - R_i) - (S_j - S_i) = (R_j - S_j) - (R_i - S_i)$$

$$J(i) = J(i-1) + (|D(i-1, i)| - J(i-1)) / 16$$

Όπου: D= διαφορά χρόνων των δύο πακέτων

R= χρόνος παράδοσης του πακέτου, i= αριθμός πακέτου

S= χρόνος έναρξης πακέτου j= i-1

J= διακύμανση (Jitter) 16= σταθερός αριθμός για μείωση τυχαίων αλλαγών

Παρακάτω ακολουθεί ο πίνακας με αριθμούς πακέτων από το 1 ως το 9 για τις χρονικές στιγμές S=0,5,10,15,20,25,30,35,40. Μετράμε ανά 5 sec από την χρονική στιγμή S0=0 όπου έγινε η έναρξη και του πρώτου πακέτου, μέχρι τη χρονική στιγμή S9=40sec, όπου ήταν και η διάρκεια της κλήσης μας στο Skype. Έπειτα, υπολογίζουμε το χρόνο παράδοσης του κάθε πακέτου (R), με βάση το χρόνο παράδοσης του προηγούμενου πακέτου ανά 5sec.

Έτσι, με βάση τους παραπάνω τύπους υπολογίζουμε το (D) που είναι η διαφορά χρόνων των δύο πακέτων ανά 5sec και υπολογίζουμε το Jitter (J)

Πίνακας: Υπολογισμός Jitter ανά 5sec

Πακέτα (i)	**S(i)**	**R(i)**	**J(i)**
1	0	12	0
2	5	49	1.375
3	10	82	29.28
4	15	125	28.735
5	20	140	27.565
6	25	164	27.035
7	30	195	26.971
8	35	220	26.541
9	40	269	27.63

Χρησιμοποιώντας τους δύο τύπους που προαναφέραμε, μπορούμε να υπολογίσουμε την διακύμανση. Όπως παρατηρούμε, από το πακέτο 3 και μετά οι αυξομειώσεις είναι πολύ μικρές, με αποτέλεσμα να μην επηρεάζουν στην ποιότητα των κλήσεων και να μην αυξάνουν και την αδράνεια(Latency) του δικτύου. Στα πρώτα πακέτα, το Jitter είναι πολύ χαμηλό και αυξάνεται απότομα γιατί ο χρόνος μεταξύ των πακέτων D και ο χρόνος έναρξης των πακέτων S είναι σχεδόν μηδέν.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Σύμφωνα με τις παραπάνω μετρήσεις, καταλήγουμε στο συμπέρασμα, ότι για να μπορούμε να παρέχουμε καλή ποιότητα υπηρεσιών- QoS, θα πρέπει η απώλεια των πακέτων, η διακύμανση και η αδράνεια του δικτύου, να βρίσκονται σε χαμηλά ποσοστά. Όταν ένα δίκτυο δεν έχει καλή σύνδεση και το υλικό του δεν είναι αξιόπιστο, υπάρχει μεγάλη πιθανότητα να αντιμετωπίζουμε προβλήματα στη σύνδεση μας και έπειτα, στις VoIP κλήσεις που κάνουμε.

Ένα από τα βασικότερα στοιχεία στην αντιμετώπιση των προβλημάτων, όπως έχουμε προαναφερθεί, είναι το TCP πρωτόκολλο. Όταν αντιμετωπίζουμε τέτοιου είδους προβλήματα στη σύνδεση μας, αυτό είναι υποχρεωμένο να προβεί σε άμεσες λύσεις. Όταν κάποια πακέτα ή τμήμα τα τους τείνουν να χαθούν, το TCP κάνει αναμετάδοση τους με αποτέλεσμα να μην επηρεάζει τη σύνδεση μας.

Δυστυχώς όμως, έχουμε παρατηρήσει, ότι αρκετές φορές, κατά την διάρκεια μιας κλήσης μας μέσω VoIP εφαρμογών (π.χ. Skype), η σύνδεση διακόπτεται. Αυτό οφείλεται στον μεγάλο όγκο πακέτων που λαμβάνει το δίκτυο με αποτέλεσμα να έχουμε υπερχείλιση και συνεπώς απώλεια πακέτων. Αυτό συμβαίνει όταν το δίκτυο δεν έχει την κατάλληλη υποδομή για να μπορέσει να δεχθεί μεγάλο όγκο πακέτων.

Έτσι, για την καλύτερη απόδοση των υπηρεσιών του δικτύου, θα πρέπει να αποφεύγουμε τις καθυστερήσεις των πακέτων, την απώλεια τους και οι διακυμάνσεις στους χρόνους αποστολής και παράδοσης να είναι αρκετά μικροί. Όταν για κάθε πακέτο δεν σταλεί μήνυμα επιβεβαίωσης μέσα σε 3msec, το TCP καταλαβαίνει ότι κάποιο πακέτο ίσως χάθηκε και ξεκινάει την διαδικασία αναμετάδοσης του. Αυτό επηρεάζει την καθυστέρηση του δικτύου και συνεπώς και εμείς βλέπουμε διαφορά στην κλήση μας.

