ΤΕΙ ΚΡΗΤΗΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΙΑΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Μέτρηση απόδοσης και αξιοπιστίας συστήματος τηλεφωνίας (VoIP) στηριγμένο στο πρωτόκολλο (SIP) με χρήση των εργαλείων SIPP και VoIP Monitor.

ΦΡΑΓΚΟΣ ΑΛΕΞΑΝΔΡΟΣ

ΑΜ: 2284

ΗΡΑΚΛΕΙΟ 2014

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω εκ βάθους καρδίας όλους όσους με στήριξαν κατά τη διάρκεια των σπουδών μου στο τμήμα Ηλεκτρολογίας του ΤΕΙ Κρήτης, και ιδιαιτέρως την οικογένειά μου, που με ανέχθηκε και με στήριξε κατά τη διάρκεια της διεκπεραίωσης καθώς και της συγγραφής αυτής της πτυχιακής. Ιδιαίτερες ευχαριστίες θα ήθελα να απευθύνω στον καθηγητή κ. Βασιλάκη Κωνσταντίνο, χωρίς την βοήθεια του οποίου η ολοκλήρωση αυτής της μελέτης θα ήταν αδύνατη, για το αμείωτο ενδιαφέρον και τη συμπαράστασή του τόσο κατά την εκτέλεση του πειραματικού μέρους όσο και κατά τη συγγραφή του. Η καθοδήγηση και οι συμβουλές του καθηγητή κ. Παναγιωτάκη Σπυρίδωνα, βοήθησαν επίσης ουσιαστικά στον εμπλουτισμό των γνώσεών μου και στην υλοποίηση αυτής της εργασίας. Τέλος, θα ήθελα να αναφερθώ και στην άψογη συνεργασία που είχαμε με το προσωπικό του Κέντρου Ελέγχου και Διαχείρισης Δικτύων του ΤΕΙ Κρήτης, που βοήθησε στην επίτευξη του στόχου μας.

Φράγκος Αλέξανδρος

Σύντομη Περίληψη.

Το **Voice over IP** ή **VoIP** χαρακτηρίζει μια ομάδα πρωτοκόλλων-τεχνολογιών (H.323, SIP), η οποία προσφέρει φωνητική συνομιλία σε πραγματικό χρόνο με σχετικά καλή ποιότητα και στην ουσία χωρίς ή με μειωμένο κόστος, χάρη στις ευρυζωνικές συνδέσεις που έχουν διαδοθεί πλέον παγκοσμίως. Το πιο διαδεδομένο πρωτόκολλο, που χρησιμοποιείται για την υλοποίηση της υπηρεσίας VoIP είναι το SIP (Session Initiation Protocol). Στην παρούσα εργασία γίνεται μελέτη με κατάλληλες μετρήσεις και test της αξιοπιστίας του πρωτόκολλου αυτού κατά τη διάρκεια της λειτουργίας του, καθώς και της επίδρασης που έχει η λειτουργία του σε ένα IP δίκτυο, με χρήση των εργαλείων SIPP και Voip Monitor.

Σημείωση:

Στα πλαίσια αυτής της πτυχιακής εργασίας, έγινε εγκατάσταση και παραμετροποίηση δυο ηλεκτρονικών υπολογιστών και χρήση διαφόρων προγραμμάτων. Μέρος της παραμετροποίησής τους που δεν παρουσιάζεται στο κύριο μέρος της εργασίας, παρουσιάζεται στο Παράρτημα Α στο τέλος της.

Πρόλογος.

Η ανάπτυξη δικτύων ηλεκτρονικών υπολογιστών από την αρχή της ιστορίας τους στηρίχτηκε στην λογική ότι η προς μετάδοση πληροφορία χωρίζεται σε πακέτα και η μεταφορά της δεν είναι απαραίτητο να γίνεται σε πραγματικό χρόνο. Η ανάπτυξη όμως, κυρίως τα τελευταία χρόνια , δικτύων (IP) με δυνατότητα μεταφοράς τεράστιου όγκου πληροφοριών σε ολόκληρο τον πλανήτη και με ασύλληπτη ταχύτητα, έδωσε ώθηση στην ανταλλαγή πληροφοριών κάθε μορφής σε πραγματικό χρόνο με την χρήση διαφόρων τεχνολογιών. Μια από τις πιο διαδεδομένες πλέον τεχνολογίες των σύγχρονων δικτύων (IP) είναι η μεταφορά φωνής. Η τεχνολογία αυτή που καθορίζει τον τρόπο μεταφοράς φωνής μέσα από ένα δίκτυο ονομάζεται Voice over Internet Protocol (VoIP). Η τεχνολογία της Τηλεφωνίας (VoIP) χρησιμοποιεί το Πρωτόκολλο διαδικτύου (Internet Protocol - IP), ώστε να μεταδώσει φωνή. Αφού πρώτα ο υπολογιστής χωρίσει το ηλεκτρικό σήμα σε πακέτα, κάνοντας κατάλληλη δειγματοληψία (CODEC), χρησιμοποιώντας κατάλληλη συμπίεση το μεταδίδει πάνω από το δίκτυο (IP) με τη χρήση κατάλληλων πρωτοκόλλων σηματοδότησης, τα οποία στην ουσία τερματίζουν την κλήση αφού διαπραγματευτούν τις δυνατότητες του δικτύου, έτσι ώστε η κλήση να είναι επιτυχημένη. Το Voip μπορεί να λειτουργήσει σε οποιοδήποτε δίκτυο το οποίο χρησιμοποιεί IP, όπως το διαδίκτυο (Internet) και τα Τοπικά Δίκτυα (**L**ocal **A**rea **N**etworks - LANs).

Αντικείμενο της πτυχιακής εργασίας είναι η μελέτη, η υλοποίηση και η λειτουργία ενός συστήματος μετρήσεων του πρωτοκόλλου SIP (**S**ession **I**nitiation **P**rotocol) χρησιμοποιώντας ως βασικά εργαλεία δυο συγκεκριμένα προγράμματα μετρήσεων και απόδοσης , το SIPp και το Voip monitor, έτσι ώστε να καθοριστεί η απόδοση ενός υπολογιστικού συστήματος, το οποίο εκτελεί χρέη SIP Server , αλλά και η συμπεριφορά του στο δίκτυο, χρησιμοποιώντας διάφορες παραμέτρους.

Τα κεφάλαια 1-5 αποτελούν το γενικό-θεωρητικό μέρος, όπου εκεί θα παρουσιαστούν οι υπάρχουσες τεχνολογίες δικτύου και πρωτόκολλα του VoIP. Στο Κεφάλαιο 1 γίνεται μια αναδρομή στο υπάρχον κλασικό δίκτυο τηλεφωνίας και μια εισαγωγή στην τεχνολογία VoIP. Στο Κεφάλαιο 2 παρουσιάζεται αναλυτικά η τεχνολογία δικτύων υπολογιστών . Στο Κεφάλαιο 3 γίνεται αναλυτική παρουσίαση των τεχνολογιών VoIP. Στο Κεφάλαιο 4 γίνεται αναλυτική περιγραφή του πρωτοκόλλου SIP. Στο Κεφάλαιο 5 γίνεται ανάλυση στα θέματα ποιότητας υπηρεσιών QoS σε ότι αφορά το VoIP γενικά αλλά και του SIP ειδικότερα.

Στο κεφάλαιο 6 γίνεται μια αναλυτική περιγραφή των στόχων της εργασίας. Στο κεφάλαιο 7 παρουσιάζονται τα προγράμματα που χρησιμοποιήθηκαν για την επίτευξη των πειραμάτων. Στο κεφάλαιο 8 παρουσιάζεται η πειραματική διαδικασία και τα αποτελέσματα της. Στο κεφάλαιο 9 τα συμπεράσματα της εργασίας.

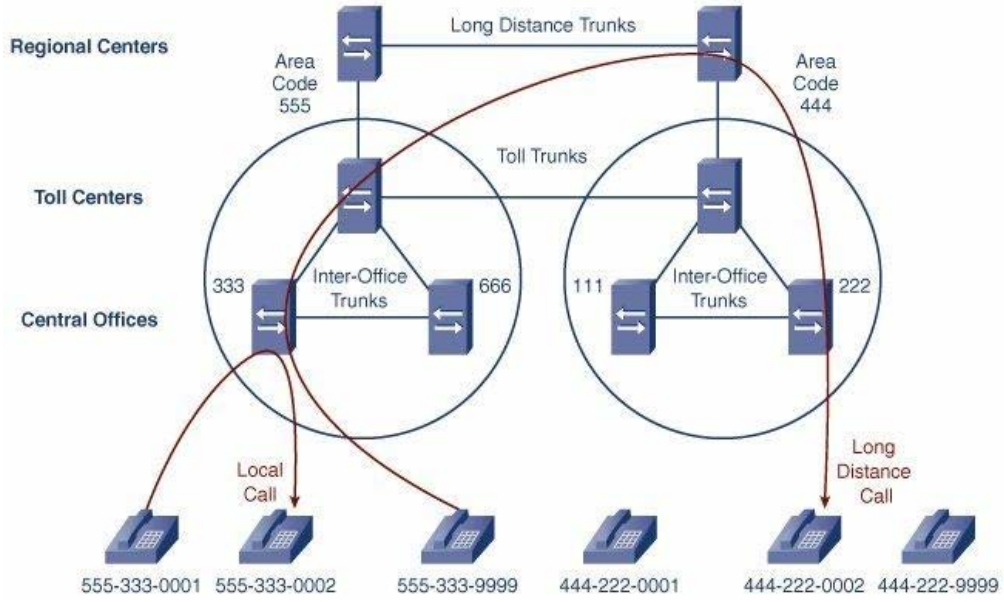
Πίνακας Περιεχομένων

Κεφάλαιο 1.

Το Τηλεφωνικό Δίκτυο.

1.1 Πως λειτουργεί το Δημόσιο τηλεφωνικό δίκτυο μεταγωγής (PSTN).

Από την εφεύρεση του τηλεφώνου από τον Bell μέχρι και σήμερα το τηλεφωνικό δίκτυο έχει περάσει πολλά στάδια εξέλιξης, καθώς η ανάπτυξη του τον περασμένο αιώνα ήταν ένας από τους βασικούς παράγοντες για την ανάπτυξη και τη βελτίωση του τρόπου ζωής . Ακόμη και σήμερα η ύπαρξη τηλεφωνικής σύνδεσης κάποιας μορφής σε ένα σημείο του πλανήτη θεωρείται δείκτης πολιτισμού και εξέλιξης. Το τηλεφωνικό σύστημα σχεδιάστηκε με μία «ιεραρχική δομή», όπως φαίνεται και στην (Εικόνα 1.1).



Εικόνα 1.1: Ιεραρχική σχεδίαση τηλεφωνικού δικτύου.

Η δομή αποτελείται από τρία (3) επίπεδα, το πρώτο επίπεδο είναι τα **C**entral **O**ffices (CO), δηλαδή τα τηλεφωνικά κέντρα εκείνα, τα οποία αποτελούν τη βάση του συστήματος και σκοπός τους είναι να συνδέσουν τις τηλεφωνικές γραμμές των συνδρομητών στο τηλεφωνικό δίκτυο. Αυτά τα τηλεφωνικά κέντρα συνδέονται με άλλα όμοια, που βρίσκονται στην ίδια περιοχή, χρησιμοποιώντας μεταξύ τους διασυνδέσεις (trunks). Οι διασυνδέσεις αυτές είναι στην ουσία ένας αριθμός καλωδίων μεταξύ των τηλεφωνικών κέντρων, ανάλογα με τις απαιτήσεις και τις ανάγκες που εμφανίζονται για την μεταξύ τους επικοινωνία. Κλήσεις που πραγματοποιούν συνδρομητές οι οποίοι ανήκουν στο ίδιο CO, εξυπηρετούνται από το ίδιο το κέντρο ή το πολύ από δύο κέντρα συνδεδεμένα μεταξύ τους.

Τα Toll Centers αποτελούν το δεύτερο επίπεδο στην ιεραρχία, και αναλαμβάνουν να συνδέσουν τα επιμέρους τοπικά τηλεφωνικά κέντρα (COs) των διάφορων περιοχών μεταξύ τους, με τη βοήθεια πάλι των απαιτούμενων διασυνδέσεων (trunks). Έτσι όλα τα COs μιας περιοχής είναι συνδεδεμένα πάνω σε

κάποιο Toll Center, το οποίο με τη σειρά του συνδέεται σε άλλα Toll Centers άλλων περιοχών.

Στην κορυφή της ιεραρχίας βρίσκονται τα Regional Centers, τα οποία με τη σειρά τους συνδέουν τα επιμέρους Toll Centers της κάθε ευρύτερης γεωγραφικής περιοχής μεταξύ τους. Συνήθως τα Regional Centers παρεμβάλλονται σε κλήσεις μεγάλων αποστάσεων.

Στην πραγματικότητα η ιεραρχία του τηλεφωνικού δικτύου αποτελείται από πέντε επίπεδα, αλλά για λόγους απλοποίησης χρησιμοποιήθηκαν τρία από αυτά, αφού αυτά είναι αρκετά για την κατανόηση της βασικής λειτουργίας του δικτύου.

1.2 Το Δίκτυο ISDN.

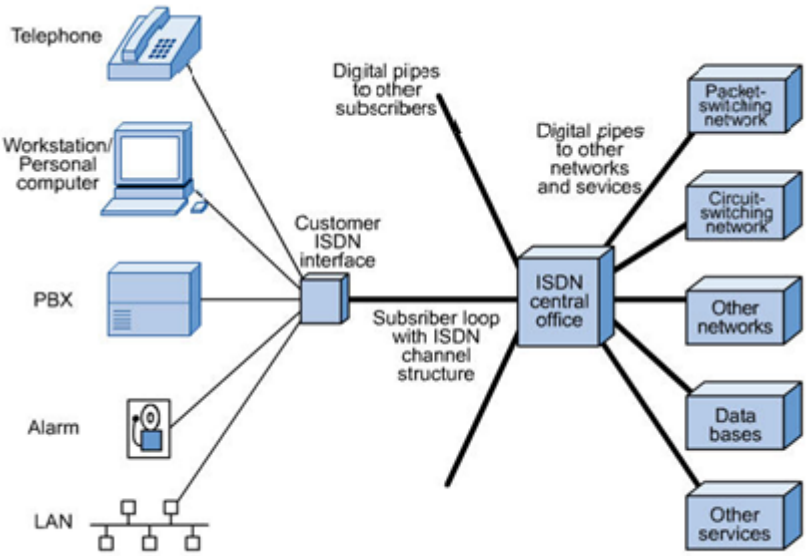
Με την πάροδο των χρόνων και την αύξηση των τηλεπικοινωνιακών αναγκών, η δημιουργία του διαδικτύου και η απαίτηση για καλύτερης ποιότητας υπηρεσίες, οδήγησαν στην ανάγκη αναβάθμισης και βελτίωσης του υπάρχοντος τηλεφωνικού δικτύου (PSTN). Αυτό πραγματοποιήθηκε το 1988 με την έλευση των ψηφιακών δικτύων ενοποιημένων υπηρεσιών (ISDN), τα οποία προσέφεραν στους συνδρομητές περισσότερες και ποιοτικότερες υπηρεσίες σε σχέση με τα POTS, ενώ παράλληλα εισήγαγαν τα ψηφιακά δίκτυα στο χώρο των τελικών χρηστών.

Η POTS (Plain Old Telephone Service) είναι η κλασική υπηρεσία τηλεφωνίας (φωνητική επικοινωνία), που παραμένει η βασική μορφή υπηρεσίας διασύνδεσης στο παγκόσμιο τηλεφωνικό δίκτυο για επιχειρήσεις αλλά και για οικιακούς συνδρομητές. Η POTS παρέχεται περίπου από την αρχή της λειτουργίας του δημόσιου τηλεφωνικού δικτύου (PSTN) στα τέλη του 19ου αιώνα, σχεδόν απαράλλακτη ως προς τον τελικό χρήστη, παρά τη διείσδυση νέων ψηφιακών τεχνολογιών όπως η δυνατότητα τονικής κλήσης, των ηλεκτρονικών ψηφιακών τηλεφωνικών κέντρων και των τηλεπικοινωνιακών οπτικών ινών στο δίκτυο.

Το ISDN (**I**ntegrated **S**ervices **D**igital **N**etwork – Ψηφιακό Δίκτυο Ενοποιημένων Υπηρεσιών) αποτελείται από ένα σύνολο τηλεπικοινωνιακών προτύπων που επιτρέπουν την ταυτόχρονη ψηφιακή μετάδοση φωνής, βίντεο, δεδομένων και άλλων υπηρεσιών, μέσω του δημόσιου τηλεφωνικού δικτύου μεταγωγής κυκλώματος (PSTN). Το βασικό χαρακτηριστικό και πλεονέκτημα του ISDN είναι ότι ενσωματώνει φωνή και δεδομένα στην ίδια γραμμή, προσθέτοντας παράλληλα χαρακτηριστικά, που δεν ήταν διαθέσιμα στην κλασική τηλεφωνία. Κάθε γραμμή ISDN αποτελείται από κάποιο πλήθος B-channels, το καθένα από το οποία προσφέρει ρυθμό μετάδοσης 64 kbps, και ένα κανάλι για σηματοδοσίες γνωστό ως D- channel. Κάθε B-channel στο ISDN μπορεί να μεταφέρει είτε φωνή, είτε εικόνα, είτε δεδομένα, ανεξάρτητα για το ποιά χρήση έχουν δεσμευθεί τα υπόλοιπα.

Υπάρχουν δύο είδη διαθέσιμης πρόσβασης στο EURO-ISDN δίκτυο (αφορά το ευρωπαϊκό πρότυπο). Αυτά είναι η βασική πρόσβαση (BRI - **B**asic **R**ate **I**nterface ή BRA – Basic Rate Access) και η πρωτεύουσα πρόσβαση (PRI – **P**rimary **R**ate **I**nterface ή PRA - **P**rimary **R**ate **A**ccess). Αντίστοιχα η ISDN BRI διαθέτει

2 κανάλια B προσφέροντας εύρος ζώνης έως 128 kbps και ένα κανάλι D των 16 kbps, ενώ η ISDN PRI διαθέτει 30 κανάλια B και ένα κανάλι D των 64 kbps, (Εικόνα 1.2) προσφέροντας έτσι συνολικό εύρος ζώνης έως 2.048 Mbps.



Εικόνα 1.2: Το δίκτυο ISDN.

1.3 Πώς λειτουργεί το VoIP.

Η διαφορά ανάμεσα στην τηλεφωνία μέσω διαδικτύου (Internet Telephone) και στο Δημόσιο Τηλεφωνικό Δίκτυο με Μεταγωγή (PSTN) παρουσιάζεται και στην αρχιτεκτονική και σε επίπεδο πρωτοκόλλων.

Η τηλεφωνία (VoIP) βασίζεται στην μεταξύ των άκρων (end-to-end) μεταφορά υπηρεσιών φωνής. Πρωτόκολλα σηματοδοσίας υπάρχουν μόνο μεταξύ των τελικών συστημάτων που παίρνουν μέρος στην κλήση, ενώ στο δίκτυο τα πακέτα σηματοδοσίας μεταφέρονται με τον ίδιο τρόπο όπως τα πακέτα δεδομένων από τους δρομολογητές.

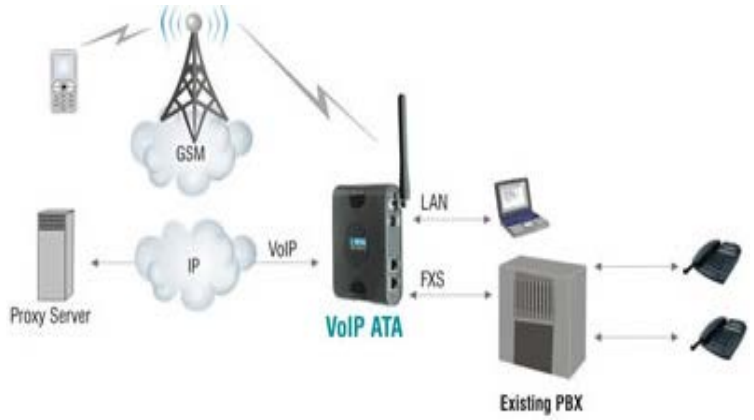
Στο Διαδίκτυο η ταυτόχρονη μεταφορά πληροφοριών που αφορούν διαφορετικές υπηρεσίες, στηρίζεται στην μεταφορά σε επίπεδο πακέτου, έτσι η επεκτασιμότητα και η ελαστικότητα είναι γεγονός, αφού για οποιαδήποτε υπηρεσία η δικτύωση επιτυγχάνεται με την χρήση πρωτοκόλλων μεγαλύτερων στρωμάτων. Έτσι έχουμε την δυνατότητα να ενσωματώσουμε νέες υπηρεσίες, όπως e-mail, Video, text, και ταυτόχρονα να χρησιμοποιούνται από όποιον έχει πρόσβαση στο δίκτυο.

Το VoIP είναι μια μέθοδος για τη μετατροπή αναλογικών ηχητικών σημάτων (ανθρώπινη φωνή) σε ψηφιακή πληροφορία, που μπορεί να μεταδοθεί στο Internet. Έτσι με μια τυπική σύνδεση Internet μπορεί κάποιος να πραγματοποιεί δωρεάν τηλεφωνικές κλήσεις χρησιμοποιώντας πλήθος προγραμμάτων. Επομένως το VoIP θεωρείται μια ανερχόμενη, και πολλά υποσχόμενη τεχνολογία μιας και που με τον τρόπο αυτό παρακάμπτονται οι τηλεφωνικές εταιρείες καθώς και η

συνδρομή σε αυτές ολοκληρωτικά. Έτσι δεν αποκλείεται στο μέλλον η επαναστατική αυτή τεχνολογία να αντικαταστήσει πλήρως το υπάρχον τηλεφωνικό σύστημα, μετατρέποντας τον παγκόσμιο ιστό σε ένα καθολικό δίκτυο, του οποίου οι υπηρεσίες φωνής θα είναι μόνο ένα μικρό κομμάτι του συνόλου των υπηρεσιών που θα παρέχει.

Η εξέλιξη της τεχνολογίας VoIP έχει φέρει στο προσκήνιο μια σειρά από ολοκληρωμένες λύσεις για διάφορες περιπτώσεις, κάνοντας έτσι την δικτύωση πολύ πιο εύκολη από το παρελθόν . Ταυτόχρονα η αγορά VoIP προϊόντων και υπηρεσιών αναπτύσσεται συνεχώς καθώς οι εταιρίες πληροφορικής αποκτούν όλο και μεγαλύτερο κομμάτι της τηλεφωνικής κίνησης, παρόλο που δεν βρίσκονται σε ανταγωνισμό με τις εταιρίες τηλεφωνίας. Παρακάτω παρατίθενται βασικά προϊόντα VoIP που καθιστούν δυνατή την επίτευξη VoIP κλήσεων. Σε μια προσπάθεια κατηγοριοποίησης αυτών των προϊόντων προκύπτουν πέντε κατηγορίες λύσεων VoIP.

ATA: Ο απλούστερος και πιο συνηθισμένος τρόπος είναι η χρήση μιας συσκευής, ονομαζόμενη ATA (**A**nalog **T**elephone **A**daptor – Μετατροπέας Αναλογικού Τηλεφώνου). Ο ATA επιτρέπει τη σύνδεση μιας τυπικής τηλεφωνικής συσκευής σε έναν υπολογιστή ή τη σύνδεση Internet για χρήση VoIP. Ο ATA (Εικόνα 1.3) είναι ένας μετατροπέας αναλογικού σήματος σε ψηφιακό (A/D converter). Λαμβάνει το αναλογικό σήμα από το κλασικό τηλέφωνο και το μετατρέπει σε ψηφιακό. Κυκλωματικά παρεμβάλλεται ανάμεσα στην απλή τηλεφωνική συσκευή και στην πρίζα του τηλεφώνου, ενώ μπορεί να συνοδεύεται από ειδικό software απλό στην εγκατάσταση και στη χρήση.



Εικόνα 1.3: Περιγραφή λειτουργιάς ATA.

IP Phones (Τηλέφωνα IP): Τα εξειδικευμένα αυτά τηλέφωνα μοιάζουν αρκετά με τα παραδοσιακά, έχοντας μικρόφωνο, ακουστικό και πλήκτρα. Όμως, αντί για τους τυπικούς RJ – 11 connectors, τα τηλέφωνα IP έχουν έναν RJ – 45 Ethernet connector. Τα τηλέφωνα IP συνδέονται κατευθείαν σε έναν router και διαθέτουν το απαραίτητο hardware και software για τη διεκπεραίωση μιας κλήσης IP. Στην ουσία είναι μικροί ηλεκτρονικοί υπολογιστές, που έχουν λειτουργικό σύστημα και επιτρέπουν τη διεξαγωγή κλήσεων από οποιαδήποτε σύνδεση στο δίκτυο (Εικόνα 1.4).

Εικόνα 1.4: IP Τηλέφωνα.

Computer – to – computer (Υπολογιστής – σε – υπολογιστή): Αυτή είναι σαφώς η ευκολότερη μέθοδος για τη χρήση του VoIP. Υπάρχει μια τεράστια πληθώρα εταιρειών που παρέχουν δωρεάν ή πολύ φθηνό software για αυτόν τον τρόπο επικοινωνίας. Εκτός από το software, αυτό που χρειάζεται είναι ένα μικρόφωνο, ηχεία, μια κάρτα ήχου, καθώς και μια σύνδεση Internet, κατά προτίμηση γρήγορη (πχ. ADSL). Εκτός από την καθιερωμένη συνδρομή στον Internet Service Provider (ISP), δεν υπάρχουν επιπλέον χρεώσεις, ανεξαρτήτως απόστασης.

Τηλεφωνικές εταιρίες που παρέχουν λύσεις VoIP: Πολλές τηλεφωνικές εταιρίες χρησιμοποιούν το διαδίκτυο έτσι ώστε να καταφέρνουν να ενοποιούν υπηρεσίες και δίκτυα, έτσι έχουν την δυνατότητα να προσφέρουν φθηνότερες και πιο αξιόπιστες λύσεις στην αγορά.

Τηλεφωνικά κέντρα VoIP PBX (Private branch exchange): Υπάρχουν τηλεφωνικά κέντρα PBX σε χρήση από ιδιώτες αλλά και από επιχειρήσεις, τα οποία έχουν την δυνατότητα, με χαμηλό κόστος κτήσης και συντήρησης να εκτελούν πολλαπλές υπηρεσίες κάνοντας την χρήση των παλιών ψηφιακών κέντρων να είναι πλέον ξεπερασμένη. Το πιο διαδεδομένο πρόγραμμα που μετατρέπει έναν τυπικό Η/Υ σε τηλεφωνικό κέντρο είναι το Asterisk από την εταιρία Digium (http://www.asterisk.org/) .

1.4 Πλεονεκτήματα και μειονεκτήματα του VoIP.

Πλεονεκτήματα:

- Η τεχνολογία VoIP χρησιμοποιεί τις δυνατότητες μεταφοράς πακέτων του παγκοσμίου ιστού για την παροχή τηλεφωνικών υπηρεσιών.

- Μικρότερο κόστος λειτουργίας, συμπεριλαμβανομένων μικρότερων τηλεφωνικών χρεώσεων.

- Ευελιξία.

- Μικρότερες ανάγκες σε υποδομές.

- Ολοκληρωμένες υπηρεσίες και καλύτερη αντιμετώπιση του χρήστη.

- Λειτουργικότητα.

- Οι εισερχόμενες τηλεφωνικές κλήσεις μπορούν αυτομάτως να δρομολογούνται στο τηλέφωνο VoIP του χρήστη, ανεξάρτητα από το σημείο σύνδεσης στο δίκτυο.

- Ρυθμιζόμενη ποιότητα: Επειδή το Internet δεν είναι δίκτυο συγκεκριμένων υπηρεσιών, η ανταλλαγή μέσων (media) επιλέγεται εξ' ολοκλήρου από τα τερματικά συστήματα. Επομένως τα τερματικά συστήματα μπορούν να επιλέξουν το μέγεθος συμπίεσης βασισμένα στο εύρος ζώνης του δικτύου ή και το περιεχόμενο που πρόκειται να μεταδοθεί.

- Οι call center agents (τηλεπικοινωνιακοί οργανισμοί) μπορούν να λειτουργούν από οποιοδήποτε σημείο με την προϋπόθεση ότι υπάρχει μια επαρκώς γρήγορη σύνδεση Internet.

- Πολλές τηλεφωνικές εταιρίες παρέχουν υπηρεσίες VoIP στα PSTN δίκτυά τους, τις οποίες χρεώνουν με επιπλέον κόστος, ή και δωρεάν όπως 3-way calling, προώθηση κλήσεων, αυτόματη επανάκληση κλπ.

- Οι συνδρομητές μπορούν να στέλνουν ή να δέχονται τοπικές τηλεφωνικές κλήσεις, ανεξαρτήτως της τοποθεσίας τους. Για παράδειγμα, αν ένας χρήστης έχει τηλεφωνικό νούμερο της Νέας Υόρκης και ταξιδεύει στην Ευρώπη, μπορεί να δεχθεί μια κλήση ακόμη και στην Ευρώπη. Αντίστοιχα, αν μια κλήση πραγματοποιηθεί από την Ευρώπη προς τη Νέα Υόρκη, θα αντιμετωπιστεί ως τοπική κλήση. Φυσικά πάντα προϋποτίθεται σύνδεση στο Internet (πχ. αυτό μπορεί να γίνει εφικτό με Wi-Fi).

- Οι τηλεφωνικές εταιρίες χρησιμοποιούν τεχνολογίες Voip για μεταξύ τους ανταλλαγή τηλεφωνικής κίνησης έτσι ώστε να μειώσουν το λειτουργικό τους κόστος.

- Οι χρήστες ενός Instant Messenger βασισμένου σε υπηρεσίες VoIP μπορεί επίσης να ταξιδεύει οπουδήποτε στον κόσμο και να δέχεται τηλεφωνικές κλήσεις.

- Ασφάλεια: Το Internet έχει τη φήμη πως δεν είναι αρκετά ασφαλές ακόμα και αν στην πραγματικότητα είναι πιο εύκολο να παγιδευτεί ένα τηλεφωνικό κέντρο παρά ένας δρομολογητής. Το Πρωτόκολλο Έναρξης Συνόδου (**S**ession **I**nitiation **P**rotocol, SIP) μπορεί να κρυπτογραφήσει και

να κρίνει την αυθεντικότητα των μηνυμάτων σηματοδοσίας. Το Πρωτόκολλο Μεταφοράς Πραγματικού Χρόνου (**R**eal – **T**ime **T**ransport **P**rotocol), RTP υποστηρίζει κρυπτογράφηση. Αυτά τα πρωτόκολλα μαζί παρέχουν κρυπτογραφημένες και ασφαλείς επικοινωνίες.

- Τα τηλέφωνα VoIP μπορούν να συνεργαστούν με άλλες υπηρεσίες που υπάρχουν στο Internet, όπως video conversation, ανταλλαγή μηνυμάτων και αρχείων παράλληλα με την ομιλία, audio conferencing, καθώς και αποστολή πληροφοριών που σχετίζονται με την παρουσία χρηστών στο δίκτυο.

- Πολλές εταιρίες και οργανισμοί υλοποιώντας λύσεις VoIP PBX έχουν την δυνατότητα να κάνουν χρήση εσωτερικού τηλεφώνου από διαφορετική φυσική τοποθεσία, π.χ. το τηλεφωνικό κέντρο του ΤΕΙ που είναι συνδεδεμένο με VoIP δίνει εσωτερικές γραμμές στα παραρτήματα του ΤΕΙ σε όλη την Κρήτη.

- Το μεγαλύτερο πλεονέκτημα του VoIP είναι η ελάττωση του κόστους. Εκτός από τα οικονομικά οφέλη, υπάρχει μια πληθώρα άλλων παράλληλων οφελών. Υπάρχει μεγάλη δυνατότητα επεκτασιμότητας.

- Αναγνώριση Χρήστη: Οι τυποποιημένες τηλεφωνικές υπηρεσίες (POTS, ISDN) παρέχουν τη δυνατότητα αναγνώρισης της ταυτότητας του καλούντος δείχνοντας τον αριθμό του, αλλά κατά τη διάρκεια μιας τηλεφωνικής συνδιάσκεψης πολλών μελών δεν υπάρχει καμία ένδειξη για το ποιος μιλάει. Το Πρωτόκολλο Μεταφοράς Πραγματικού Χρόνου (RTP) που χρησιμοποιείται από το Internet υποστηρίζει με ευκολία την ένδειξη του ποιος μιλάει και μπορεί να προσφέρει και άλλες πληροφορίες, αν εκείνος που πραγματοποιεί την κλήση το επιθυμεί.

- Λειτουργικότητα χρήστη: Τα περισσότερα τηλέφωνα POTS και ISDN έχουν μια σχετικά περιορισμένη διεπαφή χρήστη με μια οθόνη υγρών κρυστάλλων, δύο γραμμών. Εξελιγμένες δυνατότητες του PSTN, όπως προώθηση κλήσεων, χρησιμοποιούνται περιορισμένα, επειδή τα βήματα που πρέπει να γίνουν από τον χρήστη είναι πολύπλοκα και πολλές φορές δυσνόητα. Αυτό δικαιολογείται από τις περιορισμένες δυνατότητες σηματοδοσίας των τερματικών επειδή έχει επικρατήσει η φιλοσοφία των "ευφυών δικτύων" παρά των "ευφυών τερματικών". Τα τερματικά στην τηλεφωνία IP έχουν πολύ περισσότερες δυνατότητες σηματοδοσίας, η Γραφική Διεπαφή Χρήστη (**G**raphical **U**ser **I**nterface, GUI) που προσφέρεται από την τηλεφωνία Internet μπορεί να προσφέρει περισσότερες ενδείξεις και έτσι αυτές οι συσκευές είναι πιο εύχρηστες .

- Πολυμέσα: Η προσθήκη και άλλων μέσων, όπως video, είναι πολύ πιο εύκολη στο περιβάλλον του Internet, παρά στο POTS και στο ISDN, επειδή η πολυπλεξία είναι χαρακτηριστικό γνώρισμα των δικτύων πακέτου. Το γεγονός αυτό καθιστά επίσης πιο εύκολα τα πρωτόκολλα σηματοδοσίας

μιας και θέματα όπως η κατανομή του καναλιού-Β και ο συγχρονισμός δεν υφίστανται στο Internet.

- Καταστολή και Συμπίεση Σιγής: Η αποστολή ήχου με πακέτα καθιστά ευκολότερη την καταστολή περιόδων σιγής, μειώνοντας έτσι την κατανάλωση του διαθέσιμου εύρους ζώνης, ειδικά σε μια συνδιάλεξη πολλαπλών μερών. Αντίθετα με το PSTN, το οποίο γενικά πραγματοποιεί τέτοια καταστολή σιγής δια μέσου υπερατλαντικών συνδέσεων, η τηλεφωνία IP πραγματοποιεί καταστολή σιγής στα τελικά σημεία. Επιπλέον, μιας και τα δίκτυα πακέτου είναι καταλληλότερα για πολυπλεξία, δεν απαιτείται υποστήριξη δικτύου για να χρησιμοποιηθούν τα πλεονεκτήματα από την καταστολή σιγής στα τερματικά σημεία. Αυτό οδηγεί σε μείωση του κόστους. Επιπλέον, η συμπίεση μπορεί να χρησιμοποιηθεί στα τερματικά συστήματα για να μειωθεί η κατανάλωση του εύρους ζώνης σε ολόκληρο το δίκτυο. Δυστυχώς, η συμπίεση βρίσκεται σε αντίθεση με την ποιότητα της φωνής. Παρόλα αυτά, υπάρχουν κωδικοποιητές (codecs), οι οποίοι συμπιέζουν τη φωνή ευρείας ζώνης σε 16 Kbps, προσφέροντας έτσι εξαιρετική ποιότητα φωνής και μειωμένο εύρος συχνοτήτων σε σύγκριση με το PSTN. Πρέπει επίσης να τονιστεί πως η καταστολή και η συμπίεση της σιγής αντισταθμίζουν τη μειωμένη αποδοτικότητα της μεταγωγής κυκλώματος.

- Μια τοπολογία δικτύου μπορεί να τοποθετηθεί απλά και μόνο με μια δικτυακή καλωδίωση, σε αντίθεση με τις δύο καλωδιώσεις που απαιτούνται όταν χρησιμοποιείται ξεχωριστό δίκτυο κλασικής τηλεφωνίας και δίκτυο δεδομένων. Τα συστήματα VoIP μπορούν να ρυθμιστούν χρησιμοποιώντας κάποια standard δικτυακά εργαλεία, όπως το SNMP (**S**imple **N**etwork **M**anagement **P**rotocol).

Μειονεκτήματα:

- Το VoIP προϋποθέτει ύπαρξη ηλεκτρικού ρεύματος. Σε περίπτωση διακοπής, το τηλέφωνο δε μπορεί να λειτουργήσει, σε αντίθεση με τα συμβατικά τηλέφωνα που τροφοδοτούνται κατευθείαν από τις εταιρίες τηλεπικοινωνιών.

- Το δίκτυο πρέπει να είναι γρήγορο, αξιόπιστο και να προσφέρει υψηλή ποιότητα υπηρεσιών (Quality of Service). Είναι γνωστό πως στα δίκτυα δεδομένων όπως το Ethernet, τα φαινόμενα της καθυστέρησης, της σύγκρουσης ή και της καταστροφής των πακέτων πληροφορίας είναι ένα φαινόμενο πλέον συνηθισμένο. Όμως, όταν πρόκειται για μετάδοση φωνής σε πραγματικό χρόνο, πράγμα που απαιτείται σε μια τηλεφωνική συνομιλία, μια καταστροφή, αργοπορία ή λανθασμένη αλληλουχία άφιξης των πακέτων προκαλεί ανεπανόρθωτη βλάβη στην ποιότητα της επικοινωνίας.

- Η συμβατότητα με τα υπάρχοντα firewalls και μηχανισμούς security μπορεί να δημιουργήσει προβλήματα. (Τα Firewalls πρέπει να είναι H.323 και συμβατά με SIP, ανάλογα με την εκάστοτε VoIP τεχνολογία που χρησιμοποιείται)

- Η ύπαρξη ιών και hackers στο Internet μπορεί να θέσει σε κίνδυνο την ασφάλεια και τη μυστικότητα των τηλεφωνικών κλήσεων, παρά την πληθώρα των τεχνικών κρυπτογράφησης και κωδικοποίησης των συνομιλιών.

- Πολλές φορές η αναξιοπιστία των δικτύων μεταφοράς δεδομένων, δηλαδή η ύπαρξη βλάβης στο δίκτυο (φαινόμενο αρκετά συχνό δυστυχώς) οδηγεί στη μειωμένη εμπιστοσύνη του κοινού στη νέα τεχνολογία.

Κεφάλαιο 2.

Δίκτυα υπολογιστών.

2.1 Μοντέλα Αναφοράς στα Δίκτυα Υπολογιστών.

Η δημιουργία ενός δικτύου υπολογιστών στηρίζεται στην απρόσκοπτη επικοινωνία διαφόρων τύπων υπολογιστών, οι οποίοι μπορεί να χρησιμοποιούν διαφορετικά μέσα για να επικοινωνήσουν μεταξύ τους. Για να γίνει αυτή η επικοινωνία αποτελεσματική και ως εκ τούτου η δημιουργία του δικτύου εφικτή, πρέπει να τηρείται κατά την διάρκεια της επικοινωνίας μια πολύπλοκη διαδικασία για κάθε τύπο υπολογιστή, ανάλογα με τα ιδιαίτερα χαρακτηριστικά του καθενός ξεχωριστά.

Είναι άμεσα αντιληπτό ότι κάτι τέτοιο είναι πολύ δύσκολο να συμβεί και σε πολλές περιπτώσεις αδύνατο, καθώς όλα τα προγράμματα θα έπρεπε να γραφτούν με ξεχωριστό τρόπο για κάθε υπολογιστικό τύπο και δεν θα υπήρχε κανενός είδους ομοιογένεια. Έτσι για να αποφευχθούν τέτοια προβλήματα από την αρχή της δημιουργίας των δικτύων υπολογιστών δημιουργήθηκαν πρότυπα, τα οποία ξεπερνούν αυτά τα προβλήματα χωρίζοντας την επικοινωνία σε επίπεδα ή διαφορετικά σε στρώματα επικοινωνίας (Layers).

Έτσι το κάθε στρώμα είναι υπεύθυνο για μια σειρά από εργασίες, οι οποίες υποχρεωτικά θα φέρουν ένα συγκεκριμένο αποτέλεσμα, τέτοιο ώστε να μπορεί να αναπαράγεται από κάθε τύπο ηλεκτρονικού υπολογιστή και από διαφορετικούς τρόπους δικτύωσης (ενσύρματους ασύρματους κλπ.).

2.2 Το μοντέλο OSI.

Το πρότυπο που δημιουργήθηκε από τον χωρισμό σε επίπεδα (Layers) ονομάστηκε OSI (Open System Interconnection) και χωρίστηκε σε 7 επίπεδα . Η δομή που καθορίζεται από αυτό το μοντέλο δεν έχει χρησιμοποιηθεί ακριβώς σε καμία υλοποίηση. Χρησιμοποιείται πάντα όμως ως σημείο αναφοράς στην ανάλυση ενός δικτύου.

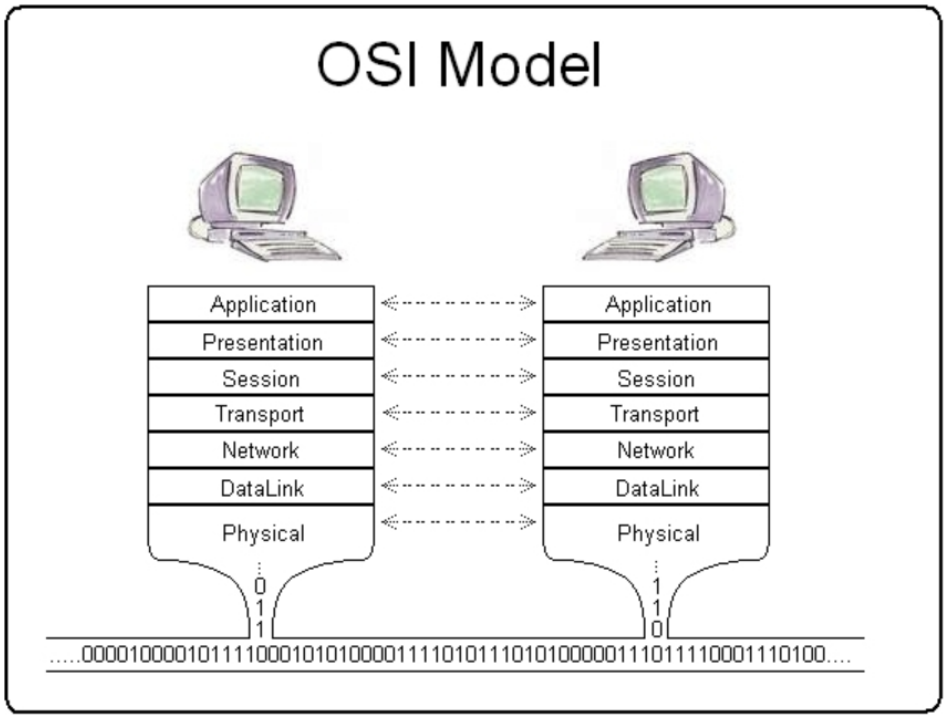
Ο διαχωρισμός αυτός σε στρώματα βοήθησε πάρα πολύ στην ανάπτυξη συμβάσεων και πρωτοκόλλων αναφορικά με το κάθε στρώμα. Βέβαια τα στρώματα αυτά διέπονται από κάποιες αρχές. Σύμφωνα με τον Andrew S. Tanenbaum, οι αρχές αυτές συνοψίζονται παρακάτω:

- Ένα στρώμα πρέπει να δημιουργηθεί οπουδήποτε χρειάζεται ένα διαφορετικό επίπεδο αφαίρεσης.
- Κάθε στρώμα πρέπει να εκτελεί μια καλά προσδιορισμένη λειτουργία.
- Η λειτουργία του κάθε στρώματος πρέπει να επιλέγεται με προοπτική τον καθορισμό διεθνώς τροποποιημένων πρωτοκόλλων.

- Τα όρια των στρωμάτων πρέπει να επιλέγονται έτσι ώστε να ελαχιστοποιείται η ροή της πληροφορίας μέσω των διεπαφών.

- Ο αριθμός των στρωμάτων πρέπει να είναι αρκετά μεγάλος, ώστε να μη στριμώχνονται κατ' ανάγκη διακεκριμένες λειτουργίες στο ίδιο στρώμα αλλά και αρκετά μικρός, ώστε να μη γίνεται η αρχιτεκτονική δύσχρηστη.

Στη συνέχεια θα περιγράψουμε συνοπτικά τη λειτουργία του κάθε επιπέδου (Εικόνα 2.1), ώστε να διευκρινιστεί η εκάστοτε χρησιμότητά του.



Εικόνα 2.1: Το μοντέλο OSI.

Επίπεδο 1: Φυσικό επίπεδο (Physical Layer).

Στο φυσικό επίπεδο καθορίζεται ο τρόπος με τον οποίο μεταδίδεται το σήμα μέσω κάποιου υλικού (καλωδίου, αέρα κ.α.) στο απέναντι άκρο της σύνδεσης. Αυτό πρακτικά σημαίνει ότι στο φυσικό στρώμα γίνεται η διευθέτηση του τρόπου μετάδοσης των bits πληροφορίας μέσα από έναν αγωγό. Πιο συγκεκριμένα, στο φυσικό επίπεδο καθορίζεται το όριο της τάσης πάνω από την οποία το αντίστοιχο bit θεωρείται "1" και κάτω από την οποία θεωρείται "0", η χρονική διάρκεια ενός bit κλπ. Γενικά το φυσικό στρώμα ασχολείται με τη λειτουργία των ηλεκτρικών κυκλωμάτων που σχηματίζονται κατά την επικοινωνία των υπολογιστών.

Επίπεδο 2: Επίπεδο Ελέγχου Γραμμής Δεδομένων / Ζεύξης Δεδομένων (Data Link Layer).

Όπως φαίνεται παραπάνω, το φυσικό επίπεδο δεν αναλαμβάνει να ασχοληθεί με τον έλεγχο της σωστής μετάδοσης των δεδομένων. Τη λειτουργία αυτή την αναλαμβάνει το επίπεδο ελέγχου γραμμής δεδομένων ή ζεύξης δεδομένων. Το επίπεδο ελέγχου γραμμής δεδομένων αναλαμβάνει τη μορφοποίηση και την ορθή μετάδοση των δεδομένων με ταυτόχρονο εντοπισμό και επιδιόρθωση των σφαλμάτων. Η στατιστική συγκυρία του δικτύου καθορίζει το χρόνο που μεσολαβεί ανάμεσα σε δύο εκπομπές διαδοχικών πλαισίων, ενώ ταυτόχρονα το επίπεδο αυτό αναλαμβάνει την εξασφάλιση της ομαλής συνεργασίας μεταξύ του φυσικού επιπέδου και των ανώτερων επιπέδων από αυτό.

