ΑΛΕΞΑΝΔΡΕΙΟ Τ.Ε.Ι. ΘΕΣΣΑΛΟΝΙΚΗΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πτυχιακή εργασία

«Τεχνολογία VoIP»

Της φοιτήτριας
Γεωργαντζά Σοφίας
Α.Μ: 042589

Επιβλέπων Καθηγητής
Αρσλάνογλου Αχιλλέας

Θεσσαλονίκη 2011

Πρόλογος

Η ιδέα της μεταφοράς μηνυμάτων σε μεγάλες αποστάσεις ξεκίνησε από παλιά, όταν ακόμα οι άνθρωποι προσπαθούσαν με σήματα καπνού να μεταδώσουν κάποια πληροφορία. Πολύ αργότερα άρχισε να αναπτύσσεται η επικοινωνία, ξεκινώντας από τη μετατροπή της φωνής σε ηλεκτρικό σήμα η οποία αποτέλεσε τη βάση για τη λειτουργία της επικοινωνίας με φωνή σε μεγάλη απόσταση (τηλέφωνο, ασύρματος).

Από τη στιγμή που η φωνή μετατράπηκε σε ηλεκτρικό σήμα έπρεπε να βρεθεί ένα κατάλληλο μέσο μεταφοράς του. Γι' αυτό το λόγο, κατασκευάστηκαν τα τηλεφωνικά δίκτυα σε όλο τον κόσμο. Εκτός από αυτά, όμως, έχουν κατασκευαστεί και δίκτυα επικοινωνίας υπολογιστών για την μεταφορά δεδομένων.

Στην ουσία αυτό αποτελεί σπατάλη. Θα μπορούσε να υπάρχει ένα σύστημα μεταφοράς δεδομένων, το οποίο θα μετέφερε πέρα από τα δεδομένα των υπολογιστών και τα «δεδομένα» της ψηφιοποιημένης φωνής. Ακριβώς αυτό άρχισε εδώ και μερικά χρόνια να γίνεται. Αρχικά η προσπάθεια εστιαζόταν στην επικοινωνία με φωνή ανάμεσα σε δύο υπολογιστές, με τη χρήση ειδικού λογισμικού. Με την πάροδο του χρόνου, τα συστήματα βελτιώθηκαν και αναπτύχθηκαν διάφορες τεχνικές, αλγόριθμοι συμπίεσης και διεθνή πρότυπα.

Η τεχνολογία της τηλεφωνικής επικοινωνίας μέσω δικτύων δεδομένων ονομάζεται VoIP (Voice over Internet Protocol). Η τεχνολογία αυτή επιτρέπει την μετάδοση δεδομένων φωνής πάνω από ένα δίκτυο IP. [8]

Περίληψη

Η πτυχιακή αυτή εργασία αναφέρεται στην τεχνολογία VoIP, μια συνεχώς εξελισσόμενη τεχνολογία η οποία αναμένεται μακροπρόθεσμα να αντικαταστήσει το παραδοσιακό τηλεφωνικό δίκτυο.
Οι πρώτες μορφές τηλεπικοινωνίας αναπτύχθηκαν από την ανάγκη μετάδοσης μηνυμάτων μεγάλων αποστάσεων μεταξύ των ανθρώπων. Αρχικά με πρωτόγονες μεθόδους όπως τα σήματα καπνού ή οι φρυκτωρίες και στη συνέχεια με τον

τηλέγραφο και το τηλέφωνο. Σήμερα με την αλματώδη ανάπτυξη των τηλεπικοινωνιών αλλά και των δικτύων δεδομένων οι πληροφορίες-δεδομένα μεταφέρονται μέσω δημόσιων δικτύων από το ένα άκρο στο άλλο όπως γίνεται με τη φωνή και το τηλεφωνικό δίκτυο. Τα δίκτυα δεδομένων διαχειρίζονται πληροφορίες σε ψηφιακή μορφή γι' αυτό και η φωνή, που είναι ένα αναλογικό σήμα, απαιτείται να μετατραπεί σε ψηφιακή μορφή. Αυτή είναι και η αρχή της τεχνολογίας VoIP η οποία βασίζεται στο ψηφιακό σύστημα επικοινωνίας. Επιτρέπει δηλαδή τη μετάδοση φωνής μέσω διαδικτύου, δηλαδή τηλεφωνία μέσω internet.

Για να μπορεί κάποιος χρήστης να πραγματοποιεί κλήσεις με τη χρήση της τεχνολογίας VoIP θα πρέπει να διαθέτει και τον κατάλληλο εξοπλισμό. Εξοπλισμό όπως κατάλληλες τηλεφωνικές συσκευές, voip switches, voip routers, analog telephone adapter (ATA) κα.

Μια απαραίτητη προϋπόθεση για την λειτουργία του VoIP είναι η ποιότητα των υπηρεσιών φωνής και βίντεο που προσφέρει. Η VoIP τεχνολογία παρέχει επικοινωνία σε πραγματικό χρόνο γι' αυτό είναι σημαντικό τα πακέτα δεδομένων που αποστέλλονται να φτάνουν στον προορισμό τους χωρίς να υπάρχουν καθυστερήσεις. Με αυτό ακριβώς το στόχο υλοποιήθηκαν μηχανισμοί που θα βοηθήσουν στη διατήρηση της σταθερής ποιότητας υπηρεσιών.

Σημαντικό κομμάτι της VoIP τεχνολογίας είναι τα πρωτόκολλα που χρησιμοποιεί για να πραγματοποιήσει μια κλήση. Υπάρχουν πρωτόκολλα που αναλαμβάνουν τη σηματοδοσία, πρωτόκολλα που βοηθούν στον έλεγχο των κλήσεων αλλά και πρωτόκολλα που χρησιμοποιούνται για την ενθυλάκωση των δεδομένων ήχου και βίντεο σε IP πακέτα.