Για να μην συμβαίνουν αυτά θα πρέπει να κρατηθούν χαμηλά τα ποσοστά του Latency (αδράνεια), το οποίο δεν πρέπει να ξεπερνάει τα 25msec, το Jitter (διακύμανση) να είναι σταθερό και το packet loss (απώλεια πακέτων) να μην ξεπερνάει το 10% γιατί διαφορετικά τα πακέτα δεν στέλνονται με διαδοχικό ρυθμό.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Εργασία στην πληροφορική(χ.χ). *Skype*. Ανακτήθηκε στις 10 Μαρτίου 2015 από: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=0CCsQFjAD&url=http%3A%2F%2F1lyk-ag-dimitr.att.sch.gr%2Ffiles%2Fb_likiu_ergasies_ypologistes%2Fskype.pptx&ei=REY1VdSFI4LoaJutgTg&usg=AFQjCNGBhKAF_P6MMM4qxYi25a7POi2ZKQ
2. iRepair(χ.χ)*Skype for Business*. Ανακτήθηκε στις 20 Απριλίου 2015 από: http://irepair.gr/blog/article/microsoft-lansarei-tin-eidiki-ekdosi-skype-for-business
3. Skype(2015). *Δυνατότητες*. Ανακτήθηκε στις 20 Μαρτίου 2015 από: http://www.skype.com/el/features/
4. Ιωάννης, Χατζηκυριάκου Ηλίας(χ.χ). *Skype*. Ανακτήθηκε στις 1Απριλίου 2015 από: http://www.net.uom.gr/NET2/DOCS/Skype.pdf
5. J.F. Kurose, K.W.Ross(2007).*Εργαστήριο Wireshark*. Ανακτήθηκε στις 22 Ιουλίου 2015 από: http://www.telecom.tuc.gr/courses/net2/exercises/Wireshark_INTRO.pdf
6. Lefkadaonline(χ.χ) *Πλεονεκτήματα VoIP κλήσεων*. Ανακτήθηκε στις 1 Απριλίου 2015 από: http://www.lefkadaonline.com/lefkasphone/pleonektimata.htm
7. Computer(χ.χ). *Προβλήματα με Voice-Over IP*. Ανακτήθηκε στις 1 Απριλίου 2015 από: http://el.wingwit.com/Networking/voice-over-ip/81642.html#.VUnx5fntmko
8. Κυριαζοπούλου Χριστιάνα (2011). *Φωνή επί Διαδικτυακού Πρωτοκόλλου Voice over Internet Protocol*. Ανακτήθηκε στις 10 Απριλίου2015 από: http://conta.uom.gr/conta/ekpaideysh/metaptyxiaka/technologies_diktywn/ergasies/2011/VOICE%20OVER%20IP.pdf
9. Article phere.com (2015). *VoIP πληροφορίες. Πλεονεκτήματα και μειονεκτήματα*. Ανακτήθηκε στις 10 Απριλίου 2015 από: http://www.articlesphere.com/el/Article/VoIP-Information--Benefits-and-Drawbacks/42283
10. Βαρτζιώτης ,Φ (2011). *Προχωρημένα Θέματα Προγραμματισμού*. ΤΕΙ Ηπείρου, Άρτα
11. question-defense.com (2015). *Capture Skype VoIP Call Packets On Your windows XP computer Using Wireshark*. Ανακτήθηκε στις 20 Αυγούστου 2015 από: http://www.question-defense.com/2009/10/16/capture-skype-voip-call-packets-on-your-windows-xp-computer-using-wireshark
12. Μαργαρίτη, Σ., & Στεργίου, Ε. (2007). *Τοπικά & Αστικά Δίκτυα (LAN-MAN)*. Έκδοση 1η. Αθήνα: Εκδόσεις Νέων Τεχνολογιών
13. Pi-schools(χ.χ.). *Δίκτυα Υπολογιστών*. Ανακτήθηκε στις 8 Δεκεμβρίου 2015 από: http://www.pi-schools.gr/programs/ktp/previous_version/book2/04_1.pdf
14. Sites.it.teithe(χ.χ). *Ανάλυση Δεδομένων δικτύου Πραγματικού Χρόνου*. Ανακτήθηκε στις 9 Δεκεμβρίου 2015 από: http://sites.it.teithe.gr/rna/?page=area
15. Casad, J.(2009). *Μάθετε το TCP/IP σε 24 Ώρες*. Έκδοση 4η. Αθήνα: Εκδόσεις Μ. Γκιούρδας
16. Math.uoc(2005). *Διερεύνηση Αναλυτικών Μοντέλων για την εκτίμηση της απόδοσης σε Ασύρματα*

Δίκτυα. Ανακτήθηκε στις 26 Δεκεμβρίου 2015 από: http://www.math.uoc.gr:1080/proptyxiakes/ptyxiakes/Alafouzos_PE.pdf

17. Auto.teipir(χ.χ). *Παράμετροι και Αρχές Μελέτης τηλεπικοινωνιακής κίνησης*. Ανακτήθηκε στις 2 Ιανουαρίου 2016 από: http://auto.teipir.gr/sites/default/files/ask_about_network_traffic.pdf
18. Techopedia(2016). *Availability*. Ανακτήθηκε στις 5 Ιανουαρίου 2016 από: https://www.techopedia.com/definition/990/availability
19. Curtis J.(2000). *Passive Measurement*. Ανακτήθηκε στις 10 Ιανουαρίου 2016 από: https://secure.wand.net.nz/pubs/19/html/node9.html
20. Shaikh A.(2004). *Active Measurement*. Ανακτήθηκε στις 10 Ιανουαρίου 2016 από: http://static.usenix.org/event/usenix04/tech/general/full_papers/akella/akella_html/node10.html
21. Cottrell L.(χ.χ.).*Passive vs Active Monitoring*. Ανακτήθηκε στις 11 Ιανουαρίου 2016 από: https://www.slac.stanford.edu/comp/net/wan-mon/passive-vs-active.html