Επίπεδο 3: Επίπεδο Δικτύου (Network Layer).

Στο επίπεδο δικτύου γίνεται η δρομολόγηση των πακέτων πληροφορίας από την αφετηρία στον προορισμό. Η δρομολόγηση αυτή είναι μια διαδικασία που, όπως είναι προφανές, έχει να κάνει με τις εκάστοτε κυκλοφοριακές συνθήκες του δικτύου κάθε χρονική στιγμή. Με άλλα λόγια, γίνεται μια χαρτογράφηση των δυνατών διαδρομών που μπορούν να ακολουθήσουν τα υπάρχοντα πακέτα και στη συνέχεια επιλέγεται η πιο συμφέρουσα, ώστε να αποφευχθεί ο τυχόν συνωστισμός και οι καθυστερήσεις. Για τη σωστή λειτουργία της δρομολόγησης έχουν αναπτυχθεί αρκετοί αλγόριθμοι που επιλύονται με κατανεμημένο τρόπο, ενώ απαιτούν τη συνεργασία των ομόλογων επιπέδων δικτύου σε κάθε κόμβο. Μία ακόμη μέριμνα του επιπέδου δικτύου είναι η διευθέτηση της χρέωσης (accounting) της επικοινωνίας. Ανάλογα με τον αριθμό των πακέτων ή των χαρακτήρων που εκπέμπονται κάθε φορά γίνεται και η ανάλογη έκδοση λογαριασμού (billing). Επίσης επιλύονται προβλήματα που σχετίζονται με τη μετάβαση πακέτων από το ένα δίκτυο στο άλλο.

Επίπεδο 4: Επίπεδο Μεταφοράς / Διακίνησης (Transport Layer).

Το επίπεδο μεταφοράς έχει ως κύρια λειτουργία τη λήψη και τον τεμαχισμό των δεδομένων του επιπέδου συνόδου και το πέρασμά τους στο επίπεδο δικτύου με επιτυχία. Κάθε ενέργεια πρέπει να γίνεται έτσι ώστε τα ανώτερα στρώματα να απομονώνονται από τα κατώτερα για την αποφυγή τυχόν αλλαγών στο υλικό. Το επίπεδο μεταφοράς δημιουργεί μία σύνδεση ανάμεσα στο επίπεδο συνόδου και στο επίπεδο δικτύου. Ανάλογα με το throughput, μπορεί να υφίστανται και περισσότερες συνδέσεις, ή να γίνεται πολυπλεξία (multiplexing) για ελάττωση του κόστους.

Το επίπεδο μεταφοράς καθορίζει επίσης ποια υπηρεσία προσφέρει το στρώμα συνόδου. Η πιο σημαντική είναι η υπηρεσία ενός διαύλου σημείου προς σημείο (point to point), ενώ υπάρχουν και άλλες υπηρεσίες, όπως η μεταφορά μηνυμάτων χωρίς εγγύηση ορθής λήψης ή η πολλαπλή εκπομπή μηνυμάτων. Στο σημείο αυτό, αξίζει να σημειωθεί ότι το επίπεδο μεταφοράς είναι ένα επίπεδο από άκρο σε άκρο (end to end) από την αφετηρία στον προορισμό.

Τέλος, το επίπεδο μεταφοράς είναι υπεύθυνο για το σχηματισμό και τον τερματισμό των συνδέσεων ενός δικτύου, καθώς και τη ρύθμιση της ροής της πληροφορίας ανάμεσα στους hosts, έτσι ώστε ένας αργός host να μην «πνίγεται» από έναν γρήγορο. Αυτός ο έλεγχος ροής (flow control) μεταξύ των hosts διαφέρει αρκετά από τον αντίστοιχο έλεγχο ροής μεταξύ των δρομολογητών (routers), αν και διέπονται από τις ίδιες βασικές αρχές. Επίσης σε κάποιες εφαρμογές αναπτύσσονται ταυτόχρονα ανεξάρτητοι διάλογοι μεταξύ ζευγών τερματικών, που είναι συνδεδεμένοι σε διαφορετικούς κόμβους. Στην περίπτωση αυτή, το επίπεδο μεταφοράς αναλαμβάνει την πολυπλεξία πακέτων για να διευκολυνθεί η λειτουργία των κατώτερων επιπέδων.

Επίπεδο 5: Επίπεδο Συνόδου (Session Layer).

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

Επίπεδο 6: Επίπεδο Παρουσίασης (Presentation Layer).

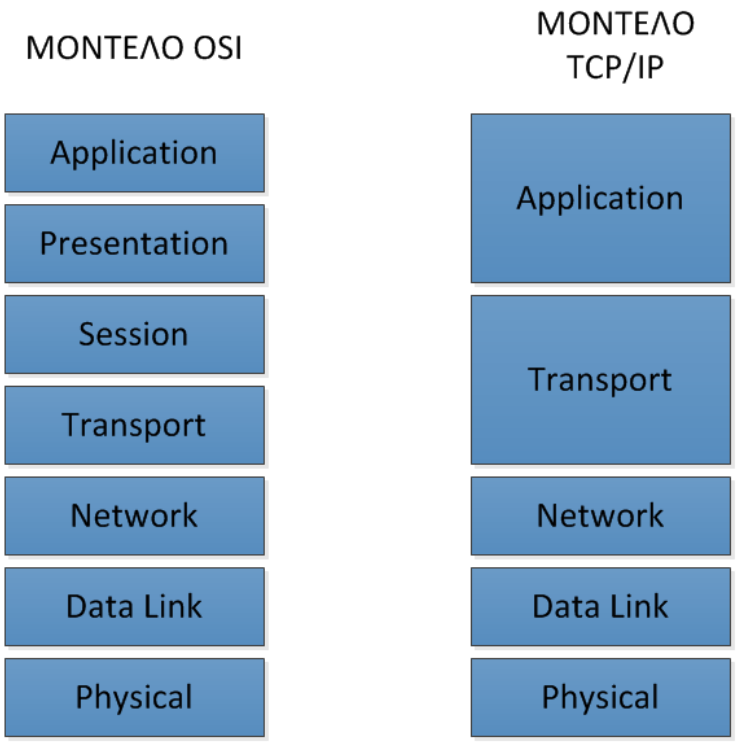
Επειδή τα δεδομένα τα οποία διακινούνται σε ένα δίκτυο είναι συνήθως συγκεκριμένου τύπου, το επίπεδο παρουσίασης ασχολείται με τη σύνταξη και τη σημασία της μεταδιδόμενης πληροφορίας. Παραδείγματα τέτοιων τύπων πληροφορίας είναι ακολουθίες χαρακτήρων με διαφορετικές κωδικοποιήσεις (ASCII, Unicode κλπ.), αριθμοί σταθερής ή κινητής υποδιαστολής, δομές δεδομένων κλπ.

Επίπεδο 7: Επίπεδο Εφαρμογών (Application Layer).

Το στρώμα εφαρμογής περιέχει έναν αριθμό συχνά χρησιμοποιούμενων πρωτοκόλλων, ενώ καθορίζει ένα δικτυακό νοητό τερματικό (network virtual terminal) για την επίτευξη της συμβατότητας μεταξύ των διάφορων υπαρχόντων τερματικών ανά τον κόσμο. Επίσης, το στρώμα αυτό επιλύει προβλήματα ασυμβατότητας σε περιπτώσεις μεταφοράς αρχείων, ηλεκτρονικού ταχυδρομείου κλπ.

2.3 Το μοντέλο TCP/IP.

Το μοντέλο TCP/IP ξεκίνησε από το δίκτυο ARPANET, το οποίο ήταν υπεύθυνο για τη σύνδεση πολλών πανεπιστημίων και κυβερνητικών εγκαταστάσεων, μέσω μισθωμένων γραμμών στις ΗΠΑ και είναι ο πρόγονος του σημερινού διαδικτύου. Με την μετέπειτα πρόσθεση ασύρματων και δορυφορικών δικτύων, χρειάστηκε να ληφθούν υπ' όψη οι τυχόν ασυμβατότητες ανάμεσα στα υπάρχοντα πρωτόκολλα, με τέτοιο τρόπο ώστε να συνδέονται μαζί πολλά δίκτυα με διαφανή τρόπο. Έτσι, προέκυψε το μοντέλο αναφοράς TCP/IP (TCP/IP Reference Model). Έπρεπε επίσης να ληφθεί υπόψη στην λειτουργία του μοντέλου η εξασφάλιση της αξιοπιστίας του δικτύου σε περίπτωση βλαβών κάποιων τμημάτων του υποδικτύου, έτσι ώστε το δίκτυο να παραμένει σε κατάσταση λειτουργίας, ακόμη και αν διαπιστωνόταν βλάβη σε κάποιο σημείο του. Έτσι και για το TCP/IP ορίζονται τα διάφορα επίπεδα συγκριτικά με τα αντίστοιχα του μοντέλου OSI όπως φαίνονται στην (Εικόνα 2.2).



Εικόνα 2.2 Το μοντέλο αναφοράς TCP/IP σε σχέση με το OSI.

Επίπεδο 1: Φυσικό επίπεδο (Physical Layer).

Το φυσικό επίπεδο είναι το ίδιο με το αντίστοιχο του μοντέλου OSI και σε αυτό καθορίζεται ο τρόπος με τον οποίο μεταδίδεται το σήμα μέσω κάποιου υλικού στο απέναντι άκρο της σύνδεσης.

Επίπεδο 2: Επίπεδο Ελέγχου Γραμμής Δεδομένων / Ζεύξης Δεδομένων (Data Link Layer).

Το επίπεδο έλεγχου γραμμής δεδομένων είναι ίδιο με το αντίστοιχο επίπεδο του μοντέλου OSI, το φυσικό επίπεδο δεν αναλαμβάνει να ασχοληθεί με τον έλεγχο της σωστής μετάδοσης των δεδομένων. Τη λειτουργία αυτή την αναλαμβάνει το επίπεδο ελέγχου γραμμής δεδομένων ή ζεύξης δεδομένων .

Επίπεδο 3: Επίπεδο Δικτύου (Network Layer).

Το επίπεδο δικτύου είναι ίδιο με το αντίστοιχο επίπεδο του μοντέλου OSI. Στο επίπεδο δικτύου γίνεται η δρομολόγηση των πακέτων πληροφορίας από την αφετηρία στον προορισμό. Η δρομολόγηση αυτή είναι μια διαδικασία που, όπως είναι προφανές, έχει να κάνει με τις εκάστοτε κυκλοφοριακές συνθήκες του δικτύου κάθε χρονική στιγμή.

Επίπεδο 4: Μεταφοράς (Transport).

Το επίπεδο μεταφοράς του μοντέλου TCP/IP είναι αντίστοιχο με το επίπεδο μεταφοράς του μοντέλου OSI. Στο επίπεδο αυτό έχουν οριστεί δύο βασικά πρωτόκολλα από άκρο σε άκρο. Το πρώτο ονομάζεται πρωτόκολλο ελέγχου μετάδοσης TCP (**T**ransmission **C**ontrol **P**rotocol) και η δουλειά του είναι να πετυχαίνει σωστή μετάδοση των δεδομένων από την αφετηρία στον προορισμό τους. Έτσι τεμαχίζει σε bytes την προς μετάδοση πληροφορία και τα περνάει μέσω του επιπέδου διαδικτύου. Στο δέκτη, το ίδιο πρωτόκολλο αναλαμβάνει τη σωστή συναρμολόγηση των δεδομένων ώστε να αναπαραχθεί η αρχική πληροφορία. Επίσης, το ίδιο πρωτόκολλο αναλαμβάνει τον έλεγχο ροής, ώστε να συγχρονίζεται η ταχύτητα του πομπού με την ταχύτητα του δέκτη. Το δεύτερο πρωτόκολλο ονομάζεται πρωτόκολλο γραφημάτων δεδομένων χρήστη UDP (**U**ser **D**atagram **P**rotocol). Το πρωτόκολλο αυτό είναι πρωτόκολλο χωρίς σύνδεση και δεν είναι τόσο αξιόπιστο, διότι δεν εκτελεί έλεγχο και διόρθωση σφαλμάτων. Είναι όμως πολύ γρηγορότερο από το TCP, γι' αυτό χρησιμοποιείται σε εφαρμογές που υπάρχει ανάγκη ταχύτατης μετάδοσης δεδομένων, όπως φωνής ή video. Ο έλεγχος της ορθής μετάδοσης της πληροφορίας αφήνεται στη δικαιοδοσία της εκάστοτε εφαρμογής.

Επίπεδο 5: Εφαρμογής (Application).

Στο μοντέλο TCP/IP δεν υπάρχουν τα επίπεδα συνόδου και παρουσίασης, λόγω της μη αναγκαιότητάς τους. Έτσι, το επίπεδο εφαρμογής είναι το μόνο ανώτερο επίπεδο που συμπεριλαμβάνει τα πρωτόκολλα των ανωτέρων στρωμάτων.

Τα πρωτόκολλα που περιλαμβάνονται είναι το νοητό τερματικό (TELNET), η μεταφορά αρχείων (FTP), το ηλεκτρονικό ταχυδρομείο (SMTP), το DNS, το NNTP, το HTTP κλπ.

2.4 Τα πρωτόκολλα μεταφοράς του Internet.

Τα δύο σημαντικότερα πρωτόκολλα μεταφοράς στο Internet είναι τα πρωτόκολλα TCP και UDP. Το Πρωτόκολλο Ελέγχου Μετάδοσης TCP (**T**ransmission **C**ontrol **P**rotocol) είναι πρωτόκολλο με σύνδεση, ενώ το Πρωτόκολλο γραφημάτων Δεδομένων Χρήστη UDP (**U**ser **D**atagram **P**rotocol) είναι πρωτόκολλο χωρίς σύνδεση.

2.4.1 Το πρωτόκολλο TCP.

Το TCP σχεδιάστηκε στην αρχή για να γίνει εφικτή η μετάδοση μιας σειράς από bits στο διαδίκτυο. Με τον όρο διαδίκτυο (Internet) εννοούμε ένα πολύ μεγάλο δίκτυο, το οποίο αποτελείται από διαφορετικού τύπου υπολογιστές, αλλά επίσης χωρίζεται σε πολλά επίπεδα δικτύωσης και εφαρμογών , τα οποία μπορεί να διέπονται από ποικίλα χαρακτηριστικά.

Τα χαρακτηριστικά αυτά είναι το εύρος ζώνης, η τοπολογία, οι καθυστερήσεις, τα μεγέθη πακέτων, καθώς και άλλες παράμετροι που μπορούν να διαφέρουν από το ένα δίκτυο στο άλλο. Το TCP αναλαμβάνει τη σωστή διασύνδεση των παραπάνω διαφορετικών δικτύων, έτσι ώστε να μπορεί να υπάρξει μια επιτυχής επικοινωνία παρά τις επιμέρους διαφορές.

Η πληροφορία δεδομένων χρήστη συνήθως τεμαχίζεται σε κομμάτια που δεν ξεπερνούν τα 64 Kbytes (στην πραγματικότητα είναι γύρω στα 1500 bytes) και κάθε τμήμα αποστέλλεται ως ένα ξεχωριστό IP Datagram (γράφημα δεδομένων). Όταν τα γραφήματα δεδομένων IP που περιέχουν δεδομένα TCP φτάνουν στον προορισμό τους, αυτά ανασυντίθενται και έτσι ανασχηματίζεται η αρχική πληροφορία όπως ακριβώς μεταδόθηκε. Επειδή δεν είναι σίγουρη η επιτυχής μετάδοση των γραφημάτων δεδομένων από το στρώμα IP, είναι δουλειά του TCP να επανεκπέμψει τα πακέτα, σε περίπτωση που περάσει ο απαραίτητος χρόνος και δεν έχει γίνει επαλήθευση της λήψης.

Το TCP είναι υπεύθυνο για τη σωστή συναρμολόγηση των γραφημάτων δεδομένων, σε περίπτωση που τα τελευταία φτάσουν με διαφορετική σειρά από αυτήν που στάλθηκαν. Με άλλα λόγια, το TCP προσπαθεί σε κάθε περίπτωση να εξασφαλίσει την αξιοπιστία της μεταφοράς της πληροφορίας.

Στην υπηρεσία TCP, τα ακραία σημεία (end points) και των δύο πλευρών ονομάζονται υποδοχές (sockets). Κάθε μία από αυτές χαρακτηρίζεται από έναν συγκεκραμένο αριθμό (διεύθυνση) υποδοχής των 16 bits για κάθε host, που αποκαλείται θύρα (port). Κάθε υποδοχή μπορεί να χρησιμοποιείται για πολλές συνδέσεις την ίδια στιγμή. Οι συνδέσεις αυτές χαρακτηρίζονται από την ταυτότητα (identifier) κάθε υποδοχής. Οι θύρες, των οποίων ο αριθμός είναι μικρότερος του 1024, ονομάζονται πασίγνωστες θύρες (well-known ports) και χρησιμοποιούνται για τις πιο τυποποιημένες υπηρεσίες.

Οι συνδέσεις TCP είναι αμφίδρομες. Μπορεί να έχουν οποιαδήποτε κατεύθυνση από σημείο σε σημείο, δηλαδή η κίνηση των πληροφοριών γίνεται από το ένα σημείο στο άλλο και αντίστροφα, χωρίς όμως να υπάρχει πολλαπλή διανομή ή εκπομπή. Επειδή η κίνηση προς τις δύο κατευθύνσεις μπορεί να γίνει ταυτόχρονα,

οι συνδέσεις αποκαλούνται πλήρως αμφίδρομες. Για τη μετάδοση της πληροφορίας από το ένα σημείο στο άλλο, τα όρια των ομάδων των bytes προς μεταφορά μπορεί να μην είναι σταθερά στην αφετηρία και στο τέλος.

Ο αποστολέας και ο παραλήπτης στέλνουν και λαμβάνουν την πληροφορία αντίστοιχα σε τεμάχια (segments). Το κάθε ένα από αυτά αποτελείται από μια σταθερή επικεφαλίδα (header) των 20 bytes. Ανάλογα με την περίσταση, το TCP software αποφασίζει κάθε φορά το πόσο μεγάλα θα είναι τα τεμάχια. Αυτό γίνεται με δύο περιορισμούς. Πρώτον, το κάθε τεμάχιο, συμπεριλαμβανομένης της επικεφαλίδας TCP, θα πρέπει να χωράει στο ωφέλιμο φορτίο IP των 65535 bytes και δεύτερον, το κάθε δίκτυο θα πρέπει να έχει μια Μέγιστη Μονάδα Μεταφοράς MTU (Maximum Transfer Unit). Κάθε τεμάχιο πρέπει να χωράει στην MTU, (η οποία είναι πρακτικά ορισμένες χιλιάδες bytes). Ανάλογα με την MTU του εκάστοτε δικτύου, ο αντίστοιχος δρομολογητής τεμαχίζει το εν λόγω κομμάτι με τέτοιο τρόπο, ώστε τα τεμάχια που προκύπτουν, να χωρούν στη συγκεκριμένη MTU. Βέβαια, σε κάθε περίπτωση προστίθεται η αντίστοιχη πληροφορία επικεφαλίδας προκαλώντας επιπλέον επιβάρυνση στο δίκτυο.

Το πιο σημαντικό πρωτόκολλο που χρησιμοποιείται είναι αυτό του ολισθαίνοντος παραθύρου (sliding window protocol). Με την αποστολή κάθε τεμαχίου ξεκινάει ταυτόχρονα η λειτουργία ενός χρονομετρητή. Με την άφιξη του τεμαχίου στον προορισμό του επιστρέφεται ένα τεμάχιο που περιέχει έναν αριθμό επαλήθευσης, που ισούται με τον επόμενο αύξοντα αριθμό του τεμαχίου, που περιμένει να παραλάβει. Αν ο χρόνος λήξει πριν την παραλαβή του τεμαχίου, το τεμάχιο αποστέλλεται εκ νέου. Υπάρχουν αρκετές δυνατές περιπτώσεις που πρέπει να ληφθούν υπόψη στο συγκεκριμένο πρωτόκολλο. Αυτές έχουν να κάνουν με ενδεχόμενη απώλεια ενός τμήματος του τεμαχίου, λανθασμένη σειρά άφιξης, πολλαπλές αφίξεις τεμαχίων κλπ. Το TCP οφείλει να αντιμετωπίζει τέτοια ζητήματα, καθώς και ζητήματα συμφόρησης, όπως θα εξεταστεί στη συνέχεια.

2.4.2 Έλεγχος συμφόρησης στο TCP.

Η συμφόρηση (congestion) εμφανίζεται όταν το προσφερόμενο φορτίο σε κάποιο δίκτυο είναι μεγαλύτερο από το φορτίο, που μπορεί το δίκτυο αυτό να αντιμετωπίσει. Παρόλο που η διαχείριση της συμφόρησης υπάγεται στο επίπεδο δικτύου, η τελική αντιμετώπιση γίνεται από το TCP. Έτσι, ο γενικός κανόνας για την αντιμετώπιση της συμφόρησης είναι η ελάττωση του ρυθμού δεδομένων. Η κεντρική ιδέα είναι να μην εισχωρεί κανένα πακέτο στο δίκτυο μέχρι την αποχώρηση ενός παλαιότερου.

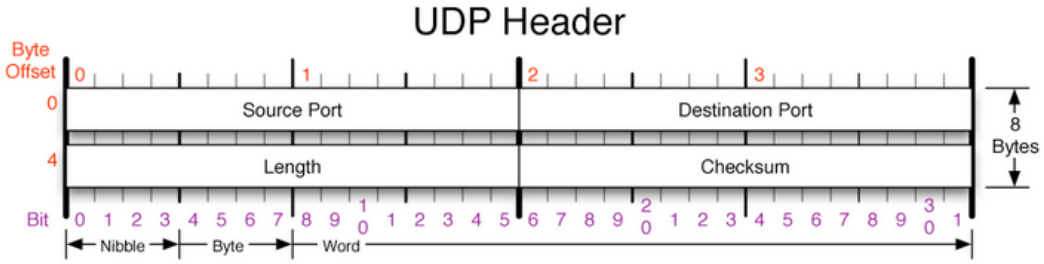
Στο παρελθόν ο εντοπισμός της συμφόρησης ήταν αρκετά δύσκολος, διότι ήταν δύσκολο να εντοπιστεί η αιτία της εκπνοής χρόνου. Η τελευταία μπορούσε να οφείλεται σε θόρυβο στη γραμμή ή σε απόρριψη πακέτου σε κάποιο δρομολογητή λόγω συμφόρησης. Στη σημερινή εποχή είναι αρκετά απίθανη η απώλεια πακέτων λόγω σφαλμάτων μετάδοσης, αφού η συντριπτική πλειοψηφία των ζεύξεων είναι οπτικές. Αυτό συνεπάγεται ότι οι περισσότερες εκπνοές χρόνου στο Internet οφείλονται στη συμφόρηση.

2.4.3 Το πρωτόκολλο UDP.

Το Πρωτόκολλο γραφημάτων δεδομένων Χρήστη UDP (User Datagram Protocol) είναι ένα πρωτόκολλο μεταφοράς του Internet χωρίς σύνδεση.

Με το UDP, οι εφαρμογές μπορούν να στέλνουν ενθυλακωμένα ακατέργαστα IP γραφήματα δεδομένων χωρίς να προϋποθέτουν την εκ των προτέρων εγκατάσταση μιας σύνδεσης. Έτσι πολλές εφαρμογές client-server χρησιμοποιούν το UDP αντί για το TCP, ώστε να αποφύγουν τη δημιουργία σύνδεσης. Η επικεφαλίδα ενός τεμαχίου UDP φαίνεται παρακάτω στην (Εικόνα 2.3), και αποτελείται από 4 πεδία των 16 bits. Αυτά είναι τα εξής:

1. **Θύρα πηγής (Source Port).**
2. **Θύρα προορισμού (Destination Port).**
3. **Μήκος UDP (Length).**
4. **Άθροισμα Ελέγχου UDP (Checksum).**



Εικόνα 2.3: Η επικεφαλίδα UDP.

2.5 Τεχνολογία Frame Relay.

Η τεχνολογία Frame Relay είναι μια υπηρεσία που έχει σαν στόχο την οικονομική δημιουργία τηλεπικοινωνιών και χρησιμοποιείται από δίκτυα που έχουν σαν στόχο την αξιόπιστη σύνδεση για να μεταδώσουν bits με λογική ταχύτητα και χαμηλό κόστος. Η υπηρεσία αυτή σχετίζεται με τη διαχείριση της τηλεπικοινωνιακής κίνησης ανάμεσα σε τοπικά δίκτυα (LANs) και ανάμεσα σε τερματικά σημεία (end points) σε ένα δίκτυο ευρείας ζώνης (WAN).

Το πρωτόκολλο Frame Relay τοποθετεί τα δεδομένα προς μετάδοση σε ομάδες μεταβλητού μήκους (συνήθως 1600 bytes), ονομαζόμενες ως frames (πλαίσια), ενώ δεν παίρνει κανένα μέτρο για τη διόρθωση τυχόν σφαλμάτων κατά τη μετάδοση, η διαδικασία διόρθωσης αφήνεται στη δικαιοδοσία των τερματικών σημείων (end points).

Η απλοποίηση αυτή επιταχύνει την όλη διαδικασία. Για τις περισσότερες υπηρεσίες το δίκτυο παρέχει ένα Μόνιμο Εικονικό Κύκλωμα (**P**ermanent **V**irtual **C**ircuit - PVC), άρα ο εκάστοτε συνδρομητής «βλέπει» μια σταθερή σύνδεση, χωρίς να πρέπει να πληρώσει για μια δεσμευμένη γραμμή για πλήρη χρόνο. Παράλληλα, ο παροχέας υπηρεσιών έχει τη δυνατότητα να παρατηρεί τη διαδρομή που διανύει

το κάθε frame και αναλόγως να κοστολογεί την κάθε επικοινωνία.

Τα διάφορα frames μπορούν να χαρακτηρίζονται από διαφορετικούς συντελεστές προτεραιότητας, ανάλογα με το πόσο σημαντικά είναι. Η διαφορά ανάμεσα στην υπηρεσία Frame Relay και στη μόνιμη μισθωμένη γραμμή είναι ότι η τελευταία επιτρέπει στον πελάτη να στέλνει δεδομένα κατά τη διάρκεια της ημέρας χρησιμοποιώντας τον μέγιστο ρυθμό μετάδοσης, ενώ για την εικονική μπορεί μεν να γίνει με μέγιστο ρυθμό, αλλά με περιορισμό του μέσου ρυθμού δεδομένων, άρα η υπηρεσία Frame Relay είναι πιο φθηνή. Η ταχύτητα του Frame Relay φθάνει το 1.5 Mbps και χρησιμοποιεί μια αφιερωμένη (dedicated) σύνδεση κατά τη διάρκεια μιας περιόδου αποστολής frames.

Η χρήση του Frame Relay είναι περιορισμένη σε ότι αφορά την μετάδοση video ή φωνής, λόγω της ανάγκης ύπαρξης σταθερής ροής. Όμως, κάτω από συγκεκριμένες συνθήκες, η χρήση του Frame Relay μπορεί να γίνει αποδεκτή. Τέλος η μετάδοση των πακέτων γίνεται στο επίπεδο ελέγχου γραμμής (data link control layer) και όχι στο επίπεδο δικτύου (network layer) του μοντέλου OSI.

2.6 Τεχνολογία ATM.

Το ATM σημαίνει **A**synchronous **T**ransfer **M**ode (Ασύγχρονος Τρόπος Μετάδοσης). Η ονομασία αυτή οφείλεται στο γεγονός ότι δεν υπάρχει συγχρονισμός στο δίκτυο, άρα το δίκτυο στηρίζεται σε ασύγχρονο τρόπο μετάδοσης των δεδομένων.

Το ATM είναι μια τεχνολογία υψηλών ταχυτήτων και έχει τη δυνατότητα να μεταφέρει ταυτόχρονα φωνή, δεδομένα, γραφικά και βίντεο σε πολύ υψηλές ταχύτητες. Πρόκειται για μια υπηρεσία υψηλού κόστους και ως εκ τούτου αρκετά ακριβή, άρα όχι και τόσο ευρέως διαδεδομένη σε παγκόσμια κλίμακα. Οι συνήθεις χρήστες αυτής της υπηρεσίας είναι μεγάλες επιχειρήσεις και οργανισμοί, οι οποίοι είναι απαραίτητο να διεκπεραιώσουν τεράστιο όγκο δεδομένων.

Η αρχική ιδέα ήθελε το ATM να είναι η τεχνολογία που θα αντικαθιστούσε το απλό PSTN με το "**B**roadband **I**ntegrated **S**ervices **D**igital **N**etwork" ή αλλιώς B-ISDN. Παρέχει προδιαγραφές για το επίπεδο 1 (φυσικό επίπεδο), το επίπεδο 2 (επίπεδο ελέγχου γραμμής) και το επίπεδο 3 (επίπεδο δικτύου) του μοντέλου OSI. Τα standards του ATM βασίστηκαν περισσότερο στις αρχές της τηλεπικοινωνιακής κοινότητας και όχι σε αυτές της κοινότητας επικοινωνίας υπολογιστών. Για το λόγο αυτό έγινε εκτενής προσπάθεια για την προσαρμογή των υπαρχουσών τηλεπικοινωνιακών τεχνολογιών και τη μετατροπή τους σε ATM.

Το ATM είναι ένα δικτυακό πρωτόκολλο που κωδικοποιεί τα δεδομένα προς μετάδοση σε κελιά (cells) 53 bytes, από τα οποία τα 48 είναι bytes πληροφορίας και τα υπόλοιπα 5 περιέχουν πληροφορίες προθέματος (header). Εφόσον μεταφέρονται μέσω δικτύου κελιά πληροφορίας, στο ATM γίνεται μεταγωγή κελιού (cell switching), και όχι μεταγωγή κυκλώματος (circuit switching) όπως στο παραδοσιακό τηλεφωνικό δίκτυο. Η μέθοδος κωδικοποίησης σε κελιά (cell relay) έρχεται σε αντίθεση με τη χρήση πακέτων μεταβλητού μήκους (ή frames), όπως συμβαίνει σε δίκτυα μεταγωγής πακέτων όπως στο **I**nternet

Protocol (IP) ή στο Ethernet. Πρόκειται για μία connection – oriented τεχνολογία, σύμφωνα με την οποία δημιουργείται μια σύνδεση ανάμεσα στα δύο τερματικά σημεία, προτού ξεκινήσει η ανταλλαγή των δεδομένων.

Οι μεταγωγείς ATM (ATM switches) είναι πολύ γρήγοροι και επιταχύνουν τα δεδομένα πάνω από το δίκτυο ATM. Το μεγάλο εύρος ζώνης που συσχετίζεται με το ATM μειώνει δραματικά τα προβλήματα συμφόρησης του δικτύου, παρέχοντας έτσι μια αρκετά αξιόπιστη υπηρεσία. Οι φορείς μπορούν έτσι να υπόσχονται στους πελάτες τους Ποιότητα Υπηρεσίας (Quality of Service – QoS).

2.7 Ethernet.

Το Ethernet είναι το συνηθέστερα χρησιμοποιούμενο πρωτόκολλο ενσύρματης τοπικής δικτύωσης υπολογιστών. Αναπτύχθηκε από την εταιρεία Xerox κατά τη δεκαετία του '70 και έγινε δημοφιλές αφότου η Digital Equipment Corporation και η Intel, από κοινού με τη Xerox, προχώρησαν στην προτυποποίησή του το 1980. Το 1985 το Ethernet έγινε αποδεκτό επίσημα από τον οργανισμό IEEE ως το πρότυπο 802.3 για ενσύρματα τοπικά δίκτυα (LAN).

Το αρχικό Ethernet επέτρεπε ονομαστικούς ρυθμούς μετάδοσης δεδομένων της τάξης των 3 Mbps, μέσω ενός ομοαξονικού καλωδίου, στο οποίο συνδέονταν οι επιμέρους υπολογιστές του δικτύου (σύνδεση token ring). Τη διασύνδεση αναλάμβανε μία κάρτα δικτύου Ethernet προσαρτημένη σε κάθε κόμβο, με κάθε κάρτα να χαρακτηρίζεται από μία μοναδική, εργοστασιακή 48-bit διεύθυνση MAC.

Σήμερα η σύνδεση token ring έχει εγκαταλειφθεί ολοκληρωτικά και οι επιμέρους υπολογιστές του δικτύου συνδέονται ο καθένας σε ανεξάρτητη θύρα ενός router ή διανομέα (hub). Έχουν εμφανιστεί νεότερες εκδόσεις του Ethernet, οι οποίες χρησιμοποιούν είτε κοινά καλώδια χαλκού με αθωράκιστα (καλώδια UTP) ή θωρακισμένα (καλώδια STP), είτε συνεστραμμένα ζεύγη αγωγών ή οπτικές ίνες:

- **Ethernet (10 MBps):** Για τις συνδέσεις με χαλκό χρησιμοποιείται το πρότυπο 10BASE-T και για τις οπτικές ίνες το πρότυπο 10BASE-F(L). Η σύνδεση χαλκού είναι συμβατή με αυτή του Fast Ethernet.

- **Fast Ethernet (100 Mbps)**: Για τις συνδέσεις με χαλκό έχει επικρατήσει το πρότυπο 100BASE-TX έναντι των ουσιαστικά εγκαταλελειμμένων 100BASE-T2, 100BASE-T4. Το 100BASE-TX χρησιμοποιεί καλώδια UTP κατηγορίας 5e (CAT-5e) με 2 ζεύγη αγωγών (ένα για αποστολή και ένα για λήψη δεδομένων), σε μήκη μέχρι 100 μ. Πρακτικά, χρησιμοποιούνται καλώδια 4 ζευγών, ώστε να είναι δυνατή η σύνδεση σε Gigabit Ethernet (1000BASE-TX). Το αντίστοιχο πρότυπο για τις οπτικές ίνες είναι το 100BASE-FX. Επιπλέον είναι δυνατή η αυτόματη ανίχνευση κυκλώματος 10BASE-T στην άλλη πλευρά του καλωδίου και η εν συνεχεία υποβάθμιση της ταχύτητας στα 10 Mbps (λειτουργία auto-negotiation).

- **Gigabit Ethernet (1 Gbps):** Για τις συνδέσεις με χαλκό έχει επικρατήσει το πρότυπο 1000BASE-T. Το 1000BASE-T χρησιμοποιεί καλώδια UTP κατηγορίας

5e (CAT-5e) με 4 ζεύγη αγωγών. Κάθε ζεύγος μεταφέρει δεδομένα προς τις δύο κατευθύνσεις ταυτόχρονα, ώστε να επιτυγχάνεται η μέγιστη δυνατή ταχύτητα μετάδοσης δεδομένων προς κάθε κατεύθυνση. Ο τρόπος σύνδεσης των ζευγών είναι τέτοιος που επιτρέπει σε μια κάρτα Gigabit Ethernet να μπορεί να ανιχνεύσει την ύπαρξη κυκλώματος Fast Ethernet στην άλλη άκρη του καλωδίου και να αλλάξει αυτόματα το πρωτόκολλό της σε 100BASE-TX (λειτουργία auto-negotiation). Το αντίστοιχο πρότυπο για τις οπτικές ίνες είναι τα 1000BASE-FX.

2.7.1 Οργάνωση δεδομένων.

Οι προδιαγραφές που ορίζει το Ethernet αφορούν στο φυσικό επίπεδο και στο υποεπίπεδο MAC του μοντέλου αναφοράς OSI. Στη μεγάλη πλειονότητα των περιπτώσεων μαζί με το Ethernet χρησιμοποιείται, στο υποεπίπεδο LLC, το πρωτόκολλο IEEE 802.2. Για τον έλεγχο πρόσβασης στο κοινό μέσο το Ethernet αξιοποιεί τον αλγόριθμο CSMA/CD (**C**arrier **S**ense **M**ultiple **A**ccess with **C**ollision **D**etection), στις περιπτώσεις όπου επιτρέπεται μόνο half-duplex σύνδεση.

Πρακτικά, το Ethernet χρησιμοποιεί τη μέθοδο μετάδοσης δεδομένων σε μορφή πακέτων (packet switching) μέγιστου μεγέθους 1500 bytes και ελάχιστου 46 bytes. Για το σκοπό αυτό, δεδομένα με μήκος μεγαλύτερο των 1500 bytes κατατέμνονται σε πακέτα των 46-1500 bytes (το λεγόμενο payload), τα οποία αποστέλλονται διαδοχικά στη γραμμή επικοινωνίας. Αν το payload έχει μήκος μικρότερο των 46 bytes, προστίθενται επιπλέον κενά bytes ώστε αυτό να αποκτήσει το επιθυμητό ελάχιστο μήκος. Εκτός από το payload, προστίθενται πληροφορίες όπως ο σειριακός αριθμός της κάρτας Ethernet, οι φυσικές διευθύνσεις (MAC addresses) αποστολέα και παραλήπτη, το μήκος του payload, καθώς και δεδομένα για έλεγχο σφαλμάτων κατά τη μετάδοση.

Κεφάλαιο 3.

Τηλεφωνία VoIP.

3.1 VoIP: Πρωτόκολλα.

Το VoIP, όπως υποδηλώνει και το όνομά του, χρησιμοποιεί το IP (**I**nternet **P**rotocol) για τη μετάδοση φωνής. Αυτό σημαίνει πως χρησιμοποιεί ως μέσο μετάδοσης οποιοδήποτε IP δίκτυο, ανεξαρτήτως των πρωτοκόλλων επιπέδου σύνδεσης δεδομένων και φυσικού επιπέδου. Δηλαδή το πρωτόκολλο που χρησιμοποιείται στο επίπεδο δικτύου είναι πάντα το IP, και στα χαμηλότερα επίπεδα μπορεί να χρησιμοποιηθεί οποιοδήποτε συμβατό πρωτόκολλο. Στο επίπεδο μεταφοράς και εφαρμογής μπορεί να υπάρχουν διαφοροποιήσεις ανάλογα με την υλοποίηση.

Η λειτουργία ενός συστήματος VoIP σε μια σύνοδο (session) θα μπορούσε να χωριστεί σε δύο μέρη:

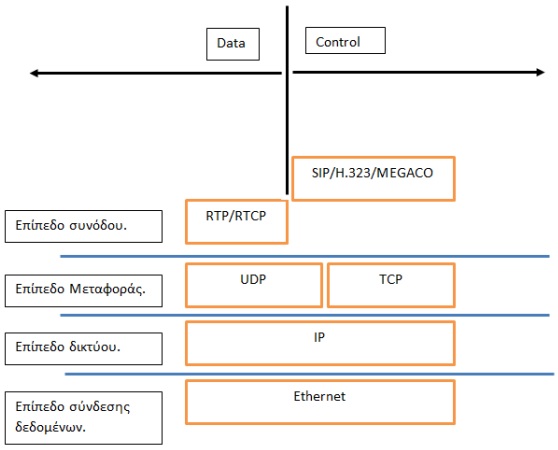
1. **Στη δημιουργία και μετάδοση πακέτων φωνής.**

   Για την μετάδοση πακέτων φωνής χρησιμοποιείται στο επίπεδο μεταφοράς, στην συντριπτική πλειοψηφία των εφαρμογών, το πρωτόκολλο RTP (**R**eal **T**ime **T**ransport **P**rotocol) πάνω από το UDP (**U**ser **D**atagram **P**rotocol).

2. **Στον έλεγχο της VoIP κλήσης.**

   Για τον έλεγχο της κλήσης χρησιμοποιούνται πρωτόκολλα επιπέδου συνόδου (OSI)/εφαρμογής (TCP/IP) τα οποία έχουν την ευθύνη για την έναρξη (call setup), την τροποποίηση και τον τερματισμό μιας VoIP κλήσης. Τα πιο διαδεδομένα πρωτόκολλα συνόδου είναι το SIP (**S**ession **I**nitiation **P**rotocol), και το σύνολο πρωτοκόλλων H.323. Αυτά τα πρωτόκολλα χρησιμοποιούν το TCP και το UDP στο επίπεδο μεταφοράς. Και τα δύο πρωτόκολλα ανήκουν στην κατηγορία των πρωτοκόλλων σηματοδοσίας και δεν συνιστούν από μόνα τους μία ολοκληρωμένη VoIP εφαρμογή. Για το λόγο αυτό, πρέπει να συνυπάρχουν και να συνεργάζονται με ήδη υπάρχοντα πρωτόκολλα, όπως τα TCP/IP, SDP, RTP, RTCP και το MEGACO/H.248 .

Τα παραπάνω πρωτόκολλα αφορούν στην περιγραφή των παραμέτρων μιας VoIP κλήσης, στη μεταφορά δεδομένων φωνής ή άλλων δεδομένων μεταξύ δύο ή περισσότερων τελικών χρηστών, ενώ επιπλέον, επιτρέπουν την επικοινωνία χρηστών που ανήκουν σε διαφορετικά δίκτυα. Στην Εικόνα 3.1 παρουσιάζεται μια στοίβα πρωτοκόλλων VoIP με χρήση RTP.



Εικόνα 3.1 : Στοίβα VoIP πρωτοκόλλων με χρήση RTP.

Όπως μπορεί να παρατηρήσει κάποιος στην (Εικόνα 3.1), το VoIP όπως όλες οι εφαρμογές internet ακολουθούν τη διαστρωμάτωση του OSI των 7 επιπέδων. Το φυσικό επίπεδο και το επίπεδο ζεύξης δεδομένων είναι κοινά με άλλες εφαρμογές του internet .

3.2 Τα πρωτόκολλα RTP/RTCP.

Για να υπάρξει επιτυχής μετάδοση πολυμέσων πάνω από IP δίκτυα, ο οργανισμός IETF πρότεινε το RTP (**R**eal **T**ime **T**ransport **P**rotocol) πρωτόκολλο. Έτσι το RTP αποτελεί το πλέον διαδεδομένο πρωτόκολλο για τη μεταφορά δεδομένων πραγματικού χρόνου όπως τα δεδομένα βίντεο και ήχου.

Στην αρχή σχεδιάστηκε για multicast επικοινωνία αλλά στην συνέχεια χρησιμοποιήθηκε και για unicast επικοινωνία. Το RTP δεν εγγυάται ποιότητα υπηρεσίας (QoS), αφού χρησιμοποιεί το UDP και όχι το TCP/IP, αλλά παρέχει υπηρεσίες που είναι πολύτιμες για την μεταφορά δεδομένων πραγματικού χρόνου.

Το RTP αποτελείται ουσιαστικά από δύο μέρη, το RTP, που είναι υπεύθυνο για τη μετάδοση των πακέτων δεδομένων, και το RTCP (**R**eal – **T**ime **T**ransport **C**ontrol **P**rotocol) που είναι υπεύθυνο για το έλεγχο της μετάδοσης.

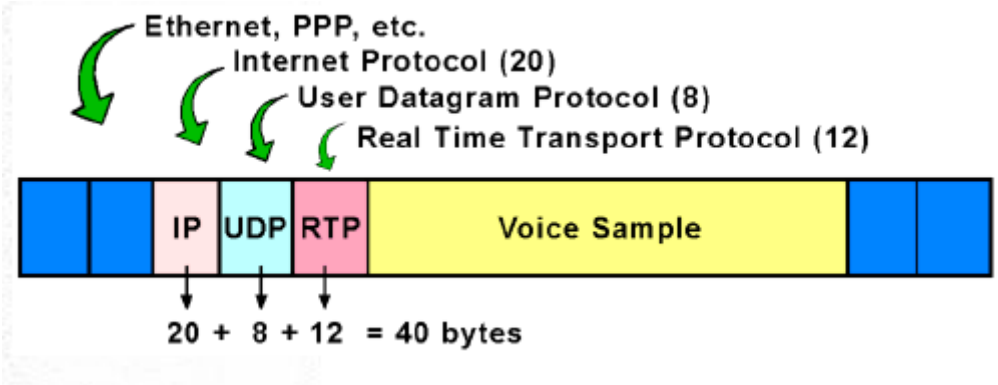
3.2.1 RTP.

Η μετάδοση εικόνας και ήχου και γενικότερα οι εφαρμογές πολυμέσων προϋποθέτουν αυστηρά χρονικά περιθώρια στην μετάδοση δεδομένων, πράγμα που δεν μπορεί να υλοποιηθεί με τα γνωστά πρωτοκολλά μεταφοράς δεδομένων (UDP/TCP). Το πρωτόκολλο RTP λειτουργώντας συμπληρωματικά κυρίως πάνω από το UDP επιτρέπει αποτελεσματική μετάδοση χρονικά κρίσιμων δεδομένων, δίνοντας την δυνατότητα χρονοσήμανσης, (time stamping) και σειριακή αρίθμηση των πακέτων (sequence numbering).

Η χρονοσήμανση παρέχει σημαντικές πληροφορίες στις εφαρμογές πραγματικού χρόνου. Ο αποστολέας βάζει σε κάθε πακέτο μια χρονοσήμανση (timestamp), την οποία χρησιμοποιεί ο παραλήπτης για να βρει τη χρονική στιγμή που πρέπει να παρουσιάσει τα δεδομένα του συγκεκριμένου πακέτου στον χρήστη. Δηλαδή, η χρονοσήμανση παρέχει την απαραίτητη πληροφορία ώστε να είναι δυνατό στους παραλήπτες να ανακατασκευάσουν τα αρχικά δεδομένα όπως αυτά μεταδόθηκαν από τον αποστολέα. Η χρονοσήμανση χρησιμοποιείται επίσης για το συγχρονισμό διαφορετικών ροών δεδομένων, όπως ροές δεδομένων βίντεο και ήχου. Χρησιμεύει επίσης στον υπολογισμό στατιστικών στοιχείων μιας ροής, όπως η διακύμανση της καθυστέρησης (jitter). Το UDP, το οποίο συνήθως χρησιμοποιείται για την μετάδοση των RTP πακέτων, δεν παραδίδει τα πακέτα με τη σειρά με την οποία στάλθηκαν, γι' αυτό τα RTP πακέτα αριθμούνται τη στιγμή που στέλνονται (sequence number), έτσι ώστε να μπορεί ο παραλήπτης να τα βάλει στη σωστή σειρά. Οι αριθμοί αυτοί χρησιμοποιούνται επίσης για να ανιχνεύονται απώλειες στη μετάδοση των πακέτων.