Προβλήματα ασφαλείας υπάρχουν σε όλες τις μορφές των τηλεπικοινωνιών. Έτσι και η επικοινωνία μέσω της τεχνολογίας VoIP απειλείται από κινδύνους. Κίνδυνοι που αποτελούν τροχοπέδη στη διαφύλαξη της ασφάλειας των μεταδιδόμενων πληροφοριών. Για την εξάλειψη των κινδύνων αυτών έχουν αναπτυχθεί τεχνολογίες, όπως της κρυπτογράφησης, για τη διαφύλαξη και τη διατήρησή της ακεραιότητας των μεταδιδόμενων δεδομένων.

Το VoIP είναι μια τεχνολογία που παρουσιάζει πολλά πλεονεκτήματα. Αυτό ακριβώς είναι που βοήθησε και στην ανάπτυξη της. Από την άλλη όπως είναι φυσικό υπάρχουν και μειονεκτήματα. Τα μειονεκτήματα αυτά όμως σε καμία περίπτωση δεν είναι ικανά να σταματήσουν την εξάπλωση του VoIP. Μια εξάπλωση η οποία θα είναι ραγδαία τα επόμενα χρόνια καθώς ήδη υπάρχουν προοπτικές για μελλοντική

εξέλιξη.

Abstract

VoIP is an evolving technology which is about to replace the traditional telephone services (POTS).

The need of broadcasting long distance messages was the main reason of the development of telecommunications. At first, with primitive methods, such as smoke signs or beacon-signals or lately with the telegraph or the telephone. Nowadays the rapid development of telecommunications and data networks has lead to the transfer of information – data through public networks. Typical example is the voice and the traditional telephone system. Public networks use data in digital form. That's the reason why voice, which is an analog signal, has to be converted into a digital form before it's been transmited through a data network. That is exactly was VoIP technology does to achive voice transfer through a data network or a network of data networks such as the Internet.

In order to make phone calls using VoIP technology a user must have the appropriate equipment. VoIP telephones, VoIP swiches, VoIP routers, analog telephone adapters are devises that are need.

The quality of voice and video services is one of the most important things VoIP calls have to offer. VoIP technology offers real time communication so it's crusial that data packets that are being transmited get to their final destination with no delay. There are several mechanisms developed to keep the quality of VoIP service in a good level.

A very important part of VoIP technology is the protocols that are being used to make a call. There are protocols that are responsible for signaling, protocols that control the calls and other protocols that are used to encapsulate voice data into IP packets.

All forms of telecommunications have their safety issues. So communicating through VoIP has also it's dangers. These dangers have made essential the development of technologies like encryption in order to secure the transmited data.

VoIP is a technology that has many advantages. That's the main reason of it's

development. On the other hand has also some disadvantages. There is no way though these disadvantages can stop the spreading of VoIP because there are already perspectives for future development.

Πίνακας Περιεχομένων

Κεφάλαιο 1

1.1 Αναφορά στις τηλεπικοινωνίες

Με τον όρο επικοινωνία εννοούμε την αποστολή ενός μηνύματος από ένα σημείο σε ένα άλλο, καθώς και την επιβεβαίωση της πλήρους, ορθής και κατανοητής λήψης του από τον παραλήπτη.

Παρουσιάζεται όμως και μία διαφοροποίηση μεταξύ των όρων *επικοινωνία* και *τηλεπικοινωνία*. Με τον όρο τηλεπικοινωνία εννοούμε την «επικοινωνία» σε μακρινές αποστάσεις.

Οι τηλεπικοινωνίες μεταξύ των ανθρώπων ξεκίνησαν από πολύ παλιά όταν ακόμα χρησιμοποιούσαν σήματα καπνού, ήχους τυμπάνων, άναμμα φωτιάς για να μπορέσουν να μεταδώσουν κάποια πληροφορία. Το σημαντικότερο μέσο μετάδοσης για την εποχή και το οποίο διατηρήθηκε για αρκετό καιρό (11^{o}-18^{o} αιώνα π. χ) ήταν οι φρυκτωρίες όπου με το άναμμα της φωτιάς από φρυκτωρία σε φρυκτωρία μετέδιδαν τον κίνδυνο.

Οι τρόποι όμως αυτοί της επικοινωνίας δεν ήταν ούτε ακριβείς αλλά ούτε και διέθεταν την βεβαιότητα της επιτυχίας. Παράλληλα η ταχύτητα μεταφοράς της πληροφορίας ήταν αρκετά μικρή, ο όγκος της πληροφορίας ελάχιστος όπως και η ασφάλεια της.

Οι πρωτόγονες αυτές μορφές επικοινωνίας διατηρήθηκαν στο χρόνο μέχρι την εμφάνιση του ηλεκτρισμού. Τότε έγιναν τα πρώτα σοβαρά βήματα με το τηλέφωνο και τον τηλέγραφο, για να φθάσουμε στη σημερινή μορφή της ψηφιακής τεχνολογίας, οπότε και η καθημερινή εξέλιξη στις τεχνικές των τηλεπικοινωνιών είναι αλματώδης και έξω από κάθε πρόβλεψη.

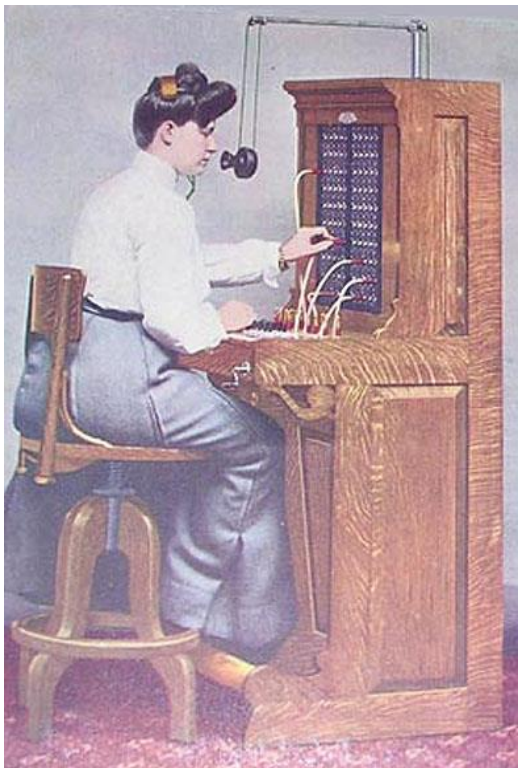
Από τον καιρό που ο ηλεκτρισμός και η ηλεκτρονική εξελίχθηκαν πολλά άλλαξαν στις τηλεπικοινωνίες οι οποίες έγιναν τεχνολογική επιστήμη. Ο Samuel Morse το 1854 με τον τηλέγραφο και ο Graham Bell το 1876 με το τηλέφωνο(Σχήμα 1.1) έθεσαν τα θεμέλια μιας νέας εποχής στον κόσμο, μιας εποχής όπου οι τηλεπικοινωνίες θα έπαιζαν πλέον βασικό ρόλο στην ανάπτυξή του.

Εικόνα 1.1: Το 1^{ο} τηλέφωνο

Θέτοντας για πρώτη φορά σε πρακτική εφαρμογή το τηλέφωνο ο Graham Bell, συνομιλούσε ο ίδιος με έναν φίλο του μέσω δύο τηλεφωνικών συσκευών και μιας γραμμής. Όταν όμως και άλλοι φίλοι του ήθελαν να έχουν το ίδιο προνόμιο, ο Bell για κάθε τέτοια σύνδεση διέθετε από δύο τηλεφωνικές συσκευές και από μία γραμμή. Έτσι ο ίδιος που μπορούσε να μιλήσει με όλους, είχε στο σπίτι του τόσες συσκευές όσες και οι συνδέσεις, ενώ παράλληλα ο ίδιος αριθμός γραμμών ξεκινούσε από το σπίτι του με προορισμό τους φίλους του.

Όσο όμως ο αριθμός των χρηστών μεγάλωνε τόσο μεγάλωνε και ο αριθμός συσκευών και των γραμμών όπου η κατάσταση αυτή δεν μπορούσε να συνεχιστεί. Έτσι προέκυψε η ανάγκη του δικτύου. Η λύση του προβλήματος πέρασε από τότε πολλά στάδια. Δημιουργήθηκαν τα πρώτα τηλεφωνικά κέντρα(Σχήμα 1.2), στα οποία κάθε συνδρομητής συνδεόταν ακτινωτά με μία αφιερωμένη γραμμή και μία συσκευή. Την εποχή εκείνη οι τηλεφωνήτριες χειρίστριες των κέντρων συνέδεαν την γραμμή του καλούντος συνδρομητή με αυτή του καλούμενου με τη βοήθεια βυσμάτων.

Αυτή ήταν και η πρώτη μορφή δικτύου επικοινωνιών φωνής. Στη συνέχεια η τεχνολογία των τηλεφωνικών κέντρων προόδευσε με την ανάπτυξη των ηλεκτρομηχανικών τηλεφωνικών κέντρων και τη χρήση της αυτόματης επιλογής. Ακολούθησε η ανάπτυξη των ηλεκτρονικών κέντρων για να καταλήξουμε στη σημερινή χρήση υπολογιστικών συστημάτων.[20]



Εικόνα 1.2 : Τηλεφωνικό κέντρο

Καθώς όμως το τηλέφωνο εξελισσόταν και έπαιρνε όλο και σημαντικότερη θέση στην καθημερινότητα των ανθρώπων, είχαν ήδη αρχίσει να γίνονται τα πρώτα βήματα για μια από τις σημαντικότερες ανακαλύψεις του 20^{ού} αιώνα, το Διαδίκτυο (Internet).

1.2 Δίκτυα δεδομένων

Παράλληλα με την παραπάνω εξέλιξη των τηλεπικοινωνιών σημειώθηκε ταυτόχρονα και ο εκσυγχρονισμός των δικτύων δεδομένων.

Το μεγάλο κόστος των ιδιωτικών δικτύων τόσο σε γραμμές επικοινωνίας όσο και σε εξοπλισμό (κόμβους κλπ) οδήγησε στην ανάπτυξη των δημόσιων δικτύων δεδομένων. Στην πράξη συναντάμε δύο τύπους δημοσίων δικτύων δεδομένων. Τα δίκτυα μεταγωγής πακέτων (packet switching) που χρησιμοποιούν X.25 τεχνική και Frame Relay και τα ψηφιακά δίκτυα που παρέχουν υπηρεσίες φορέα προσφέροντας point-to-point ψηφιακές γραμμές. Στην πρώτη κατηγορία ανήκει το δίκτυο Hellaspac και στη δεύτερη το Hellascom.

Τα δημόσια δίκτυα μεταγωγής πακέτων εκτός από μόνιμες συνδέσεις, προσφέρουν τη δυνατότητα στους συνδρομητές τους να συνδέονται κατ’ επιλογή με άλλους και

να μεταφέρουν δεδομένα από ένα σημείο σε άλλο, όπως ακριβώς γίνεται με τη φωνή και το τηλεφωνικό δίκτυο.
Κάθε τερματικό σημείο οφείλει να έχει αυστηρά καθορισμένο τρόπο σύνδεσης (interface) με το δημόσιο δίκτυο και να υπακούει στους κανόνες που έχει θέσει το δημόσιο δίκτυο.
Τα δημόσια δίκτυα μεταγωγής πακέτων λειτουργούν σε πολλές χώρες, έχουν τέτοια δυνατότητα να συνδέονται και μεταξύ τους για διεθνείς επικοινωνίες. Γνωστά δημόσια δίκτυα μεταγωγής πακέτων παρεμφερή του Hellaspac είναι τα Transpac (Γαλλία) και EPSS (Αγγλία).