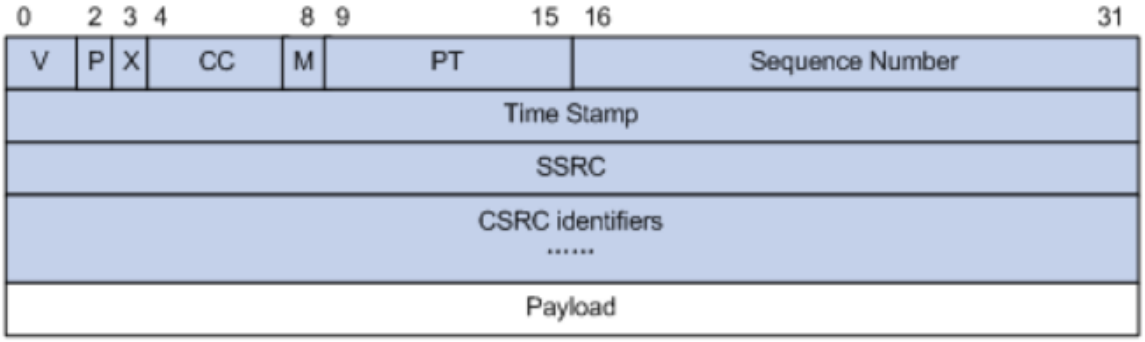
Η πληροφορία για την ταυτότητα του αποστολέα και για το περιεχόμενο της (payload type), είναι σημαντική για τον παραλήπτη, για να γνωρίζει ανά πάσα στιγμή τι είδους πληροφορία λαμβάνει, άρα να μπορεί να την ανασυνθέσει και να την παρουσιάσει στον χρήστη. Κάθε «πολυμεσική» κωδικοποίηση (π.χ. mpeg, G.711) καθορίζεται από έναν αριθμό – κωδικό (payload type) και σχετίζεται με κάποιο RTP profile. Το RTP profile καθορίζει τον τρόπο κωδικοποίησης και μετάδοσης μέσω του RTP. Έτσι ο παραλήπτης μέσω του payload type μπορεί να αναγνωρίσει το περιεχόμενο μιας ροής και με βάση το RTP profile της μπορεί να τη χειριστεί.

Το πρωτόκολλο RTP μεταδίδεται μέσω του UDP και του IP. Το header του IP είναι 20 bytes, του UDP είναι 8 bytes και του RTP 12 bytes. Άρα ένα RTP/UDP/IP πακέτο (Εικόνα 3.2) έχει συνολικό header 40 bytes. Το RTP/UDP/IP header μπορεί να μειωθεί στα 2 ή στα 4 bytes αν χρησιμοποιηθεί το συμπιεσμένο RTP (cRTP) που όμως χρησιμοποιείται μόνο σε WAN point to point συνδέσεις .



Εικόνα 3.2 : Ένα RTP/UDP/IP πακέτο.

Ένα RTP πακέτο αποτελείται από την RTP επικεφαλίδα (header) ακολουθούμενη από τα δεδομένα (payload). Το header ενός RTP πακέτου έχει μέγεθος 12 bytes και περιέχει πεδία με δομή όπως φαίνεται στην (Εικόνα 3.3).



Εικόνα 3.3: Τα πεδία ενός RTP header.

RTP header:

- **Timestamp (32 bits):** Το timestamp (χρονοσήμανση) αντανακλά τη στιγμή δειγματοληψίας του πρώτου δείγματος που περιέχεται στο RTP πακέτο είτε σε μονάδες χρόνου είτε σε αριθμό δειγμάτων που έχουν μεταδοθεί.
- **Payload Type (PT) (7 bits):** Το payload type καθορίζει τον τύπο των δεδομένων που ακολουθούν το RTP header.
- **Sequence Number (16 bits):** Το Sequence Number (αύξων αριθμός) μετρά τα πακέτα που στέλνει ο αποστολέας και αυξάνεται κατά ένα για κάθε πακέτο που μεταδίδεται. Επιτρέπει στον παραλήπτη να εντοπίσει κάποιο πακέτο που χάνεται και να αποκαθιστά την σωστή ακολουθία των πακέτων.

3.2.2 RTCP .

Το πρωτόκολλο RTCP χρησιμεύει στον έλεγχο των RTP ροών-συνόδων. Πιο συγκεκριμένα το RTCP παρέχει υπηρεσίες όπως παρακολούθηση της ποιότητας υπηρεσιών (QoS monitoring), αναγνώριση αποστολέα (source identification), συγχρονισμός ανάμεσα σε διαφορετικά μέσα, τερματισμός συνόδου.

Η παρακολούθηση της ποιότητας υπηρεσιών (QoS monitoring) είναι μια από τις βασικές λειτουργίες του πρωτοκόλλου. Το RTCP παρέχει πληροφορίες ανάδρασης (feedback) στις εφαρμογές για την ποιότητα της μετάδοσης των δεδομένων, όπως ο αριθμός των πακέτων δεδομένων που χάθηκαν, η διακύμανση της καθυστέρησης λήψης πακέτων (ιnterarrival jitter) καθώς και πληροφορίες χρόνου που επιτρέπουν τον υπολογισμό του round trip time. Το RTCP στηρίζει τις λειτουργίες του στην ανταλλαγή RTCP πακέτων διαφόρων ειδών πάνω από το UDP.

Τα είδη των RTCP πακέτων είναι:

- **Αναφορά αποστολέα (Sender Report - SR) και αναφορά παραλήπτη (Receiver Report - RR):**

  Οι παραλήπτες πληροφορίας σε μία RTP / RTCP σύνοδο επιστρέφουν στον εκάστοτε αποστολέα δεδομένα που αφορούν στην ποιότητα μετάδοσης. Αν ένα μέλος μιας συνόδου είναι μόνο παραλήπτης πληροφορίας αποστέλλει αναφορές παραλήπτη, ενώ αν είναι και αποστολέας πληροφορίας αποστέλλει και αναφορές αποστολέα.

- **Περιγραφή αποστολέα (Source Description - SDES):**

  Είναι ο τύπος του πακέτου που χρησιμοποιείται για να παρέχουν τα μέλη μιας συνόδου πληροφορίες σχετικές με τον εαυτό τους, για παράδειγμα όνομα, διεύθυνση ηλεκτρονικού ταχυδρομείου, το όνομα της εφαρμογής που χρησιμοποιείται στη σύνοδο καθώς και άλλα στοιχεία.

- **Πακέτο αποχαιρετισμού (Goodbye –BYE):**

  Ο τύπος αυτός σηματοδοτεί την αποχώρηση από τη σύνοδο ενός ή περισσοτέρων μελών.

- **Συγκεκριμένες συναρτήσεις εφαρμογής (Application specific - APP):**

  Είναι πακέτα που μπορεί να καθορίσει και να χρησιμοποιήσει μια εφαρμογή για δικές της λειτουργίες.

Το bandwidth που καταναλώνει η RTCP κίνηση μιας RTP ροής, δεν πρέπει να υπερβαίνει το 5% του συνολικού bandwidth που καταναλώνει η ροή και το ελάχιστο χρονικό διάστημα ανάμεσα στην αποστολή δύο RTCP πακέτων πρέπει να είναι 5 δευτερόλεπτα.

3.3 Το πρωτόκολλο MGCP/MEGACO.

Το MGCP (Media Gateway Control Protocol) είναι ένα πρωτόκολλο που χρησιμοποιείται για την μετατροπή των σημάτων των τηλεφωνικών κυκλωμάτων σε IP πακέτα, ώστε να μπορούν να μεταφερθούν μέσω διαδικτύου ή οποιουδήποτε δικτύου μεταγωγής πακέτων. Το MGCP αναπτύχθηκε για να υποστηρίζει και τα δύο βασικά πρωτόκολλα σηματοδοσίας (SIP και H.323), ενώ χρησιμοποιεί το Simple Gateway Control Protocol καθώς και το πρωτόκολλο IP.

Το Simple Gateway Control Protocol είναι αρμόδιο για τη μετατροπή ακουστικών σημάτων και σημάτων σηματοδοσίας των τηλεφωνικών κυκλωμάτων σε αντίστοιχα IP πακέτα και αντίστροφα. Μια εξελιγμένη έκδοση του MGCP είναι το MEGACO/H.248, το οποίο προήλθε από την συνεργασία των οργανισμών ITU και IETF και παρέχει λειτουργίες όμοιες με του MGCP.

3.4 Το πρωτόκολλο H.323.

Πιο πάνω από το επίπεδο συνοδού βρίσκεται το επίπεδο παρουσίασης. Η εισαγωγή του H.323 ήρθε σαν αποτέλεσμα της ανάγκης για τη δημιουργία ενός πρωτοκόλλου που θα μπορούσε να υποστηρίξει ικανοποιητικά εφαρμογές πολυμέσων και υπηρεσίας φωνής, με δυνατότητα για εξουδετέρωση της ανεπιθύμητης καθυστέρησης, που αποτελεί χαρακτηριστικό φαινόμενο στα κλασικά δίκτυα LAN, χωρίς ωστόσο υποχρέωση μεταβολής της υπάρχουσας υποδομής σε συσκευές και ενεργά στοιχεία δικτύου. Στοιχείο σημαντικό αποτέλεσε επίσης η ολοένα αυξανόμενη ικανότητα bandwidth των σύγχρονων δικτύων με τη μετάβαση πλέον σε ταχύτητες 10 Mbps ανά χρήστη, ή ακόμα και 100 Mbps με την εισαγωγή και ευρεία χρήση της Fast Ethernet τεχνολογίας. Οι ίδιες πλατφόρμες που χρησιμοποιεί ο χρήστης για τις εφαρμογές του έχουν αποκτήσει αξιοσημείωτη ταχύτητα τόσο αποθήκευσης, όσο και προβολής και επεξεργασίας στοιχείων. Έτσι το H.323 βρίσκεται στο επίπεδο παρουσίασης πιο πάνω από το επίπεδο συνοδού και έχει τα παρακάτω χαρακτηριστικά.

- Καθορισμό τεχνικών συμπίεσης δεδομένων, ακόμα κι αν ο αποστολέας και ο παραλήπτης ανήκουν σε διαφορετικούς κατασκευαστές.

- Ανεξαρτησία από την ήδη εγκατεστημένη δικτυακή υποδομή αφού δρα στην κορυφή των πρωτοκόλλων που χρησιμοποιούνται από την υπάρχουσα αρχιτεκτονική.

- Ανεξαρτησία από το είδος των συσκευών χρήστη (PC, Workstations κτλ).

- Δυνατότητα υποστήριξης Multicasting για ταυτόχρονη αποστολή πακέτων στους χρήστες ενός κοινού group.

- Διαχείριση bandwidth για έλεγχο των παράλληλων ενεργών H.323 συνδέσεων.

Η είσοδος του H.323 αποτέλεσε λοιπόν μία ολοκληρωμένη πρόταση για τη δημιουργία ενός δικτυακού περιβάλλοντος που ενσωματώνει πολλαπλές παλαιές και νέες τεχνολογίες από διαφορετικούς κατασκευαστές σε ένα ενιαίο πλαίσιο διαχείρισης πληροφορίας ήχου και εικόνας (Εικόνα 3.4).

Το Η.323 καθορίζει 4 είδη συντελεστών για να μπορεί να παρέχει τηλεπικοινωνιακές υπηρεσίες point- to-point και point-to-multipoint τα οποία είναι:

1. Terminal.

Πρόκειται για τα τελικά σημεία χρηστών, που υποστηρίζουν αμφίδρομη επικοινωνία, υποχρεωτικά επικοινωνιών φωνής και προαιρετικά βίντεο και δεδομένων. Το Η.323 καθορίζει τον τρόπο με τον οποίο διαφορετικοί τερματικοί σταθμοί είναι δυνατό να επικοινωνήσουν. Τα τερματικά θα πρέπει να υποστηρίζουν το Η.245 που κατευθύνει τη χρήση των καναλιών επικοινωνίας μεταξύ τερματικών σταθμών, το Q.931 για call και setup signaling, το RAS (**R**egistrationm **A**dmission **S**tatus) για επικοινωνία με το Gatekeeper καθώς επίσης και το RTP/RTCP για την αποστολή και λήψη των πακέτων ήχου. Ειδικά για την περίπτωση της επικοινωνίας με φωνή, απαιτείται το πρότυπο (CODEC) G.711 για συμπίεση και απόδοση πακέτων με ρυθμούς 54 ή 64 kbps σε ένα τοπικό δίκτυο δεδομένων.

Gateway.

Είναι το μοναδικό προαιρετικό στοιχείο του Η.323 και παρέχει τόσο το φυσικό όσο και το λογικό interface μεταξύ των τηλεφωνικών συσκευών και του επικοινωνιακού δικτύου και χρησιμοποιείται συνήθως για τους παρακάτω λόγους.

- Την επικοινωνία μεταξύ αναλογικών PSTN τερματικών.
- Την επικοινωνία με απομακρυσμένους Η.320 σταθμούς ISDN δικτύων.
- Την επικοινωνία με απομακρυσμένους Η.323 σταθμούς PSTN δικτύων.

Παρέχει standard interfaces προς την PSTN υπηρεσία και χρησιμοποιεί CODECs για τη μετατροπή τηλεφωνικών κυκλωμάτων σε πακέτα δεδομένων.

2. Gatekeeper.

Μέσω του RAS ο ελεγκτής πύλης (Gatekeeper) δρομολογεί πακέτα στο IP based δίκτυο. Όπως προαναφέρθηκε, η ύπαρξη του Gateway δεν είναι υποχρεωτική στην περίπτωση που οι τερματικοί σταθμοί θέλουν να επικοινωνούν μεταξύ τους εντός του τοπικού δικτύου και δεν ενδιαφέρονται για επικοινωνία εκτός αυτού. Αν όμως είναι παρών τότε οι πύλες και τα τερματικά πρέπει να χρησιμοποιούν τις υπηρεσίες που προσφέρουν. Γενικά παρέχει υπηρεσίες έλεγχου κλήσης όπως μετάφραση διευθύνσεων και διαχείριση εύρους ζώνης (Bandwidth), όπως αυτές έχουν οριστεί στο RAS. Ο ελεγκτής πύλης δεν είναι υποχρεωτικό τμήμα του δικτύου.

Το Η.323 ορίζει ότι ένας ελεγκτής πύλης (Gatekeeper) πρέπει να προσφέρει υποχρεωτικά κάποιες υπηρεσίες οι οποίες παρατίθενται παρακάτω.

- Μετάφραση διευθύνσεων (address translation).
- Έλεγχος εισόδου (admission control).
- Έλεγχος εύρους ζώνης (bandwidth control).
- Διαχείριση ζωνών (zone management).

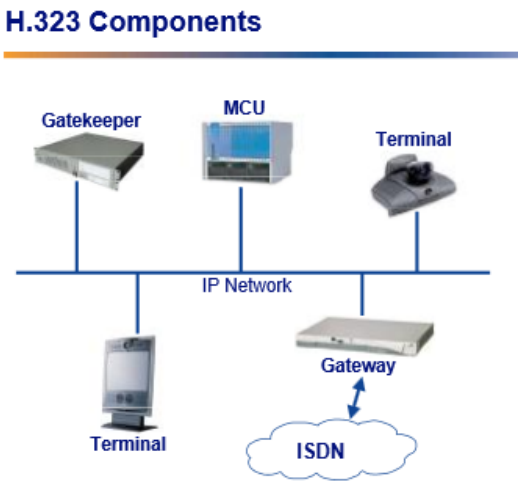
Επιπλέον ορίζονται και κάποιες προαιρετικές δυνατότητες :

- Σηματοδότηση έλεγχου κλήσης (call control signaling).
- Άδεια κλήσης (call authorization).
- Διαχείριση κλήσεων (call management).
- Δρομολόγηση σηματοδότησης κλήσης (call signaling routing).

Δεν είναι απαραίτητο να υπάρχει ως αυτόνομη συσκευή. Μπορεί να υλοποιείται σαν μέρος της πύλης ή του MCU.

3. Multipoint Conference Unit (MCU).

Το MCU καθορίζει και ελέγχει την ταυτόχρονη διασύνδεση (συνεδρία) περισσότερων των δύο τερματικών σταθμών. Αποτελείται από δύο διακριτά τμήματα, τον MC (**M**ultipoint **C**ontroller), (η ύπαρξη του οποίου είναι αναγκαστική) και κανέναν, έναν ή και περισσότερους MP (**M**ultipoint **P**rocessors). Ο MC ελέγχει την H.245 συνεννόηση μεταξύ των τερματικών προκειμένου να καθοριστούν οι κοινές τους δυνατότητες για επικοινωνία, ενώ συμπληρωματικά ανακαλύπτει τους αποστολείς multicast πακέτων. Ο MP από την άλλη πλευρά είναι αυτός που ασχολείται με το πραγματικό streaming της φωνής ή του βίντεο, υλοποιώντας τεχνικές για mixing και switching.



Εικόνα 3.4: Αρχιτεκτονική H.323.

3.5 Το πρωτόκολλο σηματοδοσίας SIP.

Το SIP είναι ένα πρωτόκολλο σηματοδοσίας, το οποίο άνοιξε το δρόμο για τη ταχύτατη ανάπτυξη του VoIP και άλλων εφαρμογών πολυμέσων, που έχουν κάνει ιδιαίτερα αισθητή την παρουσία τους στην αγορά των τηλεπικοινωνιών, κυρίως την τελευταία δεκαετία. Αναπτύχθηκε από την IETF (Internet Engineering Task Force) και η πρώτη έκδοσή του δημοσιεύθηκε το 1999. Το μεγάλο ενδιαφέρον και η απήχηση που είχε το νέο αυτό πρωτόκολλο, τόσο ερευνητικά όσο και εμπορικά, οδήγησε στη δημιουργία της δεύτερης έκδοσής του, SIP v2 το 2002, η οποία περιλαμβάνει βελτιώσεις και επιπλέον διευκρινίσεις σε σχέση με την προηγούμενη. Αποτελεί μια εναλλακτική επιλογή του παλαιότερου πρωτοκόλλου H.323n, προσφέροντας αρκετά επιπλέον πλεονεκτήματα, ιδιαίτερα στις περιοχές της επεκτασιμότητας, της ευκολίας υλοποίησης και της ελευθερίας επιλογών. Εκμεταλλευόμενη αυτά τα χαρακτηριστικά, η κοινότητα ελεύθερου λογισμικού έχει αρχίσει να προσφέρει όλο και περισσότερες λύσεις για την τεχνολογία SIP που χρειάζονται για την υλοποίηση τερματικών άκρων ή proxy servers ή registrar servers, επιτυγχάνοντας έτσι την ακόμα ταχύτερη ενσωμάτωση της τεχνολογίας σε όλο τον κόσμο.

Το πρωτόκολλο SIP σχεδιάστηκε αμιγώς ως πρωτόκολλο σηματοδοσίας, έτσι ώστε να αξιοποιεί και να συνεργάζεται με τα ήδη υπάρχοντα πρωτόκολλα του διαδικτύου για τις υπόλοιπες λειτουργίες, όπως τα RTP, SDP, TCP, UDP, IP, DNS κ.α. Ενσωματώνει στοιχεία από δύο ευρέως χρησιμοποιούμενα πρωτόκολλα του Internet, το HTTP (**H**yper **T**ext **T**ransfer **P**rotocol) που χρησιμοποιείται για πλοήγηση στο διαδίκτυο, και το SMTP (**S**imple **M**ail **T**ransfer **P**rotocol) που χρησιμοποιείται για το ηλεκτρονικό ταχυδρομείο (e-mail). Από το HTTP, το SIP δανείστηκε την "client - server" αρχιτεκτονική και τη χρήση URLs (**U**niform **R**esource **L**ocators) (στο SIP έχουμε αντίστοιχα τα URI (**U**niform **R**esource **I**dentifier), ενώ από το SMTP, το SIP δανείστηκε τη μορφή κειμένου (text-encoding style) και τη μορφή των κεφαλίδων (headers). Ένα URI είναι ο τρόπος που παίρνουν διευθύνσεις οι χρήστες στο κόσμο του SIP.

Η γενική μορφή ενός SIP URI είναι:

SIP:user:password@host:port;uri-parameters?headers

Αποτελεί ένα πρωτόκολλο του στρώματος εφαρμογής του TCP/IP, και χρησιμοποιείται κυρίως για να εγκαθιστά, να τροποποιεί και να τερματίζει διμερείς (unicast) ή πολυμερείς (multicast) συνόδους επικοινωνίας πολυμέσων, αποτελούμενες από ένα ή περισσότερα τερματικά, όπως κλήσεις φωνής (π.χ. VoIP) και βίντεο μέσω δικτύου. Η τροποποίηση μπορεί να περιλαμβάνει αλλαγή διευθύνσεων και θυρών, την πρόσκληση επιπλέον συμμετεχόντων, την προσθήκη ή αφαίρεση φορέων ροής δεδομένων, την αλλαγή κωδικό-αποκωδικοποιητών, κ.α. Είναι σχεδιασμένο έτσι ώστε να είναι ανεξάρτητο από το επίπεδο μεταφοράς του TCP/IP, και έτσι μπορεί να τρέξει πάνω από TCP, UDP ή SCTP (**S**ream **C**ontrol **T**ransmission **P**rotocol) .

Μια βασική λειτουργία του SIP είναι η δυνατότητα διαπραγμάτευσης των παραμέτρων της συνόδου, έτσι ώστε όλοι οι συμμετέχοντες να ενημερώνονται και να «συμφωνούν» για τα βασικά χαρακτηριστικά της επικοινωνίας, όπως για παράδειγμα τους κωδικό-αποκωδικοποιητές (CODECs) ήχου που θα χρησιμοποιηθούν, τη θύρα επικοινωνίας, κ.α. Η περιγραφή, ωστόσο, όλων αυτών των παραμέτρων μιας VoIP κλήσης, δεν μπορεί να πραγματοποιηθεί άμεσα μέσω του πρωτοκόλλου SIP, και για το λόγο αυτό, το SIP εκμεταλλεύεται τη χρήση του **S**ession **D**escription **P**rotocol (SDP), για τον προσδιορισμό των παραμέτρων της συνόδου.

Αφού εγκατασταθεί μια σύνοδος μέσω SIP, πλέον οι πολυμεσικές ροές δεδομένων (μετάδοση πακέτων φωνής στην περίπτωση του VoIP) μεταφέρονται χρησιμοποιώντας το RTP πάνω από UDP πρωτόκολλο.

Αναλυτικά για την λειτουργία του SIP, το οποίο είναι και το βασικό θέμα αυτής της εργασίας θα γίνει αναφορά στο επόμενο κεφάλαιο.

3.6 Το πρωτόκολλο SDP (Session Description Protocol).

Το Session Description Protocol, προσδιορισμένο από το RFC 4566, είναι περισσότερο ένα περιγραφικό συντακτικό σύστημα παρά ένα πρωτόκολλο, με την έννοια ότι δεν παρέχει στα μέσα κάποια δυνατότητα πλήρους διαπραγμάτευσης. Γενικά, χρησιμοποιείται για να περιγράφει συνόδους πολυμέσων που εγκαθίστανται από το SIP.

Πιο συγκεκριμένα περιγράφει:

- την IP διεύθυνση (host name ή κατά IPv4, IPv6).
- τον αριθμό του port (το οποίο χρησιμοποιείται από το UDP ή το TCP για τη μεταφορά).
- τον τύπο των δεδομένων (ήχος, video, διαδραστικές πλατφόρμες κ.λπ.).
- τον αλγόριθμο κωδικοποίησης των δεδομένων (PCM A-Law, MPEG II video κ.λπ.).
- το θέμα της συνόδου.
- το χρόνο έναρξης και λήξης της συνόδου.

Ομοίως με το SIP, το SDP χρησιμοποιεί κώδικα κειμένου. Ένα μήνυμα SDP αποτελείται από ένα μπλοκ γραμμών, που ονομάζονται πεδία, των οποίων τα ονόματα έχουν συντμηθεί σε ένα πεζό γράμμα και βρίσκονται σε συγκεκριμένη σειρά για να διευκολυνθεί η σάρωσή τους.

Κεφάλαιο 4.

Session Initiation Protocol (SIP).

4.1 Το πρωτόκολλο SIP.

Το SIP (**S**ession **I**nitiation **P**rotocol) είναι ένα πρωτόκολλο που αναπτύχθηκε από την ομάδα IETF MMUSIC και είναι το προτεινόμενο πρότυπο για την έναρξη, την τροποποίηση και τον τερματισμό μιας interactive συνεδρίας χρήστη που περιλαμβάνει στοιχεία πολυμέσων, όπως βίντεο, φωνή, instant messaging, online παιχνίδια και εικονική πραγματικότητα. Αρχικά είχε δημοσιευθεί το 1996 ως RFC 2543, το 2002 αντικαταστάθηκε από την νεότερη έκδοση του, το RFC 3261.

Το SIP έχει σχεδιαστεί να συμβαδίζει πλήρως με το πρότυπο του Internet. Είναι ένα end-to-end προσανατολισμένο πρωτόκολλο σηματοδοσίας για τηλεφωνία μέσω Internet στο επίπεδο εφαρμογής και ελέγχου, στην ουσία προσομοιώνει την κλασική σηματοδότηση των παραδοσιακών τηλεφωνικών κέντρων, κατά συνέπεια μπορεί να εγκαταστήσει, τροποποιήσει και τερματίσει συνόδους (sessions).

Ενσωματώνει στοιχεία δύο πολύ γνωστών πρωτοκόλλων του Internet: του HTTP (**H**yper **T**ext **T**ransport **P**rotocol) και του SMTP (**S**imple **M**ail **T**ransport **P**rotocol) SMTP. Από το HTTP έχει δανειστεί τη σχεδίαση πελάτη-εξυπηρετητή (client-server) και τη χρήση των URL (**U**niform **R**esource **L**ocators) και URI (**U**niform **R**esource **I**dentifiers), ενώ από το SMTP την κωδικοποίηση του κειμένου και την μορφή της επικεφαλίδας των μηνυμάτων.

4.2 Περιγραφή του πρωτοκόλλου.

Το SIP εκτελεί αντιστοίχηση ονομάτων και υπηρεσίες ανακατεύθυνσης, καθιστώντας εφικτή την κινητικότητα του χρήστη, αφού ο κάθε χρήστης μπορεί να διατηρεί ένα μοναδικό αναγνωριστικό για την ταυτότητά του (identifier), ανεξαρτήτως της θέσης του στο δίκτυο.

Το SIP δεν είναι ένα ανεξάρτητο σύστημα επικοινωνίας, αλλά ένα κομμάτι που μπορεί να λειτουργήσει σε συνεργασία με άλλα πρωτόκολλα και κάνει εφικτή την λειτουργία μιας ολοκληρωμένης αρχιτεκτονικής πολυμέσων. Στα πρωτόκολλα αυτά περιλαμβάνονται τα πρωτόκολλα που παρουσιάστηκαν στο προηγούμενο κεφάλαιο δηλαδή το RTP (**R**eal **T**ime **T**ransport **P**rotocol) για τη μεταφορά δεδομένων πραγματικού χρόνου, το RTSP (**R**eal **T**ime **S**treaming **P**rotocol) για την εγκατάσταση και τον έλεγχο ροών δεδομένων on-demand, το MGCP και το Megaco (**Me**dia **Ga**teway **C**ontrol **P**rotocol), το SDP (**S**ession **D**escription **P**rotocol) για την περιγραφή συνεδριών πολυμέσων.

Οι λειτουργίες του SIP είναι:

- Εύρεση της διεύθυνσης δικτύου για την επικοινωνία με το χρήστη.
- Έλεγχος της διαθεσιμότητας του καλούμενου χρήστη (callee).
- Καθορισμός των μέσων που θα χρησιμοποιηθούν κατά τη διάρκεια της επικοινωνίας.
- Εγκατάσταση του sesion και για τα δύο μέρη.
- Διαχείριση του session και τερματισμός του.

Έτσι το SIP δίνει τη δυνατότητα στους αποκαλούμενους UA (**U**ser **A**gents), Πράκτορες Χρηστών να επικοινωνούν μεταξύ τους, αφού πρώτα έχει καθοριστεί η θέση τους στο δίκτυο και έχουν προσδιοριστεί τα τεχνικά χαρακτηριστικά της σύνδεσης που θα δημιουργηθεί. Αυτό γίνεται με τη βοήθεια των SIP Εξυπηρετητών (SIP Servers), οι οποίοι στην ουσία παρουσιάζονται στο δίκτυο σαν τηλεφωνικά κέντρα ή καλύτερα σαν κέντρα αναφοράς, όπου εκεί υπάρχουν καταχωρημένα τα στοιχεία των χρηστών και των συσκευών ειδικών λειτουργιών, τα οποία κάνουν εφικτή την επικοινωνία μεταξύ των αντισυμβαλλόμενων μερών, κρατούν στατιστικά στοιχεία και εκτελούν πλήθος άλλων λειτουργιών εκτός από SIP.

Ο κάθε χρήστης έχει ένα μοναδικό χαρακτηριστικό της ταυτότητάς του, που έχει μορφή παρόμοια με αυτή των e-mails και αποτελείται από το όνομα του χρήστη και το όνομα του host. Η διαδικασία εντοπισμού του χρήστη (που γίνεται από τους SIP Servers) βασίζεται σε αυτό το αναγνωριστικό. Για να γίνει εφικτή η επικοινωνία ο χρήστης ή η συσκευή πρέπει να είναι συνδεδεμένα με τον εξυπηρετητή την συγκεκριμένη χρονική στιγμή που γίνεται αίτηση από κάποιον άλλο χρήστη για σύνδεση, έτσι ο SIP Server εκτελώντας τις κατάλληλες διαδικασίες κάνει εφικτή την επικοινωνία μεταξύ τους.

Τα μηνύματα που ανταλλάσσονται μεταξύ των αντισυμβαλλόμενων μερών δηλαδή των χρηστών χωρίζονται σε δύο κατηγορίες, σε αιτήσεις και απαντήσεις (requests και responses). Οι αιτήσεις στέλνονται από τους User Agents για τη δήλωση της θέσης κάποιου χρήστη, την έναρξη μίας συνόδου με κάποιον άλλον χρήστη ή και τον τερματισμό της, ενώ οι απαντήσεις περιλαμβάνουν πληροφορίες για την κατάσταση των αιτήσεων.

Η φύση της λειτουργίας του SIP ως πρωτόκολλο γενικής χρήσης καθιστά την ασφάλεια των συνόδων ένα πολύ σημαντικό θέμα. Για το λόγο αυτό παρέχονται μια σειρά από λειτουργίες σχετικές με την ασφάλεια, όπως είναι η πιστοποίηση των χρηστών που συμμετέχουν στην ανταλλαγή μηνυμάτων (authentication), η προστασία από την αλλοίωση των δεδομένων, καθώς και η κρυπτογράφησή τους.

4.3 Η ορολογία του πρωτοκόλλου SIP.

- **Address-Of-Record (AOR):**

  Το AOR είναι το αναγνωριστικό κάθε χρήστη, το οποίο καθορίζει τον τομέα (χώρο), (domain) και έτσι φανερώνει τη θέση του χρήστη.

- **Call:**

  Κλήση (call) είναι ο όρος που χρησιμοποιείται για να ανακοινωθεί η έναρξη μιας συνομιλίας πολυμέσων ανάμεσα σε δυο οντότητες του συστήματος.

- **Call Stateful:**

  Ένας proxy αποκαλείται stateful ενεργός, αν η κατάσταση του παραμένει σταθερά ενεργή από την αρχή μιας συνομιλίας (INVITE) μέχρι το πέρας της BYE.

- **Client:**

  Ένας client (Πελάτης) μπορεί να είναι οποιοδήποτε στοιχειό ενός δικτύου, το οποίο στέλνει αιτήματα SIP (requests) και δέχεται απαντήσεις SIP (responses). Ένας Client δεν είναι απαραίτητο να διαδρά με έναν ανθρώπινο χρηστή.

- **Conference:**

  Conference είναι μια συνδιάσκεψη πολυμέσων που περιέχει πολλούς συμμετέχοντες.

- **Final Response:**

  Τελική απάντηση (Final Response) είναι η απάντηση, η οποία τερματίζει την SIP συναλλαγή αντίθετα με μια προσωρινή απάντηση, η οποία δεν τερματίζει τη συναλλαγή SIP μηνυμάτων. Όλες οι απαντήσεις που έχουν την μορφή 2xx, 3xx, 4xx, 5xx και 6xx είναι τελικές απαντήσεις.

- **Request:**

  Το Request είναι ένα SIP μήνυμα που στέλνεται από έναν πελάτη (Client) σε έναν εξυπηρετητή (Server), έχοντας σκοπό να προκαλέσει την απάντηση του Server κάνοντας τον να εκτελέσει μια συγκεκριμένη διαδικασία.

- **Response:**

  Το Response είναι ένα SIP μήνυμα που στέλνεται από έναν εξυπηρετητή (Server) σε έναν πελάτη (Client) δίνοντας απάντηση για την κατάσταση του αιτήματος του πελάτη.

- **Ringback:**

  Το Ringback είναι το τονικό σήμα που παράγεται από την συσκευή που καλεί δίνοντας την πληροφορία ότι ο καλούμενος έχει ειδοποιηθεί και στην συσκευή του αναπαράγεται ήχος κλήσης.

- **Dialog:**

  Διάλογος (dialog) είναι μία peer-to-peer σύνδεση ανάμεσα σε δύο User Agents, με στόχο να εγκατασταθεί μέσω της ανταλλαγής SIP μηνυμάτων επικοινωνία μεταξύ τους. Κάθε διάλογος αναγνωρίζεται από ένα αναγνωριστικό κλήσης (Call-ID).

- **Header:**

  Η επικεφαλίδα (header) είναι ένα κομμάτι του SIP μηνύματος, που περιέχει πληροφορίες για το μήνυμα. Δημιουργείται από μια ακολουθία πεδίων επικεφαλίδας (header fields). Τα header fields περιέχουν το όνομα ενός χαρακτηριστικού και μία ή περισσότερες τιμές για το συγκεκριμένο χαρακτηριστικό.

- **Home Domain:**

  Είναι το domain που παρέχει κάποια υπηρεσία στο χρήστη του SIP. Το domain αυτό βρίσκεται και στην AOR του χρήστη.

- **Location Service:**

  Είναι η υπηρεσία θέσης (Location Service) και χρησιμοποιείται από συγκεκριμένους SIP Servers για να βρουν την πιθανή θέση του καλούμενου χρήστη. Περιέχει μια λίστα αντιστοίχησης των AORs σε μία ή περισσότερες διευθύνσεις, όπου μπορεί να είναι διαθέσιμος ο χρήστης.

- **SIP Server:**

  Ο SIP Εξυπηρετητής είναι μια οντότητα του δικτύου, που δέχεται αιτήσεις με σκοπό να τις εξυπηρετήσει και στέλνει πίσω απαντήσεις σε αυτές τις αιτήσεις.

- **SIP Transaction:**

  Μια SIP συναλλαγή (SIP transaction) γίνεται μεταξύ ενός πελάτη και ενός εξυπηρετητή και περιέχει όλα τα μηνύματα που ανταλλάσσονται μεταξύ τους.

- **User Agent:**

  Ο πράκτορας χρήστη, είναι η λογική οντότητα που μπορεί να έχει καταχωρηθεί σαν πελάτης UAC (**U**ser **A**gent **C**lient) ή σαν εξυπηρετητής UAS (**U**ser **A**gent **S**erver).

4.4 Η Δομή του Πρωτοκόλλου.

Το SIP ανταλλάσει μηνύματα που έχουν την μορφή text και χρησιμοποίει το UTF-8 (**U**niform **T**ransformation **F**ormat-**8**) σύνολο χαρακτήρων.

Όλα τα μηνύματα έχουν την παρακάτω δομή. Αποτελούνται από μία γραμμή έναρξης (start-line), που μπορεί να είναι είτε μία γραμμή αίτησης (Request-line), είτε μια γραμμή κατάστασης (Status-line) αναλόγως αν πρόκειται για αίτηση ή απάντηση, ένα ή περισσότερα πεδία επικεφαλίδας (header fields), που χρησιμοποιούνται για να μεταφέρουν τα χαρακτηριστικά του μηνύματος, μία κενή γραμμή που καθορίζει το τέλος των πεδίων της επικεφαλίδας και ένα προαιρετικό σώμα (body), όπως φαίνεται και στο παρακάτω παράδειγμα μηνύματος (Εικόνα 4.1):

Request-line	INVITE: sip:alf@alf.com SIP/2.0
Header Fields	Via: SIP/2.0/UDP alf.com:5060 From: George <sip:ger@alf.com> To: Alex <sip:alf@alf.com> Call-ID: 12345678@alf.com Cseq: INVITE Subject: Hello Contact: gef<sip:gef@alf.com> Content-Type: application /sdp
Separator	Blank line
Body	V=0 o=User 6945812000 6945812001 IN IP V4 alf.com s=Session SDP c=IN IP4 192.168.1.103 t=0 0 m=audio 49172 RTP/AVP 0 a=rtpmap: 0 PCMU/8000 Content-Length: 147

Εικόνα 4.1 Παράδειγμα Μηνύματος SIP.

4.4.1 Header Fields.

Στο κάθε πεδίο επικεφαλίδας ενός μηνύματος SIP υπάρχει το όνομα του πεδίου (field name) και μερικές τιμές (field values). Δεν έχει καμία σημασία η σειρά με την οποία εμφανίζονται τα πεδία στην επικεφαλίδα.

Η σύνταξη είναι: field name : field value

Το SIP χρησιμοποιεί τα παρακάτω header fields. Μερικά χρησιμοποιούνται μόνο στα SIP Requests, και άλλα μόνο στα SIP Responses, ενώ κάποια είναι κοινά και στους δύο τύπους μηνυμάτων.

1. **Accept:** Ρυθμίζει τους τύπους μέσων (media types).
2. **Accept-Encoding:** Καθορίζει τις αποδεκτές κωδικοποιήσεις των μέσων.
3. **Accept-Language:** Καθορίζει τις προτιμώμενες γλώσσες.
4. **Alert-Info:** Καθορίζει έναν εναλλακτικό ήχο για τις εισερχόμενες κλήσεις του χρήστη.
5. **Allow:** Δηλώνει το σύνολο μεθόδων που υποστηρίζει ο UA.
6. **Authentication-Info:** Δίνει τη δυνατότητα αμοιβαίας πιστοποίησης με χρήση του HTTP Digest.
7. **Authorization:** Περιέχει πληροφορίες για την ταυτοποίηση του UA.
8. **Call-ID:** Παράμετρος που καθορίζει μονοσήμαντα μια αίτηση για έναρξη συνεδρίας από ένα UA.
9. **Call-Info:** Περιέχει επιπρόσθετες πληροφορίες για τον αποστολέα του μηνύματος.
10. **Contact:** Περιέχει ένα URI, του οποίου το νόημα εξαρτάται από τον τύπο του μηνύματος.
11. **Content-Disposition:** Περιγράφει τον τρόπο με τον οποίο πρέπει να ερμηνευτεί το σώμα του μηνύματος.
12. **Content-Encoding:** Αναφέρει τους μηχανισμούς αποκωδικοποίησης/ συμπίεσης που έχουν εφαρμοστεί στο σώμα του μηνύματος.
13. **Content-Language:** Αναφέρει τη γλώσσα στην οποία είναι γραμμένο το σώμα του μηνύματος.
14. **Content-Length:** Αναφέρει το μέγεθος του σώματος του μηνύματος. Η τιμή 0 δηλώνει πως δεν υπάρχει σώμα στο μήνυμα.
15. **Content-Type:** Καθορίζει τον τύπο του μέσου στο σώμα του μηνύματος.

16. **CSeq:** Περιέχει ένα δεκαδικό αριθμό, που αυξάνεται για κάθε αίτηση και τη μέθοδο της αίτησης που χρησιμοποιείται στο μήνυμα.

17. **Date:** Καθορίζει την ημερομηνία και την ώρα.

18. **Error-Info:** Περιέχει δείκτη σε επιπρόσθετες πληροφορίες για το σφάλμα που συνέβη.

19. **Expires:** Είναι το χρονικό διάστημα (σε δευτερόλεπτα) μετά από το οποίο, το μήνυμα δεν έχει πια ισχύ.

20. **From:** Πληροφορίες για την οντότητα που ξεκίνησε την αρχική αίτηση, στην οποία αναφέρεται το μήνυμα.

21. **In-Reply-To:** Περιέχει το call-ID, στο οποίο αναφέρεται το συγκεκριμένο μήνυμα ή στο οποίο επιστρέφει το μήνυμα (υπάρχει μόνο στα SIP Requests).

22. **Max-Forwards:** Καθορίζει το μέγιστο αριθμό των κόμβων που μπορούν να προωθήσουν το συγκεκριμένο Request.

23. **Min-Expires:** Καθορίζει τον ελάχιστο χρόνο, για τον οποίο στοιχεία της information base ενός SIP Server δεν μπορούν να αλλαχτούν.

24. **MIME-Version:** Μηνύματα που έχουν δημιουργηθεί με βάση το Multipurpose Internet Mail Extensions πρωτόκολλο (MIME) περιέχουν αυτό το header field που καθορίζει την έκδοσή του.

25. **Organization:** Περιέχει το όνομα του οργανισμού στον οποίο ανήκει η SIP οντότητα που εξέδωσε το μήνυμα.

26. **Priority:** Περιέχει την προτεραιότητα που πρέπει να δοθεί στο συγκεκριμένο μήνυμα σε περιπτώσεις συμφόρησης. Ορίζονται τέσσερις κλάσεις προτεραιότητας: όχι επείγον (non-urgent), κανονικό (normal), άμεσης προτεραιότητας (urgent) και επείγον (emergency).

27. **Proxy-Authenticate:** Περιέχει δεδομένα απαραίτητα για την ταυτοποίηση του UA, που έστειλε το μήνυμα, από τον Πληρεξούσιο Εξυπηρετητή (Proxy Server - ένα είδος SIP server), που πρόκειται να το επεξεργαστεί.

28. **Proxy-Authorization:** Το περιεχόμενο του είναι στις περισσότερες περιπτώσεις ίδιο με του Proxy-Authenticate header field.

29. **Proxy-Require:** Περιέχει τις προδιαγραφές που πρέπει να πληρεί ο Proxy Server για να επεξεργαστεί το μήνυμα.

30. **Record-Route:** Προστίθεται από κάποιον Proxy Server για να δηλώσει ότι όλα τα μηνύματα που αφορούν σε έναν συγκεκριμένο διάλογο πρέπει να δρομολογηθούν μέσω αυτού.

31. **Reply-To:** Περιέχει ένα URI, όχι κατά ανάγκη ίδιο με αυτό του From header field. Μπορεί να χρησιμοποιηθεί για να αποστέλλονται λίστες με χαμένες ή ανεπιτυχείς κλήσεις.

32. **Require:** Χρησιμοποιείται από τους UAC για να ενημερώσουν τους UAS για τις επιλογές που πρέπει να υποστηρίζουν, ώστε να επεξεργαστούν επιτυχώς το μήνυμα.

33. **Retry-After:** Πρόκειται για έναν ακέραιο αριθμό, που ισούται με το χρόνο (σε δευτερόλεπτα) που πρέπει ο καλών να περιμένει πριν ξανακαλέσει σε περίπτωση που λάβει κάποιο συγκεκριμένο μήνυμα αποτυχίας.

34. **Route:** Περιέχει μια λίστα από Proxy Servers, μέσα από τους οποίους πρέπει να δρομολογηθεί το συγκεκριμένο μήνυμα.

35. **Server:** Περιέχει πληροφορίες σχετικά με το software που χρησιμοποιεί ο UAS για να επεξεργαστεί το request.

36. **Subject:** Αναφέρει το θέμα του μηνύματος.

37. **Supported:** Περιέχει όλες τις επεκτάσεις που υποστηρίζει ο UA.

38. **Timestamp:** Καθορίζει την ακριβή ώρα που στάλθηκε το Request μήνυμα.

39. **To:** Περιέχει το URI και ίσως και άλλες πληροφορίες για τον τελικό παραλήπτη του μηνύματος.

40. **Unsupported:** Περιέχει λίστα με χαρακτηριστικά που δεν υποστηρίζονται από τον UAS.

41. **User-Agent:** Περιέχει πληροφορίες για τον UA που δημιούργησε το request.

42. **Via:** Περιέχει τη διαδρομή που ακολούθησε το μήνυμα μέχρι τώρα (ως ακολουθία IP διευθύνσεων), αν πρόκειται για Request μήνυμα, ή καθορίζει τη διαδρομή που θα πρέπει να ακολουθηθεί, αν πρόκειται για μήνυμα απάντησης.

43. **Warning:** Περιέχει επιπρόσθετες πληροφορίες για την κατάσταση της απάντησης.

44. **WWW-Authenticate:** Χρησιμοποιείται για την πιστοποίηση του UAC από τον UAS.

4.4.2 SIP Requests.

Οι αιτήσεις SIP αναγνωρίζονται στη γραμμή αίτησης (Request-line). Η Request-line περιέχει το όνομα της μεθόδου, ένα ζητούμενο URI (Request-URI) και την έκδοση του πρωτοκόλλου, χωρισμένα μεταξύ τους με ένα κενό χαρακτήρα.

Στις προδιαγραφές του πρωτοκόλλου αναφέρονται έξι μέθοδοι:

- **REGISTER.**
- **INVITE.**
- **ACK.**
- **CANCEL.**
- **BYE.**
- **OPTIONS.**

Το Request-URI δηλώνει τον χρήστη ή την υπηρεσία, στην οποία αναφέρεται η συγκεκριμένη αίτηση.

4.4.2.1 REGISTER Method

Η μέθοδος REGISTER χρησιμοποιείται από τον User Agent για να δηλώσει στο SIP δίκτυο την τρέχουσα διεύθυνση επικοινωνίας του (Contact URI, IP address) και το URI (ουσιαστικά το AOR του χρήστη), για το οποίο όλες οι αιτήσεις θα πρέπει να κατευθύνονται στη συγκεκριμένη διεύθυνση (Εικόνα 4.2).

Τα πεδία που πρέπει να υπάρχουν σε ένα REGISTER Request είναι:

- **Call-ID.**
- **CSeq.**
- **From.**
- **To.**
- **Via.**
- **Max-Forwards.**

```
REGISTER sip:registrar.sip.teicreta.gr SIP/2.0
Via  : SIP/2.0/UDP sipclient.teicreta.gr:5060
Max-Forwards: 70
To: alf  <sip:alf@ sip.teicreta.gr>
From: alf <sip:alf@ sip.teicreta.gr >
Call-ID: 525235652152@565fdgf365
CSeq: 1826 REGISTER
Contact: sip:alf@192.168.1.20
Content-Length: 0
```

Εικόνα 4.2 Παράδειγμα REGISTER SIP.

4.4.2.2 INVITE Method.

Ένας χρήστης UA χρησιμοποιεί τη μέθοδο INVITE, όταν θέλει να ξεκινήσει τη διαδικασία για επικοινωνία με έναν άλλο χρηστή UA. Το μήνυμα μιας αίτησης INVITE μπορεί να περιέχει σώμα με τις πληροφορίες μέσου (media information) του αποστολέα. Μπορεί επίσης να περιέχει άλλες πληροφορίες για τη συνεδρία, όπως την ποιότητα υπηρεσίας (Quality of Service - QoS) ή πληροφορίες ασφάλειας. Ένα επιτυχές INVITE Request εγκαθιστά ένα διάλογο μεταξύ των δύο UAs, που διαρκεί, ώσπου μια αίτηση BYE να σταλεί από έναν από τους δύο για να τερματίσει τη συνεδρία. Ο χρήστης που στέλνει το αρχικό INVITE κατασκευάζει ένα μοναδικό Call-ID, που χρησιμοποιείται κατά τη διάρκεια της συνεδρίας (Εικόνα 4.3).

```
REGISTER sip:registrar.sip.teicreta.gr SIP/2.0
Via  : SIP/2.0/UDP sipclient.teicreta.gr:5060
Max-Forwards: 70
To: Alf <sip: alf@ sip.teicreta.gr >
From: Gef <sip:gef@sip.teicreta.gr>
Call-ID: d15v4a56e745823
CSeq: 314159 INVITE
Contact: sip:gef@192.168.1.21
Content-Length: 0
```

Εικόνα 4.3 Παράδειγμα INVITE SIP.

Τα πεδία που πρέπει να υπάρχουν σε ένα INVITE Request είναι:

- **Call-ID.**
- **CSeq.**
- **From.**
- **To.**
- **Via.**
- **Contact.**
- **Max-Forwards.**

4.2.2.3 ACK Method

Η ACK είναι η μέθοδος που χρησιμοποιείται για την επιβεβαίωση ότι ο χρήστης έχει λάβει μια τελική απάντηση για ένα INVITE request που έστειλε προηγουμένως. Να σημειωθεί ότι το ACK request χρησιμοποιείται για να επιβεβαιώσει την λήψη τελικής απάντησης μόνο για τα αντίστοιχα INVITE requests. Το πεδίο CSeq της επικεφαλίδας δεν αυξάνεται για ένα ACK Request, αλλά αλλάζει μόνο η μέθοδος που εμφανίζεται. Με αυτόν τον τρόπο μπορεί ένας UA να ταιριάξει τον αριθμό του CSeq του ACK με τον αντίστοιχο αριθμό του INVITE στο οποίο αναφέρεται.

Τα πεδία που πρέπει να υπάρχουν σε ένα ACK Request είναι:

- **Call-ID.**
- **CSeq.**
- **From.**
- **To.**
- **Via.**
- **Max-Forwards.**

4.4.2.4 CANCEL Method.

Η μέθοδος CANCEL χρησιμοποιείται για τον τερματισμό αναζητήσεων ή κλήσεων. Μπορεί να κατασκευαστεί είτε από έναν UA, είτε από έναν Proxy Server, εφόσον έχει ληφθεί μια 1xx απάντηση. Ο UA χρησιμοποιεί το CANCEL για να ακυρώσει μια προσπάθεια κλήσης σε εκκρεμότητα που ξεκίνησε νωρίτερα.

Τα πεδία που πρέπει να υπάρχουν σε ένα CANCEL Request είναι:

- **Call-ID.**
- **CSeq.**
- **From.**
- **To.**
- **Via.**
- **Max-Forwards.**

4.4.2.5 BYE Method.

Η μέθοδος BYE χρησιμοποιείται για τον τερματισμό μιας συνεδρίας. Μπορεί να σταλεί μόνο από τους UAs που συμμετέχουν στο διάλογο, σε καμία περίπτωση από κάποιον SIP Server ή από κάποιον τρίτο. Η αίτηση στέλνεται απευθείας στον άλλο UA που συμμετέχει στη σύνοδο και η απάντηση επίσης.

Τα πεδία που πρέπει να υπάρχουν σε ένα BYE είναι:

- **Call-ID.**
- **CSeq.**
- **From.**
- **To.**
- **Via.**
- **Max-Forwards.**

4.5 SIP Responses.

Ένα μήνυμα απάντησης SIP (SIP Response) δημιουργείται από έναν SIP Server ή από έναν UAS προς απάντηση μιας αίτησης από έναν UAC. Η απάντηση έχει μια γραμμή κατάστασης (Status-line), η οποία περιέχει έναν τριψήφιο κωδικό (status code) και την εξήγηση που αντιστοιχεί σε αυτόν τον κωδικό (reason). Οι κωδικοί αυτοί χωρίζονται σε έξι ομάδες οι οποίες κατά σειρά είναι οι ακόλουθες.

- 1xx (Informational).

- 2xx (Success).
- 3xx (Redirection).
- 4xx (Client error).
- 5xx (Server failure).
- 6xx (Global failure).

4.5.1 Informational (1xx).

Οι κωδικοί Informational 1xx παρουσιάζουν πληροφορίες που αφορούν την εξέλιξη της κλήσης.

Οι κωδικοί αυτής της κατηγορίας είναι:

- **100 Trying.**

  Η απάντηση αυτή δηλώνει την προσπάθεια ενός Proxy Server ή ενός UAS γενικά για κάποιου είδους ενέργεια για λογαριασμό της αίτησης. Παρουσιάζεται συνήθως όταν υπάρχει κάποιο σφάλμα στο δίκτυο ή όταν κάτι δεν έχει δηλωθεί σωστά, επομένως το σύστημα αδυνατεί να εκτελέσει το συγκεκριμένο request.

- **180 Ringing.**

  Η απάντηση αυτή χρησιμοποιείται για να δηλώσει ότι το INVITE έχει ληφθεί από τον UA και ότι αναμένεται κάποια άλλη εξέλιξη.

- **181 Call is Being Forwarded.**

  Η απάντηση αυτή δηλώνει ότι η κλήση προωθείται.

- **182 Call Queued.**

  Η απάντηση αυτή δηλώνει ότι ο UA δεν είναι διαθέσιμος. Ωστόσο η κλήση μπήκε σε ουρά προτεραιότητας και δεν απορρίφθηκε.

- **183 Session progress.**

  Η απάντηση αυτή περιέχει πληροφορίες για την κατάσταση της κλήσης.

4.5.2 Success (2xx).

Ο κωδικός Success 2xx παρουσιάζει το γεγονός ότι η αίτηση ολοκληρώθηκε με επιτυχία και ότι έγινε δεκτή.

Ο κωδικός αυτής της κατηγορίας είναι:

- **200 (OK).**

  Αυτή η απάντηση δείχνει ότι η αίτηση έγινε δεκτή.

4.5.3 Redirection (3xx).

Οι κωδικοί Redirection 3xx χρησιμοποιούνται για να δηλωθεί ότι το αίτημα πρέπει να κατευθυνθεί σε κάποια άλλη οντότητα.

Οι κωδικοί αυτής της κατηγορίας είναι:

- **300 Multiple Choices.**

  Αυτή η απάντηση αφορά πολλά Contact πεδία επικεφαλίδας, που δείχνουν ότι ο Location Service απάντησε ότι υπάρχουν πολλές πιθανές θέσεις και άρα υπάρχουν πολλές επιλογές για το URI που υπάρχει στο Request-URI.

- **301 Moved Permanently.**

  Αφορά ένα πεδίο επικεφαλίδας Contact με τη νέα διεύθυνση (URI) του καλούμενου μέρους. Η διεύθυνση μπορεί να αποθηκευτεί και να χρησιμοποιηθεί σε μελλοντικά INVITE Requests προς το χρήστη.

- **302 Moved Temporarily.**

  Η απάντηση περιέχει μια διεύθυνση που είναι προσωρινά αποδεκτή για τον εντοπισμό του χρήστη, αλλά όχι μόνιμη.

- **305 Use Proxy.**

  Η συγκεκριμένη απάντηση δείχνει ότι ο χρήστης πρέπει να ξαναστείλει το request, αυτή τη φορά όμως μέσω του Proxy Server, του οποίου το URI περιέχεται στο Contact header field.

- **380 Alternative Service.**

  Η συγκεκριμένη απάντηση επιστρέφει ένα URI, που δείχνει το είδος της υπηρεσίας που θα ήθελε το καλούμενο μέρος.

4.5.4 Client Error (4xx).

Οι κωδικοί Client Error 4xx χρησιμοποιούνται για να δηλωθεί από έναν UAS ή από ένα SIP Server ότι η εξυπηρέτηση της αίτησης δεν μπορεί να ολοκληρωθεί.

Οι κωδικοί αυτής της κατηγορίας είναι:

- **400 Bad Request.**

  Η αίτηση δεν έγινε κατανοητή, λόγω λανθασμένης σύνταξης.

- **401 Unauthorized.**

  Απαιτείται πιστοποίηση του χρήστη.

- **402 Payment Required.**

  Απαιτείται πληρωμή για την χρήση της υπηρεσίας.

- **403 Forbidden.**

  Όταν ο Server δεχθεί μια σωστή αίτηση, αλλά αρνείται να την εξυπηρετήσει λόγω κάποιας απαγόρευσης, η οποία όμως δεν οφείλεται σε τεχνικό λόγο.

- **404 Not Found.**

  Δείχνει ότι ο χρήστης, του οποίου το URI φαίνεται στο Request-URI της αίτησης δεν μπορεί να εντοπιστεί.

- **405 Method Not Allowed.**

  Όταν ο Server δεχθεί μια σωστή αίτηση, αλλά αρνείται να την εξυπηρετήσει επειδή δεν είναι υπεύθυνος για αυτή.

- **406 Not Acceptable.**

  Η αίτηση δε γίνεται να επεξεργασθεί, επειδή λείπει κάτι από αυτή.

- **407 Proxy Authentication Required.**

  Απαιτείται πιστοποίηση του χρήστη. Χρησιμοποιείται από Proxy Servers.

- **408 Request Timeout.**

  Η αίτηση δεν μπόρεσε να επεξεργασθεί επιτυχώς εντός της χρονικής προθεσμίας που υπήρχε.

- **410 Gone.**

  Ο χρήστης δε θα είναι διαθέσιμος.

- **413 Request Entity Too Large.**

  Απόρριψη μιας αίτησης με πολύ μεγάλο μήνυμα.

- **414 Request-URI Too Long.**

  Απόρριψη μιας αίτησης με πολύ μεγάλο Request-URI.

- **415 Unsupported Media Type.**

  Δεν υποστηρίζει τον τύπο του μέσου (media type) που υπάρχει στο INVITE.

- **416 Unsupported URI Scheme.**

  Δεν υποστηρίζει ένα σχήμα URI στο Request-URI.

- **420 Bad Extension.**

  Δεν υποστηρίζεται η επέκταση που υπάρχει στο header field Require από τον Proxy ή τον UA.

- **421 Extension Required.**

  Ο Server χρειάζεται μια επέκταση για να επεξεργαστεί την αίτηση, η οποία επέκταση δεν υπάρχει σε ένα Supported header field.

- **423 Interval Too Brief.**

  Όταν ο χρόνος λήξης που αναφερόταν στην αίτηση ήταν πολύ μικρός η απάντηση αυτή επιστρέφεται από ένα Registrar που απορρίπτει ένα REGISTER Request.

- **480 Temporarily Unavailable.**

  Ο χρήστης έλαβε την κλήση, αλλά δεν είναι διαθέσιμος.

- **481 Call/Transaction Does Not Exist.**

  Δίνεται ως απάντηση, αν σταλεί μια αίτηση για μια συναλλαγή, για την οποία ο Server δεν έχει καμία πληροφορία.

- **482 Loop Detected.**

  Δείχνει ότι κατά τη δρομολόγηση της αίτησης διαπιστώθηκε ότι υπάρχει ατέρμονος βρόχος (loop).

- **483 Too Many Hops.**

  Όταν κατά τη δρομολόγηση του μηνύματος έχει ξεπεραστεί ο μέγιστος αριθμός κόμβων που μπορεί να μεσολαβεί μεταξύ αποστολέα και παραλήπτη, όπως καθορίζεται στο header field Max-Forwards.

- **484 Address Incomplete.**

  Όταν η διεύθυνση που υπάρχει στο Request-URI δεν είναι ολοκληρωμένη.

- **485 Ambiguous.**

  Όταν το Request-URI ήταν ασαφές.

- **486 Busy Here.**

  Όταν ο UA δε μπορεί να δεχτεί την κλήση γιατί είναι απασχολημένος.

- **487 Request Terminated.**

  Η απάντηση αυτή στέλνεται από ένα UA που έχει λάβει ένα CANCEL Request για ένα INVITE, που βρίσκεται σε εκκρεμότητα.

- **491 Request Pending.**

  Όταν η αίτηση έχει παραληφθεί από τον UA, ενώ υπήρχε προγενέστερη αίτηση του ίδιου dialog σε αναμονή.

- **493 Undecipherable.**

  Η αίτηση λήφθηκε κανονικά, αλλά έχει ένα κρυπτογραφημένο MIME, για το οποίο δεν υπάρχει διαθέσιμο κλειδί αποκρυπτογράφησης.

4.5.5 Server Failure (5xx).

Οι κωδικοί Server Failure 5xx χρησιμοποιούνται όταν η αίτηση δεν μπορεί να εξυπηρετηθεί, λόγω ενός σφάλματος που υπάρχει στο εξυπηρετητή (Server)

Οι κωδικοί αυτής της κατηγορίας είναι:

- **500 Server Internal error.**

  Υπάρχει κάποιο σφάλμα στον Server, το οποίο τον εμποδίζει να εξυπηρετήσει την αίτηση.

- **501 Not Implemented.**

  Η λειτουργικότητα που χρειάζεται για να εξυπηρετηθεί η αίτηση δεν υποστηρίζεται από το Server.

- **502 Bad Gateway.** `

  Χρησιμοποιείται σε περίπτωση που ο Proxy λειτουργεί ως Gateway σε ένα άλλο δίκτυο και δείχνει πως υπάρχει κάποιο πρόβλημα με το άλλο δίκτυο.

- **503 Service Unavailable.**

  Ο Server δεν είναι προσωρινά διαθέσιμος, λόγω φόρτου ή συντήρησης.

- **504 Server Time-out.**

  Ο Server δεν έλαβε έγκαιρα απάντηση σε ένα μήνυμα που έστειλε σε άλλο Server προσπαθώντας να εξυπηρετήσει το request.

- **505 Version Not Supported.**

  Η έκδοση του πρωτοκόλλου που υπάρχει στην αίτηση δεν υποστηρίζεται από το Server.

- **513 Message Too Large.**

  Το μέγεθος της αίτησης ήταν πολύ μεγάλο για να μπορέσει να το επεξεργαστεί.

4.5.6 Global Failure (6xx).

Οι κωδικοί Global Failure 6xx χρησιμοποιούνται όταν ο Server γνωρίζει ότι η εξυπηρέτηση της αίτησης θα αποτύχει.

Οι κωδικοί αυτής της κατηγορίας είναι:

- **600 Busy Everywhere.**

Η αίτηση δεν μπορεί να εξυπηρετηθεί πουθενά.

- **603 Decline.**

Το καλούμενο μέρος είναι απασχολημένο ή απλά δε θέλει να αποδεχτεί την αίτηση.

- **604 Does Not Exist Anywhere.**

Όταν ο χρήστης που αναφέρεται στο Request-URI δεν υπάρχει πουθενά.

- **606 Not Acceptable.**

Όταν η αίτηση παραδόθηκε κανονικά, αλλά κάποιες από τις παραμέτρους της δεν έγιναν δεκτές.

4.6 SIP Οντότητες.

Στο SIP υπάρχουν τέσσερις τύποι οντοτήτων (SIP Entities):

- **Οι Πράκτορες Χρήστη (User Agents).**

- **Οι Εξυπηρετητές Εγγραφών (Registrars).**

- **Οι Πληρεξούσιοι Εξυπηρετητές (Proxy Server).**

- **Οι Εξυπηρετητές Ανακατεύθυνσης (Redirect Servers).**

Η κάθε οντότητα έχει την δική της λειτουργία έτσι ώστε με την χρήση και των τεσσάρων μαζί να μπορεί να υπάρξει ένα ολοκληρωμένο σύστημα. Κάθε φυσική συσκευή μπορεί να έχει τη λειτουργία περισσοτέρων από μίας λογικών οντοτήτων.

4.6.1User Agent.

Οι SIP User Agents (UAs) είναι το λογισμικό που εκτελείται στις συσκευές των τελικών χρηστών. Υπάρχουν δυο τύποι πρακτόρων χρηστών (User Agent). Ο UAC (User Agent Client) είναι μια εφαρμογή πελάτη, που εκκινεί τα SIP Requests, ενώ ο UAS (User Agent Server) είναι μια εφαρμογή εξυπηρετητή, που επικοινωνεί με το χρήστη σε περίπτωση που ληφθεί ένα SIP Request και επιστρέφει μια απάντηση για λογαριασμό του χρήστη. Γίνεται εύκολα λοιπόν αντιληπτό ότι οι User Agents είναι αυτοί που καθιστούν την επικοινωνία ανάμεσα στους χρήστες εφικτή, είτε ως πελάτες Clients, είτε ως εξυπηρετητές Servers.

4.6.2 Redirect Server.

Ο SIP Redirect Server δεν προωθεί requests σε επόμενους SIP Redirect Servers, όπως στην περίπτωση ενός SIP Proxy Server, αλλά αποκρίνεται σε ένα SIP request, με μία ή περισσότερες νέες τρέχουσες διευθύνσεις, έτσι ώστε οι SIP UACs να αποστείλουν νέα SIP requests σε εναλλακτικές τοποθεσίες. Οι SIP Redirect Servers μπορούν να συνυπάρχουν στο ίδιο υλικό με SIP Registrar Servers και SIP Proxy Servers.

4.6.3 Registrar Server.

Ένας SIP Registrar Server αποδέχεται REGISTER requests και δημιουργεί εγγραφές με φυσικές διευθύνσεις της τρέχουσας θέσεις τους που αντιστοιχούν στις λογικές διευθύνσεις των χρηστών του domain για το οποίο είναι υπεύθυνοι. Για παράδειγμα, διεύθυνση sip:user@teicrete.gr του χρήστη user, αντιστοιχείται για παράδειγμα στη φυσική διεύθυνση sip:user@192.168.1.5, η οποία περιέχει πληροφορία για την τρέχουσα θέση του. Οι SIP Registrar Servers δημιουργούν βάσεις δεδομένων με τέτοιες εγγραφές για όλους τους ενεργούς χρήστες (UAs) του domain τους.

Κατά την διάρκεια εγκατάστασης μιας κλήσης ο SIP Registrar Server ανακτά και στέλνει την τρέχουσα φυσική διεύθυνση του καλούμενου χρήστη στον SIP Proxy Server για την κατάλληλη προώθηση του αρχικού SIP request.

4.6.4 Proxy Server

Οι SIP Proxy Servers είναι το λογισμικό που εκτελείται από τους κεντρικούς κόμβους ενός VoIP δικτύου και αποδέχεται τα requests που υποβάλλονται από τους SIP UAs (UAC) για εγκατάσταση επικοινωνίας. Όταν οι SIP Proxy Servers λαμβάνουν ένα SIP request από ένα χρήστη, αρχικά επικοινωνούν με τον SIP

Registrar Server για να λάβουν πληροφορία για την τρέχουσα θέση του χρήστη που καλείται. Στην περίπτωση που ο χρήστης αυτός εντοπιστεί τότε το SIP request προωθείται στον UAS του χρήστη, αλλιώς το SIP request προωθείται στον επόμενο κόμβο SIP Proxy Server. Εάν ο χρήστης που καλείται δεν βρεθεί μετά από έναν αριθμό προσπαθειών, τότε ο SIP Proxy Server απαντά κατάλληλα, αποστέλλοντας ένα SIP response, στον αρχικό χρήστη που έστειλε το αίτημα για επικοινωνία. Ένας SIP Proxy Server ερμηνεύει και εάν είναι απαραίτητο, τροποποιεί ένα SIP request πριν το αποστείλει στον αντίστοιχο SIP UA ή σε άλλον SIP Proxy Server.

4.7 Διευθυνσιοδότηση.

Ο τρόπος που δίνεται μια διεύθυνση στο πρωτόκολλο SIP δεν είναι συγκεκριμένος καθώς το SIP υποστηρίζει πολλά URL και URI σχήματα, όπως το SIP (SIP URI), sips (Secure SIP URI),tel (Telephone URI) το οποίο είναι παρόμοιο με την λογική της κλασικής τηλεφωνίας και μοιάζουν με εκείνα των e-mail.

Παραδείγματα.

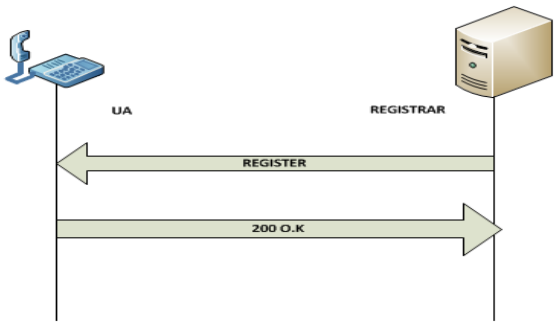
- **user_name@host_name.**
- **user_name@IP_address.**
- **phone_number@gateway.**

4.8 Παραδείγματα επικοινωνίας με το πρωτόκολλο SIP.

Για να γίνει κατανοητή η λειτουργία του πρωτοκόλλου, ο τρόπος με τον οποίο μεταδίδονται τα μηνύματα και τελικά γίνεται η επικοινωνία, παραθέτονται τα παρακάτω παραδείγματα.

4.8.1 Παράδειγμα REGISTER

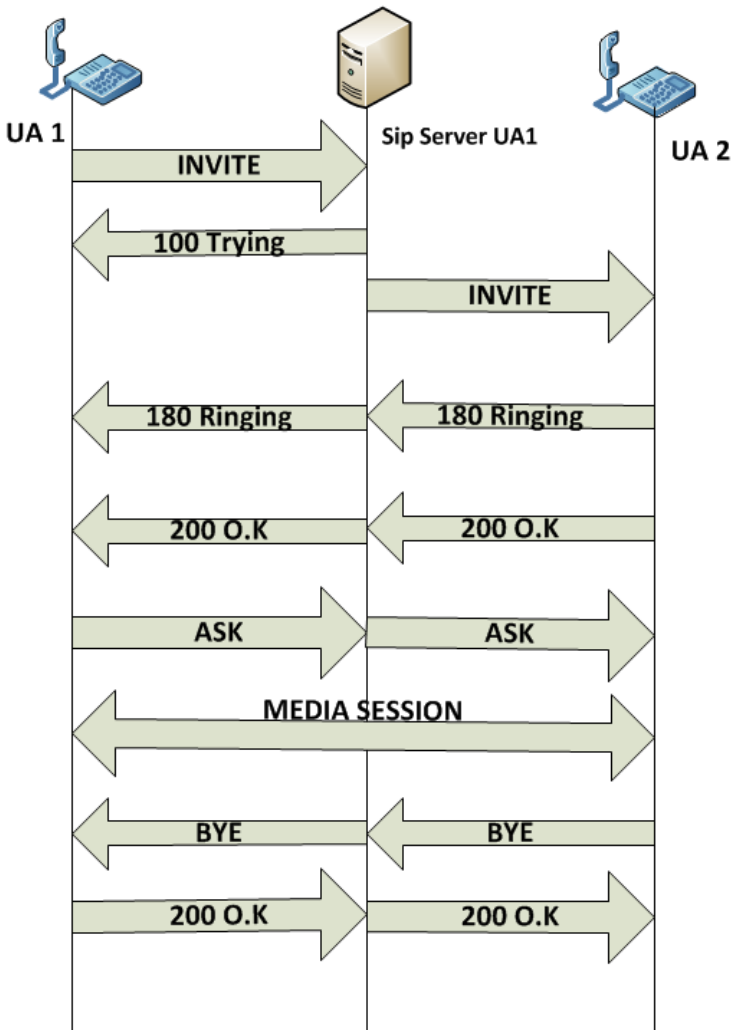
Στην παρακάτω εικόνα (εικόνα 4.4) παρουσιάζεται ένα παράδειγμα REGISTER Request. Ο UA στέλνει την αίτηση στο Registrar και αφού αυτός κάνει πιστοποίηση της ταυτότητας του χρήστη και εγγραφή επιστρέφει μια απάντηση 200 (OK), που σημαίνει ότι καταχωρήθηκε σωστά η εγγραφή.



Εικόνα 4.4: Παράδειγμα REGISTER Request.

4.8.2 Παράδειγμα INVITE

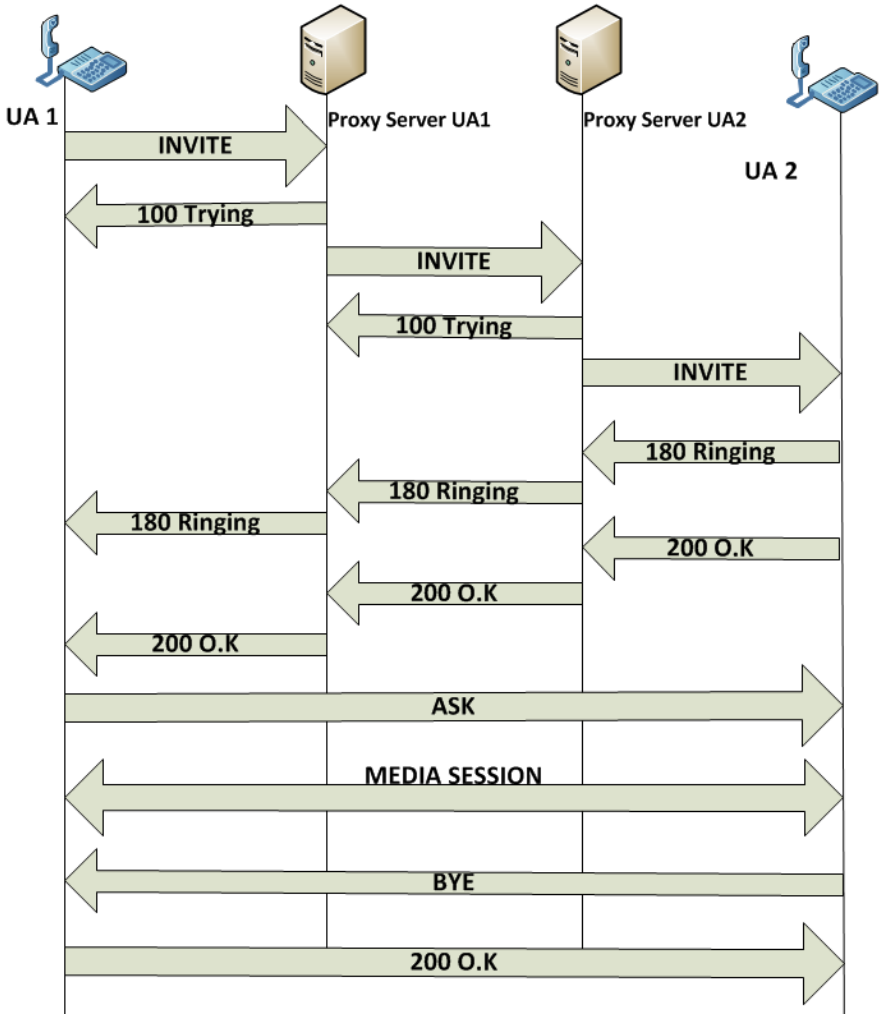
Στην παρακάτω εικόνα (Εικόνα 4.5) παρουσιάζεται ένα παράδειγμα INVITE Request, με έναν SIP Server. Ο UA1 θέλει να επικοινωνήσει με τον UA2 . Ο UA1 στέλνει ένα INVITE Request στον SIP Server, εκείνος με την σειρά του βρίσκει τον UA2 και του στέλνει το INVITE, από την στιγμή που και οι δυο χρήστες είναι register στον ίδιο Server, τον βρίσκει αμέσως. Στέλνει στον χρηστή UA1, μια απάντηση 100 (Trying) για να δείξει ότι έχει προβεί σε κάποια ενέργεια για τη εξυπηρέτηση της αίτησής του. Με το που λάβει την αίτηση ο UA2 στέλνει μια 180 (Ringing) απάντηση, ως σημάδι ότι την έχει λάβει. Αν τελικά δεχτεί την αίτηση για συνεδρία, δίνει μία 200 (OK) τελική απάντηση. Όλες οι απαντήσεις δρομολογούνται προς τον UA1 μέσω SIP Server και αφού ο UA1 στέλνει επιβεβαίωση ACK για την τελική απάντηση στον UA2, γίνεται η εγκατάσταση του διαλόγου μεταξύ τω δύο χρηστών. Όταν πια κάποιος από τους δύο χρήστες θέλει να τερματίσει την επικοινωνία, στέλνει μία αίτηση BYE στον άλλον.



Εικόνα 4.5 :Παράδειγμα INVITE με Proxy Server.

Στην παρακάτω εικόνα (Εικόνα 4.6) παρουσιάζεται ένα παράδειγμα INVITE Request, όπου μεσολαβούν δύο Proxies. Ο UA1 θέλει να επικοινωνήσει με τον UA2 . Ο UA1 στέλνει ένα INVITE Request στον Proxy UA1 , εκείνος με την σειρά του

βρίσκει ότι ο UA2 εξυπηρετείται από τον SIP Proxy UA2 οπότε μεταβιβάζει το INVITE στον Proxy UA2, και εκείνος με την σειρά του στον χρηστή UA2, στέλνει μια απάντηση 100 (Trying) στον UA1 για να δείξει ότι έχει προβεί σε κάποια ενέργεια για τη εξυπηρέτηση της αίτησής του. Ο δεύτερος Proxy στέλνει με τη σειρά του μια απάντηση 100 στον πρώτο. Αφού τον εντοπίσει, κατευθύνει την αίτηση σε αυτόν. Με το που λάβει την αίτηση ο UA2 στέλνει μια 180 (Ringing) απάντηση, ως σημάδι ότι την έχει λάβει. Αν τελικά δεχτεί την αίτηση για συνεδρία, δίνει μία 200 (OK) τελική απάντηση. Όλες οι απαντήσεις δρομολογούνται προς τον UA1 μέσω των δύο Proxy Servers και αφού ο UA1 στέλνει επιβεβαίωση ACK για την τελική απάντηση στον UA2, γίνεται η εγκατάσταση του διαλόγου μεταξύ τω δύο χρηστών. Όταν πια κάποιος από τους δύο χρήστες θέλει να τερματίσει την επικοινωνία, στέλνει μία αίτηση BYE στον άλλον.



Εικόνα 4.6: INVITE Request με Proxies.

Κεφάλαιο 5.

Ποιότητα Υπηρεσιών (QoS).

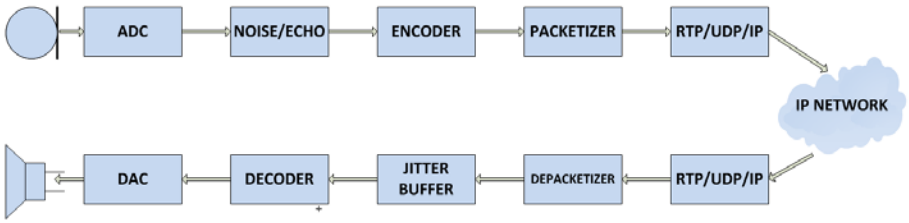
5.1 Ποιότητα υπηρεσιών.

Η μετάβαση από την συμβατική τηλεφωνία στην VoIP τηλεφωνία είναι μεγάλη και συνεχώς αυξανόμενη. Οι περισσότεροι χρήστες VoIP συστημάτων έχουν την απαίτηση η ποιότητα της VoIP υπηρεσίας (VoIP Quality of Service - QoS) να προσεγγίζει αυτήν της παραδοσιακής PSTN τηλεφωνίας που είχαν συνηθίσει. Με δεδομένη την πάρα πολύ καλή ποιότητα υπηρεσιών στα δίκτυα PSTN, καθώς τα προβλήματα τους έχουν αποσαφηνιστεί και σε μεγάλο βαθμό λυθεί εδώ και πολλά χρόνια, αυτή η απαίτηση αποτελεί από μόνη της μια πρόκληση, καθώς το VoIP που μεταδίδεται πάνω από ένα IP δίκτυο μπορεί να εμφανίσει πολλά προβλήματα ποιότητας σε διάφορους τομείς.

Στην κλασική τηλεφωνία, η ποιότητα υπηρεσιών περιορίζεται στην ποιότητα της ομιλίας, επειδή είναι αυτό που αντιλαμβάνεται ο χρήστης της υπηρεσίας. Στην περίπτωση του Voip το κριτήριο αξιολόγησης είναι η ποιότητα της συνομιλίας καθώς αυτή εξαρτάται όχι μόνο από την ποιότητα φωνής αλλά και από άλλους παράγοντες που επηρεάζουν την επιτυχημένη επίτευξη μιας συνομιλίας. Η VoIP QoE (Quality of Experience) επηρεάζεται αθροιστικά από παράγοντες του δικτύου, που διαμορφώνουν την QoS του IP δικτύου, και από παράγοντες της εφαρμογής που χρησιμοποιείται κάθε φορά.

5.2 Δομή και λειτουργία.

Ένα απλοποιημένο διάγραμμα που δείχνει την δομή ενός συστήματος VoIP φαίνεται στην (Εικόνα 5.1). Στον αποστολέα η φωνή του χρήστη αρχικά ψηφιοποιείται, τεμαχίζεται σε κομμάτια φωνής μικρής χρονικής διάρκειας, τα οποία μετά συμπιέζονται στον encoder (κωδικοποιητή). Η έξοδος του encoder είναι συμπιεσμένα κομμάτια φωνής που ονομάζονται πλαίσια (frames). Στη συνέχεια στον packetizer ένα ή περισσότερα frames πακετάρονται και σχηματίζουν το φορτίο (payload) ενός πακέτου (όπως RTP). Τέλος προστίθενται οι επικεφαλίδες των πρωτοκόλλων που χρησιμοποιούνται για τη μετάδοση (όπως RTP/UDP/IP) και το πακέτο αποστέλλεται στον παραλήπτη μέσω ενός IP δικτύου. Στον παραλήπτη ο depacketizer ανακτά το payload των IP πακέτων που περιέχουν τα δεδομένα φωνής και τοποθετεί τα frames σε ένα χώρο προσωρινής αποθήκευσης (buffer). Ο buffer αυτός παίζει σημαντικό ρόλο στην εξάλειψη της διακύμανσης της καθυστέρησης (jitter) των πακέτων που λαμβάνονται και ονομάζεται jitter buffer. Ένα frame παραμένει στον buffer μέχρι τη στιγμή που πρέπει να παρουσιαστεί, οπότε και αποσυμπιέζεται με τον κατάλληλο αποκωδικοποιητή (decoder), μετατρέπεται σε αναλογικό και τελικά σε ηχητικό σήμα. Προφανώς ο decoder και ο encoder πρέπει να αφορούν ίδιου τύπου συμπίεση. Το ζεύγος encoder/decoder ονομάζεται CODEC.



Εικόνα 5.1 :Δομή ενός Voip συστήματος.

5.3 Παράγοντες που επηρεάζουν το VoIP QoE.

Οι κύριοι παράγοντες που επηρεάζουν τη VoIP QoE είναι:

- Η συνολική καθυστέρηση που επηρεάζει την ποιότητα μιας συνδιάλεξης και έχει να κάνει με την ποιότητα υπηρεσιών του IP δικτύου.

- Η ποιότητα του φωνητικού σήματος που φτάνει στον χρήστη.

5.3.1 Ποιότητα υπηρεσιών των δικτύων IP.

Τα χαρακτηριστικά των IP δικτύων που διαμορφώνουν την ποιότητα υπηρεσιών (QoS) είναι:

5.3.1.2 Εύρος ζώνης (bandwidth).

Εύρος ζώνης είναι η ποσότητα των πληροφοριών την οποία έχει την ικανότητα το δίκτυο να μεταφέρει, σε συγκεκριμένο χρονικό διάστημα σε bits/s δεδομένων ανά δευτερόλεπτο. Ανάμεσα σε κόμβους σε ένα δίκτυο υπάρχει μια σειρά από δικτυακές ζεύξεις που η καθεμιά έχει το δικό της εύρος ζώνης. Όταν μία από αυτές είναι πιο αργή σε σχέση με τις υπόλοιπες τότε δημιουργείται συμφόρηση (bottleneck) γιατί περιορίζεται το εύρος ζώνης.

5.3.1.3 Ρυθμός απώλειας πακέτων (packet loss rate – plr).

Ο ρυθμός απώλειας πακέτων (PLR) επηρεάζει απευθείας την ποιότητα φωνής επειδή με την απώλεια πακέτων παραμορφώνεται το αρχικό φωνητικό σήμα.

Έχει παρατηρηθεί ότι η απώλεια συνεχόμενων πακέτων (bursty loss) έχει μεγαλύτερη επίδραση στην ποιότητα από ότι η απώλεια μεμονωμένων πακέτων. Σημαντικό ρόλο στο βαθμό επίδρασης του PLR παίζει ο PLC (Packet Loss Concealment) αλγόριθμος του κωδικοποιητή που χρησιμοποιείται κάθε φορά . Ο ρυθμός απώλειας θεωρείται ανεκτός αν είναι έως 5% .

Ρυθμός απώλειας πακέτων είναι ο λόγος των συνολικών πακέτων που δεν φτάνουν στον παραλήπτη προς τον συνολικό αριθμό των απεσταλμένων πακέτων. Η απώλεια των πακέτων οφείλεται σε συμφόρηση στο δίκτυο, άρα γίνεται απόρριψη πακέτων όταν το buffer των δρομολογητών γεμίζει και δεν μπορεί να διαχειριστεί πλέον άλλα πακέτα και όταν προκύπτουν λάθη μετάδοσης σε κάποια ζεύξη. Το φυσικό επίπεδο βάζει αρκετούς περιορισμούς στο εύρος ζώνης, έτσι σε μια κλασική σύνδεση ADSL για παράδειγμα, το upstream είναι κατά πολύ

μικρότερο από το downstream (1mbps/24mbps) άρα για να εκτελεστεί σωστά μια συνδιάλεξη δίνεται προτεραιότητα στα πακέτα φωνής ώστε να ικανοποιείται η απαίτηση πραγματικού χρόνου και το υπόλοιπο εύρος ζώνης δίνεται στα δεδομένα, αν όμως ο router σε κάποια στιγμή δεν μπορεί να ανιχνεύσει διαθέσιμο εύρος ζώνης δεν θα δοθεί προτεραιότητα και θα υπάρχουν απώλειες και στα πακέτα φωνής και δεδομένων. Τα πακέτα δεδομένων όμως θα μεταδοθούν ξανά ενώ τα πακέτα φωνής χάνονται.

Η καθυστέρηση των πακέτων στο δίκτυο, το jitter και τα λάθη στα πακέτα μπορούν να προκαλέσουν απώλεια των πακέτων στην είσοδο του αποκωδικοποιητή. Το μέγεθος του jitter buffer επιδρά σημαντικά στο ποσοστό του packet loss, ο jitter buffer ρυθμίζει τη ροή πακέτων ανάμεσα στα εισερχόμενα πακέτα και τον κωδικοποιητή φωνής όπου αναπαράγονται τα πακέτα στο δέκτη, έτσι ένας μεγάλος jitter buffer αυξάνει το delay και μειώνει το packet loss ενώ ένας μικρός ναι μεν ικανοποιεί την απαίτηση για μικρό delay ωστόσο αυξάνει την απόρριψη πακέτων. Ένας adaptive jitter buffer διατηρεί το μικρότερο ποσοστό απώλειας πακέτων με τη μικρότερη δυνατή καθυστέρηση στον buffer. Για να ελαχιστοποιήσουμε την επίδραση των χαμένων πακέτων εφαρμόζουμε διάφορες τεχνικές γνωστές και ως PLC (Packet Loss Concealment).

5.3.1.4 Καθυστέρηση (end-to-end delay).

Ως καθυστέρηση (delay) εννοείται ο χρόνος που υπερβαίνει τον κανονικό που χρειάζεται ένα πακέτο για να μεταδοθεί μέσα στο δίκτυο και να φτάσει τον προορισμό του.

Σύμφωνα με την ITU (International Telecommunication Union) προσδιορίζονται τα όρια της καθυστέρησης για one way μετάδοση και πιο συγκεκριμένα γίνεται χρήση echo canceller (ακυρωτή ηχούς). Οι συστάσεις γίνονται για επικοινωνία σε εθνικό και διεθνές επίπεδο όπου η χρήση echo canceller είναι επιβεβλημένη. Η χρήση echo canceller επιβάλλεται όταν η one way καθυστέρηση ξεπερνά τα 25 ms.

Η καθυστέρηση σύμφωνα με την ITU:

- 0-150 ms : αποδεκτή καθυστέρηση.
- 150-400 ms : αποδεκτή αλλά με επίδραση στην ποιότητα συνομιλίας.
- 400 ms: μη αποδεκτή για την εφαρμογή του VoIP.

5.3.1.4.1 Καθυστέρηση λόγο CODEC (CODEC delay).

Το πρώτο είδος καθυστέρησης το εισάγει ο CODEC (**CODEC delay**). Ο CODEC εκτελεί διάφορες πράξεις με πιο σημαντικές την κωδικοποίηση της φωνής, την συμπίεση και την τοποθέτηση των δεδομένων φωνής σε πακέτα συγκεκριμένου μήκους (packetization). Συνολικά ο (CODEC) μπορεί να προκαλέσει καθυστέρηση ως και 35 msec (ανάλογα με το είδος του CODEC) και στο σημείο προορισμού η καθυστέρηση είναι πολύ μικρότερη από ότι στο σημείο εκκίνησης (λιγότερο από το μισό).

5.3.1.4.2 Καθυστέρηση των πακέτων στη ουρά εξόδου (Output Queuing Delay).

Το δεύτερο είδος καθυστέρησης παρατηρείται στο σημείο εκκίνησης και προέρχεται από την καθυστέρηση των πακέτων στην ουρά εξόδου (**Output Queuing Delay**) του δρομολογητή. Εξαρτάται από πολλούς παράγοντες μεταξύ των οποίων και τα ίδια τα χαρακτηριστικά του δρομολογητή. Πρέπει γενικά να διατηρείται σε επίπεδα κάτω των 10 msec.

5.3.1.4.3 Καθυστέρηση της επεξεργασίας στο δίκτυο (Output Queuing Delay).

Το τρίτο είδος καθυστέρησης είναι η καθυστέρηση που παρατηρείται λόγω της επεξεργασίας μέσα στο δίκτυο. Σαν καθυστέρηση επεξεργασίας μέσα στο δίκτυο ορίζεται ο χρόνος που θα χρειαστεί το πακέτο να φτάσει από τον δρομολογητή εκκίνησης στον δρομολογητή προορισμού, σε αυτό το είδος της καθυστέρησης παίζουν ρόλο 3 παράγοντες.

- Ο ρυθμός μετάδοσης των δεδομένων από το σημείο εκκίνησης προς το δίκτυο (serialization Up-link delay).

- Ο ρυθμός μετάδοσης από το δίκτυο προς το σημείο προορισμού (serialization Down-link delay).

- Οι εσωτερικές καθυστερήσεις του ίδιου του δικτύου κορμού (General Network Delay)

5.3.1.4.4 Άλλου είδους καθυστερήσεις.

- **Καθυστέρηση Μετάδοσης (Transmission Delay)**

  Ο χρόνος που χρειάζεται για να μεταφερθούν όλα τα bits ενός πακέτου μέσα στη ζεύξη.

- **Καθυστέρηση Διάδοσης (Propagation Delay)**

  Ο χρόνος που χρειάζεται ένα bit για να διασχίσει το μήκος της ζεύξης μέσω της οποίας γίνεται η μεταφορά δεδομένων.

- **Καθυστέρηση Επεξεργασίας (Processing Delay)**

  Ο χρόνος που χρειάζεται για την επεξεργασία ενός πακέτου στους κόμβους.

- **Καθυστέρηση Ουράς (Queuing Delay)**

  Ο χρόνος που πρέπει να περιμένει ένα πακέτο στην ουρά (όπως για παράδειγμα η ουρά στον buffer ενός δρομολογητή) μέχρι να ξεκινήσει η μετάδοσή του.

5.3.1.4.5 Συνολικός προϋπολογισμός καθυστέρησης.

Αν υπολογίσει κάποιος όλες τις επιμέρους καθυστερήσεις του δικτύου μπορεί να γνωρίζει εκ των προτέρων την καθυστέρηση που μπορεί να συναντήσει ένα πακέτο φωνής κατά τη διάρκεια του ταξιδιού του. Με το δεδομένο ότι μερικά είδη καθυστέρησης είναι γνωστά όπως η καθυστέρηση των COSECs και το serialization delay των γραμμών, με έναν σωστό προγραμματισμό στην περίπτωση του serialization delay και την σωστή επιλογή CODEC γίνεται εφικτή η αντιμετώπιση των προβλημάτων που προκύπτουν. Εξαιρούνται τα έκτακτα γεγονότα όπως βλάβες και υπερφόρτωση του δικτύου, που και πάλι με σωστούς μηχανισμούς έλεγχου ακόμα και αυτές μπορούν να εξαλειφθούν έτσι ώστε να υπάρχει ιδανική σχέση ποιότητας-απόδοσης στη μετάδοση, τόσο φωνής όσο και δεδομένων.

5.3.2 Η ποιότητα του φωνητικού σήματος που φτάνει στον χρήστη.

Η ποιότητα του φωνητικού σήματος που φτάνει στον τελικό χρήστη επηρεάζεται από μια σειρά από παραμέτρους που αναλύονται στην συνέχεια.

5.3.2.1 Jitter Delay Διακύμανση καθυστέρησης (delay variation ή jitter).

Το jitter είναι το σημαντικότερο πρόβλημα στα δίκτυα δεδομένων, ειδικότερα σε εφαρμογές που απαιτούν επικοινωνία πραγματικού χρόνου όπως το VoIP. Ορίζεται ως η διαφορά μεταξύ του αναμενόμενου χρόνου άφιξης ενός πακέτου στο σημείο προορισμού και του πραγματικού χρόνου άφιξης. Αυτό οφείλεται στο γεγονός ότι τα πακέτα αδυνατούν να φτάσουν στον δέκτη σε ίσα χρονικά διαστήματα γιατί μέσα στο δίκτυο δέχονται διαφορετικές καθυστερήσεις . Έτσι η ποιότητα φωνής μειώνεται σημαντικά και ταυτόχρονα η ποιότητα της συνδιάλεξης καταρρέει κάνοντας μη εφικτή την επικοινωνία .

Η λύση στο πρόβλημα του jitter δίνεται με την χρήση buffering στο σημείο προορισμού, έτσι ώστε ο δρομολογητής προορισμού να παράγει με σταθερό ρυθμό τα πακέτα φωνής στον τελικό χρήστη. Καθυστέρηση ναι μεν υπάρχει, επειδή όμως τα πακέτα είναι συγχρονισμένα δεν γίνεται αντιληπτή στον χρήστη .

Όσο μεγαλύτερος είναι ο χρόνος αποθήκευσης (buffer delay) στον jitter buffer τόσο πιο απίθανο είναι να φτάσει κάποιο πακέτο αργοπορημένο. Όμως μεγαλώνοντας τον χρόνο αποθήκευσης μεγαλώνει και η συνολική καθυστέρηση

(latency), μειώνοντας έτσι την ποιότητα της συνδιάλεξης.