1.2.1 Δίκτυα μεταγωγής (Switching)

Κύριο χαρακτηριστικό των δικτύων αυτών είναι η δυνατότητα του κάθε συνδρομητή να καλεί επιλογικά τον ανταποκριτή του. Τα δίκτυα μεταγωγής αποτελούνται από κόμβους συνδεδεμένους μεταξύ τους οι οποίοι αναλαμβάνουν τη δρομολόγηση της εκπεμπόμενης από τον εκάστοτε αποστολέα πληροφορίας. Δεδομένα που εισέρχονται στο δίκτυο από κάποιον τερματικό σταθμό, δρομολογούνται από κόμβο σε κόμβο μέχρι τον προκαθορισμένο δέκτη. Μερικοί κόμβοι δεν έχουν συνδεδεμένους τερματικούς σταθμούς, απλά παίζουν το ρόλο του διεκπεραιωτή πληροφορίας. Για λόγους αύξησης της αξιοπιστίας οι συνδέσεις των κόμβων γίνονται με τέτοιο τρόπο ώστε να υπάρχει εναλλακτικός δρόμος μεταξύ των τερματικών σημείων. Τα δίκτυα μεταγωγής συνήθως προσφέρονται από τους οργανισμούς τηλεπικοινωνιών.
Υπάρχουν τρεις βασικοί μέθοδοι αποκατάστασης σύνδεσης δύο τερματικών σταθμών στα δίκτυα μεταγωγής.

- Μεταγωγή κυκλώματος (Circuit Switching)
- Μεταγωγή μηνυμάτων (Message Switching)
- Μεταγωγή πακέτων (Packet Switching)

1.2.1.1 Μεταγωγή κυκλώματος (Circuit Switching)

Η μεταγωγή κυκλώματος είναι τεχνική κατά την οποία αφιερώνεται μία φυσική ζεύξη μεταξύ των συνδρομητών για όλη τη διάρκεια της επικοινωνίας τους. Η σύνδεση είναι τμηματική και αποτελείται από τμήματα γραμμών που συνδέουν τους

διάφορους κόμβους του δικτύου. Με τη μεταγωγή κυκλώματος κάθε γραμμή που καταλαμβάνεται για μία σύνδεση απασχολείται πλήρως και αποκλειστικά με την επικοινωνία των δύο συνδρομητών. Κλασικό παράδειγμα αυτού του είδους τεχνικής είναι το κοινό τηλεφωνικό δίκτυο.

Στην περίπτωση της μεταγωγής κυκλώματος η γραμμή παραμένει κατειλημμένη ακόμα και κατά τα χρονικά διαστήματα όπου δεν μεταφέρονται δεδομένα. Έχει αποδειχθεί στατιστικά ότι ο κενός χρόνος σε μία σύνδεση τερματικών σημείων είναι σχετικά μεγάλος.

Όμως με την τεχνική circuit switching έχουμε το πλεονέκτημα ότι σε μία αποκατασταθείσα σύνδεση οι χρήστες μπορούν να χρησιμοποιήσουν όλη τη μεταφορική ικανότητα της γραμμής, με μόνη καθυστέρηση το μικρό χρόνο μετάβασης και την αρχική καθυστέρηση για την αποκατάσταση της σύνδεσης.

1.2.1.2 Μεταγωγή μηνυμάτων (Message Switching)

Με αυτή την τεχνική ο αποστολέας οργανώνει την προς μετάδοση πληροφορία σε μήνυμα που το δίνει στο δίκτυο για να προωθηθεί από κόμβο σε κόμβο μέχρι τον τελικό παραλήπτη.

Η τεχνική μεταγωγής μηνυμάτων αναλαμβάνει τη διεκπεραίωση των μηνυμάτων και όχι την αποκατάσταση του φυσικού δρόμου. Το δίκτυο εκμεταλλεύεται τις φυσικές συνδέσεις μεταξύ των κόμβων για την αποστολή μηνυμάτων όλων των συνδρομητών. Σε κάθε μήνυμα είναι σημειωμένη η διεύθυνση του παραλήπτη, έτσι ώστε ο κάθε κόμβος να το προωθεί στον επόμενο όταν βρει ελεύθερο κανάλι.

Οι κόμβοι ενός δικτύου μεταγωγής μηνυμάτων δεν είναι απλώς ένα ηλεκτρομηχανικό κέντρο που συνδέει κανάλια για να περάσει το μήνυμα, αλλά υπολογιστές επικοινωνιών με αρκετό χώρο μνήμης προκειμένου να αποθηκεύσουν τα μηνύματα που λαμβάνουν πριν τα αποστείλουν στον επόμενο κόμβο. Σε κάθε έναν από τους κόμβους αυτούς το μήνυμα καθυστερεί γιατί πρέπει να παραληφθεί πρώτα στο σύνολο του και μετά να βρεθεί ο κατάλληλος κενός δρόμος για την περαιτέρω αποστολή του.

1.2.1.3 Μεταγωγή πακέτων (Packet Switching)

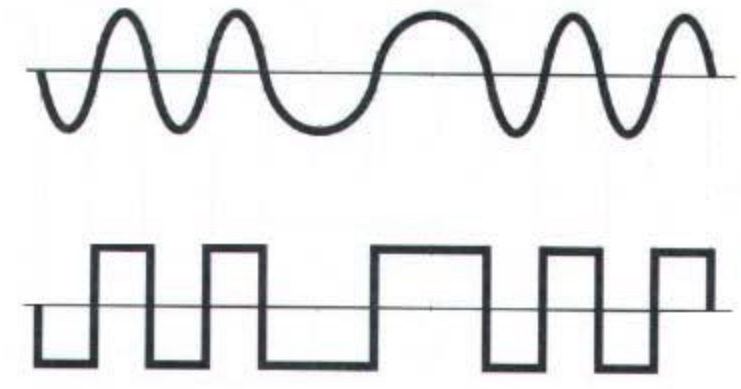
Με την τεχνική μεταγωγής πακέτων το κάθε μήνυμα που πρέπει να μεταφερθεί μέσω ενός τέτοιου δικτύου τεμαχίζεται σε πακέτα. Το μήκος των πακέτων είναι μικρό, συνήθως 128 ή 256 χαρακτήρες. Οι κόμβοι οφείλουν να έχουν επεξεργαστική ικανότητα για την προώθηση των πακέτων. Οι μέθοδοι προώθησης των πακέτων είναι δύο:

- Datagram
- Virtual Circuit

Με τη μέθοδο datagram τα πακέτα ενός μηνύματος θα φθάσουν στον παραλήπτη χρησιμοποιώντας το καθένα το δικό του συντομότερο δρόμο.
Η τεχνική αυτή συναντάται και με τον όρο connectionless με τυπικό παράδειγμα το πρωτόκολλο IP. Τα πακέτα ενώ έχουν τον ίδιο προορισμό δεν ακολουθούν όλα τον ίδιο δρόμο και λόγω αυτού υπάρχει η πιθανότητα να φθάσουν με διαφορετική σειρά από αυτή που ξεκίνησε. Ως εκ τούτου η τεχνική αυτή έχει μειωμένη αξιοπιστία οπότε απαιτείται από τους τελικούς σταθμούς του δικτύου η χρήση πρόσθετων πρωτοκόλλων ανωτέρων επιπέδων. Τυπικό παράδειγμα είναι το πρωτόκολλο TCP πάνω από τα δίκτυα IP.
Με τη μέθοδο virtual circuit (νοητού κυκλώματος), πριν αποσταλούν τα πακέτα αποκαθίσταται μία σταθερή νοητή σύνδεση μεταξύ των δύο τερματικών σταθμών από όπου στη συνέχεια θα περάσουν όλα τα πακέτα του μηνύματος. Για το λόγο αυτό η τεχνική αυτή ονομάζεται connection oriented.[20]

1.3 Ψηφιακή μετάδοση αναλογικών σημάτων (κωδικοποίηση φωνής)

Τα δίκτυα δεδομένων που αναπτύξαμε παραπάνω διαχειρίζονται δεδομένα σε ψηφιακή μορφή. Η φωνή είναι ένα αναλογικό σήμα άρα για την μετάδοση φωνής μέσω κάποιου δικτύου δεδομένων απαιτείται η μετατροπή της σε ψηφιακή μορφή.



Σχήμα 1.1 : Αναλογικό και ψηφιακό σήμα

Η πιο διαδεδομένη τεχνική μετατροπής αναλογικού σήματος σε ψηφιακή μορφή είναι η διαμόρφωση πλάτους παλμών και ειδικότερα η παλμοκωδική διαμόρφωση PCM (Pulse Code Modulation).

Η δειγματοληψία ή αλλιώς διαμόρφωση πλάτους παλμών είναι γνωστή ως PAM (Pulse Amplitude Modulation). Το ύψος των σταθερής διάρκειας και θέσης παλμών είναι ανάλογο με το πλάτος του αναλογικού σήματος. Κάθε δείγμα του σήματος PAM οδηγείται σε έναν μετατροπέα αναλογικού / ψηφιακού σήματος (A/D Converter) και αναπαρίσταται με έναν αριθμό από ένα bit.

Η διαμόρφωση PCM χρησιμοποιεί δειγματοληψία 8000 δειγμάτων το δευτερόλεπτο και μετατροπή κάθε δείγματος σε δυαδικό κώδικα. Ο αριθμός των bit που μεταδίδεται για κάθε δείγμα είναι σταθερός (συνήθως 8), η δυαδική τιμή όμως της σειράς των bit αυτών μας δίνει την τιμή του πλάτους του αναλογικού σήματος τη στιγμή της δειγματοληψίας. Τα bit αυτά εκπέμπονται προς το δέκτη όπου μετατρέπονται πάλι σε αναλογικό σήμα.

1.4 Πολυπλεξία

Με τη ραγδαία αύξηση των χρηστών των τηλεπικοινωνιών δημιουργήθηκε η ανάγκη για εξοικονόμηση τηλεφωνικών γραμμών και συσκευών. Για την κάλυψη αυτής της ανάγκης αναπτύχθηκε η τεχνική της πολυπλεξίας. Πολυπλεξία ονομάζεται η τεχνική κατά την οποία δεδομένα από πολλούς χρήστες συμπιέζονται σε ένα φυσικό κανάλι μετάδοσης.

Γνωστοί τύποι πολυπλεξίας είναι:

- Πολύπλεξη Χρόνου- TDM (Time Division Multiplexing)
- Πολύπλεξη Συχνότητας- FDM (Frequency Division Multiplexing)

- Πολύπλεξη Κώδικα- CDM (Code Division Multiplexing)
- Πολύπλεξη Μήκους Κύματος- WDM (Wavelength Division Multiplexing)[20]

1.5 Τι είναι το VoIP

Μία νέα αλλά και με μεγάλο ρυθμό ανάπτυξης τεχνολογία που βασίζεται στο ψηφιακό σύστημα επικοινωνίας είναι η τεχνολογία VoIP. Η τεχνολογία αυτή είναι ένας τρόπος επικοινωνίας σε πραγματικό χρόνο που έχει φέρει καινοτομικές αλλαγές στην κόσμο της τηλεφωνίας.

Το VoIP (Voice Over IP) είναι τεχνολογία που μας επιτρέπει την μετάδοση φωνής μέσω διαδικτύου - με άλλα λόγια την τηλεφωνία μέσω Internet.
Είτε με κάποιο ειδικό πρόγραμμα στον υπολογιστή μας (softphone), είτε με κάποια ειδική VoIP τηλεφωνική συσκευή, μπορούμε να λαμβάνουμε και να πραγματοποιούμε τηλεφωνικές κλήσεις με πολύ χαμηλότερο κόστος από την συμβατική τηλεφωνία (POTS).