Το buffer delay μπορεί να είναι σταθερό ή μεταβλητό (adaptive jitter buffer). Στους adaptive jitter buffers αυξομειώνεται ο χρόνος αποθήκευσης ανάλογα με το jitter του δικτύου. Για παράδειγμα όταν το jitter είναι μικρό δε χρειάζεται μεγάλο buffer delay και έτσι το buffer μπορεί να μειωθεί, μειώνοντας ταυτόχρονα και την συνολική καθυστέρηση. Αν κάποια στιγμή όμως το jitter αυξηθεί για κάποιο λόγο, τότε μπορεί να αυξηθεί και το buffer delay. Στους adaptive jitter buffers υπάρχει λοιπόν ένας αλγόριθμος (playout buffer algorithm) που καθορίζει πότε ένα πακέτο θα βγει από τον buffer και θα αναπαραχθεί (playout time). Η ρύθμιση-αλλαγή του buffer delay γίνεται συνήθως σε περιόδους σιγής (όταν ο χρήστης δεν μιλάει) ώστε να μη γίνεται αντιληπτή από τον χρήστη.

5.3.2.1.2 Υπολογισμός της καθυστέρησης στο πρωτόκολλο RTP.

Το RTP με τη βοήθεια των RTCP SR και RR πακέτων μπορεί να υπολογίσει το Round Trip Time μεταξύ των δύο κόμβων που συμμετέχουν σε μία RTP σύνοδο. Ο αποστολέας βάζει στα SR πακέτα που στέλνει το χρόνο αποστολής τους. Ο παραλήπτης όταν στείλει ένα RR πακέτο βάζει στο πεδίο LSR τον χρόνο αποστολής του τελευταίου SR πακέτου που έλαβε καθώς και τον χρόνο που μεσολάβησε ανάμεσα στη αποστολή του και στην λήψη του τελευταίου SR πακέτου (DLSR). Έτσι αν ο αποστολέας λάβει ένα RR πακέτο τη χρονική στιγμή A, το RTT μπορεί να υπολογισθεί ως A – DLSR – LSR.

5.3.2.1.3 Υπολογισμός της διακύμανσης καθυστέρησης (jitter).

Για να αντιμετωπιστεί το πρόβλημα του jitter χρησιμοποιείται το real time control Protocol (RTCP), έτσι το jitter μετριέται σε timestamps.

Ο υπολογισμός της διακύμανσης καθυστέρησης γίνεται με την παρακάτω συνάρτηση:

$$\mathbf{J(i)} = \frac{(\mathbf{i-1}) + (|\mathbf{D(i-1,i)}| - \mathbf{j(i-1)})}{\mathbf{16}}$$

Όπου:

- $\mathbf{J(i)}$: Η διακύμανση καθυστέρησης (jitter).
- $\mathbf{D}$: Η χρονική απόκλιση που έχουν δυο συνεχόμενα πακέτα.

Αφού γίνει λήψη το i-οστό πακέτο, υπολογίζεται η αλλαγή στο interarrival time και αφού γίνει διαίρεση με το 16 για να μειωθεί ο θόρυβος και η επίδραση τυχαίων παραγόντων, προστίθεται η προηγούμενη τιμή του jitter.

Η χρονική απόκλιση υπολογίζεται με την παρακάτω συνάρτηση.

$$\mathbf{D(i,j)} = \mathbf{(R_j - R_i) - (S_j - S_i) = (R_j - S_j) - (R_i - S)}$$

Όπου:

- $\mathbf{S_i}$: Το RTP timestamp του πακέτου i.

- $\mathbf{R_i}$: Ο χρόνος άφιξης σε μονάδα χρόνου ίδια με του RTP timestamp για το πακέτο i.

Επομένως δημιουργείται ένα RR πακέτο στο οποίο τοποθετείται η τρέχουσα τιμή του jitter.

5.3.2.2 Κωδικοποίηση και συμπίεση CODEC:

CODEC ονομάζεται ο συνδυασμός encoder και decoder (en**COD**er-**DEC**oder), που αφορούν κάποια συγκεκριμένη κωδικοποίηση. Οι CODECs χρησιμοποιούνται για την συμπίεση ήχου, εικόνας και βίντεο και έχουν μεγάλη σημασία καθώς βοηθούν στη μετάδοση φωνής μέσα από ένα δίκτυο, μειώνοντας το απαιτούμενο εύρος ζώνης.

Η ποιότητα και το είδος της κωδικοποίησης/συμπίεσης επηρεάζει τη VoIP QoE, δηλαδή όταν ένα σήμα κωδικοποιείται και μετά αποκωδικοποιείται, υφίσταται μόνιμη παραμόρφωση.

Οι CODECs φωνής μπορούν να κατηγοριοποιηθούν σε τρεις κύριες κατηγορίες με βάση την αρχή λειτουργίας τους.

- **Waveform Coders (κυματομορφής):** είναι εξαιρετικά απλοί και εκμεταλλεύονται την αυτοσυσχέτιση των δεδομένων ήχου στο πεδίο του χρόνου και της συχνότητας για τη συμπίεση. Σε αυτή τη κατηγορία ανήκει ο G.711 PCM (64Kb/s) και ο G.726 ADPCM (40/32/24/16 Kb/s)

- **Parametric Vocoders (voice coders):** βασίζονται στην μοντελοποίηση της ανθρώπινης ομιλίας. Η έξοδος του decoder είναι συνθετική φωνή και δε βασίζεται καθόλου στην αρχική κυματομορφή.

- **Hybrid coders (υβριδικοί):** συνδυάζουν τις δύο παραπάνω τεχνικές και πετυχαίνουν πολύ καλή ποιότητα φωνής και μεγάλη συμπίεση. Σε αυτή τη κατηγορία ανήκουν οι περισσότεροι σύγχρονοι CODECs: G.729 CS-ACELP (8Kb/s), G.723.1 MP-MLQ/ACELP (6.3/5.3 Kb/s), AMR (Adaptive Multi- Rate, ACELP), Speex και iLBC (Internet Low Bit Rate CODEC).

Ο στόχος της χρήσης CODEC είναι να υλοποιηθούν όσο το δυνατόν περισσότερες τηλεφωνικές συνδέσεις μέσα από ένα δίκτυο δεδομένων, κάνοντας συμπίεση που φτάνει σε ρυθμούς 8 προς 1. Επίσης οι CODECs εισάγουν νέες δυνατότητες στην ψηφιακή επεξεργασία φωνής.

Μερικά από τα επιπλέον χαρακτηριστικά που περιλαμβάνουν οι κωδικοποιητές είναι η ανίχνευση φωνής (voice activity detection), η απόκρυψη απώλειας πακέτων (packet loss concealment), η αναπαραγωγή του περιβάλλοντα θορύβου (comfort noise generation) αλλά και η κωδικοποίηση ασφαλείας (security encoding) .

Codec και Bit Rate	Μέγεθος Πακέτου(Bytes)	Ποιότητα MOS	Bandwidth Ethernet (Kbps)
ADPCM (32 Kbps)	-	3,8	43,6
ITU G.711 a- (64 Kbps)	80	4,4	87,2
ITU G.711 u-Law(USA) (64 Kbps)	80	4,4	87,2
ITU G.722 (48 Kbps)	-	4,1	87,2
ITU G.722 (56 Kbps)		3	64
ITU G.722 (64 Kbps)	80	3	64
ITU G.723.1 (5,3 Kbps)	20	3,62	20,8
ITU G.723.1 (6,3 Kbps)	24	3,9	21,9
ITU G.726 (16 Kbps)	-	-	-
ITU G.726 (24 Kbps)	15	-	47,2
ITU G.726 (32 Kbps)	20	3.8	55,2
ITU G.726 (40 Kbps)	-	-	-
ITU G 728 (16 Kbps)	10	3,61	31,5
ITU G 729 (8 Kbps)	10	3,7	31,2
GSM (13 kbps)	-	3,5	
iLBC (13,3)	50	4,14	28,8
iLBC (15,2)	50	-	38,4
LPC-10 (2,5)	-	-	-
Speex (2,15)	-	-	-
Speex (44,2)	-	-	-

Πίνακας 5.1: Πίνακας Codec με τα χαρακτηριστικά τους.

5.3.2.3 Δημιουργός Πακέτων Packetizer:

Ο Packetizer ομαδοποιεί έναν αριθμό από πλαίσια (frames), σχηματίζοντας έτσι το φορτίο (payload) ενός πακέτου (πχ. RTP), το οποίο αποστέλλεται στον προορισμό του, αφού προστεθούν σε αυτό οι κατάλληλες επικεφαλίδες (headers), ανάλογα με τα χρησιμοποιούμενα πρωτόκολλα (πχ. RTP/UDP/IP).

Ανάλογα με τον αριθμό των frames που ενσωματώνονται σε ένα πακέτο, διαμορφώνεται και το μέγεθός του πακέτου, με αποτέλεσμα όσο μεγαλύτερο είναι το πακέτο, τόσο περισσότερο χρόνο να χρειάζεται για να μεταδοθεί, εισάγοντας έτσι μεγαλύτερη καθυστέρηση στην επικοινωνία.

5.3.2.4 Ηχώ (Echo)

Η ηχώ είναι επιστροφή της φωνής του χρήστη με καθυστέρηση, με διαφορετική στάθμη ήχου στο ακουστικό του τηλεφώνου. Στις τηλεπικοινωνίες η ηχώ μπορεί να είναι είτε ακουστική είτε ηλεκτρική. Η ακουστική ηχώ δημιουργείται στο ακουστικό μέσω ενός τηλεφώνου, ενώ η ηλεκτρική δημιουργείται στο υλικό της γραμμής. Για να βελτιωθεί η ποιότητα της κλήσης χρησιμοποιούμε echo cancellers, έτσι αναγνωρίζεται η ηχώ και κόβεται.

Η ηχώ παρουσιάζεται όταν η καθυστέρηση επιστροφής είναι πάνω από 50 msec. Η ηχώ είναι πάντα ανεπιθύμητη. Ένα μικρό ποσό ηχούς ονομάζεται παράπλευρη (sidetone) και είναι επιθυμητή. Στα δίκτυα μεταγωγής κυκλώματος η καθυστέρηση επιστροφής της ηχούς είναι λιγότερη από 50 msec επειδή τα δίκτυα μεταγωγής κυκλώματος διαμορφώνονται έτσι ώστε να απαλείφουν κάθε αντήχηση πάνω από 45 ή 50 msec ανάλογα με το δίκτυο. Αυτά τα πρότυπα καθορίζονται από την ITU στο G.131. Τα 50 msec ορίστηκαν επειδή είναι το μέγιστο ποσοστό που δεν γίνεται αντιληπτό από τον ομιλητή. Εξαιτίας της καθυστέρησης δικτύου η καθυστέρηση στα IP δίκτυα μπορεί να είναι πολύ μεγάλη.

5.4 Κατηγοριοποίηση μεθόδων αξιολόγησης VoIP QoE

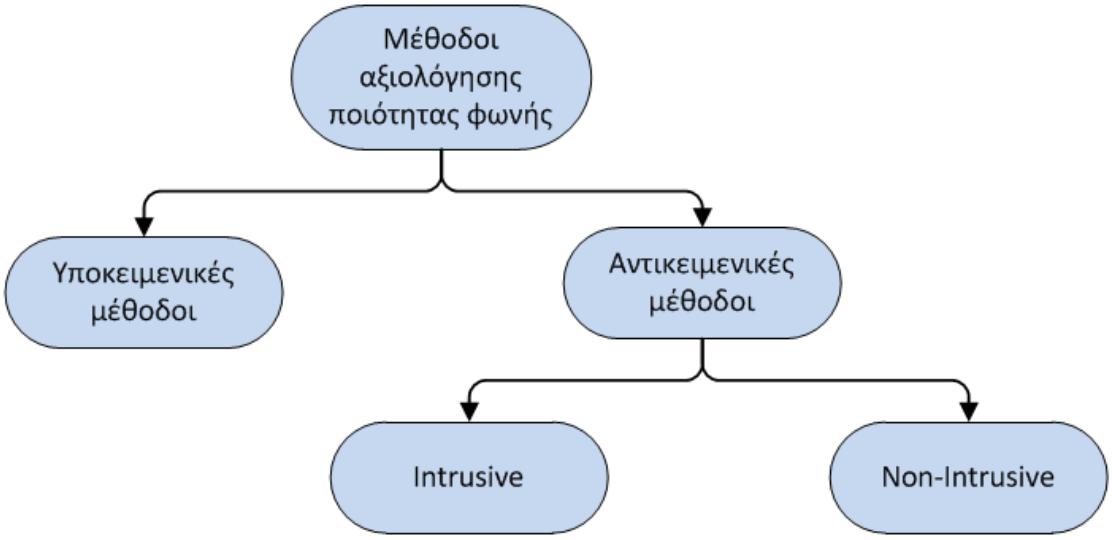
Η ύπαρξη αξιόπιστων μεθόδων μέτρησης της ποιότητας της φωνής αποτελεί θεμελιώδη απαίτηση στις τηλεπικοινωνίες για τεχνικούς, εμπορικούς και νομικούς λόγους, έτσι έχουν προκύψει πολλές τέτοιες μέθοδοι, οι οποίες είναι αρκετά διαφορετικές μεταξύ τους και διακρίνονται σε υποκειμενικές και αντικειμενικές.

Στις υποκειμενικές μεθόδους κάποια δείγματα ομιλίας στέλνονται μέσω του συστήματος δικτύου και ένας αριθμός ανθρώπων καλείται να αξιολογήσει τα δείγματα ομιλίας. Οι υποκειμενικές μέθοδοι έχουν πολλά μειονεκτήματα όπως το κόστος, τη δύσκολη επανάληψη τους, επειδή είναι χρονοβόρες και το ότι δεν μπορούν να χρησιμοποιηθούν σε μεγάλη κλίμακα.

Οι αντικειμενικές μέθοδοι χωρίζονται σε δύο κατηγορίες, σε παρεμβατικές (intrusive) και μη παρεμβατικές (non-intrusive).

- Στις intrusive μεθόδους γίνεται μία αλγοριθμική σύγκριση μεταξύ ενός αρχικού φωνητικού σήματος αναφοράς, που περνάει μέσω ενός συστήματος/δικτύου και του παραλαμβανόμενου παραμορφωμένου σήματος. Οι intrusive μέθοδοι είναι ακριβείς, αλλά η ανάγκη των μεθόδων αυτών να χρησιμοποιούν το σήμα αναφοράς, τις καθιστά ακατάλληλες για τον έλεγχο της ποιότητας της φωνής ενός συστήματος σε πραγματικό χρόνο.
- Οι non-intrusive μέθοδοι μπορούν να εφαρμοστούν σε πραγματικό χρόνο. Για την αξιολόγηση χρησιμοποιούν είτε το προς αξιολόγηση σήμα (signal-based) είτε κάποιες παραμέτρους του σήματος ή/και του δικτύου μετάδοσης (parameter-based).

Θα πρέπει να σημειωθεί ότι από τις μεθόδους που μπορούν να χρησιμοποιηθούν για την αξιολόγηση μιας VoIP υπηρεσίας, μερικές αξιολογούν μόνο την ποιότητα της λαμβανόμενης ομιλίας (listening quality), ενώ άλλες την ποιότητα της συνομιλίας (conversational quality). Παρακάτω παρατίθεται εικόνα που δείχνει την κατηγοριοποίηση των μεθόδων (Εικόνα 5.2).



Εικόνα 5.2 Κατηγοριοποίηση μεθόδων αξιολόγησης ποιότητας φωνής.

5.4.1 Η μέθοδος MOS.

Η μέθοδος αξιολόγησης MOS (Mean Opinion Score) είναι η ευρύτερα χρησιμοποιούμενη υποκειμενική μέθοδος και προτάθηκε από τον ITU. Η μέθοδος αυτή στηρίζεται στην αξιολόγηση της ομιλίας σε μία κλίμακα 1-5 από έναν αριθμό χρηστών κάτω από συγκεκριμένες πειραματικές συνθήκες.

Οι τεχνικές της υποκειμενικής μέτρησης είναι :

- Η απόλυτη βαθμολογική κατηγορία (ACR).

  Στο ACR οι συμμετέχοντες, οι οποίοι είναι τουλάχιστον 16, ακούν επεξεργασμένα δείγματα ομιλίας και χρησιμοποιούν μία κλίμακα MOS από 1-5 (Πίνακας 5.2) για να αξιολογήσουν την ποιότητα και στη συνέχεια βγαίνει ένας μέσος όρος. Ανάμεσα σε 4 και 5 θεωρείται απόλυτη ποιότητα, μεταξύ 3 και 4 θεωρείται τηλεπικοινωνιακή ποιότητα, ενώ MOS μικρότερο του 3 θεωρείται συνθετική ποιότητα.

Βαθμός MOS	**Ποιότητα ομιλίας**
1	Κακή
2	Φτωχή
3	Μέτρια
4	καλή
5	εξαιρετική

Πίνακας 5.2: Πίνακας Βαθμονόμησης της μεθόδου MOS.

- Η υποβαθμισμένη κατηγορία (DCR).

  Στη DCR υπάρχουν δύο δείγματα ομιλίας, το ένα είναι ένα δείγμα αναφοράς με καθορισμένη ποιότητα και αναφέρεται σε ένα σήμα λίγων δευτερολέπτων, ενώ το δεύτερο είναι μία υποβαθμισμένη σε ποιότητα έκδοση του πρώτου. Οι ακροατές πρέπει να συγκρίνουν τα 2 σήματα και να βαθμολογήσουν από το 1 – 5 , μόνο που εδώ το 1 μεταφράζεται σε άριστη ποιότητα.

- Η συγκριτική βαθμολογική κατηγορία (CCR).

  Στη CCR οι χρήστες καλούνται να ακούσουν δύο σειρές δειγμάτων, μία με δείγματα αναφοράς και μία με τα υποβαθμισμένα. Η δοκιμή είναι παρόμοια με DCR, εκτός από το ότι η σειρά των δειγμάτων που υποβλήθηκαν στους ακροατές έχει αλλάξει σε διαφορετικές επαναλήψεις. Η σειρά δειγμάτων αναφοράς και υποβαθμισμένων δεν έχει δηλωθεί στον ακροατή.

5.4.2 Η μέθοδος PESQ.

Η πιο σύγχρονη και εξελιγμένη μέθοδος αξιολόγησης φωνής είναι η PESQ (Perceptual Evaluation of Speech Quality), η οποία έχει προταθεί από τον ITU με κύριο στόχο την χρήση της για αξιολόγηση περιορισμένου εύρους ζώνης τηλεφωνικών δικτύων και CODEC. Πρόκειται για μία intrusive αντικειμενική μέθοδο που συνδυάζει τις λειτουργίες δύο άλλων αντικειμενικών μεθόδων των PSQM+ και PAMS.

Το PESQ συγκρίνει δύο φωνητικά σήματα, όπως για παράδειγμα ένα αρχικό φωνητικό σήμα που μεταδίδεται μέσω ενός δικτύου με το τελικό σήμα που παραλαμβάνεται, έτσι ανάλογα με τα χαρακτηριστικά και το μέγεθος της παραμόρφωσης κάνει μια αξιολόγηση στην κλίμακα MOS.

Η βασική λειτουργία της μεθόδου είναι η σύγκριση μικρών τμημάτων δύο σημάτων για υπολογισμό της καθυστέρησης και των χαρακτηριστικών της παραμόρφωσης. Για την παραμόρφωση, κάθε block των δύο σημάτων αναλύεται ως προς το περιεχόμενο των συχνοτήτων του με μετασχηματισμό Fourier, οπότε από τη σύγκριση των συντελεστών του μετασχηματισμού προκύπτει ο βαθμός και τα χαρακτηριστικά της παραμόρφωσης έτσι ώστε το PESQ με βάση ένα ψυχό-ακουστικό μοντέλο να αξιολογεί την επίδραση της παραμόρφωσης στην ακουστικότητα του σήματος, χρησιμοποιώντας την κλίμακα MOS.

Συγκριτικά με την υποκειμενική μέτρηση ποιότητας (actual listeners) η μέθοδος pesq δίνει καλύτερα αποτελέσματα για χαμηλής ποιότητας σήματα και πιο αναλυτικές τιμές για καλά σήματα φωνής.

5.4.3 Η μέθοδος E-Model.

Η μέθοδος E-Model είναι μια μέθοδος που χρησιμοποιεί non-intrusive αντικειμενική μέθοδος αξιολόγησης της ποιότητας μιας συνδιάλεξης, ορίστηκε από τον οργανισμό ETSI και αργότερα μετεξελίχθηκε στο πρότυπο ITU G.107.

Το E-Model δίνει μια εκτίμηση της ποιότητας μιας συνδιάλεξης υπολογίζοντας έναν παράγοντα R, για τον οποίο λαμβάνονται υπόψη μια σειρά από παραμέτρους .Ο υπολογισμός του R factor στηρίζεται στην παραδοχή ότι η επίδραση διαφορετικών παραμέτρων στη συνολική ικανοποίηση του χρήστη είναι αθροιστική και εκφράζει το συνολικό αποτέλεσμα της επίδρασης στη μετάδοση και στην ποιότητα της λαμβανόμενης ομιλίας . Κυμαίνεται από 0 ως 120 και οι τυπικές τιμές του R για περιορισμένου εύρους ζώνης τηλεφωνία είναι 50-94.

Το R υπολογίζεται από την εξίσωση:

$$\boldsymbol{R = R_o - I_s - I_d - I_e + A}$$

Όπου:

- $\mathbf{R_o}$**:** Είναι ο λόγος του σήματος προς τον θόρυβο (SNR – Signal to Noise Ratio).

- $\mathbf{I_s}$**:** Είναι το άθροισμα των επιδράσεων παραγόντων που συμβαίνουν σχεδόν ταυτόχρονα (simultaneous) με την ομιλία (π.χ. ένταση, παραμόρφωση κβαντοποίησης).

- $\mathbf{I_d}$**:** Είναι η επίδραση παραγόντων που σχετίζονται με την καθυστέρηση (delay) όπως η ηχώ και η δυσκολία συνομιλίας λόγω καθυστέρησης.

- $\mathbf{I_e}$**:** Είναι η επίδραση παραγόντων που σχετίζονται με τον "εξοπλισμό" (equipment) όπως CODEC και packet loss rate

- $\boldsymbol{A}$**:** Είναι ένας παράγοντας πλεονεκτήματος ή προσδοκίας (advantage or expectation factor).

Οι τιμές του R μπορούν να μετατραπούν στην κλίμακα MOS (Πίνακας 5.3) με βάση στην εξίσωση.

$$\boldsymbol{MOS} = \begin{cases} \mathbf{1} & \boldsymbol{R \leq 0} \\ \mathbf{1 + 0,035R + R(R - 60)(100 - R)7 \times 10^{-6}} & \mathbf{0 < R < 100} \\ \mathbf{4,5} & \boldsymbol{R \geq 100} \end{cases}$$

R-factor	MOS	Ποιότητα Ομιλίας	Ικανοποίηση χρήστη
100-90	4,34	εξαιρετική	Πολύ ικανοποιημένος
90-80	4,03	καλή	Ικανοποιημένος
80-70	3,6	μέτρια	Μερικοί χρήστες δυσαρεστημένοι
70-60	3,1	φτωχή	Αρκετοί χρήστες δυσαρεστημένοι
60-50	2,58	κακή	Σχεδόν όλοι οι χρήστες δυσαρεστημένοι

Πίνακας 5.3: Πίνακας αντιστοίχησης του R-factor με την μέθοδο MOS.

Από τις παραμέτρους που χρειάζονται για τον υπολογισμό των παραγόντων του R, οι περισσότερες σχετίζονται με τα κλασικά αναλογικά δίκτυα τηλεφωνίας και τις παραμέτρους των απλών τηλεφωνικών συσκευών, έτσι για αυτές τις παραμέτρους μπορούν να χρησιμοποιηθούν συγκεκριμένες τιμές που ορίζονται στο πρότυπο ITU G.108 σε ότι αφορά στο Voip. Επιπλέον μπορεί να γίνει περαιτέρω απλοποίηση θεωρώντας ότι στο VoIP η κύρια επίδραση στην ποιότητα προέρχεται από την καθυστέρηση στον CODEC και την απώλεια πακέτων.

Αρά Με βάση τα παραπάνω η εξίσωση μπορεί να απλοποιηθεί :

$$\boldsymbol{R = 94.2 - I_d - I_e + A}$$

5.4.3.1 Υπολογισμός του $\mathbf{I_d}$.

Ο παράγοντας ($\mathrm{I_d}$) είναι η καθυστέρηση στο σήμα και περιέχει τις επιδράσεις της ηχούς ακροατή ($\mathrm{I_{dIe}}$) (listener echo), της ηχούς ομιλητή (talker echo) ($\mathrm{I_{dte}}$) ,την απόλυτη καθυστέρηση του κύριου σήματος ($\mathrm{I_{dd}}$) και εκφράζεται με την εξίσωση:

$$\boldsymbol{I_d = I_{dte} + I_{dIe} + I_{dd}}$$

Η καθυστέρηση με την οποία σχετίζεται το ($\mathrm{I_{dd}}$) είναι η end-to-end καθυστέρηση, το ($\mathrm{I_{dte}}$) σχετίζεται με την μέση μονόδρομη καθυστέρηση (T) από την πλευρά του παραλήπτη προς το σημείο όπου προκαλείται η ηχώ. Το Idle σχετίζεται με το round-trip-time ($\mathrm{T_r}$). Κάνοντας ορισμένες παραδοχές και θεωρώντας ότι η μετάδοση γίνεται πάνω από IP δίκτυο, τότε το ($\mathrm{I_d}$) μπορεί να εκφραστεί ως συνάρτηση της end-to-end καθυστέρησης (d) με την εξίσωση.

$$\boldsymbol{d = T_a = T = \frac{T_r}{2}}$$

Παίρνοντας τις προϋπολογισμένες τιμές για μια σειρά από παραμέτρους που ορίζονται στο ITU G.107, τότε το Id μπορεί να εκφραστεί ως μονοδιάστατη συνάρτηση της καθυστέρησης d και από αυτήν την συνάρτηση μπορεί να προκύψει με καμπύλες προσαρμογής curve fitting η απλή εξίσωση.

$$I_d = 0,024d + 0,11(d - 177,3)H(d - 177.3)$$

$$\text{Όπου } H(x) = \begin{cases} 0 \text{ για } x < 0 \\ 1 \text{ για } x \geq 0 \end{cases}$$

5.4.3.2 Υπολογισμός του I_e.

Ο κύριος παράγοντας που επηρεάζει το (I_e) στις εφαρμογές VoIP είναι η απόδοση του CODEC, που με τη σειρά του εξαρτάται κυρίως από τον τύπο του CODEC που έχει επιλεχθεί και από το ρυθμό απώλειας πακέτων. Έτσι το Ie μπορεί να εκφραστεί προσεγγιστικά συναρτήσει τριών παραμέτρων (λ1, λ2, λ3), που χαρακτηρίζουν τον τύπο του CODEC, την απόδοσή του και τον ρυθμό απώλειας πακέτων και δίνεται με την παρακάτω εξίσωση.

$$I_e = \lambda 1 + \lambda 2 \ln(1 + \lambda 3 p)$$

Η παράμετρος λ1 εκφράζει την επίδραση της παραμόρφωσης του CODEC όταν δεν υπάρχουν απώλειες πακέτων στην ποιότητα της φωνής, ενώ οι λ2 και λ3 εκφράζουν την επίδραση της απώλειας πακέτων στην απόδοση του CODEC.

Πειραματικός προσδιορισμός των συντελεστών (λ1, λ2, λ3) για κάποιο CODEC:

- Αρχικά με τη μέθοδο PESQ αξιολογείται η απόδοση του CODEC στην κλίμακα MOS για διάφορους ρυθμούς απώλειας πακέτων plr (**p**acket **l**oss **r**ate).

- Στη συνέχεια η απόδοση συναρτήσει του (plr) αντιστοιχίζεται στην κλίμακα του E-Model. Για δεδομένες τιμές καθυστέρησης, η εξίσωση μπορεί να εκφραστεί συναρτήσει του plr με μοναδικές παραμέτρους τους συντελεστές (λ1, λ2, λ3). Έτσι μπορούν να υπολογιστούν οι συντελεστές (λ1, λ2, λ3) (Πίνακας 5.4) με τη μέθοδο των ελαχίστων τετραγώνων ανάμεσα στις πειραματικές τιμές της απόδοσης του CODEC και της εξίσωσης του E-Model.

Το (I_e) θα πρέπει να λαμβάνει υπόψη του και τον αριθμό των frames του CODEC που μπαίνουν σε ένα πακέτο (από τον packetizer ή τον CODEC). Η απώλεια συνεχόμενων frames (bursty loss) που μπορεί να περιέχονται σε ένα πακέτο έχει μεγαλύτερη επίδραση στην ποιότητα της φωνής από ότι η απώλεια ισάριθμων μεμονωμένων frames.

CODEC	**Frames/packet**	**λ1**	**λ2**	**λ3**
G.711	1	0	30	15
G.729	1	10	47.82	18

Πίνακας 5.4 : Πειραματικοί συντελεστές (λ1, λ2, λ3) για τα CODEC G.711, G.729.

5.5 Τρόποι βελτίωσης της VoIP QoS

Υπάρχουν διάφοροι τρόποι για τη βελτίωση της VoIP QoS και μπορούν να χωριστούν σε δύο κατηγορίες.

- Η πρώτη κατηγορία είναι τρόποι βελτίωσης της VoIP QoS σε επίπεδο δικτύου.
- Η δεύτερη κατηγορία είναι τρόποι βελτίωσης της VoIP QoS σε επίπεδο εφαρμογής.

5.5.1 Βελτίωση της VoIP QoS στο επίπεδο δικτύου

Ο στόχος είναι η βελτίωση των IP δικτύων σε ότι αφορά τα χαρακτηριστικά εκείνα που επηρεάζουν τις εφαρμογές VoIP, δηλαδή της καθυστέρησης του jitter και του ρυθμού απώλειας πακέτων. Σε ιδιωτικά δίκτυα αυτό μπορεί να επιτευχθεί τροποποιώντας σε δρομολογητές και gateways τις πολιτικές ουράς (queues policies), έτσι ώστε να εξασφαλίζεται εύρος ζώνης (bandwidth) για τις VoIP ροές. Σε μη ιδιόκτητα δίκτυα, όπως το Internet, δεν μπορούν να εφαρμοστούν τα παραπάνω, γίνεται όμως προσπάθεια από τον IETF να τυποποιηθούν κάποιοι μηχανισμοί διασφάλισης της ποιότητες υπηρεσιών QoS στο Internet. Τα πρώτα αποτελέσματα αυτών των προσπαθειών είναι οι μηχανισμοί IntServ (Integrated Services) και DiffServ (Differentiated Services).

- Στο IntServ μοντέλο πριν την μετάδοση των πακέτων προηγείται η δέσμευση (reservation) πόρων με χρήση του πρωτοκόλλου RSVP, και ακολουθεί η κατηγοριοποίηση των πακέτων (packet classification) και η έξυπνη χρονοδρομολόγησή τους (intelligent scheduling), για να επιτευχθεί το επιθυμητό επίπεδο εξυπηρέτησης.

- Στο DiffServ γίνεται κατηγοριοποίηση των πακέτων σε ένα μικρό αριθμό από κατηγορίες υπηρεσιών και χρησιμοποιούνται μηχανισμοί απόδοσης προτεραιότητας για να προσφέρουν το επιθυμητό επίπεδο εξυπηρέτησης σε κάθε κατηγορία. Σε αυτό το πρωτόκολλο δεν γίνεται χρήση οποιουδήποτε μηχανισμού δέσμευσης πόρων (resource reservation) αλλά χρήση μηχανισμών διαχείρισης των ουρών κατά τη διάρκεια της μετάδοσης.

5.5.2 Βελτίωση της VoIP QoS στο επίπεδο εφαρμογής

Στο επίπεδο της εφαρμογής μπορούν να υλοποιηθούν μηχανισμοί που βελτιώνουν την QoS στις τερματικές συσκευές (VoIP phones) καθώς και σε άλλα στοιχεία ενός VoIP δικτύου, όπως gateways και gatekeepers. Παρακάτω αναφέρονται συνοπτικά κάποιοι τέτοιοι μηχανισμοί:

- Η βελτίωση της απόδοσης των CODEC ώστε να έχουν μεγάλη συμπίεση και ταυτόχρονα μικρή παραμόρφωση, και η υλοποίηση αποδοτικών αλγορίθμων plc (packet loss concealment) για τους CODEC σε τερματικές συσκευές ή και gateways, που μπορεί να βελτιώσει άμεσα τη VoIP QoS .

- Η υλοποίηση adaptive playout algorithms στους jitter buffers. Οι αλγόριθμοι αυτοί μεταβάλλουν το χρόνο που θα παρουσιαστεί ένα πακέτο φωνής στον παραλήπτη (playout time) ανάλογα με τη μέση διακύμανση της καθυστέρησης του δικτύου, με στόχο την διατήρηση της καθυστέρησης και του ρυθμού απόρριψης πακέτων στον jitter buffer σε χαμηλά επίπεδα .

- Η υλοποίηση μηχανισμού ελέγχου συμφόρησης (congestion control) που ανάλογα με τη συμφόρηση μεταβάλλει τον ρυθμό αποστολής δεδομένων (απαιτεί multi-rate CODEC), μπορεί σε ορισμένες περιπτώσεις να οδηγήσει σε καλύτερες συνθήκες δικτύου (κυρίως μείωση του ρυθμού απόρριψης πακέτων από τους δρομολογητές). Ο μηχανισμός ελέγχου συμφόρησης συνήθως γίνεται από τις τερματικές συσκευές (end-to-end), αλλά θα μπορούσε να επιτευχθεί και κεντρικά (για παράδειγμα από gatekeepers).

- Έχουν επίσης προταθεί μηχανισμοί που όταν ανιχνεύουν λάθη μετάδοσης σε ένα δίκτυο, προσαρμόζουν κατάλληλα τον τρόπο μετάδοσης της φωνής (όπως εισαγωγή πλεονάζουσας πληροφορίας) ώστε να εμφανίζει το σύστημα σθεναρότητα στην απώλεια πακέτων.

- Τέλος έχει παρατηρηθεί ότι ορισμένα κομμάτια-πακέτα φωνής είναι πιο σημαντικά από ορισμένα άλλα για να γίνει αντιληπτό ένα φωνητικό σήμα, έτσι για παράδειγμα τα πρώτα τμήματα φωνής που ακολουθούν μία περίοδο σιγής είναι πολύ σημαντικά και έχουν προταθεί μηχανισμοί που ανιχνεύουν αυτά τα πακέτα και τα μαρκάρουν ως πακέτα υψηλής προτεραιότητας (στο κατάλληλο πεδίο του IP header) ώστε να έχουν καλύτερη μεταχείριση από το δίκτυο.

Κεφάλαιο 6.

Περιγραφή πειραματικής διαδικασίας (Test-bed).

Για την υλοποίηση του συνόλου των πειραμάτων εγκαταστάθηκαν δυο Η/Υ, ο πρώτος εκτελεί χρέη διακομιστή Server και ο δεύτερος χρέη πελάτη Client.

6.1 Προδιαγραφές συστημάτων.

Στον SIPp/Sip Server, ο οποίος έχει λειτουργικό Ubuntu Server 12.04.3 LTS 64 Bit είναι εγκατεστημένα τα παρακάτω προγράμματα:

SIPp .

Asterisk .

VoIPmonitor .

- **Το σύστημα έχει χαρακτηριστικά:**

  Intel P4 Συχνότητα 3 GHZ.

  1 G RAM.

  80 GB HD.

- **Στον SIPp Client, ο οποίος έχει λειτουργικό Ubuntu Server 12.04.3 LTS είναι εγκατεστημένο το παρακάτω πρόγραμμα:**

  SIPp.

- **Το σύστημα έχει χαρακτηριστικά:**

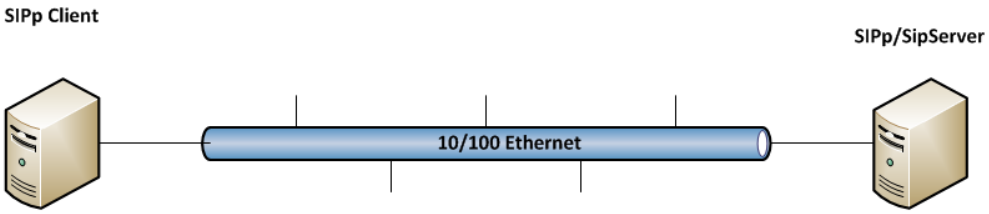
  AMD Phenom II X6, 1055T. Συχνότητα 2.8 GHZ.

  8 G RAM.

  750 GB HD.

6.2 Προδιαγραφές Δικτύου.

Όλα τα πειράματα έγιναν σε τοπικό δίκτυο LAN (Εικόνα 6.1), και οι δυο Η/Υ είναι εφοδιασμένοι με κάρτα δικτύου 10/100 Mbps Ethernet και το switch που είναι υπεύθυνο για την λειτουργία του τοπικού δικτύου έχει 5 πόρτες σύνδεσης RJ45 με δυνατότητα μεταγωγής πακέτων στα 100 Mbps σε κάθε πόρτα 148800 pps.



Εικόνα 6.1: Σχέδιο δικτύου στο οποίο υλοποιήθηκαν τα πειράματα.

Κατά την διαδικασία σύνδεσης στο δίκτυο, όπως αναφέρεται αναλυτικά στο παράρτημα, η τοπολογία δικτύου είναι δεδομένη και για τους 2 Η/Υ και είναι η ίδια σε όλα τα πειράματα, έτσι ο μεν SIP Server έχει διεύθυνση δικτύου IP <192.168.1.100> και όνομα <SipServer.local> και ο Client διεύθυνση δικτύου IP <192.168.1.120> και όνομα <TestClient.local>.

6.3 Προγράμματα που χρησιμοποιήθηκαν.

Για την παραγωγή τηλεφωνικών κλήσεων SIP από τον Client προς τον Server χρησιμοποιείται το πρόγραμμα SIPp, το οποίο παράγει τηλεφωνικές κλήσεις SIP με διαφορετική παραμετροποίηση κάθε φορά, έτσι ώστε να επιτευχθούν τα επιθυμητά αποτελέσματα και η ανάλυση και λήψη των δεδομένων έγινε με το πρόγραμμα VoIP Monitor.Το τηλεφωνικό κέντρο SIP υλοποιήθηκε με εγκατάσταση και παραμετροποίηση του προγράμματος Asterisk.

Επιπλέον προγράμματα που χρησιμοποιήθηκαν για λιγότερο σημαντικές ανάγκες παρουσιάζονται στο επόμενο κεφάλαιο. Η αναλυτική εγκατάσταση και παραμετροποίηση των συστημάτων παρουσιάζεται στο παράρτημα αυτής της εργασίας.

6.4 Στόχοι πειραμάτων.

Ο στόχος του πειράματος είναι η Μέτρηση απόδοσης και αξιοπιστίας του τηλεφωνικού κέντρου που υλοποιήθηκε με βάση το πρωτόκολλο SIP, έτσι μετρήθηκαν οι δυνατότητες του συστήματος για μια σειρά από παραμέτρους, ώστε να γίνει δυνατή η εξυπηρέτησης ταυτόχρονων κλήσεων με στόχο τον ορισμό προδιαγραφών για το σύστημα.

Κεφάλαιο 7

Παρουσίαση των εργαλείων που χρησιμοποιήθηκαν στα πειράματα.

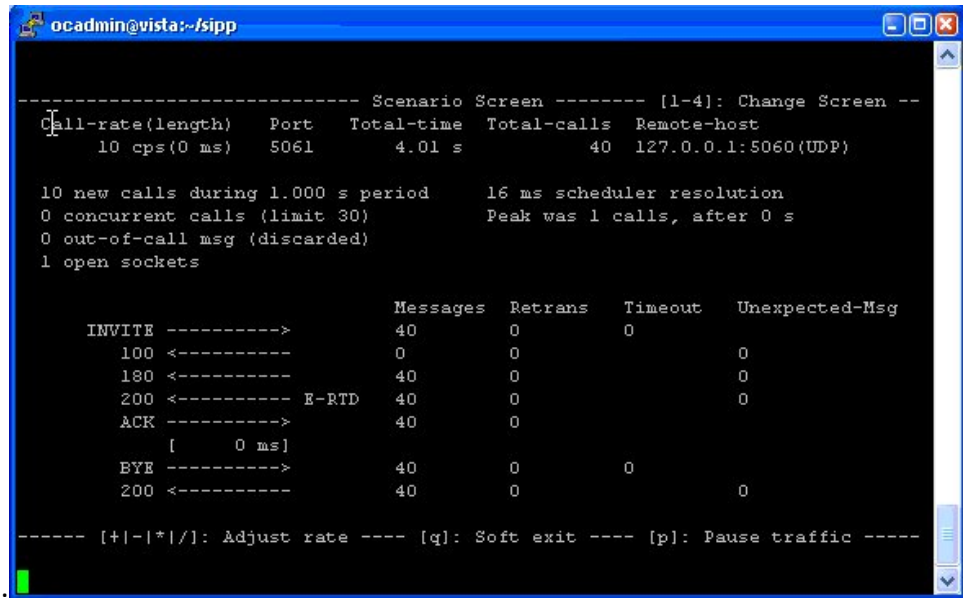
7.1 Εργαλεία.

Τα βασικά εργαλεία που χρησιμοποιήθηκαν είναι το SIPp για προσομοίωση του πρωτοκόλλου SIP, έλεγχο αλλά και Stress Testing, το VoIP monitor ως μια ολοκληρωμένη λύση έλεγχου και το Asterisk που θα εκτελεί χρέη SIP server .

7.2 Παρουσίαση του εργαλείου SIPp.

Το SIPp είναι ένα εργαλείο για τον έλεγχο της απόδοσης του πρωτόκολλου SIP. Περιλαμβάνει μερικά βασικά σενάρια SipStone user agent scenarios (UAC και UAS), δημιουργεί και απελευθερώνει πολλές κλήσεις με τις μεθόδους INVITE και BYE. Μπορεί επίσης να διαβάζει αρχεία XML, των οποίων το σενάριο μπορεί να περιγράφει οποιαδήποτε διαμόρφωση τηλεφωνικών κλήσεων για έλεγχο της απόδοσης ή την προσομοίωση πραγματικών προβλημάτων.

Διαθέτει δυναμική απεικόνιση των στατιστικών στοιχείων (Εικόνα 7.1) σχετικά με την εκτέλεση δοκιμών (ποσοστό κλήσεων, καθυστέρηση επιστροφής, καθώς και των στατιστικών μηνυμάτων call rate, round trip delay, and message statistics), περιοδικών στατιστικών (periodic CSV statistics dumps), TCP και UDP σε πολλαπλά sockets ή πολυπλέγμενα με τη διαχείριση αναμετάδοσης και δυναμικά ρυθμιζόμενα ποσοστά κλήσης. Το SIPp μπορεί επίσης να χρησιμοποιηθεί για τη δοκιμή και την προσομοίωση πραγματικών SIP συσκευών.



Εικόνα 7.1 : Η κεντρική οθόνη του προγράμματος SIPp.

7.2.1 Άδεια χρήσης.

Για το SIPp ισχύει η άδεια GNU GPL (http://www.gnu.org/copyleft/gpl.html). Όλοι οι όροι της άδειας χρήσης ισχύουν. Αρχικά δημιουργήθηκε και παρέχεται στη SIP κοινότητα από την Hewlett-Packard (http://www.hp.com) με την ελπίδα ότι μπορεί να είναι χρήσιμο, αλλά η HP δεν παρέχει καμία υποστήριξη ούτε εγγύηση για το SIPp.

7.2.2 Για ποιες πλατφόρμες είναι διαθέσιμο προς εγκατάσταση.

Το SIPp είναι διαθέσιμο για όλες σχεδόν τις πλατφόρμες UNIX: HPUX, Tru64, Linux (RedHat, Debian, FreeBSD), Solaris / SunOS. Επίσης υπάρχει μια έκδοση των Windows.

7.2.3 Εγκατάσταση του SIPp.

Στο Linux, το SIPp παρέχεται με τη μορφή πηγαίου κώδικα, γι' αυτό Θα πρέπει να γίνει compile. Προαπαιτούμενα για την εγκατάσταση του SIPp είναι:

- C++ Compiler
- curses or ncurses library
- Για υποστήριξη TLS : OpenSSL >= 0.9.8
- Για υποστήριξη pcap play: libpcap and libnet
- Για υποστήριξη SCTP: lksctp-tools

Υπάρχουν τέσσερις επιλογές για να γίνει compile το SIPp:

- Χωρίς υποστήριξη TLS (Transport Layer Security), SCTP ή PCAP: Αυτή είναι η προτεινόμενη εγκατάσταση, αν δεν χρειάζονται SCTP, TLS ή PCAP. Σε αυτή την περίπτωση δεν υπάρχουν προαπαιτούμενα για την εγκατάσταση πριν από το compile του SIPp.

  Οι εντολές εγκατάστασης είναι:

  ```
  # tar -xvzf sipp-xxx.tar
  # cd sipp
  # autoreconf -ivf
  # ./configure
  # make
  ```

- Με υποστήριξη TLS, θα πρέπει να έχει γίνει εγκατάσταση του OpenSSL library (http://www.openssl.org/) (> = 0.9.8).

  Οι εντολές εγκατάστασης είναι:

  ```
  # tar -xvzf sipp-xxx.tar.gz
  # cd sipp
  # autoreconf -ivf
  # ./configure --with-openssl
  # make
  ```

Το Transport Layer Security (TLS) και ο προκάτοχός του, Secure Sockets Layer (SSL), είναι πρωτόκολλα κρυπτογράφησης, που έχουν σχεδιαστεί για να παρέχουν ασφάλεια στις επικοινωνίες μέσω διαδικτύου.

- Με υποστήριξη PCAP play:

Οι εντολές εγκατάστασης είναι:

```
# tar -xvzf sipp-xxx.tar.gz
# cd sipp
# autoreconf -ivf
# ./configure --with-pcap
# make
```

Το PCAP play είναι η δυνατότητα αυτόματης αναπαραγωγής ενός αρχείου πληροφοριών σε ένα δίκτυο. Το αρχείο έχει δημιουργηθεί με καταγραφή της κίνησης δικτύου σε προγενέστερο χρόνο, ή περιλαμβάνει πληροφορίες με συγκεκριμένη κωδικοποίηση.

- Με υποστήριξη SCTP:

```
# tar -xvzf sipp-xxx.tar.gz
# cd sipp
# autoreconf -ivf
# ./configure --with-sctp
# make
```

Το πρωτόκολλο ελέγχου μετάδοσης Stream Control Transmission Protocol (SCTP) είναι ένα πρωτόκολλο επιπέδου μεταφοράς, που εξυπηρετεί παρόμοιο ρόλο με το δημοφιλές πρωτόκολλο Transmission Control Protocol (TCP) και το User Datagram Protocol (UDP). Παρέχει μερικά από τα χαρακτηριστικά και των δύο αυτών πρωτοκόλλων, δηλαδή το μήνυμα-προσανατολισμένο, όπως UDP και εξασφαλίζει αξιόπιστη εν σειρά μεταφορά των μηνυμάτων με τον έλεγχο συμφόρησης όπως το TCP.