Με την πάροδο του χρόνου οι παραδοσιακές τηλεφωνικές γραμμές αποσύρονται σταδιακά καθώς οι επιχειρήσεις αλλά και ένας μεγάλος αριθμός σπιτιών παγκοσμίως αποδέχονται τα οφέλη και τις υπηρεσίες που τους προσφέρει η VoIP τεχνολογία.
Η τεχνολογία VoIP χρησιμοποιεί ως μέθοδο αποκατάστασης συνδεσης τη μεταγωγή πακέτων (Packet Switching) έναντι των τηλεφωνικών συστημάτων (POTS) που χρησιμοποιούνται στο PSTN δίκτυο και χρησιμοποιούν την τεχνική μεταγωγής κυκλώματος (Circuit Switching).

1.7 Αναδρομή στο VoIP

Το 1973 χρησιμοποιήθηκαν για πρώτη φορά Voice over IP πρωτόκολλα για τη μετάδοση σημάτων φωνής πάνω από IP δίκτυα. Πρόκειται για μια πραγματική υλοποίηση του δικτυακού πρωτοκόλλου φωνής (Network Voice Protocol) της εταιρίας APRANET. Πολύ αργότερα, το 1995, μια μικρή εταιρία με όνομα Vocaltec έθεσε σε κυκλοφορία στη αγορά το πρώτο δικτυακό λογισμικό τηλεφώνου. Το λογισμικό σχεδιάστηκε ώστε να τρέχει σε ηλεκτρονικούς υπολογιστές και

χρησιμοποιούσε κάρτες ήχου και μικρόφωνο. Η ονομασία της υπηρεσίας ήταν “Internet Phone” και χρησιμοποιούσε το H.323 πρωτόκολλο σε αντίθεση με το SIP πρωτόκολλο που επικρατεί σήμερα. Η Vocaltec είχε αρχικά μεγάλη επιτυχία με το “Internet Phone”. Ένα μεγάλο όμως μειονέκτημα ήταν η έλλειψη ευρυζωνικής διαθεσιμότητας και συνεπώς για το λογισμικό χρησιμοποιήθηκαν modems. Το γεγονός αυτό, είχε ως αποτέλεσμα την παροχή χαμηλής ποιότητας φωνής σε σύγκριση με την μετάδοση της φωνής σε μια κανονική τηλεφωνική κλήση. Παρόλα αυτά όμως το “Internet Phone” αποτέλεσε ορόσημο καθώς αντιπροσωπεύει το πρώτο IP τηλέφωνο.

Μέχρι το 1998, έρευνες έδειξαν ότι το 1% του πληθυσμού της Αμερικής χρησιμοποιούσε τη VoIP τεχνολογία. Η σταδιακή αποδοχή της από το ευρύ κοινό οδήγησε την κατασκευή συσκευών που υποστηρίζουν επικοινωνία από PC-to-phone και από phone-to-phone. Διάφοροι κατασκευαστές του διαδικτύου, όπως η Cisco, εισήγαγαν εξοπλισμό που μπορούσε να δρομολογήσει και να μεταγάγει την VoIP κίνηση. Ως αποτέλεσμα, το 2000, η VoIP κίνηση υπολογιζόταν να αποτελεί το 3% της παγκόσμιας κυκλοφορίας φωνής.

Σήμερα περισσότεροι από 600 εκατομύρια άνθρωποι σε όλο τον κόσμο χρησιμοποιούν τεχνολογίες VoIP για την επικοινωνία τους, είτε το ξέρουν (Skype) είτε δεν το ξέρουν (εναλλακτικοί πάροχοι). Το VoIP λειτουργεί είτε μόνο για εξερχόμενες κλήσεις, είτε και για εισερχόμενες με χρήση κανονικού τηλεφωνικού αριθμού (DID). [10]

Μέσα στο 2009 έκαναν την εμφάνιση τους και οι πρώτες ελληνικές εταιρείες που παρέχουν ελληνικά νούμερα για χρήση με VoIP υπηρεσίες, που εκτός από εξερχόμενες κλήσεις δέχονται και εισερχόμενες από όλους σχεδόν τους τηλεπικοινωνιακούς παρόχους. Παραδείγματα τέτοιων εταιρειών είναι η Viva και η Omnivoice.

Σήμερα, σημαντικά ζητήματα που αφορούν την ποιότητα φωνής έχουν διευθετηθεί και η VoIP κίνηση μπορεί να έχει προτεραιότητα έναντι της κίνησης δεδομένων ώστε να εξασφαλισθούν αξιόπιστες, υψηλής ποιότητας ήχου και μη διακοπτόμενες τηλεφωνικές κλήσεις. Το γεγονός αυτό οφείλεται στην δυνατότητα πραγματοποίησης απεριόριστων κλήσεων χαμηλού κόστους καθώς και στην αφθονία των βελτιωμένων και χρήσιμων υπηρεσιών τηλεφωνίας που σχετίζονται με την VoIP τεχνολογία.

Στην πραγματικότητα, πρόκειται για φαινομενικούς ρυθμούς ανάπτυξης και σε συνδυασμό με την εισαγωγή της *Video over IP* τεχνολογίας, το μέλλον του VoIP διαγράφεται εξαιρετικά συναρπαστικό και δίνει την δυνατότητα στο ευρύ κοινό να απολαύσει προϊόντα και υπηρεσίες που πρόγονοί μας δεν θα πίστευαν ποτέ ότι ήταν εφικτά.

Κεφάλαιο 2

2.1 Πώς λειτουργεί το VoIP;

Η τεχνολογία VoIP διαχειρίζεται τη φωνή όπως και κάθε άλλη πληροφορία που αποστέλλεται μέσω Διαδικτύου, μετατρέποντας την σε πακέτα δεδομένων, τα οποία στη συνέχεια συμπιέζονται και αποστέλλονται μέσω του Internet σε υψηλές ταχύτητες. Όταν τα δεδομένα φθάσουν στον προορισμό τους, περνούν από την αντίστροφη διαδικασία της αποσυμπίεσης και τη μετατροπή σε αναλογικό σήμα. Ακόμα κι αν αυτό φαίνεται περίπλοκο, η όλη διεργασία πραγματοποιείται σε πραγματικό χρόνο, κάτι που σημαίνει ότι δεν θα υπάρξει καμία καθυστέρηση μεταξύ των δύο ομιλητών. [7]

Αν θα θέλαμε τώρα να δούμε τη διαδικασία αυτή με λίγη περισσότερη λεπτομέρεια θα μπορούσαμε να πούμε ότι από τη στιγμή που κάποιος χρήστης αποφασίσει να καλέσει κάποιον άλλο χρησιμοποιώντας την τεχνολογία VoIP μια σειρά πρωτοκόλλων αναλαμβάνουν να φέρουν εις πέρας αυτή την αποστολή.