7.2.4 Χρήση του SIPp και οι βασικές του εντολές.

Το SIPp επιτρέπει να δημιουργηθούν μία ή πολλές κλήσεις SIP σε ένα απομακρυσμένο σύστημα.

7.2.4.1 Βασικά χαρακτηριστικά.

Το εργαλείο λειτουργεί από την γραμμή εντολών. Στο πιο κάτω παράδειγμα, δύο SIPp λειτουργούν σε ένα σύστημα για την επίδειξη των δυνατοτήτων του.

Εκτελείται ένα SIPp με το ενσωματωμένο βασικό σενάριο (UAS) σαν Server, με την παρακάτω εντολή:

./sipp -sn uas

Στον ίδιο υπολογιστή, τρέχει ένα δεύτερο SIPp με το ενσωματωμένο βασικό σενάριο (UAC), σαν client με την παρακάτω εντολή:

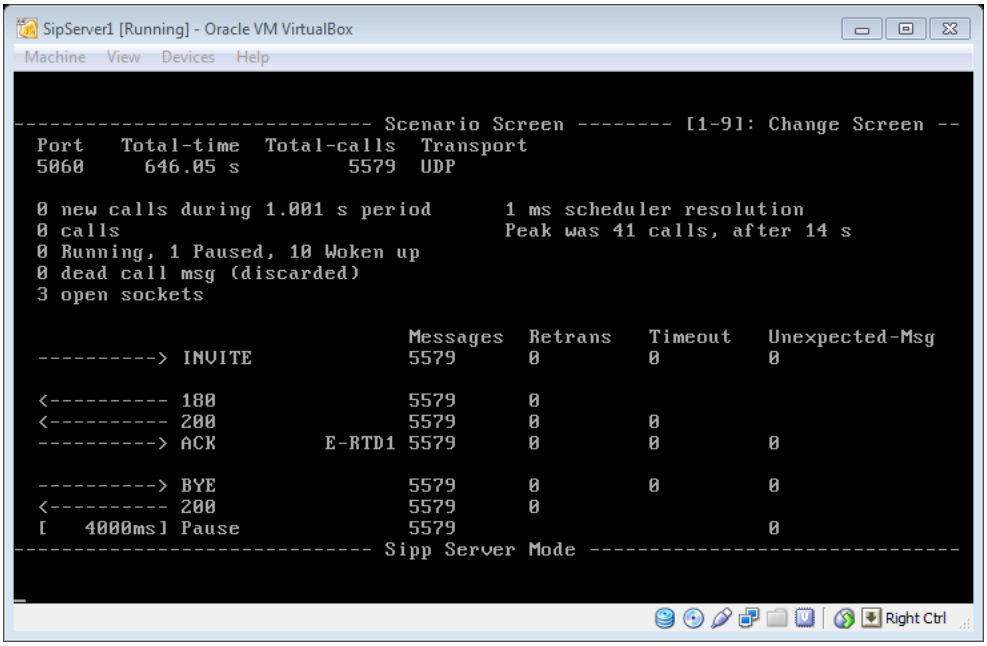
./sipp -sn uac 127.0.0.1

Περιγραφή βασικού σεναρίου.

(UAS) σαν Server.

Στην πρώτη οθόνη (Εικόνα 7.2 σεναρίων scenario screen παρατηρούνται οι παρακάτω πληροφορίες:

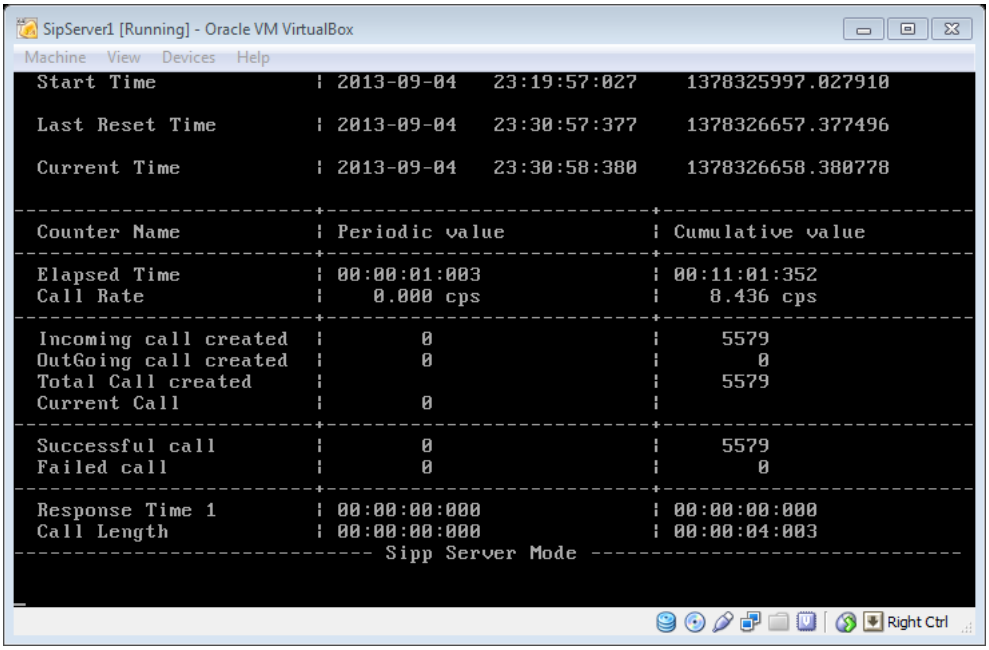
Συνολικός χρόνος χρήσης 645,05s, συνολικός αριθμός κλήσεων 5579, μια σειρά από πληροφορίες σχετικά με τον τρόπο που απάντησε ο Server στις κλήσεις, όπως ότι διαχειρίστηκε ταυτόχρονα μέχρι 41 κλήσεις μετά από 14 s, το πλάνο κλήσης ,τις αποτυχημένες κλήσεις κλπ.



Εικόνα 7.2 : Η κεντρική οθόνη SIPp (UAS) σαν Server.

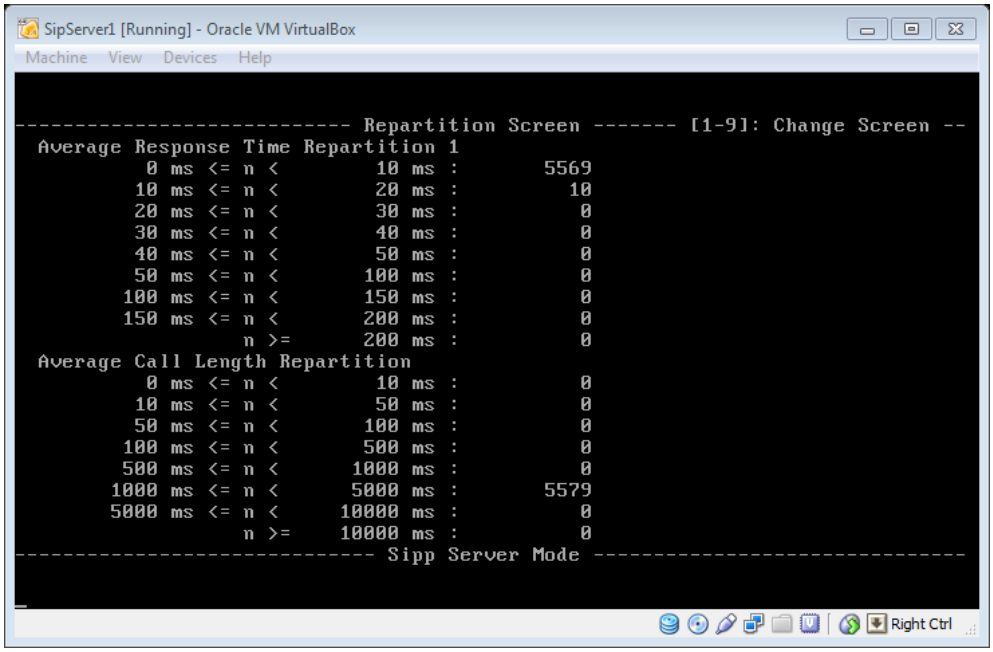
Στην δεύτερη οθόνη (Εικόνα 7.3) στατιστικής (statistics screen) παρατηρούνται οι παρακάτω πληροφορίες:

Πότε ξεκίνησε και ποτέ σταμάτησε να λειτουργεί η προσομοίωση. Πόσες ήταν επιτυχημένες, πόσες αποτυχημένες κλήσεις και πόσες δημιούργησε.



Εικόνα 7.3 : Δεύτερη οθόνη SIPp (UAS) σαν Server.

Στην τρίτη οθόνη (Εικόνα 7.4) ανάλυση κλήσεων (repartition screen) παρατηρείται η αναλυτική διάρκεια των κλήσεων.



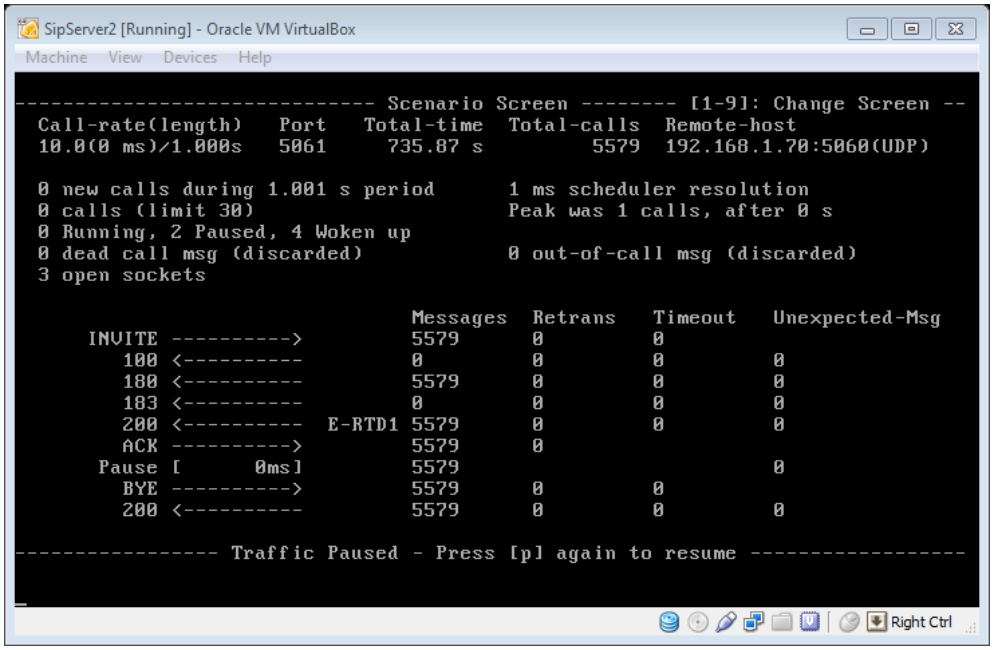
Εικόνα 7.4 : Τρίτη οθόνη SIPp (UAS) σαν Server.

Περιγραφή βασικού σεναρίου.

(UAC) σαν Client.

Στην πρώτη οθόνη (Εικόνα 7.5) σεναρίων (scenario screen) παρατηρούνται οι παρακάτω πληροφορίες:

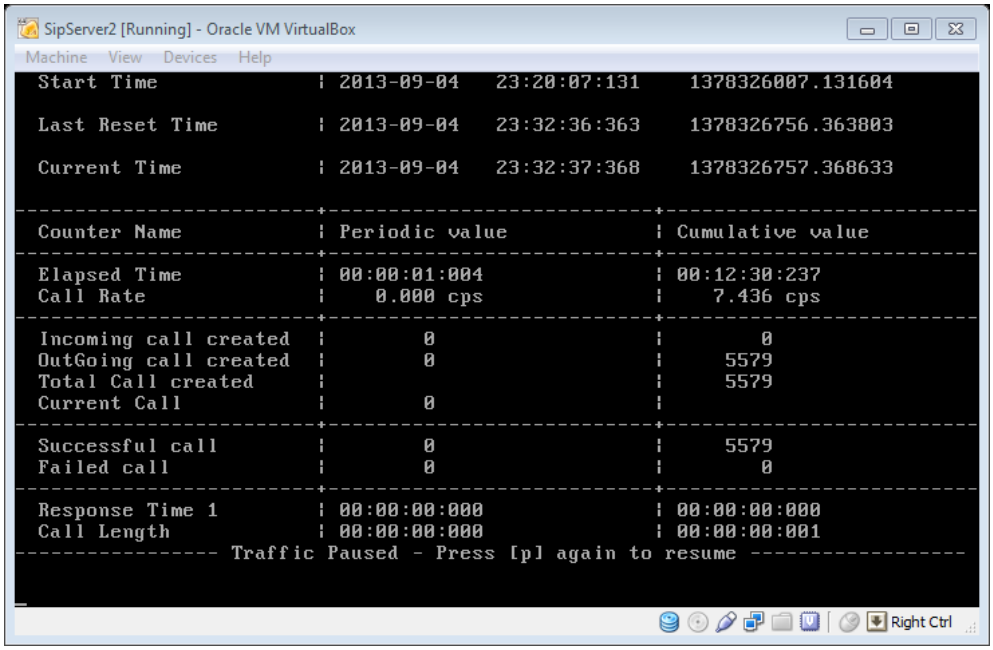
Συνολικός χρόνος χρήσης 645,05s, συνολικός αριθμός κλήσεων 5579, μια σειρά από πληροφορίες σχετικά με τον τρόπο που εκτελεί ο client τις κλήσεις, όπως ότι εκτελεί δέκα (10) κλήσεις ανά ένα (1) sec, τον συνολικό χρόνο που χρειάστηκε για να εκτελέσει την προσομοίωση, το πλάνο κλήσης, τις αποτυχημένες κλήσεις κλπ.



Εικόνα 7.5 : Πρώτη οθόνη SIPp (UAC) σαν Client.

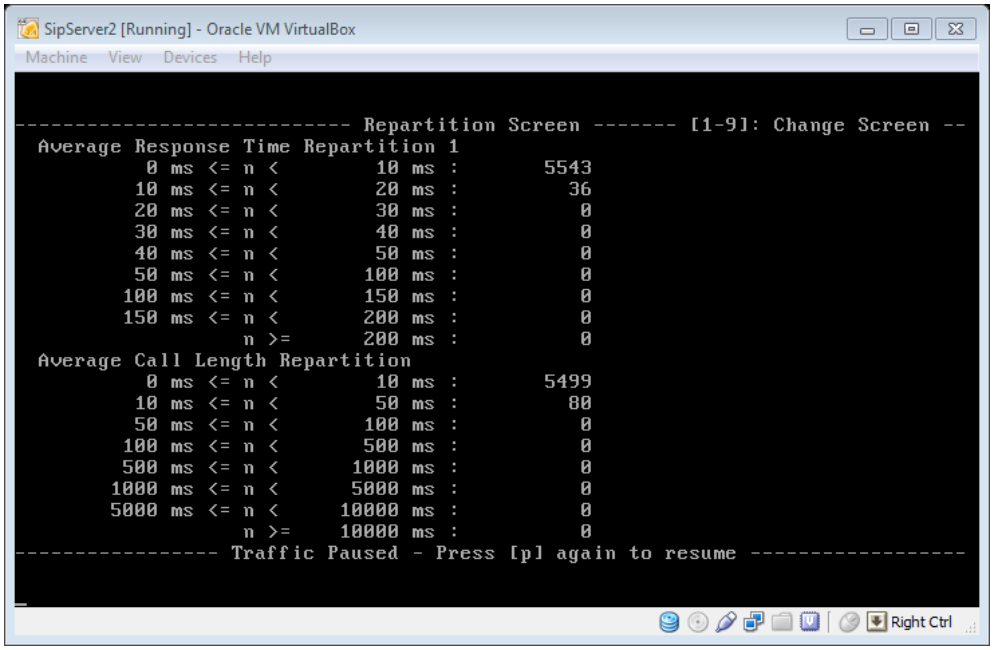
Στην δεύτερη οθόνη (Εικόνα 7.6) στατιστικής (statistics screen) παρατηρούνται οι παρακάτω πληροφορίες:

Πότε ξεκίνησε και ποτέ σταμάτησε να λειτουργεί η προσομοίωση. Πόσες ήταν επιτυχημένες, πόσες αποτυχημένες κλήσεις και πόσες δημιούργησε.



Εικόνα 7.6 : Δεύτερη οθόνη SIPp (UAC) σαν Client.

Στην τρίτη οθόνη (Εικόνα 7.7) ανάλυση κλήσεων (repartition screen) παρατηρείται η αναλυτική διάρκεια των κλήσεων.



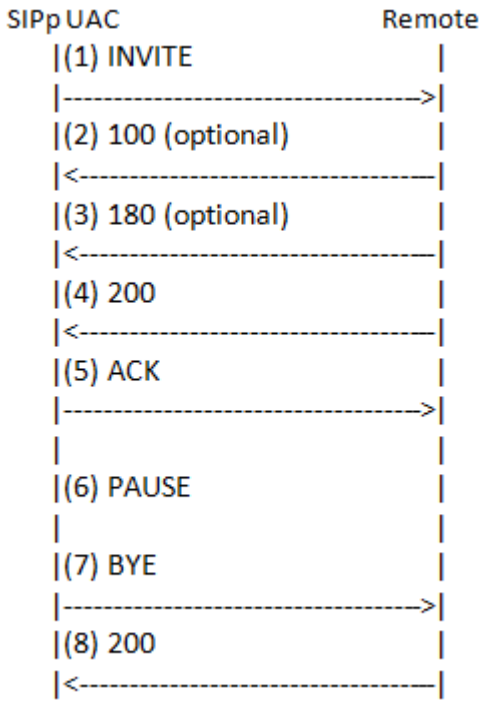
Εικόνα 7.7 : Τρίτη οθόνη SIPp (UAC) σαν Client.

7.2.4.2 Ολοκληρωμένα ενσωματωμένα σενάρια.

Υπάρχουν ολοκληρωμένα ενσωματωμένα σενάρια σε εκτελέσιμο SIPp και παράλληλα υπάρχει η δυνατότητα να δημιουργηθούν καινούργια σενάρια για νέες ανάγκες με χρήση XML. Παρακάτω περιγράφονται τα βασικά σενάρια που περιλαμβάνονται στο SIPp .

(UAC) σαν Client.

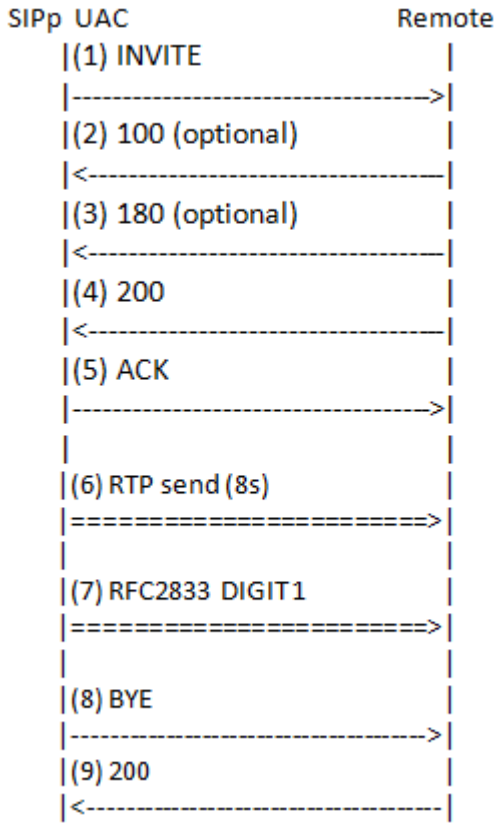
Σενάριο: uac.xml (Παράρτημα)



Το SIPp στέλνει ένα INVITE για να μπορέσει να εγκαταστήσει μια SIP σύνοδο με κάποιο χρήστη. Ένα τέτοιο request θα απαντηθεί από τον SIP server με 100 που σημαίνει ότι ο server προωθεί το invite στον υποτιθέμενο χρήστη, τότε ο remote client δέχεται ένα response 180 ότι ο υποτιθέμενος χρήστης μπορεί να δεχτεί την κλήση, έπειτα δέχεται μια απάντηση 200 ότι η προώθηση του σήματος εκτελέστηκε. Όταν απαντηθεί η κλήση τότε στέλνεται ένα ACK request ότι έλαβε την απάντηση, γίνετε παύση PAUSE της διαδικασίας για να συμπληρωθεί ο χρόνος κλήσης και στο τέλος της κλήσης στέλνει ένα σήμα BYE τέλους κλήσης και έρχεται απάντηση 200 ότι η προώθηση του σήματος εκτελέστηκε.

(UAC) σαν Client με αυτόματη αναπαραγωγή ενός αρχείου πληροφοριών Pcap Play media.

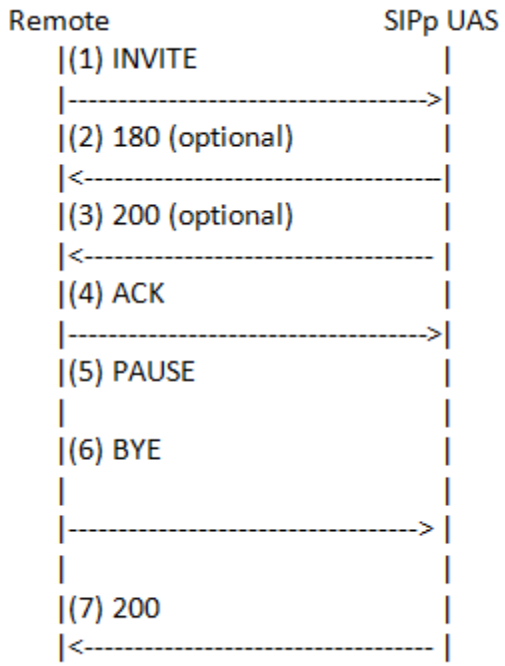
Σενάριο: uac_pcap.xml (Παράρτημα)



Το SIPp στέλνει ένα INVITE για να μπορέσει να εγκαταστήσει μια SIP σύνοδο με κάποιο χρήστη. Αν έρθει ένα τέτοιο request θα απαντηθεί από τον SIP server με 100 που σημαίνει ότι ο server προωθεί το invite στον υποτιθέμενο χρήστη, τότε δέχεται από τον remote client ένα response 180 ότι ο υποτιθέμενος χρήστης μπορεί να δεχτεί την κλήση, έπειτα δέχεται μια απάντηση 200 ότι η προώθηση του σήματος εκτελέστηκε. Όταν απαντηθεί η κλήση τότε στέλνεται ένα ACK request ότι έλαβε την απάντηση, ανοίγει ένα κανάλι RTP για 8 sec, και μετά ανοίγει RFC2833 κανάλι επικοινωνίας, στο οποίο αναπαράγεται ένα αρχείο πληροφοριών pcap play media που έχει κατασκευαστεί σε προγενέστερο χρόνο και στο τέλος της κλήσης στέλνει ένα σήμα BYE τέλους κλήσης και έρχεται απάντηση 200 ότι η προώθηση του σήματος εκτελέστηκε.

(UAS) σαν Server.

Σενάριο: uas.xml (Παράρτημα)



Το SIPp δέχεται ένα INVITE που ζητά να εγκαταστήσει μια SIP σύνοδο με κάποιο χρήστη, τότε το SIPp στέλνει ένα response 180 ότι ο υποτιθέμενος χρήστης μπορεί να δεχτεί την κλήση, έπειτα στέλνει μια απάντηση 200 ότι η προώθηση του σήματος εκτελέστηκε. Όταν απαντηθεί η κλήση τότε λαμβάνει ένα ACK request ότι έλαβε την απάντηση και η συνομιλία ξεκινά, γίνετε παύση PAUSE της διαδικασίας για να συμπληρωθεί ο χρόνος κλήσης και στο τέλος της κλήσης λαμβάνει ένα σήμα BYE τέλους κλήσης και στέλνει απάντηση 200 ότι η προώθηση του σήματος εκτελέστηκε.

7.2.4.3 Έλεγχος SIPp μέσω εντολών και πλήκτρων συντόμευσης .

Το SIPp μπορεί να ελέγχεται μέσω του πληκτρολογίου ή μέσω εντολών UDP. Τα πλήκτρα συντόμευσης είναι:

Πλήκτρο	Εντολή
+	Αύξηση αριθμού κλήσεων κατά 1 * rate_scale.
*	Αύξηση αριθμού κλήσεων κατά 10 * rate_scale.
-	Μείωση αριθμού κλήσεων κατά 1 * rate_scale.
/	Μείωση αριθμού κλήσεων κατά 10 * rate_scale.
C	Είσοδο στην γραμμή εντολών
Q	Τερματισμός SIPp αφού ολοκληρωθεί η εργασία .
Q	Τερματισμός SIPp αμέσως

S	Τοποθέτηση πληροφοριών σε αρχείο log
P	Διακοπή κίνησης (Pause traffic).
1	Οθόνη σεναρίων.
2	Οθόνη στατιστικής.
3	Ανάλυση κλήσεων.

Στη γραμμή εντολών μπορεί κάποιος να πληκτρολογήσει μια ενιαία γραμμή εντολών. Η γραμμή εντολών είναι πιο ευέλικτη από τα hot keys, αλλά χρειάζεται περισσότερο χρόνο για να γίνει εισαγωγή πληροφοριών .

Οι παρακάτω εντολές είναι διαθέσιμες:

dump tasks	Εκτυπώνει μια λίστα των ενεργών εργασιών στο αρχείο καταγραφής σφαλμάτων.	dump tasks
set rate X	Ρυθμίζει το ποσοστό κλήσεων.	set rate 10
set rate-scale X	Ορίζει το ποσοστό της κλίμακας, η οποία ρυθμίζει την ταχύτητα με «+», «-», «*», και «/».	set rate-scale 10
set users X	Ορίζει τον αριθμό των χρηστών (ισχύει μόνο όταν -usersis έχει οριστεί	set rate 10
set limit X	Ορίζει το όριο της ανοικτής πρόσκλησης (που ισοδυναμεί με την επιλογή-l)	set limit 100
set index <true|false>	Εμφανίζει μηνύματα indexes στην οθόνη σεναρίου	set index true
-s	Σύνδεση με λογαριασμό χρήστη.	
-p	Πόρτα δικτύου.	
-d	Εισαγωγή καθυστέρησης κλήσεων.	
-r	Αριθμός κλήσεων.	
-sf	Εκτέλεση σεναρίου xml.	
-sn	Βασικό σενάριο	

7.2.5 Έλεγχος Traffic.

Το SIPp δημιουργεί SIP Traffic σύμφωνα με το καθορισμένο σενάριο. Γίνεται έλεγχος του αριθμού των κλήσεων που ξεκινούν ανά δευτερόλεπτο. Με την επιλογή -users, ελέγχεται ο αριθμός των χρηστών.

Παράδειγμα

Εκτέλεσε 7 κλήσεις κάθε 2 δευτερόλεπτα (3,5 κλήσεις ανά δευτερόλεπτο).

```
./sipp -sn uac -r 7 -rp 2000 127.0.0.1
```

7.3 Παρουσίαση του εργαλείου Voip Monitor.

Το VoIP Monitor είναι ένα ολοκληρωμένο εργαλείο ανοικτού κώδικα (open source) που επιτρέπει την παρακολούθηση πακέτων σε ένα δίκτυο IP, και συνδυάζεται με μια εμπορική εφαρμογή GUI WEB, η οποία δίνει την δυνατότητα για ενδελεχή ανάλυση πληροφοριών σε ότι αφορά τα πρωτόκολλα του Voip.

Πιο συγκεκριμένα ελέγχει SIP συνομιλίες πάνω σε πρωτόκολλα RTP, RTCP και SCCP, κάνει ανάλυση της διακύμανσης, της καθυστέρησης και της απώλειας πακέτων σύμφωνα με την ITU-T G.107 χρησιμοποιώντας το μοντέλο E-model, το οποίο προβλέπει την ποιότητα στην κλίμακα MOS. Οι κλήσεις με όλα τα σχετικά στατιστικά στοιχεία αποθηκεύονται σε MySQL ή ODBC βάση δεδομένων. Προαιρετικά κάθε κλήση μπορεί να αποθηκευτεί στο pcap αρχείο είτε με SIP πρωτόκολλο είτε με SIP/RTP/RTCP/T.38/udptl.

Το VoIP monitor μπορεί να παρακολουθήσει, να καταγράψει την συνομιλία και να την αναπαράγει μέσω της εμπορικής εφαρμογής, GUI WEB ή να την αποθηκεύσει στον σκληρό δίσκο ως WAV.

Υποστηριζόμενα CODECs είναι το G.711 alaw / ulaw και εμπορικά plugins υποστηρίζουν G.722 G.723 G.729a iLBC Speex GSM Silk Isac OPUS. Το GUI WEB interface δίνει επίσης την δυνατότητα για στατιστική παρακολούθηση του δικτύου σε πραγματικό χρόνο.

7.3.1 VoIPmonitor sniffer

Το VoIPmonitor sniffer χρησιμοποίει SIP, Cisco SKINNY, RTP, RTCP και UDPTL πρωτόκολλα ανάλυσης της ποιότητας των κλήσεων VOIP και περιλαμβάνει πακέτο διακύμανσης καθυστέρησης και απώλειας πακέτων σύμφωνα με την ITU-T G.107 E-model, το οποίο υπολογίζει την ποιότητα στην κλίμακα MOS. Είναι γραμμένο σε γλώσσα C + + και έχει σχεδιαστεί για να χειρίζεται χιλιάδες ταυτόχρονες κλήσεις.

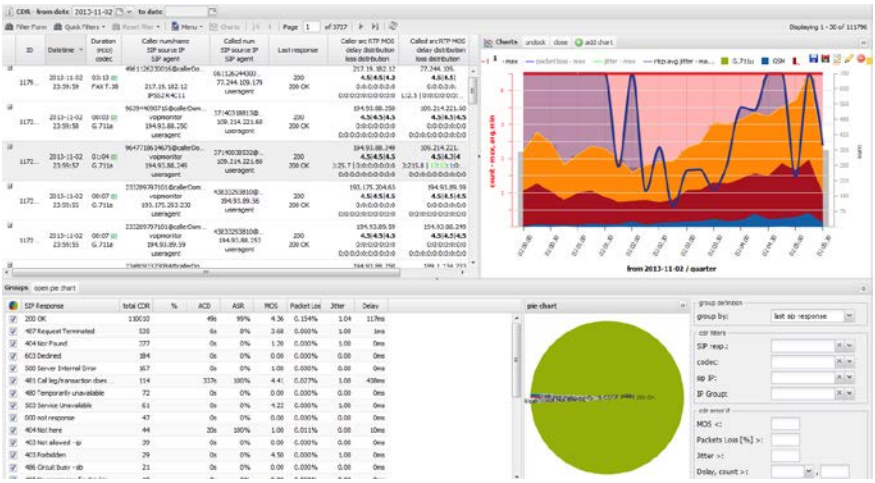
Οι κλήσεις προαιρετικά μπορούν να αποθηκευτούν σε αρχείο pcap είτε με μόνο σηματοδότηση SIP ή συμπεριλαμβανομένων και των πρωτοκόλλων RTP, RTCP και UDPTL. Το VoIPmonitor μπορεί επίσης να αποκωδικοποιήσει ήχο και να τον αναπαράγει με την εμπορική εφαρμογή GUI WEB ή να αποθηκευτεί στο δίσκο ως WAV. Υποστηριζόμενα CODECs είναι G.711 alaw / ulaw και με την βοήθεια εμπορικών plugins υποστηρίζει G.729a/G.723/G.722/iLBC/Speex/GSM/Isac/Silk. Το VoIPmonitor χρησιμοποιεί προσομοιωτή jitterbuffer για να μπορέσει να κρατήσει τις κλήσεις συγχρονισμένες προς τις δυο κατευθύνσεις.

7.3.2 GUI WEB

Μέσω του GUI WEB δίνεται η δυνατότητα για στατιστική παρακολούθηση του δικτύου σε πραγματικό χρόνο αφού είναι ένα εργαλείο ολοκληρωμένου ελέγχου των συνομιλιών που διενεργούνται στο δίκτυο και ταυτόχρονα δίνει την δυνατότητα στον χρήστη να προχωρήσει σε ενδελεχή ανάλυση των δεδομένων και παρουσίαση του σε διαγράμματα και λίστες εύχρηστες και κατανοητές.

Το βασικότερο εργαλείο του GUI WEB είναι το CDR (Εικόνα 7.8), το οποίο δίνει την δυνατότητα για πλήρη παρακολούθηση του δικτύου σε πραγματικό χρόνο με στοιχειά όπως :

- IP, User name και περιεχόμενο κλήσεων.
- Αριθμό κλήσεων, χρόνο και στατιστική ανάλυση.
- Σφάλματα ανάλυσης της διακύμανσης, της καθυστέρησης και της απώλειας πακέτων.
- Απεικόνιση πληροφοριών σε διαγράμματα και λίστες.
- Δυνατότητα παρακολούθησης σε πραγματικό χρόνο συγκεκριμένων χαρακτηριστικών .



Εικόνα 7.8: Το εργαλείο CDR.

7.4 Asterisk.

Το Asterisk είναι ελεύθερο λογισμικό, που λειτουργεί υπό τη γενική άδεια δημόσιας χρήσης GNU (GPL), αλλά για λόγους λειτουργικότητας (π.χ. υποστήριξη του ιδιωτικού CODEC G.729) υπάρχει επίσης και η εμπορική διανομή του Asterisk (όπως συμβαίνει και με τη MySQL).

Το Asterisk είναι πλατφόρμα πολυπλεξίας με διαίρεση χρόνου (TDM) και ανταλλαγής πακέτων φωνής. Αυτό σημαίνει ότι υποστηρίζει τα υπάρχοντα TDM πρωτόκολλα τηλεπικοινωνιών όπως το ψηφιακό δίκτυο ενοποιημένων υπηρεσιών (ISDN-BRA-PRI), το δημόσιο τηλεπικοινωνιακό δίκτυο μεταγωγής (PSTN), το FXS, το FXO, το E1, το T1 και σε γενικές γραμμές οτιδήποτε χρησιμοποιείται στην κλασική τηλεφωνία όπως είναι γνωστή μέχρι σήμερα.

Παράλληλα όμως υποστηρίζει και τα καινούργια VoIP (Voice over Internet Protocol) πρωτόκολλα όπως το SIP, το IAX, το H.323, το MGCP, το SCCP (Cisco-Skinny) και το Jingle (Google Talk).

Η γεφύρωση των τεχνολογιών προσφέρει στο χρήστη δυνατότητα μετάβασης στις νέες μορφές επικοινωνίας χωρίς όμως να αναγκαστεί να αποχωριστεί τις παλιές του συνήθειες και εγκαταστάσεις. Ξεφεύγει από τα όρια του τηλεπικοινωνιακού προγράμματος και χαρακτηρίζεται σωστότερα από την έννοια της τηλεπικοινωνιακής πλατφόρμας. Δημιουργεί δηλαδή ένα πλαίσιο μέσα στο οποίο θα μπορούσε να αναπτυχθεί το οποιοδήποτε υπάρχον (ή μελλοντικό) τηλεπικοινωνιακό σύστημα. Μπορεί να λειτουργήσει σαν αυτόνομος εξυπηρετητής επεξεργασίας κλήσεων ή ακόμα και σαν προσθήκη σε κάποιο ήδη εγκατεστημένο κέντρο. Μπορεί να χρησιμοποιηθεί μόνο σε επίπεδο λογισμικού, μεταφέροντας φωνή μέσω IP ή να επικοινωνήσει με TDM (Time Division Multiplexing) και να χρησιμοποιήσει το τηλεφωνικό δίκτυο.

Κεφάλαιο 8.

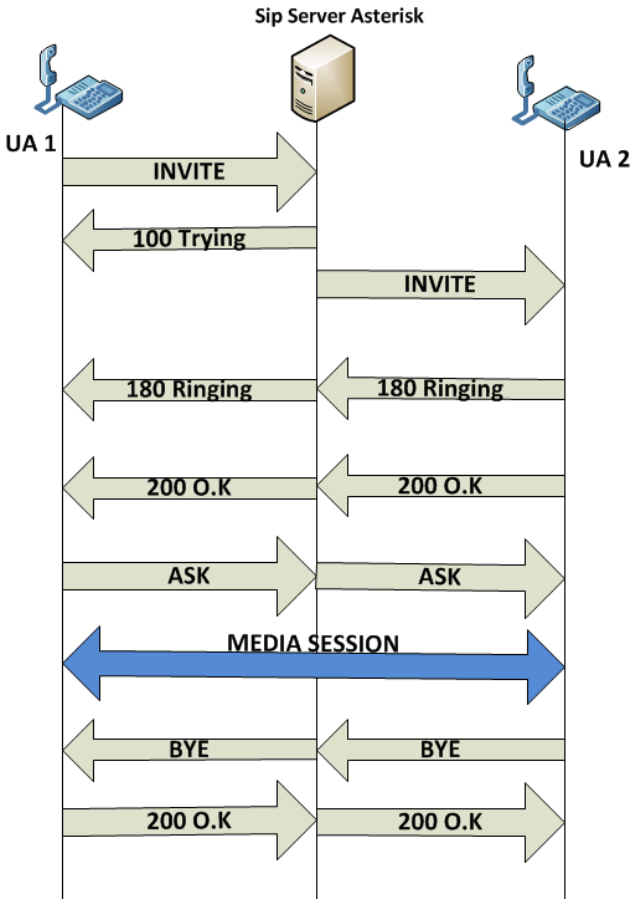
Πειράματα.

Η πειραματική διαδικασία έγινε πάνω στο σύστημα που έχει περιγραφεί στο κεφαλαίο 6. Η διαδικασία χωρίστηκε σε δυο κύριες κατηγορίες πειραμάτων: μία όταν το σύστημα εκτελεί χρέη SIP server και μία όταν το σύστημα εκτελεί χρέη PBX/SIP.

8.1 Απόδοση συστήματος PBX/SIP.

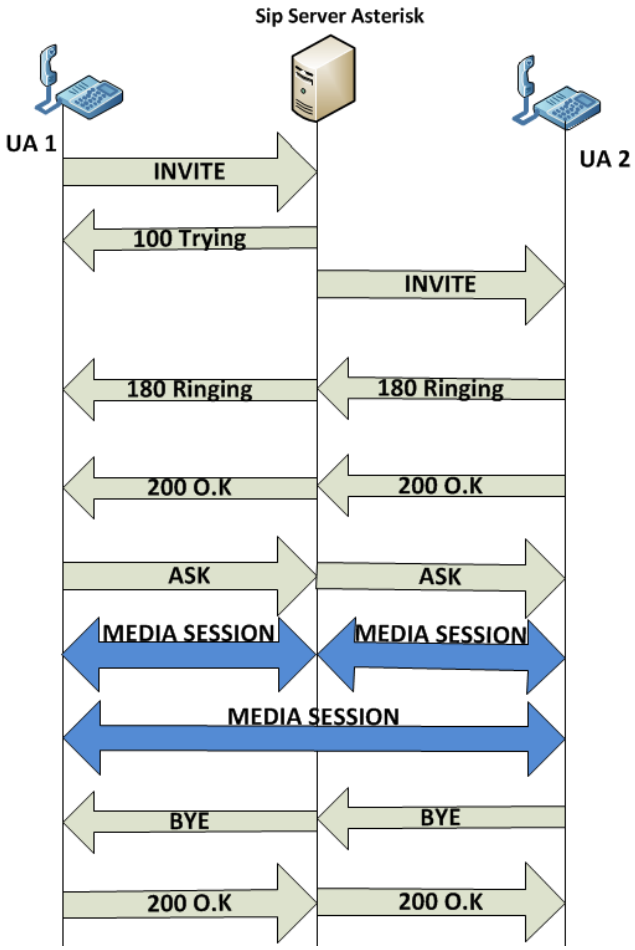
Για γίνει η μέτρηση της απόδοσης ενός συστήματος PBX SIP είναι απαραίτητο να χωριστεί η διαδικασία σε δυο κύριες κατηγορίες.

Στην πρώτη κατηγορία το σύστημα εκτελεί μόνο χρέη SIP Server, δηλαδή τα δεδομένα της πραγματικής συνομιλίας δεν περνούν από το σύστημα αλλά το σύστημα κάνει μόνο σηματοδότηση Signaling, όπως φαίνεται στην (Εικόνα 8.1). Έτσι λοιπόν για να οριστεί η δυνατότητα κλήσεων του συστήματος, πρέπει να οριστεί η μεγίστη δυνατή εξυπηρέτηση ταυτοχρόνων κλήσεων σχετικά με τις τρεις βασικές παραμέτρους του πρωτοκόλλου SIP (δηλαδή το REGISTER , INVITE, call setup delay).



Εικόνα 8.1: Τυπική διαδικασία κλήσης σε ένα σύστημα SIP.

Στην δεύτερη κατηγορία το σύστημα εκτελεί χρέη PBX/SIP Server, δηλαδή τα δεδομένα της πραγματικής συνομιλίας περνούν από το σύστημα και το σύστημα δεν κάνει μόνο σηματοδότηση Signaling, όπως φαίνεται στην (Εικόνα 8.2). Έτσι λοιπόν για να οριστεί η δυνατότητα κλήσεων του συστήματος, πρέπει να οριστεί η μέγιστη δυνατή εξυπηρέτηση ταυτόχρονων κλήσεων σχετικά με τις τρεις βασικές παραμέτρους του πρωτοκόλλου SIP δηλαδή το REGISTER, INVITE, call setup delay, σε συνδυασμό με πόσες ζεύξεις δεδομένων RTP, μπορεί το σύστημα να εξυπηρετήσει ταυτόχρονα.



Εικόνα 8.2: Τυπική διαδικασία κλήσης σε ένα σύστημα SIP/PBX.

8.1.1 Απόδοση συστήματος SIP.

Το σύστημα εκτελεί μόνο χρέη SIP Server, δηλαδή τα δεδομένα της πραγματικής συνομιλίας δεν περνούν από το σύστημα αλλά το σύστημα κάνει μόνο σηματοδότηση Signaling. Έτσι λοιπόν για να οριστεί η δυνατότητα κλήσεων του συστήματος, πρέπει να οριστεί η μέγιστη δυνατή εξυπηρέτηση ταυτόχρονων

κλήσεων σχετικά με τις τρεις βασικές παραμέτρους του πρωτοκόλλου SIP (δηλαδή το REGISTER , INVITE, call setup delay).

Οι τρεις παράγοντες είναι:

- Καθυστέρηση εγκατάστασης κλήσης (call setup delay (σε ms) χωρίς φορτίο.
- Ικανότητα δημιουργίας κλήσεων (INVITE capacity (UDP)).
- Ικανότητα σύνδεσης με το PBX (REGISTER capacity, (UDP)).

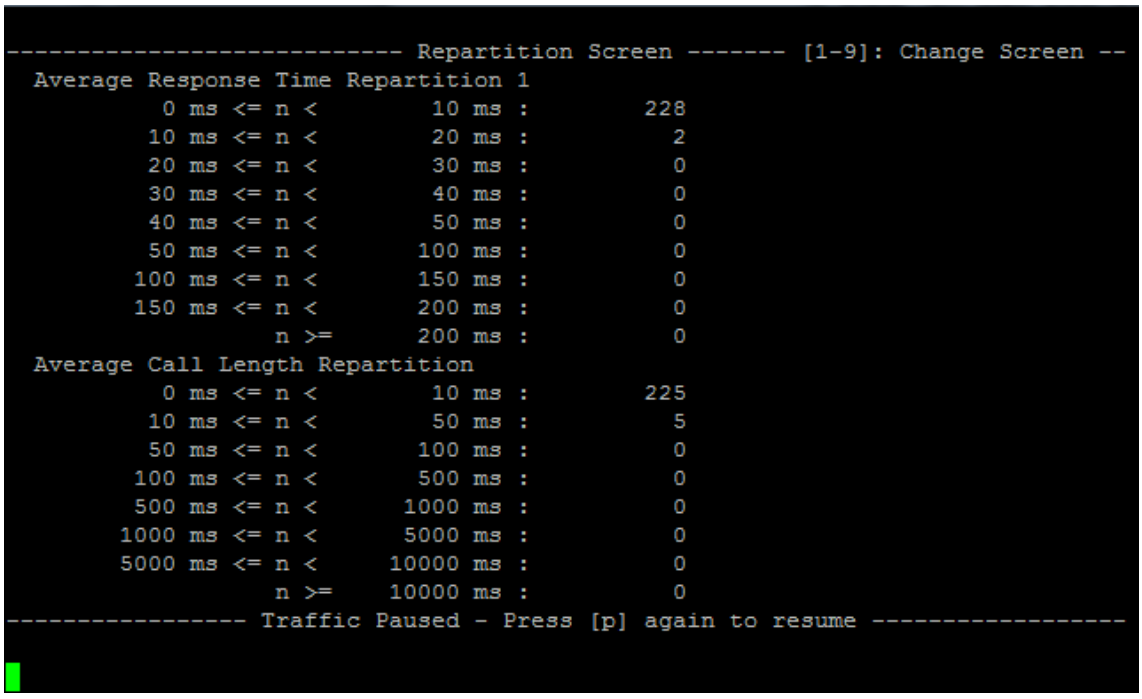
Χρησιμοποιήθηκε το βασικό σενάριο uac του SIPp, για την υλοποίηση της διαδικασίας σύνδεσης με το PBX και δημιουργήθηκε ένα Xml, το register.xml.

8.1.1.1 Μέτρηση καθυστέρησης εγκατάστασης κλήσης (call setup delay (σε ms)) χωρίς φορτίο.

Για τη μέτρηση της καθυστέρησης εγκατάστασης κλήσης εκτελέστηκε η πιο κάτω εντολή στον Test Client, με το –sn ορίζεται το βασικό σενάριο, με το –s 3000 το SIPp συνδέεται στο τηλεφωνικό κέντρο με τον λογαριασμό χρηστή #3000, και με το –r1 ορίζεται ότι οι κλήσεις θα αυξάνονται κατά μία το δευτερόλεπτο (cps 1.0).

./ sipp -sn uac 192.168.1.100 -s 3000 -r 1

Πιο συγκεκριμένα, η μέση καθυστέρηση εγκατάστασης κλήσης ήταν μέσα στα 10 ms (Εικόνα 8.3) .



Εικόνα 8.3: Μέσος χρόνος καθυστέρησης εγκατάστασης κλήσης όπως τον παρουσιάζει το SIPp.

8.1.1.2 Μέτρηση Ικανότητας δημιουργίας κλήσεων (INVITE capacity (UDP)) χωρίς φορτίο.