Πριν ακόμη γίνει κάποια ανταλλαγή δεδομένων φωνής ή βίντεο μεταξύ των χρηστών θα πρέπει να βρεθεί ο απομακρυσμένος χρήστης, να γίνει μια «διαπραγμάτευση» και να συμφωνηθούν οι λεπτομέρειες για τον τρόπο μετάδοσης των δεδομένων μεταξύ των δύο χρηστών. Τα δημοφιλέστερα πρωτόκολλα που πραγματοποιούν αυτή τη διαδικασία είναι το H.323 και το SIP (Session Initiation Protocol).

Από τη στιγμή που έχει αποκατασταθεί η σύνδεση μεταξύ των απομακρυσμένων χρηστών το πρωτόκολλο σηματοδοσίας χρησιμοποιεί το πρωτόκολλο RTP για να ενθυλακώσει τα δεδομένα ήχου ή βίντεο σε πακέτα UDP έτσι ώστε αυτά να δρομολογηθούν μέχρι τον άλλο συνομιλητή.

Καθ' όλη τη διάρκεια της συνομιλίας πραγματοποιούνται αποστολές δεδομένων εκατέρωθεν, που έχουν να κάνουν με τη διατήρηση και τη ρύθμιση της σύνδεσης. Τα δεδομένα αυτά αποστέλλονται από το πρωτόκολλο RVP (Remote Voice Protocol) Control Protocol.
Τη στιγμή όπου κάποιος από τους συνομιλητές θελήσει να τερματίσει τη συνομιλία το πρωτόκολλο σηματοδοσίας που χρησιμοποιείται αναλαμβάνει να τερματίσει τη σύνδεση μεταξύ τους.[36][37]

2.2 Εξοπλισμός VoIP

Για να μπορέσει κάποιος χρήστης να χρησιμοποιήσει την τεχνολογία VoIP θα πρέπει να προμηθευτεί κάποιον εξοπλισμό. Ο εξοπλισμός αυτός δεν είναι ούτε ακριβός, ούτε και δύσκολο να αποκτηθεί.

1.Σύνδεση στο internet

Το πιο βασικό αυτών που χρειάζεται κάποιος είναι μια υψηλής ταχύτητας σύνδεση στο Internet (πχ μιας ADSL σύνδεσης). Αν κάποιος έχει ήδη μια ADSL σύνδεση μπορεί να την χρησιμοποιήσει χωρίς καμία απολύτως τροποποίηση. Παρότι δεν είναι απαγορευτική η χρήση σύνδεσης χαμηλότερης ταχύτητας (πχ dial up σύνδεσης), είναι προτιμότερη και πιο αξιόπιστη η χρήση ADSL σύνδεσης. Η τεχνολογία VoIP δεν μπορεί να λειτουργήσει το ίδιο αποδοτικά με μια dial up σύνδεση γιατί απλούστατα δεν είναι αρκετά γρήγορη έτσι ώστε να μεταφέρει τον όγκο πληροφορίας που απαιτείται. [11]

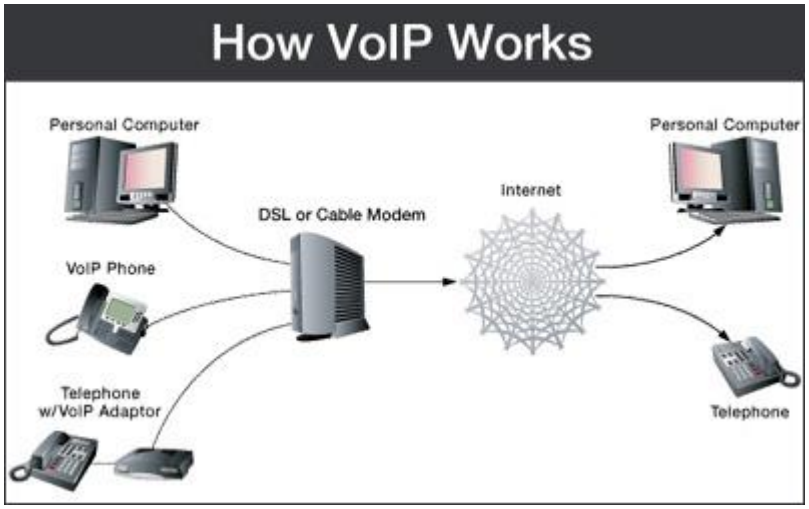
2.Τηλεφωνική συσκευή

Θα χρειαστεί μία τηλεφωνική συσκευή συμβατή με το VoIP. Τα VoIP τηλέφωνα είναι αυτά που μας επιτρέπουν τη λήψη και την πραγματοποίηση κλήσεων χρησιμοποιώντας το διαδίκτυο και την τεχνολογία VoIP.

Τα VoIP τηλέφωνα μπορούμε να τα συναντήσουμε σε δυο μορφές:

- **Εικονικό τηλέφωνο (SoftPhone):** Το εικονικό τηλέφωνο είναι μια εφαρμογή η οποία χρησιμοποιείται για να γίνονται τηλεφωνικές κλήσεις με τη χρήση ηλεκτρονικού υπολογιστή με μικρόφωνο και ακουστικά χωρίς τη χρήση τηλεφωνικής συσκευής. Με άλλα λόγια προσομοιώνει την τηλεφωνική συσκευή στην οθόνη ενός υπολογιστή. Πολύ συχνά η διεπαφή αυτών των εφαρμογών παρουσιάζει ένα panel τηλεφώνου με κουμπιά στο οποίο ο χρήστης μπορεί να πατήσει και να πραγματοποιήσει μια κλήση.