Για τη μέτρηση της ικανότητας δημιουργίας κλήσης εκτελέστηκε η πιο κάτω εντολή στον Test Client, με το –sn ορίζεται το βασικό σενάριο, με το –d 2000 ορίζεται ότι η κλήση θα διαρκέσει 2000 ms δηλαδή 2 sec, με το –s 3000 το SIPp συνδέεται στο τηλεφωνικό κέντρο με τον λογαριασμό χρηστή #3000, και με το –r1 ορίζεται ότι οι κλήσεις θα αυξάνονται κατά μια κλήση το δευτερόλεπτο (cps 1.0). Κατά την διάρκεια του πειράματος αυξανόταν σταδιακά ο ρυθμός παραγωγής των κλήσεων μέχρι το σύστημα να φτάσει στα όρια του και να έχουμε αιτήματα αναμετάδοσης των σημάτων από το τηλεφωνικό κέντρο προς την γεννήτρια τηλεφωνικών κλήσεων, έτσι θεωρούμε ότι το τηλεφωνικό κέντρο έχει φτάσει στα όρια του και δεν μπορεί πλέον να εξυπηρετήσει άλλες κλήσεις.

./sipp -sn uac –d 2000 192.168.1.100 -s 3000 -r 1

Φαινομενικά η εντολή είναι η ίδια με το προηγούμενο πείραμα αλλά στην πραγματικότητα το γεγονός ότι η μαζικότητα των κλήσεων είναι απεριόριστη και ότι η διάρκεια τους είναι 1000 ms δηλαδή είναι πολύ σύντομες, κάνει το σύστημα προσπαθώντας να τις εξυπηρετήσει να φτάνει στα όρια του και αυτό ακριβώς είναι ο στόχος του πειράματος.

Με την πρώτη ματιά γίνεται αντιληπτό ότι η παράμετρος –d είναι ορισμένη στα 2000 ms και όχι στα 1000 ms όπως περιγράφεται στην προηγούμενη παράγραφο. Αυτό γίνεται για να αποφευχθεί μια αρκετά πολύπλοκη κατάσταση που δεν επέτρεπε να εκτελεστεί το πείραμα για λόγους ασφαλείας και η οποία θα αναλυθεί παρακάτω.

Το Asterisk έχει σχεδιασθεί για να είναι αρκετά ασφαλές, έτσι όταν ένας χρήστης, στην προκειμένη περίπτωση ο χρήστης #3000 εκτελεί εκατοντάδες τηλεφωνήματα σχεδόν ταυτόχρονα, το Asterisk το εκλαμβάνει σαν επίθεση άρνησης υπηρεσιών (Denial-of-service attack), ή αλλιώς DoS attack. Για να μην συμβαίνει αυτό το Asterisk έχει παραμετροποιήθει, σε ότι αφορά τον χρηστή #3000 να τερματίζει την κλήση του μετά την παρέλευση ενός 1 sec, άρα δεν εκλαμβάνει πλέον την πληθώρα τηλεφωνημάτων σαν επίθεση και τερματίζει την κλήση κανονικά. Η παραμετροποίηση του Asterisk περιγράφεται αναλυτικά στο παράρτημα, στο τέλος αυτής της εργασίας.

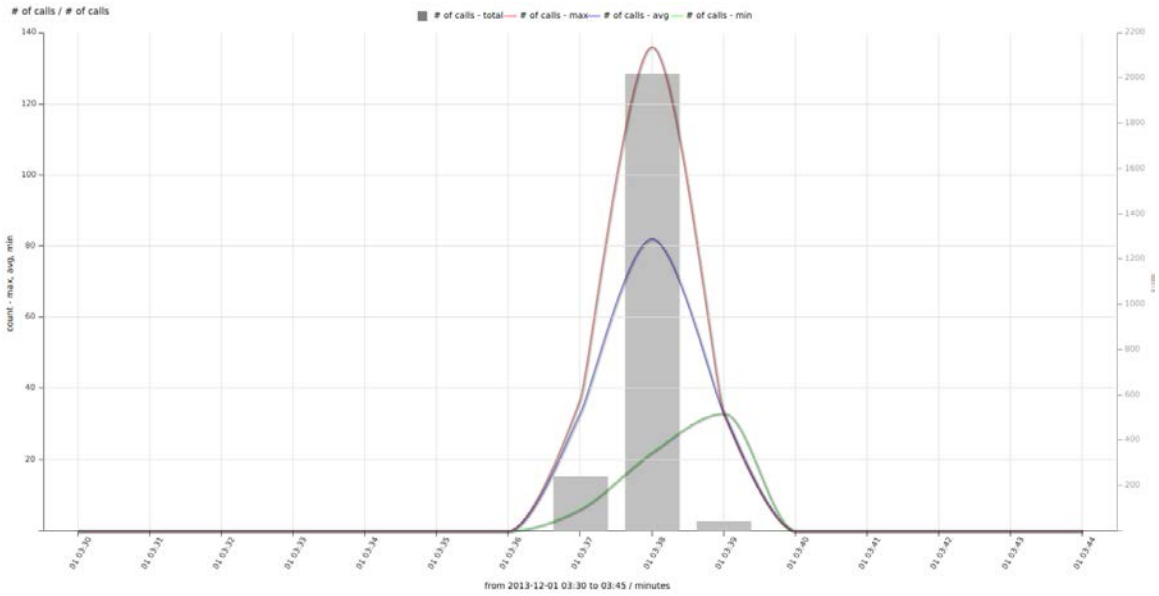
Τα αποτελέσματα του πειράματος παρουσιάζονται παρακάτω (Εικόνα 8.4). Ο μέγιστος ρυθμός κλήσεων έφτασε τις 125 cps και τότε το σύστημα έφτασε στα όρια του αρχίζοντας να ζητά από τον Client αναμετάδοση πακέτων (Retrans) και να παρουσιάζει σφάλματα στην απάντηση του INVITE, δηλαδή στο 100. Όλες οι κλήσεις τερματίστηκαν από το Asterisk με 200 μετά το πέρας του πρώτου δευτερολέπτου μετά το Pause. Το SIPp, όπως προαναφέρθηκε, δέχτηκε απροσδιόριστο σφάλμα στο σύνολο των συνομιλιών, οι οποίες τερματίστηκαν από το Asterisk και όχι από το SIPp, όπως ανέμενε εκείνο να γίνει. Έτσι τα στατιστικά του δεν παρουσιάζουν την πραγματικότητα, όπως φαίνεται αναλυτικά στην εικόνα.

```
  Call-rate(length)    Port   Total-time  Total-calls  Remote-host
125.0(2000 ms)/1.000s   5060     172.46 s        11282  192.168.1.100:5060(UDP)

  125 new calls during 1.003 s period    1 ms scheduler resolution
  144 calls (limit 750)                  Peak was 190 calls, after 162 s
  0 Running, 463 Paused, 210 Woken up
  0 dead call msg (discarded)            0 out-of-call msg (discarded)
  3 open sockets

                                Messages  Retrans   Timeout   Unexpected-Msg
      INVITE ---------->        11282     80        0
         100 <----------        10823     0         0         317
         180 <----------        0         0         0         0
         183 <----------        0         0         0         0
         200 <----------  E-RTD1 10822     0         0         0
         ACK ---------->        10822     0
       Pause [   2000ms]        10822                         10820
         BYE ---------->        1         0         0
         200 <----------        1         0         0         0

------ [+|-|*|/]: Adjust rate ---- [q]: Soft exit ---- [p]: Pause traffic -----

Last Error: Aborting call on unexpected message for Call-Id '11138-1706@...
```

Εικονα 8.4:Μέτρηση δυνατότητας INVITE.

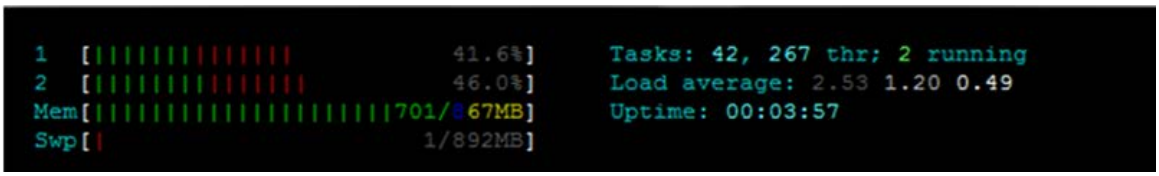
Το VoIP Monitor από την άλλη πλευρά παρακολουθούσε όλη την κίνηση κλήσεων που πραγματοποιήθηκαν μεταξύ των δυο προγραμμάτων και κράτησε αναλυτικά στατιστικά, τα οποία παρουσιάζονται παρακάτω στην (Εικόνα 8.5) και είναι.

1. Το πείραμα κράτησε τέσσερα λεπτά 4 min.
2. Το σύνολο των επιτυχημένων κλήσεων είναι 2010 cps.
3. Ο μέγιστος αριθμός ταυτόχρονων κλήσεων είναι 136 cps.
4. Ο ελάχιστος αριθμός ταυτόχρονων κλήσεων είναι 33 cps.
5. Ο μέσος όρος ταυτόχρονων κλήσεων είναι 82cps .



Εικόνα 8.5: Στατιστικά κλήσεων της μέτρησης INVITE του VOIP MONITOR.

Με την βοήθεια του προγράμματος htop, το οποίο επιτρέπει την παρακολούθηση της κατανομής των πόρων ενός συστήματος Linux σε πραγματικό χρόνο (Εικόνα 8.6), την στιγμή του μέγιστου αριθμού κλήσεων ο υπολογιστής παρουσίασε 46% CPU και μέγιστη μνήμη, όπως φαίνεται στην εικόνα.



Εικόνα 8.6: Htop κατανομή πόρων του συστήματος κατά την διάρκεια του πειράματος.

Είναι προφανές ότι το πρωτόκολλο SIP δεν εξαρτάται τόσο από την επεξεργαστική ισχύ ενός υπολογιστή αλλά από την μνήμη που είναι διαθέσιμη, Αυτό οφείλεται στο γεγονός ότι είναι υποχρεωμένο να διαχωρίζει απλά μηνύματα, να δημιουργεί αρχεία στην προσωρινή μνήμη με μεγάλη ταχύτητα και να τα διατηρεί όσο χρειάζεται για την διεκπεραίωση των κλήσεων.

8.1.1.3 Ικανότητα σύνδεσης με το PBX (REGISTER capacity, UDP).

Για την μέτρηση της ικανότητας REGISTER στο μητρώο εγκατάστασης κλήσεων του τηλεφωνικού κέντρου εκτελέστηκε η πιο κάτω εντολή στον Test Client, με το –sf ορίζεται το σενάριο REGISTER.xml, που δημιουργήθηκε έτσι ώστε να συνεργάζεται με το SIPp και παρουσιάζεται παρακάτω, με το –s 3000 το SIPp συνδέεται στο τηλεφωνικό κέντρο με τον λογαριασμό χρηστή #3000, και με το –r 15 ορίζεται ότι οι κλήσεις θα αυξάνονται κατά 15 το δευτερόλεπτο (cps 15 .0).

./sipp -sf REGISTER.xml 192.168.1.100 -s 3000 –r 15.

Με την δημιουργία ενός .xml αρχείου υπάρχει η δυνατότητα να δημιουργηθεί ένα ξεχωριστό σενάριο, που στην προκειμένη περίπτωση δίνει την δυνατότητα στο SIPp να εγγράφει το extension #3000 στο τηλεφωνικό κέντρο. Ο κώδικας αυτού του σεναρίου παρουσιάζεται αναλυτικά παρακάτω.

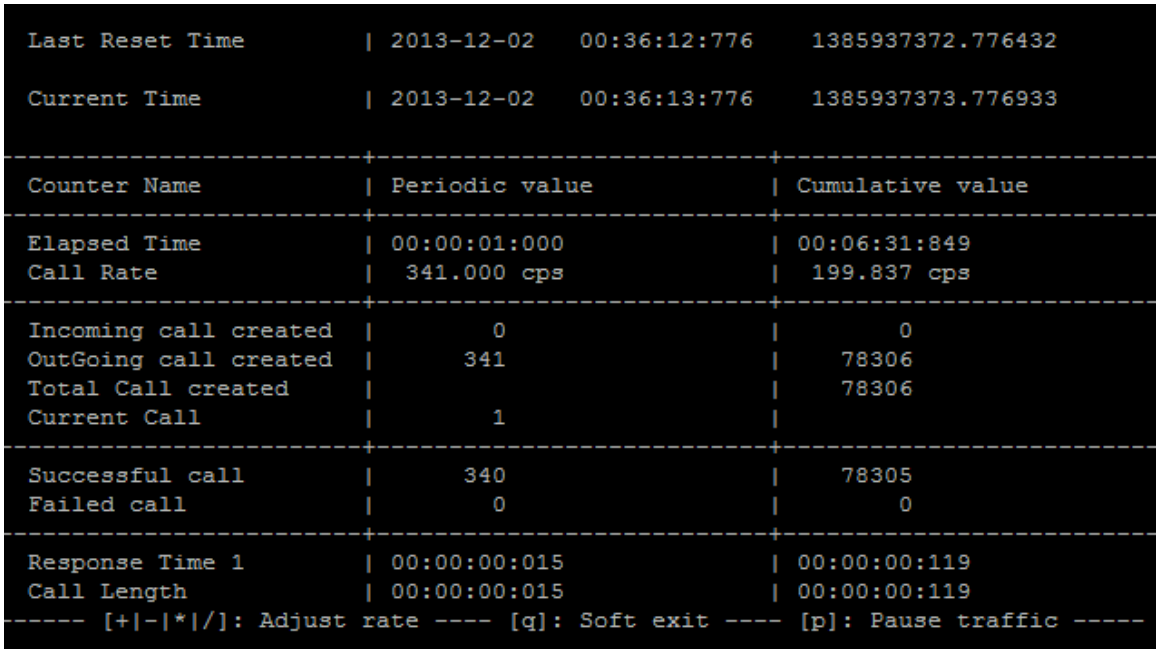
```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<scenario name="register">
<!—Όνομα σεναρίου. -->
<send retrans="500">
<!—Σε περίπτωση αποτυχίας της αποστολής όρισε retrans="500". -->
<![CDATA[
REGISTER sip:[service]@[remote_ip]:[remote_port] SIP/2.0
<!—Αποστολή μηνύματος REGISTER σε σύστημα με την συγκεκριμένη μορφή διεύθυνσης -->
Via: SIP/2.0/[transport] [local_ip]:[local_port];branch=[branch]
<!—Αποστολή μηνύματος REGISTER μέσω της τοπικής διεύθυνσης -->
From: sipp <sip:sipp@[local_ip]:[local_port]>;tag=[call_number]
<!—Συμπλήρωση του αριθμού τηλεφώνου -->
 To: sut sip:[service]@[remote_ip]:[remote_port]
```

```
<!—Αποστολή μηνύματος  στο απομακρυσμένο σύστημα  -->
Call-ID: [call_id]
<!—Συμπλήρωση του αριθμού κλήσης.  -->
CSeq: 1 REGISTER
<!—Ακολουθία εντολών 1 Register.  -->
Contact: sip:sipp@[local_ip]:[local_port]
<!—Αναφορά στην τοπική διεύθυνση  -->
Expires: 300
<!—λήξη συμπλήρωση 300.  -->
 ]]>
</send>
<recv response="200" rtd="true" />
<!—από την στιγμή που έχει λάβει απάντηση στέλνει 200 διαφορετικά όχι.  -
->
</scenario>
```

Αυτό το σενάριο λοιπόν στέλνει αιτήσεις σύνδεσης στο τηλεφωνικό κέντρο και δέχεται απαντήσεις από αυτό. Τα αποτελέσματα εμφανίζονται στις (Εικόνες 8.7,8.8). Παρατηρείται πως η ικανότητα είναι 340 κλήσεις το δευτερόλεπτο (340 cps).

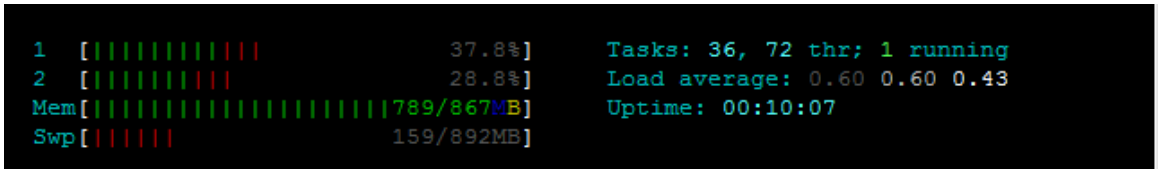
```
------------------------------ Scenario Screen -------- [1-9]: Change Screen --
  Call-rate(length)   Port   Total-time  Total-calls  Remote-host
 340.0(0 ms)/1.000s   5060     373.81 s        72173  192.168.1.100:5060(UDP)

  340 new calls during 1.001 s period    0 ms scheduler resolution
  184 calls (limit 1020)                 Peak was 1023 calls, after 370 s
  0 Running, 11169 Paused, 984 Woken up
  0 dead call msg (discarded)            0 out-of-call msg (discarded)
  3 open sockets

                                Messages  Retrans   Timeout   Unexpected-Msg
    REGISTER ---------->         72173     6213      0
         200 <----------  E-RTD1 71989     0         0         0
------ [+|-|*|/]: Adjust rate ---- [q]: Soft exit ---- [p]: Pause traffic -----
```

Εικόνα 8.7 Μέτρηση δυνατότητας REGISTER.



Εικόνα 8.8 Μέτρηση δυνατότητας REGISTER.

Την στιγμή του μέγιστου αριθμού συνδέσεων REGISTER το σύστημα παρουσιάζει 33,3% CPU και μέγιστη μνήμη (Εικόνα 8.9).



Εικόνα 8.9 Htop κατανομή πόρων του συστήματος κατά την διάρκεια του πειράματος REGISTER.

8.1.2 Απόδοση συστήματος PBX/SIP από το οποίο περνούν όλα τα δεδομένα μιας Voip συνομιλίας.

Ένα σύγχρονο PBX όπως το σύστημα Asterisk έχει την δυνατότητα να εκτελεί για παράδειγμα χρέη αυτόματης τηλεφωνήτριας AVR, Voice mail και να καταγράφει κλήσεις, να συνδέει δίκτυα γραμμές VOIP , GSM, PSTN, ISDN, και ταυτόχρονα ο ίδιος υπολογιστής να τρέχει μια σειρά από τις κλασικές πια υπηρεσίες υπολογιστών, όπως e-mail server , DNS server, File Server, Database Server, κλπ. Αυτού του είδους τα συστήματα ονομάζονται PBX (Private Branch Exchange) και έχουν την δυνατότητα γενικής διασύνδεσης συστημάτων επικοινωνιών, οπότε τα δεδομένα της συνομιλίας περνούν αναγκαστικά από το σύστημα, είτε για να καταγραφούν, είτε για να μετατραπούν σε κάποια άλλη μορφή και να σταλούν σε ένα διαφορετικό δίκτυο για παράδειγμα σε ένα δίκτυο PSTN.

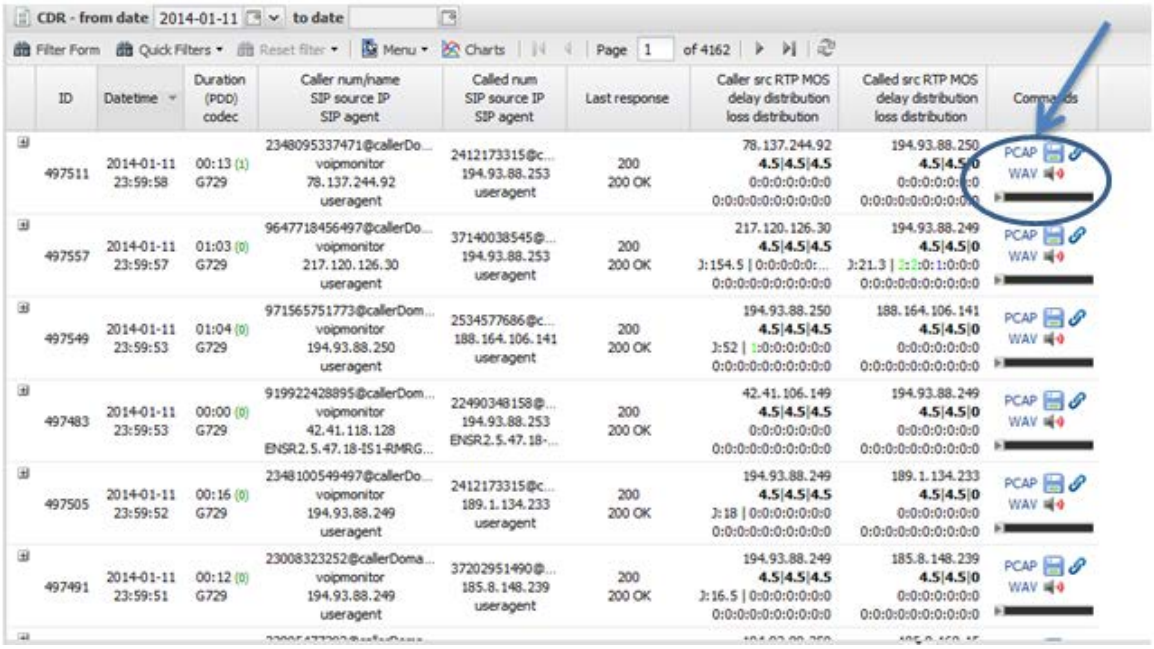
Τον σημαντικότερο ρόλο στις μετρήσεις απόδοσης ενός τέτοιου συστήματος παίζει ο CODEC, καθώς ο κάθε CODEC έχει διαφορετικό bit rate, διαφορετικό μέγεθος πακέτου και κατά συνέπεια καταλαμβάνει διαφορετικό bandwidth, άρα και διαφορετικό τρόπο επεξεργασίας, όπως αναφέρεται στο κεφάλαιο 5 .

Στα πλαίσια του πειράματος έγιναν μετρήσεις με διαφορετικούς CODEC, για να γίνει εφικτός ο καθορισμός της απόδοσης του PBX/SIP μέσω της σύγκρισής τους.

Το γεγονός ότι σε αυτή την δεύτερη φάση θα μας απασχολήσει το θέμα των CODEC δεν αναιρεί καθόλου τις μετρήσεις που έγιναν μέχρι στιγμής, καθώς δεν αλλάζει τίποτε στις παραμέτρους του πρωτοκόλλου REGISTER , INVITE, call setup delay εφόσον πρόκειται για το ίδιο σύστημα.

Για την υλοποίηση των πειραμάτων συγκεντρώθηκαν Pcap Play για δυο βασικούς CODEC. Ο πρώτος είναι ο g11a, που έχει την ίδια ποιότητα με την σταθερή τηλεφωνία PSTN και ο δεύτερος είναι GSM, που είναι γνωστός για την χρήση του στην κινητή τηλεφωνία και είναι πολύ φτωχός σε ποιότητα.

Την δημιουργία Pcap Play αρχείων υποστηρίζει απευθείας το VoIP Monitor, έτσι έγινε μια κλήση χρησιμοποιώντας τον συγκεκριμένο CODEC κάθε φορά και αφού την κατέγραψε το VoIP Monitor την μετέτρεψε αυτόματα σε Pcap Play αρχείο. Έπειτα χρησιμοποιήθηκε το αρχείο για χρήση από το SIPp. Όπως παρατηρείται στην (Εικόνα 8.10) υπάρχει η δυνατότητα απευθείας λήψης μετά από κάθε καταγραφή μιας κλήσης.



Εικόνα 8.10 Λήψη αρχείου Pcap Play από το VoIP Monitor.

8.1.2.1 Απόδοση συστήματος PBX/SIP με CODEC g11a.

Για την μέτρηση της απόδοσης με CODEC g11a έγινε η χρήση του uac_pcap.xml, το οποίο συμπεριλαμβάνεται στο πακέτο του SIPp, και έγινε παραμετροποίησή του, έτσι ώστε να διαβάζει τα συγκεκριμένα Pcap Play κάθε φορά, στην προκειμένη περίπτωση παραμετροποιήθηκε ένα αρχείο για το g11a.

Από τον client εκτελέστηκε η πιο κάτω εντολή, με το –sf ορίζεται το σενάριο uac_pcap.xml που δημιουργήθηκε έτσι ώστε να δημιουργεί κλήσεις με κίνηση δικτύου, με το –s 3000 το SIPp συνδέεται στο τηλεφωνικό κέντρο με τον

λογαριασμό χρηστή #3000. Η αύξηση του αριθμού των κλήσεων έγινε χειροκίνητα χρησιμοποιώντας τις εντολές του SIPp, έτσι ώστε να παρουσιαστεί μέγιστος αριθμός κλήσεων, δηλαδή το σύστημα να μην μπορεί πλέον να ανταπεξέλθει λόγω του πλήθους των κλήσεων, το xml ρυθμίστηκε με τέτοιον τρόπο έτσι ώστε μέχρι τα 8000 ms να γίνεται αποστολή δεδομένων και για τα επόμενα 1000 ms να γίνεται λήψη. Τα αποτελέσματα παρουσιάζονται παρακάτω.

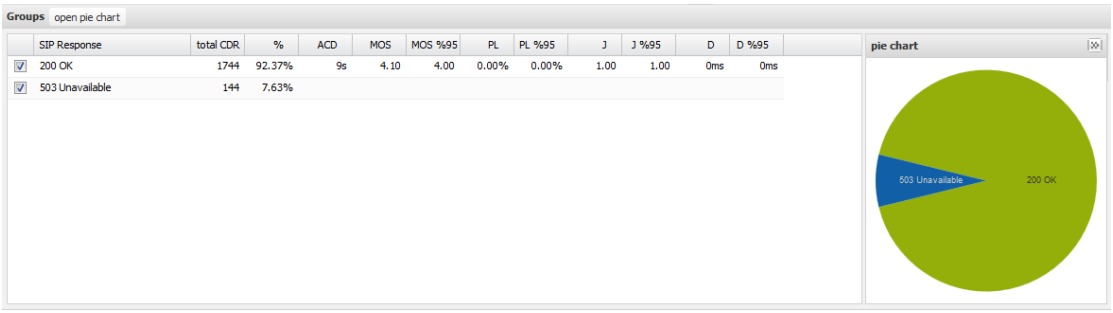
./ sipp –sf uac_pcap.xml 192.168.1.100 -s 3000

Τα αποτελέσματα παρουσιάζονται στις πιο κάτω εικόνες, με μέγιστο αριθμό ταυτόχρονων κλήσεων 91 έπειτα από 9 sec(Εικόνα 8.11).

```
  18 calls (limit 972)                    Peak was 91 calls, after 9 s
  0 Running, 676 Paused, 64 Woken up
  0 dead call msg (discarded)             0 out-of-call msg (discarded)
  3 open sockets
  480748 Total RTP pckts sent             100.360 last period RTP rate (kB/s)

                                 Messages  Retrans   Timeout   Unexpected-Msg
      INVITE ----------->         2670       0         0
         100 <-----------         2122       0         0         548
         180 <-----------         0          0         0         0
         200 <-----------  E-RTD1 2122       0         0         0

         ACK ----------->         2122       0
               [ NOP ]
       Pause [   8000ms]         2122                           173
               [ NOP ]
       Pause [   1000ms]         1935                           0
         BYE ----------->         1931       0         0
         200 <-----------         1931       0         0         0

------ [+|-|*|/]: Adjust rate ---- [q]: Soft exit ---- [p]: Pause traffic -----
```

Εικόνα 8.11: Απόδοση συστήματος PBX/SIP με CODEC g11a.

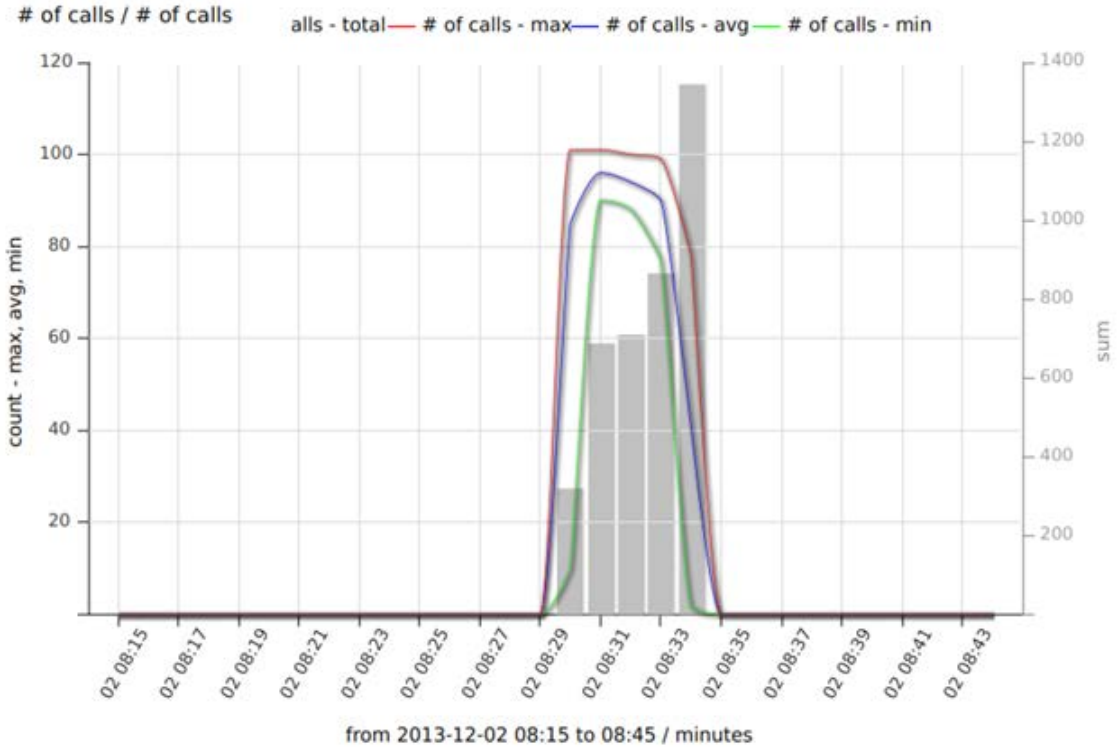
Κατά την διάρκεια διεξαγωγής του πειράματος έγιναν 1744 κλήσεις που τερματίστηκαν κανονικά και 144 που έληξαν απρόσμενα (Εικόνα 8.12), λόγω υπερφόρτωσης του συστήματος.



Εικόνα 8.12: Στατιστική κατανομή κλήσεων.

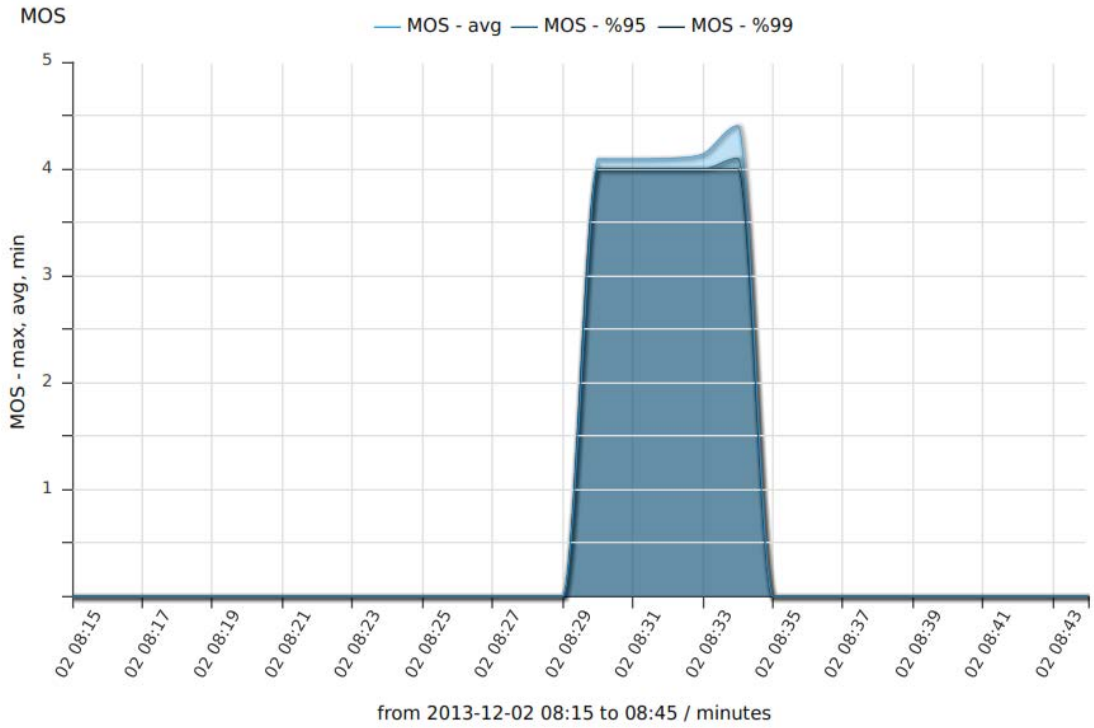
Το VoIP Monitor παρακολουθούσε όλη την κίνηση κλήσεων που πραγματοποιήθηκαν μεταξύ των δυο προγραμμάτων και κράτησε αναλυτικά στατιστικά, τα οποία παρουσιάζονται παρακάτω στην (Εικόνα 8.13) και είναι.

1. Το πείραμα κράτησε έξι λεπτά 6 min.
2. Το σύνολο των επιτυχημένων κλήσεων είναι 1744 cps.
3. Ο μέγιστος αριθμός ταυτόχρονων κλήσεων είναι 100 cps.
4. Ο ελάχιστος αριθμός ταυτόχρονων κλήσεων είναι 88 cps.
5. Ο μέσος όρος ταυτόχρονων κλήσεων είναι 82 cps.



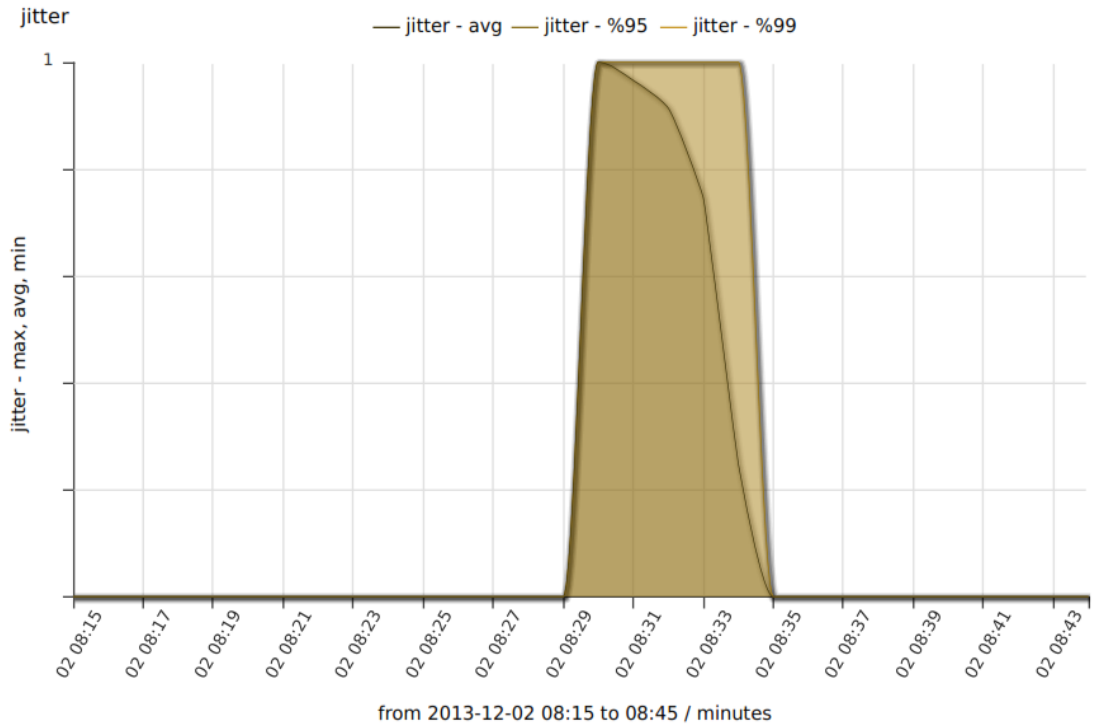
Εικονα 8.13: Στατιστικά κλήσεων.

Με βάση την μέθοδο αξιολόγησης MOS (Mean Opinion Score) η ποιότητα των κλήσεων υπολογίστηκε πολύ κοντά στο 4 (Εικόνα 8.14) και χαρακτηρίζεται ως πολύ καλή.



Εικόνα 8.14: Ποιότητα κλήσεων με βάση την μέθοδο αξιολόγησης MOS.

Ο μέσος όρος του jitter (Εικόνα 8.15) ξεκινά από 1 και μειώνεται κατά την διάρκεια διεξαγωγής του πειράματος καθώς ο χρόνος περνά· στο 95% και 99 % των κλήσεων έχει τιμή 1.



Εικονα 8.15: Μέτρηση jitter.

8.1.2.2 Απόδοση συστήματος PBX/SIP με CODEC gsm.

Για την μέτρηση της απόδοσης με CODEC GSM έγινε η χρήση του uac_pcap.xml, το οποίο συμπεριλαμβάνεται στο πακέτο του SIPp, και έγινε παραμετροποίησή του, έτσι ώστε να διαβάζει τα συγκεκριμένα Pcap Play κάθε φορά, στην προκειμένη περίπτωση παραμετροποιήθηκε ένα αρχείο για το GSM.

Από τον client εκτελέστηκε η πιο κάτω εντολή, με το –sf ορίζεται το σενάριο uac_pcap.xml που δημιουργήθηκε έτσι ώστε να δημιουργεί κλήσεις με κίνηση δικτύου, με το –s 3000 το SIPp συνδέεται στο τηλεφωνικό κέντρο με τον λογαριασμό χρηστή #3000. Η αύξηση του αριθμού των κλήσεων έγινε χειροκίνητα χρησιμοποιώντας τις εντολές του SIPp έτσι ώστε να παρουσιαστεί μέγιστος αριθμός κλήσεων, δηλαδή το σύστημα να μην μπορεί πλέον να ανταπεξέλθει λόγω του πλήθους των κλήσεων, το xml ρυθμίστηκε με τέτοιον τρόπο έτσι ώστε μέχρι τα 8000 ms να γίνεται αποστολή δεδομένων και για τα επόμενα 1000 ms να γίνεται λήψη. Τα αποτελέσματα παρουσιάζονται παρακάτω.

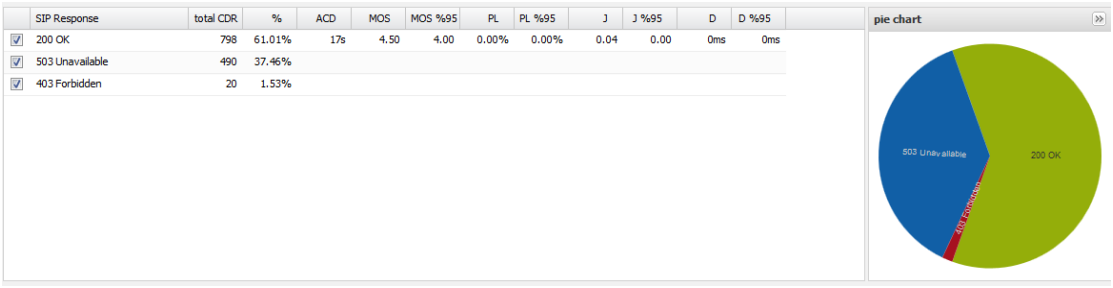
./ sipp –sf uac_pcap.xml 192.168.1.100 -s 3000

Τα αποτελέσματα παρουσιάζονται στις πιο κάτω εικόνες, με μέγιστο αριθμό ταυτόχρονων κλήσεων 181 έπειτα από 18 sec (Εικόνα 8.16).

```
 169 calls (limit 540)                  Peak was 181 calls, after 18 s
 0 Running, 222 Paused, 33 Woken up
 0 dead call msg (discarded)            0 out-of-call msg (discarded)
 3 open sockets
 77696 Total RTP pckts sent             184.094 last period RTP rate (kB/s)

                             Messages  Retrans   Timeout   Unexpected-Msg
     INVITE ---------->         220       0         0
        100 <----------         209       0         0         11
        180 <----------         0         0         0         0
        200 <----------  E-RTD1 209       0         0         0

        ACK ---------->         209       0
            [ NOP ]
      Pause [   8000ms]         209                           0
            [ NOP ]
      Pause [    10.0s]         140                           0
        BYE ---------->         40        0         0
        200 <----------         40        0         0         0

------ [+|-|*|/]: Adjust rate ---- [q]: Soft exit ---- [p]: Pause traffic -----
```

Εικόνα 8.16 :Απόδοση συστήματος PBX/SIP με CODEC GSM**.**

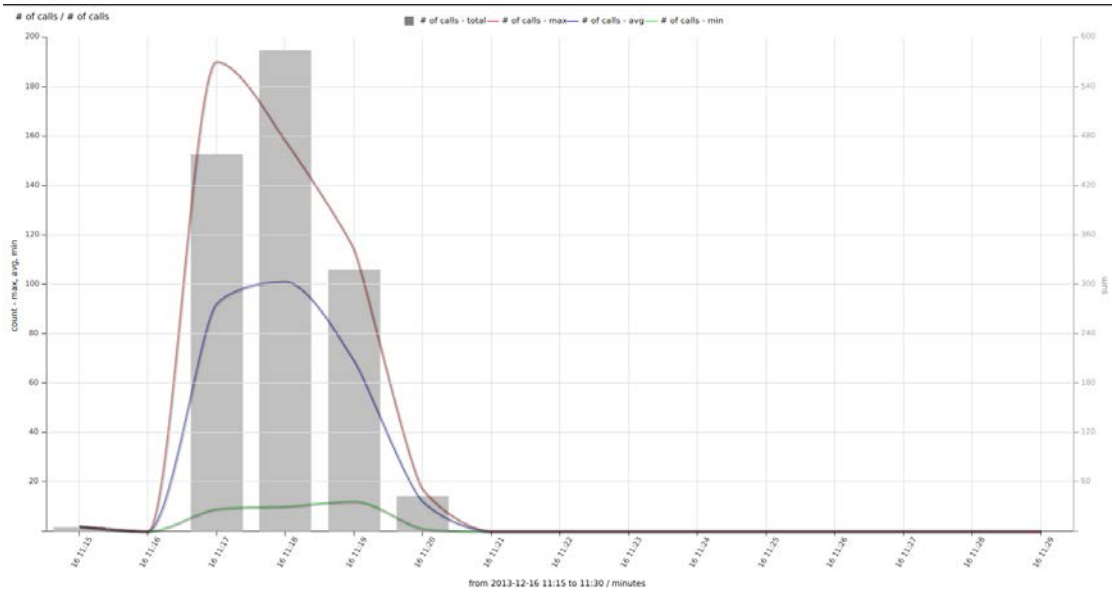
Κατά την διάρκεια διεξαγωγής του πειράματος (Εικόνα 8.17) έγιναν 798 κλήσεις που τερματίστηκαν κανονικά, 503 που έληξαν απρόσμενα και 403 που ακυρωθήκαν από το σύστημα λόγω υπερφόρτωσης.



Εικόνα 8.17: Στατιστική κατανομή κλήσεων.

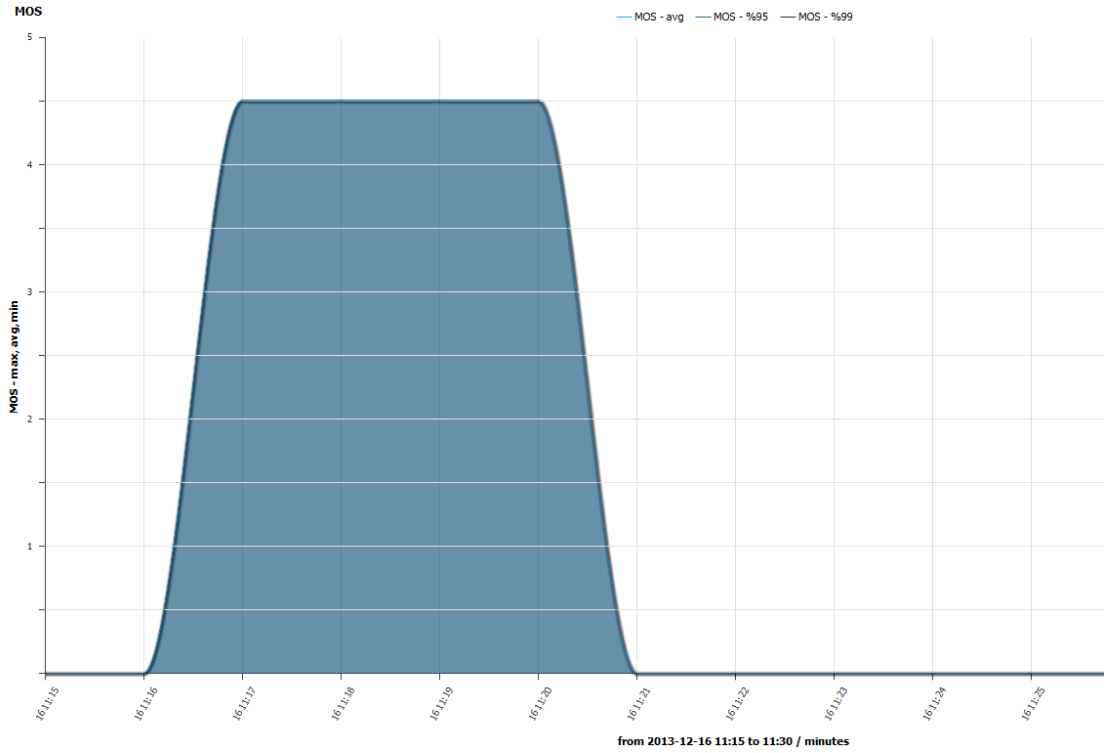
Το VoIP Monitor παρακολουθούσε όλη την κίνηση κλήσεων που πραγματοποιήθηκαν μεταξύ των δυο προγραμμάτων και κράτησε αναλυτικά στατιστικά, τα οποία παρουσιάζονται παρακάτω στην (Εικόνα 8.18) και είναι:

1. Το πείραμα κράτησε έξι λεπτά 6 min.
2. Το σύνολο των επιτυχημένων κλήσεων είναι 798 cps.
3. Ο μέγιστος αριθμός ταυτόχρονων κλήσεων είναι 190 cps.
4. Ο ελάχιστος αριθμός ταυτόχρονων κλήσεων είναι 15 cps.
5. Ο μέσος όρος ταυτόχρονων κλήσεων είναι 100 cps.

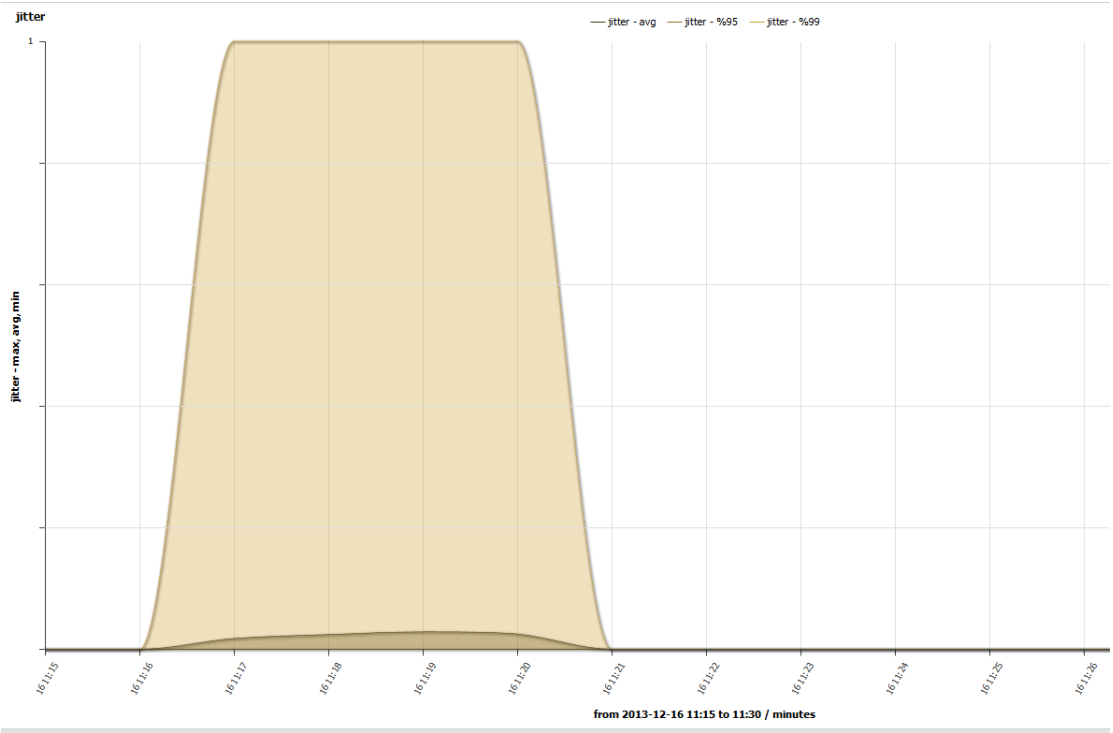


Εικόνα 8.18: Στατιστικά κλήσεων.

Με βάση την μέθοδο αξιολόγησης MOS (Mean Opinion Score) η ποιότητα των κλήσεων υπολογίστηκε πολύ κοντά στο 4,5 (Εικόνα 8.19) και χαρακτηρίζεται από πολύ καλή έως εξαιρετική.



Εικόνα 8.19: Ποιότητα κλήσεων με βάση την μέθοδο αξιολόγησης MOS.



Εικόνα 8.20 Μέτρηση jitter.

Ο μέσος όρος του jitter (Εικόνα 8.20) δεν ξεπερνά το 0.2 και μειώνεται κατά την διάρκεια διεξαγωγής του πειράματος καθώς ο χρόνος περνά· στο 95% και 99 % των κλήσεων έχει τιμή 1.

8.2 Συγκεντρωτικά αποτελέσματα πειραμάτων.

- Για την μέτρηση καθυστέρησης εγκατάστασης κλήσης (call setup delay) του συστήματος υπήρχε καθυστέρηση 10 ms.

- Για την μέτρηση της ικανότητας δημιουργίας κλήσεων (INVITE capacity (UDP)).

    1. Το πείραμα κράτησε τέσσερα λεπτά 4 min.
    2. Το σύνολο των επιτυχημένων κλήσεων είναι 2010 cps.
    3. Ο μέγιστος αριθμός ταυτόχρονων κλήσεων είναι 136 cps.
    4. Ο ελάχιστος αριθμός ταυτόχρονων κλήσεων είναι 33 cps.
    5. Ο μέσος όρος ταυτόχρονων κλήσεων είναι 82 cps.

- Για την μέτρηση της ικανότητας σύνδεσης με το PBX (REGISTER capacity, UDP).

    1. 340 κλήσεις το δευτερόλεπτο (340 cps).

- Για την απόδοση συστήματος PBX/SIP με CODEC g11a.

    1. Το πείραμα κράτησε έξι λεπτά 6 min.
    2. Το σύνολο των επιτυχημένων κλήσεων είναι 1744 cps.
    3. Ο μέγιστος αριθμός ταυτόχρονων κλήσεων είναι 100 cps.
    4. Ο ελάχιστος αριθμός ταυτόχρονων κλήσεων είναι 88 cps.
    5. Ο μέσος όρος ταυτόχρονων κλήσεων είναι 82 cps.
    6. Με βάση την μέθοδο αξιολόγησης MOS (Mean Opinion Score) η ποιότητα των κλήσεων υπολογίστηκε πολύ κοντά στο 4.
    7. Το jitter είναι 1 στο 95% και 99% των κλήσεων .

- Για την απόδοση συστήματος PBX/SIP με CODEC gsm.

    1. Το πείραμα κράτησε έξι λεπτά 6 min.
    2. Το σύνολο των επιτυχημένων κλήσεων είναι 798 cps.
    3. Ο μέγιστος αριθμός ταυτόχρονων κλήσεων είναι 190 cps.
    4. Ο ελάχιστος αριθμός ταυτόχρονων κλήσεων είναι 15 cps.
    5. Ο μέσος όρος ταυτόχρονων κλήσεων είναι 100 cps.
    6. Με βάση την μέθοδο αξιολόγησης MOS (Mean Opinion Score) η ποιότητα των κλήσεων υπολογίστηκε πολύ κοντά στο 4,5.
    7. Το jitter είναι 1 στο 95% και 99% των κλήσεων .

Κεφάλαιο 9.

Συμπεράσματα.

Έπειτα από τις μετρήσεις που έγιναν βγήκαν τα παρακάτω συμπεράσματα αναφορικά με το πρωτόκολλο SIP, την συμπεριφορά του, σε σχέση με το σύστημα προς μέτρηση, όπως επίσης και για τα εργαλεία που χρησιμοποιηθήκαν στα πειράματα.

Σε ότι αφορά τους CODEC, επιβεβαιώνεται ότι είναι ένα από τα σημαντικότερα στοιχεία σε ένα τηλεφωνικού κέντρο, αφού το κέντρο παρουσίασε καλύτερη συμπεριφορά με τον GSM CODEC σε σχέση με τον G11a, επειδή το bandwidth έχει διαφορά στην τιμή. Βέβαια αυτό έχει επιπτώσεις στην ποιότητα, όπως αναλύθηκε εκτενώς στο Κεφάλαιο 5, έτσι εξηγείται η διαφορά ανάμεσα στους δύο CODEC, με μέσο όρο ταυτόχρονων κλήσεων 100 για τον GSM και 82 για τον G11a.

Θα αναμενόταν, όταν το τηλεφωνικό κέντρο κάνει μόνο σηματοδότηση, δηλαδή διαχειρίζεται μόνο το πρωτόκολλο SIP, να παρουσιάζεται αύξηση των δυνατοτήτων του κατά πολύ σε σχέση με την περίπτωση που το τηλεφωνικό κέντρο κάνει ταυτόχρονα αποστολή και λήψη δεδομένων σε κάθε κλήση άρα τα δεδομένα περνούν μέσα από το τηλεφωνικό κέντρο. Αντίθετα παρατηρήθηκε ότι τα αποτελέσματα είναι παρόμοια και η μόνη διαφορά , άξια αναφοράς είναι ανάμεσα σε διαφορετικούς CODEC. Αυτό προφανώς οφείλεται στο γεγονός ότι η διαδικασία σηματοδότησης καλύπτει το όριο δυνατοτήτων του τηλεφωνικού κέντρου, αφού δεσμεύει πόρους του συστήματος, όπως μνήμη, πολύ πιο γρήγορα από επεξεργαστική ισχύ, η οποία δεσμεύεται όταν γίνεται encoding και decoding με την χρήση ενός CODEC. Προφανώς αν το τηλεφωνικό κέντρο, που έγιναν τα πειράματα είχε περισσότερη μνήμη, θα αυξανόταν αυτό το όριο.

Το Asterisk, επειδή είναι ένα ολοκληρωμένο σύστημα και συμπεριλαμβάνει πολύ περισσότερα υποπρογράμματα και διαδικασίες από ένα απλό SIP σύστημα, κάνει επιμερισμό πόρων, έτσι ώστε να επιτυγχάνει καλύτερα αποτελέσματα στο σύνολο των υπηρεσιών που προσφέρει, και όχι σε κάποια επιμέρους υπηρεσία συγκεκριμένα. Προφανώς σε μεγάλες εγκαταστάσεις υπάρχει η δυνατότητα διάσπασης των υπηρεσιών σε διάφορα υπολογιστικά συστήματα, έτσι ώστε το συνολικό σύστημα που θα προκύψει να μπορεί να εξυπηρετήσει μεγαλύτερο αριθμό χρηστών.

Σύμφωνα με τις μετρήσεις το σύστημα έχει τις παρακάτω δυνατότητες.

- Καθυστέρηση εγκατάστασης κλήσης (call setup delay) του συστήματος. Υπήρχε καθυστέρηση 10 ms.

- Ικανότητα δημιουργίας κλήσεων (INVITE capacity (UDP)), με μέσο όρο ταυτόχρονων κλήσεων 82, με CODEC g11a μέσο όρο ταυτόχρονων κλήσεων επίσης 82, ενώ με CODEC GSM ο μέσος όρος ταυτόχρονων κλήσεων είναι 100.

- Το jitter είναι 1 στο 95% και 99% των κλήσεων .

- Με βάση την μέθοδο αξιολόγησης MOS (Mean Opinion Score) η ποιότητα των κλήσεων υπολογίστηκε μεταξύ 4 και 4,5.

- Η ικανότητα σύνδεσης με το PBX (REGISTER capacity, UDP) μετρήθηκε στις 340 κλήσεις το δευτερόλεπτο (340 cps).

Το πρόγραμμα SIPp είναι μια πανίσχυρη γεννήτρια τηλεφωνικών κλήσεων, για το πρωτόκολλο SIP. Είναι ένα ελεύθερο πρόγραμμα το οποίο μπορεί να κάνει μετρήσεις αλλά και προσομοίωση κλήσεων, έτσι το καθιστά ένα πολύ χρήσιμο εργαλείο δοκιμής, ελέγχου αλλά και εκμάθησης διαδικασιών για το πρωτόκολλο SIP.

Το πρόγραμμα Voip Monitor δίνει την δυνατότητα ελέγχου του δικτύου σε πραγματικό χρόνο και κάνει στατιστική ανάλυση των κλήσεων δίνοντας την δυνατότητα στον χρήστη να κάνει παρεμβάσεις στο δίκτυο και στα προγράμματα με στόχο την βελτίωση της ποιότητας υπηρεσιών σε ένα ολοκληρωμένο σύστημα VOIP.

Βιβλιογραφία.

[1] ΕΙΣΑΓΩΓΗ ΣΤΙΣ ΝΕΕΣ ΤΕΧΝΟΛΟΓΙΕΣ ΕΠΙΚΟΙΝΩΝΙΩΝ, ΠΟΜΠΟΡΤΣΗΣ ΑΝΔΡΕΑΣ, Εκδόσεις: ΤΖΙΟΛΑ ISBN: 960-7219-64-3.

[2] ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ ,ΠΟΜΠΟΡΤΣΗΣ ΑΝΔΡΕΑΣ, ΠΑΠΑΔΗΜΗΤΡΙΟΥ ΓΙΩΡΓΟΣ, Εκδόσεις: ΤΖΙΟΛΑ, ISBN: 960-8050-88-X.

[3] Voice over IP Networks , Quality of Service , Pricing and Security , Promode K.Verma , Ling Wang , ISBN 978-3-642-14329-8

[4] SIPp reference documentation,by Richard GAYRAUD [initial code], Olivier JACQUES [code/documentation], Robert Day [code/documentation], Charles P. Wright [code], Many contributors [code]

[5] SIP: Session Initiation Protocol RFC - Proposed Standard (July 2002; Errata) , Updated by RFC 5630, RFC 4320, RFC 5922, RFC 3853, RFC 5621, RFC 6878, RFC 3265, RFC 5626, RFC 5393, RFC 6026, RFC 4916, RFC 6665, RFC 6141, RFC 5954, Obsoletes RFC 2543.

[6] RFC3550, "RTP: A Transport Protocol for Real-Time Applications", July 2003, Source of RFC: avt (rai),Errata ID: 3263,Status: Held for Document Update,Type: Technical,Reported By: Pieter Demuytere, Date Reported: 2012-06-18, Held for Document Update by: Robert Sparks

[7] ITU-T,TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU SERIES P: TELEPHONE TRANSMISSION QUALITY,Methods for objective and subjective assessment of Quality ,ETHODS TRANSMISSION ,ITU-T Recommendation P.800(Previously CCITT Recommendation),(08/96).

[8] I T U - T , TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU, SERIES G: TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS, International telephone connections and circuits – Transmission planning and the E-model, G.107 (12/2011).

Σύνδεσμοι.

[1] http://sipp.sourceforge.net/

[2] http://tools.ietf.org/html/rfc3261

[3] http://tools.ietf.org/html/rfc3550

[4] http://www.voipmonitor.org/doc/Content

[5] http://www.asterisk.org/community/documentation

[6] https://help.ubuntu.com/12.04/index.html

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

[8] http://en.wikipedia.org/wiki/Mean_opinion_score

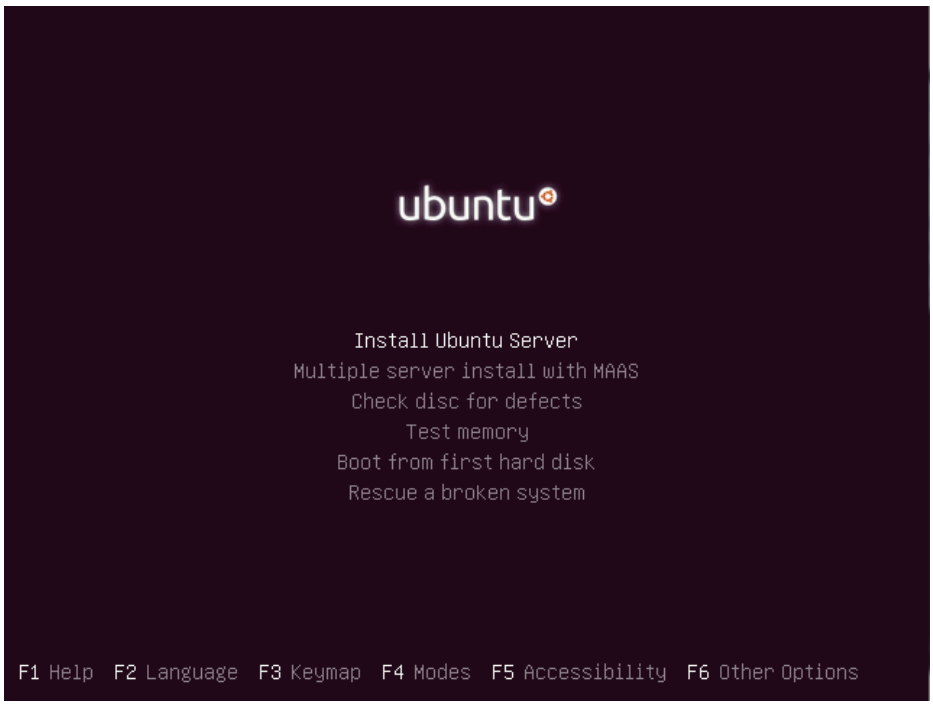
Παράρτημα Α.

1. Εγκατάσταση συστημάτων.

Για την υλοποίηση του συνόλου των πειραμάτων εγκαταστάθηκαν δυο Η/Υ, ο πρώτος εκτελεί χρέη διακομιστή Server και ο δεύτερος χρέη πελάτη Client

1.1 Εγκατάσταση Server.

Στους δυο υπολογιστές έγινε εγκατάσταση του λειτουργικού συστήματος Ubuntu Server 12.04.3 LTS 64 Bit (Εικόνα 1.1) και ακολουθήθηκε η διαδικασία τυπικής εγκατάστασης.



Εικόνα 1.1: εκκίνηση τυπικής εγκατάστασης Ubuntu Server 12.04.3 LTS 64 Bit.

1.2 Εγκατάσταση Asterisk.

Η εγκατάσταση του προγράμματος Asterisk έγινε αυτόματα μέσω δικτύου εκτελώντας την παρακάτω εντολή.

- **sudo apt-get install asterisk**

1.3 Εγκατάσταση VoIP Monitor.

Η εγκατάσταση του VoIP Monitor έγινε μέσω δικτύου εκτελώντας μια σειρά από εντολές, έτσι ώστε να γίνει η εγκατάσταση των απαιτούμενων πακέτων και του προγράμματος, όπως αναφέρονται στο.

http://www.voipmonitor.org/doc/Ubuntu_12.04_LTS

- **sudo bash**
- **apt-get -y install php5-gd php5-mysql php5 php5-cli apache2 libapache2-mod-php5 tshark mtr mysql-server php5-mcrypt librsvg2-bin gsfonts**
- **cd /usr/src/**
- **wgethttp://sourceforge.net/projects/voipmonitor/files/8.3/voipmonitor-amd64-8.3-static.tar.gz**
- **cd /usr/src/**
- **tar xzf voipmonitor*.tar.gz**
- **cd voipmonitor***
- **./install-script.sh**
- **mysqladmin create voipmonitor**
- **edit /etc/voipmonitor.conf and set appropriate mysql password**
- **/etc/init.d/voipmonitor start**
- **cd /var/www**
- **wget "http://www.voipmonitor.org/download-gui?version=latest&major=5&festry" -O w.tar.gz**
- **tar xzf w.tar.gz**
- **mv voipmonitor-gui*/* ./**
- **rm index.html**
- **wget http://voipmonitor.org/ioncube/x86_64/ioncube_loader_lin_5.3.so -O /usr/lib/php5/20090626/ioncube_loader_lin_5.3.so**
- **mkdir /var/spool/voipmonitor/**
- **chown www-data /var/spool/voipmonitor/**

- **wget http://sourceforge.net/projects/voipmonitor/files/wkhtml/0.10.0_rc2/wkhtmltoimage-x86_64 -O "/var/www/bin/wkhtmltoimage-x86_64"**

- **chmod +x "/var/www/bin/wkhtmltoimage-x86_64"**

- **wget http://sourceforge.net/projects/voipmonitor/files/wkhtml/0.10.0_rc2/wkhtmltopdf-x86_64 -O "/var/www/bin/wkhtmltopdf-x86_64"**

- **chmod +x "/var/www/bin/wkhtmltopdf-x86_64"**

- **wget http://voipmonitor.org/ioncube/x86_64/ioncube_loader_lin_5.3.so -O /usr/lib/php5/20090626/ioncube_loader_lin_5.3.so**

- **echo "zend_extension = /usr/lib/php5/20090626/ioncube_loader_lin_5.3.so" > /etc/php5/apache2/conf.d/ioncube.ini**

- **chown -R www-data /var/www**

- **/etc/init.d/apache2 restart**

1.4 Εγκατάσταση SIPp.

Η εγκατάσταση του SIPp έγινε μέσω δικτύου εκτελώντας τις παρακάτω εντολές, έτσι ώστε να γίνει η εγκατάσταση των απαιτούμενων πακέτων και του προγράμματος με υποστήριξη Pcap Play.

- **sudo bash**
- **apt-get install sip-tester**
- **apt-get install libssl-dev libpcap-dev libncurses5-dev**

2.1 Παραμετροποίηση Asterisk.

Η βασική παραμετροποίηση του Asterisk γίνεται σε δυο αρχεία που βρίσκονται στο /etc/asterisk , το sip.conf και το extensions.conf.

sip.conf

Στο sip.conf δηλώνονται οι τηλεφωνικές συσκευές και οι γραμμές που συνδέονται στο Asterisk, όπως φαίνεται παρακάτω.

[2002]

type=friend

host=dynamic

secret=ab2002

[2003]

type=friend

host=dynamic

secret=ab2003

[sipp]

type=friend

context=sipp

host=dynamic

[3000]

type=friend

host=dynamic

Στο extensions.conf δηλώνονται οι διαδικασίες και οι κανόνες με τους οποίους θα λειτουργεί το τηλεφωνικό κέντρο, δηλαδή γίνεται ο προγραμματισμός του.

Παρακάτω παρουσιάζεται η παραμετροποίηση του τηλεφωνικού κέντρου που έγινε για την ανάγκη των πειραμάτων.

extensions.conf

[default]

internal

exten => _2XXX,1,Dial(SIP/${EXTEN},30)

[sipp]

exten => 3000,1,Answer()

;exten => 3000,n,Playback(hello-world)

;exten => 3000,n,Playback(/home/alf/test)

exten => 3000,n,wait(20)

exten => 3000,n,Hangup() ns.conf

Στο Internal δηλώθηκε η παρακάτω εντολή που σημαίνει ότι όταν κάποιος χρήστης με κωδικό από 2000 έως 2999 καλεί κάποιο extension από 2000 έως 2999 ,

το τηλεφωνικό κέντρο του κάνει σύνδεση και το καλούμενο extension περιμένει 30 δευτερόλεπτα για να απαντήσει ο χρήστης.

exten => _2XXX,1,Dial(SIP/${EXTEN},30)

Στο SIPp δηλώθηκε μια σειρά εντολών που επιτρέπει την διασύνδεση του τηλεφωνικού κέντρου με το πρόγραμμα SIPp , με λογαριασμό 3000.

Στην πρώτη γραμμή το τηλεφωνικό κέντρο απαντά στην κλήση, στην επομένη είτε περιμένει για 20 δευτερόλεπτα, είτε παίζει ένα αρχείο από τον σκληρό δίσκο, ή κατευθείαν από το πρόγραμμα asterisk, όπως είναι το hello-world που είναι ένα αρχείο ήχου από τα πολλά που έρχονται με την βασική εγκατάσταση του προγράμματος ή ένα αρχείο από τον σκληρό δίσκο κατευθείαν (/home/alf/test), στην τρίτη γραμμή τερματίζει την συνομιλία.

[sipp]

exten => 3000,1,Answer()

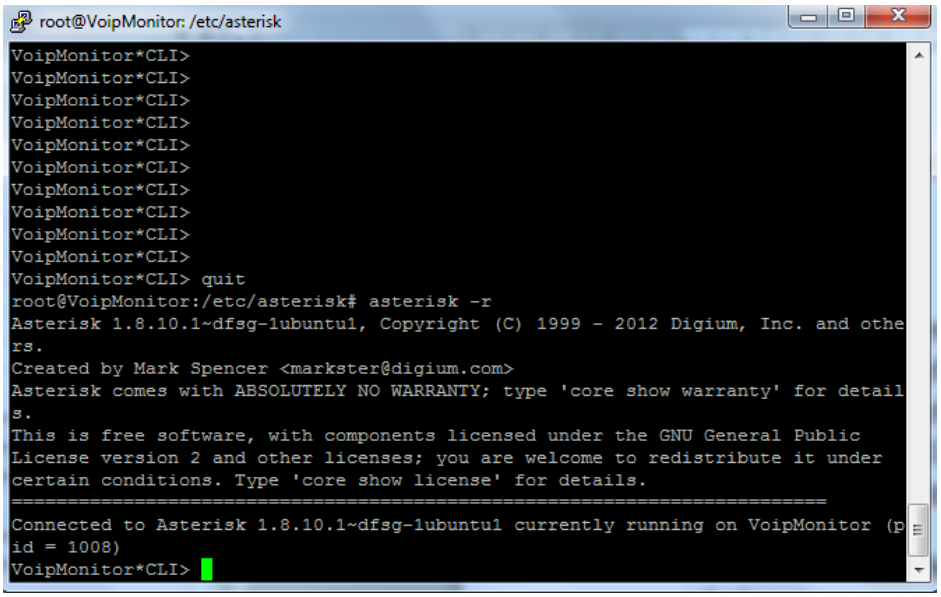
;exten => 3000,2,Playback(hello-world)

;exten => 3000,2,Playback(/home/alf/test)

exten => 3000,2,wait(20)

exten => 3000,n,Hangup() ns.conf

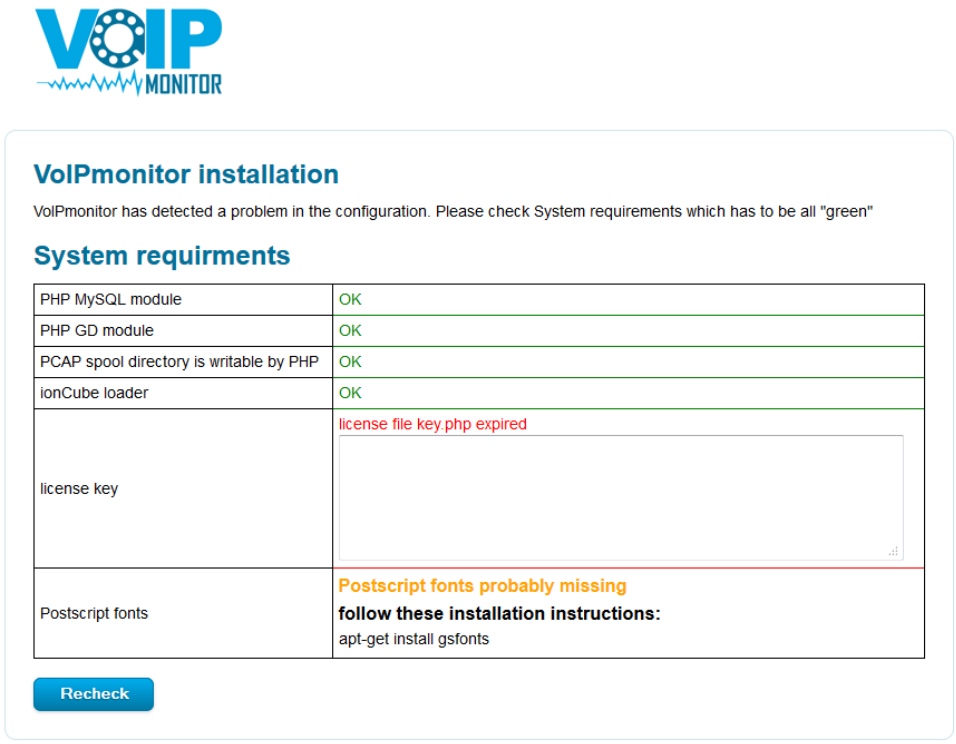
Ο έλεγχος του προγράμματος γίνεται από την κονσόλα CLI του asterisk που εμφανίζεται με την εντολή asterisk –r (Εικονα 1.2). Ο χρήστης βλέπει οποιοδήποτε σφάλμα ή αναφορά προκύπτει κατά την διάρκεια λειτουργίας του προγράμματος.



Εικόνα 1.2 Κονσόλα CLI του asterisk.

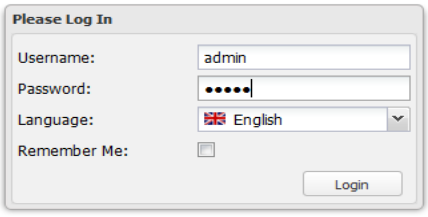
2.2 Παραμετροποίηση του VoIP Monitor.

Αφού εγκατασταθεί το πρόγραμμα στην κεντρική σελίδα του WEB GUI, πρέπει να καταχωρηθεί το κλειδί ενεργοποίησης (Εικόνα 1.3). Τα πειράματα πραγματοποιηθήκαν με το δοκιμαστικό κλειδί που παρέχεται από το http://www.voipmonitor.org/download-gui?version=license , αφού γίνει εγγραφή νέου χρήστη.



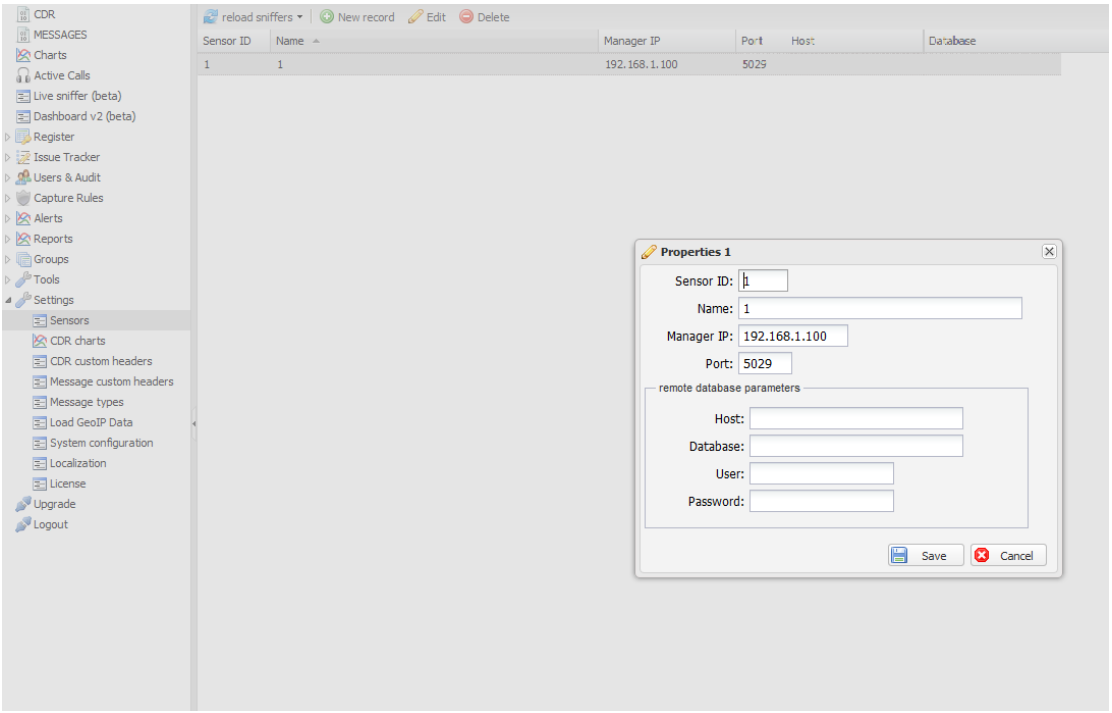
Εικόνα 1.3: Ενεργοποίηση Voip Monitor.

Μετά την ενεργοποίηση παρουσιάζεται η κεντρική οθόνη (Εικόνα 1.4) εισόδου του προγράμματος, στην οποία η είσοδος γίνεται με λογαριασμό χρήστη admin και κωδικό πρόσβασης admin.



Εικόνα 1.4 Κεντρική οθόνη εισόδου του Voip Monitor.

Μετά την είσοδο στο πρόγραμμα είναι απαραίτητο να ρυθμιστεί το sniffer στο πεδίο Settings Sniffer (Εικόνα 1.5), έτσι ώστε να γίνει σύνδεση με το sniffer, το οποίο παρακολουθεί τις κλήσεις στον SIP Server.



Εικόνα 1.5 Ρύθμιση του sniffer στο Voip Monitor.

2.3 Παραμετροποίηση SIPp.

Το SIPp δεν χρειάζεται κάποια ιδιαίτερη παραμετροποίηση. Αυτό που είναι απαραίτητο είναι η διαχείριση και παραμετροποίηση των xml αρχείων, όπου αυτό χρειάζεται.

Παρακάτω παρουσιάζονται τα .xml αρχεία που χρησιμοποιηθήκαν στα πειράματα.

Το πρώτο .xml αρχείο που χρησιμοποιήθηκε είναι το uac.xml, το οποίο χρησιμοποιήθηκε αυτούσιο χωρίς αλλαγές.

uac.xml

```
 1:<?xml version="1.0" encoding="ISO-8859-1" ?>
 2:<!DOCTYPE scenario SYSTEM "sipp.dtd">
 3:
 4:<!-- This program is free software; you can redistribute it and/or      -->
 5:<!-- modify it under the terms of the GNU General Public License as     -->
 6:<!-- published by the Free Software Foundation; either version 2 of the -->
 7:<!-- License, or (at your option) any later version.                    -->
 8:<!--                                                                    -->
 9:<!-- This program is distributed in the hope that it will be useful,    -->
10:<!-- but WITHOUT ANY WARRANTY; without even the implied warranty of     -->
11:<!-- MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the      -->
12:<!-- GNU General Public License for more details.                       -->
13:<!--                                                                    -->
14:<!-- You should have received a copy of the GNU General Public License  -->
15:<!-- along with this program; if not, write to the                      -->
16:<!-- Free Software Foundation, Inc.,                                    -->
17:<!-- 59 Temple Place, Suite 330, Boston, MA  02111-1307 USA             -->
18:<!--                                                                    -->
19:<!--                 Sipp default 'uac' scenario.                       -->
20:<!--                                                                    -->
21:
22:             <scenario name="Basic Sipstone UAC">
23:<!-- In client mode (sipp placing calls), the Call-ID MUST be         -->
24:<!-- generated by sipp. To do so, use [call_id] keyword.               -->
25:<send retrans="500">
26:  <![CDATA[
27:
```

```
28:   INVITE sip:[service]@[remote_ip]:[remote_port] SIP/2.0
29:   Via: SIP/2.0/[transport] [local_ip]:[local_port];branch=[branch]
30:   From: sipp <sip:sipp@[local_ip]:[local_port]>;tag=[call_number]
31:   To: sut <sip:[service]@[remote_ip]:[remote_port]>
32:   Call-ID: [call_id]
33:   CSeq: 1 INVITE
34:   Contact: sip:sipp@[local_ip]:[local_port]
35:   Max-Forwards: 70
36:   Subject: Performance Test
37:   Content-Type: application/sdp
38:   Content-Length: [len]
39:
40:   v=0
41:   o=user1 53655765 2353687637 IN IP[local_ip_type] [local_ip]
42:   s=-
43:   c=IN IP[media_ip_type] [media_ip]
44:   t=0 0
45:   m=audio [media_port] RTP/AVP 0
46:   a=rtpmap:0 PCMU/8000
47:
48:    ]]>
49:  </send>
50:
51:  <recv response="100"
52:        optional="true">
53:  </recv>
54:
55:  <recv response="180" optional="true">
56:  </recv>
57:
58:  <!-- By adding rrs="true" (Record Route Sets), the route sets         -->
59:  <!-- are saved and used for following messages sent. Useful to test   -->
60:  <!-- against stateful SIP proxies/B2BUAs.                             -->
61:  <recv response="200" rtd="true">
62:  </recv>
63:
64:  <!-- Packet lost can be simulated in any send/recv message by         -->
```

```
<!-- by adding the 'lost = "10"'. Value can be [1-100] percent.       -->
<send>
  <![CDATA[

    ACK sip:[service]@[remote_ip]:[remote_port] SIP/2.0
    Via: SIP/2.0/[transport] [local_ip]:[local_port];branch=[branch]
    From: sipp <sip:sipp@[local_ip]:[local_port]>;tag=[call_number]
    To: sut <sip:[service]@[remote_ip]:[remote_port]>[peer_tag_param]
    Call-ID: [call_id]
    CSeq: 1 ACK
    Contact: sip:sipp@[local_ip]:[local_port]
    Max-Forwards: 70
    Subject: Performance Test
    Content-Length: 0

  ]]>
</send>

<!-- This delay can be customized by the -d command-line option       -->
<!-- or by adding a 'milliseconds = "value"' option here.             -->
<pause/>

<!-- The 'crlf' option inserts a blank line in the statistics report. -->
<send retrans="500">
  <![CDATA[

    BYE sip:[service]@[remote_ip]:[remote_port] SIP/2.0
    Via: SIP/2.0/[transport] [local_ip]:[local_port];branch=[branch]
    From: sipp <sip:sipp@[local_ip]:[local_port]>;tag=[call_number]
    To: sut <sip:[service]@[remote_ip]:[remote_port]>[peer_tag_param]
    Call-ID: [call_id]
    CSeq: 2 BYE
    Contact: sip:sipp@[local_ip]:[local_port]
    Max-Forwards: 70
    Subject: Performance Test
    Content-Length: 0

```

```
102:    ]]>
103:  </send>
104:
105:  <recv response="200" crlf="true">
106:  </recv>
107:
108:  <!-- definition of the response time repartition table (unit is ms)   -->
109:  <ResponseTimeRepartition value="10, 20, 30, 40, 50, 100, 150, 200"/>
110:
111:  <!-- definition of the call length repartition table (unit is ms)     -->
112:  <CallLengthRepartition value="10, 50, 100, 500, 1000, 5000, 10000"/>
113:
114:</scenario>
115:
```

Το δεύτερο .xml αρχείο που χρησιμοποιήθηκε είναι το uac_pacp.xml, το οποίο χρησιμοποιήθηκε με αλλαγές στα σημεία που είναι υπογραμμισμένα με μπλε χρώμα, και αφορούν στα ονόματα των εξωτερικών αρχείων που χρησιμοποιηθήκαν και στον χρόνο αποστολής και λήψης δεδομένων.

uac_pacp.xml

```
  1:<?xml version="1.0" encoding="ISO-8859-1" ?>
  2:<!DOCTYPE scenario SYSTEM "sipp.dtd">
  3:
  4:<!-- This program is free software; you can redistribute it and/or      -->
  5:<!-- modify it under the terms of the GNU General Public License as     -->
  6:<!-- published by the Free Software Foundation; either version 2 of the -->
  7:<!-- License, or (at your option) any later version.                    -->
  8:<!--                                                                    -->
  9:<!-- This program is distributed in the hope that it will be useful,    -->
 10:<!-- but WITHOUT ANY WARRANTY; without even the implied warranty of     -->
 11:<!-- MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the      -->
 12:<!-- GNU General Public License for more details.                       -->
 13:<!--                                                                    -->
 14:<!-- You should have received a copy of the GNU General Public License  -->
 15:<!-- along with this program; if not, write to the                      -->
 16:<!-- Free Software Foundation, Inc.,                                    -->
 17:<!-- 59 Temple Place, Suite 330, Boston, MA  02111-1307 USA             -->
 18:<!--                                                                    -->
```

```
19:<!--                 Sipp 'uac' scenario with pcap (rtp) play           -->
20:<!--                                                                    -->
21:
22:<scenario name="UAC with media">
23:  <!-- In client mode (sipp placing calls), the Call-ID MUST be         -->
24:  <!-- generated by sipp. To do so, use [call_id] keyword.                -->
25:  <send retrans="500">
26:    <![CDATA[
27:
28:      INVITE sip:[service]@[remote_ip]:[remote_port] SIP/2.0
29:      Via: SIP/2.0/[transport] [local_ip]:[local_port];branch=[branch]
30:      From: sipp <sip:sipp@[local_ip]:[local_port]>;tag=[call_number]
31:      To: sut <sip:[service]@[remote_ip]:[remote_port]>
32:      Call-ID: [call_id]
33:      CSeq: 1 INVITE
34:      Contact: sip:sipp@[local_ip]:[local_port]
35:      Max-Forwards: 70
36:      Subject: Performance Test
37:      Content-Type: application/sdp
38:      Content-Length: [len]
39:
40:      v=0
41:      o=user1 53655765 2353687637 IN IP[local_ip_type] [local_ip]
42:      s=-
43:      c=IN IP[local_ip_type] [local_ip]
44:      t=0 0
45:      m=audio [auto_media_port] RTP/AVP 8
46:      a=rtpmap:8 PCMA/8000
47:      a=rtpmap:101 telephone-event/8000
48:      a=fmtp:101 0-11,16
49:
50:    ]]>
51:  </send>
52:
53:  <recv response="100" optional="true">
54:  </recv>
55:
```

```
56:  <recv response="180" optional="true">
57:  </recv>
58:
59:  <!-- By adding rrs="true" (Record Route Sets), the route sets         -->
60:  <!-- are saved and used for following messages sent. Useful to test   -->
61:  <!-- against stateful SIP proxies/B2BUAs.                             -->
62:  <recv response="200" rtd="true" crlf="true">
63:  </recv>
64:
65:  <!-- Packet lost can be simulated in any send/recv message by         -->
66:  <!-- by adding the 'lost = "10"'. Value can be [1-100] percent.       -->
67:  <send>
68:    <![CDATA[
69:
70:      ACK sip:[service]@[remote_ip]:[remote_port] SIP/2.0
71:      Via: SIP/2.0/[transport] [local_ip]:[local_port];branch=[branch]
72:      From: sipp <sip:sipp@[local_ip]:[local_port]>;tag=[call_number]
73:      To: sut <sip:[service]@[remote_ip]:[remote_port]>[peer_tag_param]
74:      Call-ID: [call_id]
75:      CSeq: 1 ACK
76:      Contact: sip:sipp@[local_ip]:[local_port]
77:      Max-Forwards: 70
78:      Subject: Performance Test
79:      Content-Length: 0
80:
81:    ]]>
82:  </send>
83:
84:  <!-- Play a pre-recorded PCAP file (RTP stream)                       -->
85:  <nop>
86:    <action>
87:      <exec play_pcap_audio="pcap/g711a.pcap"/>
88:    </action>
89:  </nop>
90:
91:  <!-- Pause 8 seconds, which is approximately the duration of the      -->
92:  <!-- PCAP file                                                       -->
```

```
 93:  <pause milliseconds="8000"/>
 94:
 95:  <!-- Play an out of band DTMF '1'                                    -->
 96:  <nop>
 97:    <action>
 98:      <exec play_pcap_audio="pcap/dtmf_2833_1.pcap"/>
 99:    </action>
100:  </nop>
101:
102:  <pause milliseconds="1000"/>
103:
104:  <!-- The 'crlf' option inserts a blank line in the statistics report. -->
105:  <send retrans="500">
106:    <![CDATA[
107:
108:      BYE sip:[service]@[remote_ip]:[remote_port] SIP/2.0
109:      Via: SIP/2.0/[transport] [local_ip]:[local_port];branch=[branch]
110:      From: sipp <sip:sipp@[local_ip]:[local_port]>;tag=[call_number]
111:      To: sut <sip:[service]@[remote_ip]:[remote_port]>[peer_tag_param]
112:      Call-ID: [call_id]
113:      CSeq: 2 BYE
114:      Contact: sip:sipp@[local_ip]:[local_port]
115:      Max-Forwards: 70
116:      Subject: Performance Test
117:      Content-Length: 0
118:
119:    ]]>
120:  </send>
121:
122:  <recv response="200" crlf="true">
123:  </recv>
124:
125:  <!-- definition of the response time repartition table (unit is ms)   -->
126:  <ResponseTimeRepartition value="10, 20, 30, 40, 50, 100, 150, 200"/>
127:
128:  <!-- definition of the call length repartition table (unit is ms)     -->
129:  <CallLengthRepartition value="10, 50, 100, 500, 1000, 5000, 10000"/>
```

```
130:
131:</scenario>
132:
```

Το τρίτο .xml αρχείο που χρησιμοποιήθηκε είναι το uac.xml , το οποίο χρησιμοποιήθηκε αυτούσιο χωρίς αλλαγές.

Uas.xml

```
  1:<?xml version="1.0" encoding="ISO-8859-1" ?>
  2:<!DOCTYPE scenario SYSTEM "sipp.dtd">
  3:
  4:<!-- This program is free software; you can redistribute it and/or      -->
  5:<!-- modify it under the terms of the GNU General Public License as     -->
  6:<!-- published by the Free Software Foundation; either version 2 of the -->
  7:<!-- License, or (at your option) any later version.                    -->
  8:<!--                                                                    -->
  9:<!-- This program is distributed in the hope that it will be useful,    -->
 10:<!-- but WITHOUT ANY WARRANTY; without even the implied warranty of     -->
 11:<!-- MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the      -->
 12:<!-- GNU General Public License for more details.                       -->
 13:<!--                                                                    -->
 14:<!-- You should have received a copy of the GNU General Public License  -->
 15:<!-- along with this program; if not, write to the                      -->
 16:<!-- Free Software Foundation, Inc.,                                    -->
 17:<!-- 59 Temple Place, Suite 330, Boston, MA  02111-1307 USA             -->
 18:<!--                                                                    -->
 19:<!--                 Sipp default 'uas' scenario.                       -->
 20:<!--                                                                    -->
 21:
 22:<scenario name="Basic UAS responder">
 23:  <!-- By adding rrs="true" (Record Route Sets), the route sets         -->
 24:  <!-- are saved and used for following messages sent. Useful to test   -->
 25:  <!-- against stateful SIP proxies/B2BUAs.                             -->
 26:  <recv request="INVITE" crlf="true">
 27:  </recv>
 28:
 29:  <!-- The '[last_*]' keyword is replaced automatically by the          -->
 30:  <!-- specified header if it was present in the last message received  -->
```

```
31:  <!-- (except if it was a retransmission). If the header was not       -->
32:  <!-- present or if no message has been received, the '[last_*]'       -->
33:  <!-- keyword is discarded, and all bytes until the end of the line    -->
34:  <!-- are also discarded.                                              -->
35:  <!--                                                                  -->
36:  <!-- If the specified header was present several times in the         -->
37:  <!-- message, all occurences are concatenated (CRLF seperated)        -->
38:  <!-- to be used in place of the '[last_*]' keyword.                    -->
39:
40:  <send>
41:    <![CDATA[
42:
43:      SIP/2.0 180 Ringing
44:      [last_Via:]
45:      [last_From:]
46:      [last_To:];tag=[call_number]
47:      [last_Call-ID:]
48:      [last_CSeq:]
49:      Contact: <sip:[local_ip]:[local_port];transport=[transport]>
50:      Content-Length: 0
51:
52:    ]]>
53:  </send>
54:
55:  <send retrans="500">
56:    <![CDATA[
57:
58:      SIP/2.0 200 OK
59:      [last_Via:]
60:      [last_From:]
61:      [last_To:];tag=[call_number]
62:      [last_Call-ID:]
63:      [last_CSeq:]
64:      Contact: <sip:[local_ip]:[local_port];transport=[transport]>
65:      Content-Type: application/sdp
66:      Content-Length: [len]
67:
```

```
68:      v=0
69:      o=user1 53655765 2353687637 IN IP[local_ip_type] [local_ip]
70:      s=-
71:      c=IN IP[media_ip_type] [media_ip]
72:      t=0 0
73:      m=audio [media_port] RTP/AVP 0
74:      a=rtpmap:0 PCMU/8000
75:
76:    ]]>
77:  </send>
78:
79:  <recv request="ACK"
80:        optional="true"
81:        rtd="true"
82:        crlf="true">
83:  </recv>
84:
85:  <recv request="BYE">
86:  </recv>
87:
88:  <send>
89:    <![CDATA[
90:
91:      SIP/2.0 200 OK
92:      [last_Via:]
93:      [last_From:]
94:      [last_To:]
95:      [last_Call-ID:]
96:      [last_CSeq:]
97:      Contact: <sip:[local_ip]:[local_port];transport=[transport]>
98:      Content-Length: 0
99:
100:   ]]>
101: </send>
102:
103: <!-- Keep the call open for a while in case the 200 is lost to be     -->
104: <!-- able to retransmit it if we receive the BYE again.               -->
```

```
105:  <pause milliseconds="4000"/>
106:
107:
108:  <!-- definition of the response time repartition table (unit is ms)   -->
109:  <ResponseTimeRepartition value="10, 20, 30, 40, 50, 100, 150, 200"/>
110:
111:  <!-- definition of the call length repartition table (unit is ms)     -->
112:  <CallLengthRepartition value="10, 50, 100, 500, 1000, 5000, 10000"/>
113:
114:</scenario>
115:
```

Ευρετήριο