- **VoIp τηλεφωνικές συσκευές (Hardware Phones):** είναι συσκευές (ασύρματες ή ενσύρματες) σαν τις απλές αναλογικές με την μόνη διαφορά ότι χρησιμοποιούν το πρωτόκολλο SIP και έτσι μας επιτρέπουν να πραγματοποιούμε και να δεχόμαστε κλήσεις μέσω του διαδικτύου. Μερικές από αυτές συνδέονται μέσω Ethernet στο router ενώ άλλες μέσω USB στον Η/Υ. Επίσης αρκετές συνδέονται και με την απλή αναλογική γραμμή ενώ άλλες όχι. Επίσης υπάρχουν και WiFi VoIP συσκευές οι οποίες μπορούν να λειτουργήσουν χωρίς να συνδεθούν καλωδιακά με το Adsl Router. [10]



Εικόνα 2.1: Σύνδεση Συσκευών VoIP

3.VoIP Switches

Είναι συσκευές που επιτρέπουν σε πολλαπλές γραμμές τηλεφώνου να συνδεθούν σε μία θύρα Ethernet. Αυτό επιτρέπει σε όποιο τηλέφωνο είναι

συνδεδεμένο στο switch να εκτελεί κλήσεις VoIP.

4.Πύλες VoIP

Οι πύλες VoIP συνδέουν δίκτυα VoIP σε δίκτυα PSTN. Υπάρχουν δύο μεγάλες κατηγορίες πυλών. Οι VoIP Gateways και τα Analog Telephone Adapters(ATA).

5.VoIP Gateway(Πύλη VoIP)

Μία πύλη VoIP, ή αλλιώς φωνή μέσω πύλης IP (Voice over IP Gateway),είναι μία συσκευή δικτύου που βοηθάει τη μετατροπή της φωνής και των κλήσεων fax, σε πραγματικό χρόνο, μεταξύ ενός δικτύου IP και του Public Switched Telephone Network (PSTN). Είναι μία πύλη υψηλών επιδόσεων κατασκευασμένη ειδικά για εφαρμογές Voice over IP. Έχουν τη δυνατότητα να υποστηρίξουν τουλάχιστον δύο T1/E1 ψηφιακά κανάλια. Οι περισσότερες πύλες VoIP έχουν τουλάχιστον μία πόρτα Ethernet και μία τηλεφωνική πόρτα. Η ρύθμιση μιας πύλης γίνεται με τη βοήθεια διαφόρων πρωτοκόλλων όπως MGCP,SIP, IAX ή LTP.

Το μεγαλύτερο πλεονέκτημα μιας πύλης VoIP είναι ότι παρέχει σύνδεση με το υπάρχον τηλεφωνικό δίκτυο (στην Ελλάδα, το τηλεφωνικό δίκτυο του Ο.Τ.Ε). Συνδέει τηλεφωνικές συσκευές καθώς και συσκευές fax που βρίσκονται ήδη συνδεδεμένες με τηλεφωνικά δίκτυα και τηλεφωνικά κέντρα. Όλο αυτό κάνει τη διαδικασία της πραγματοποίησης μιας κλήσης μέσω του IP δικτύου οικεία στους νέους. Οι πύλες μπορούν να τερματίσουν μια κλήση από την τηλεφωνική τους συσκευή, μπορούν να παρέχουν διαδραστικότητα μέσω συστήματος IVR (Interactive Voice Response) ή ακόμη να ηχογραφήσουν μια κλήση. Ακόμη βοηθούν στο να κατευθύνουν κλήσεις από έξω (δηλαδή, δίκτυο Ο.Τ.Ε.) σε συγκεκριμένο προορισμό, ή μπορούν να τερματίσουν μια κλήση από άλλη πύλη και να τη στείλουν στο δίκτυο PSTN.

Οι κυριότερες λειτουργίες μιας VoIP πύλης, συμπεριλαμβάνουν τη συμπίεση ή την αποσυμπίεση φωνής και fax, τον έλεγχο για τη σηματοδοσία, τη δρομολόγηση κλήσεων και τη δημιουργία πακέτων δεδομένων. Οι VoIP πύλες είναι ακόμη εφοδιασμένες με επιπλέον δυνατότητες όπως εξόδους προς άλλους ελεγκτές, όπως Gatekeepers ή Softswitches ή συστήματα χρεώσεων.

Εικόνα 2.2: VoIP Gateway

6. Analog Telephone Adapter

Υπάρχει η δυνατότητα να χρησιμοποιούμε τη συσκευή που ήδη έχουμε, αυτό μπορεί να γίνει με τη χρήση ενός Analog Telephone Adapter(ATA). Είναι μία ηλεκτρονική συσκευή που χρησιμοποιείται για να επιτρέψει απλές αναλογικές τηλεφωνικές συσκευές ή μηχανήματα fax να δουλέψουν για VoIP κλήσεις. Το ATA δημιουργεί μια φυσική σύνδεση με τη χρήση μιας τηλεφωνικής συσκευής και ενός καλωδίου δικτύου μεταξύ μιας συμβατικής τηλεφωνικής συσκευής ή μηχανήματος fax και ενός υπολογιστή ή μιας πύλης Ethernet. Το ATA καταστεί δυνατό την πραγματοποίηση κλήσεων και fax μέσω του Internet χωρίς ο χρήστης να αναβαθμίσει τον υπάρχοντα τηλεφωνικό του εξοπλισμό.
Αμέσως οι συσκευές αυτές έχουν μεγάλο πλεονέκτημα λόγω κόστους. Στοιχίζει λιγότερο να πραγματοποιήσεις μία κλήση μέσω Internet ή να στείλεις ένα fax. Ταυτόχρονα, δεν υπάρχει ανάγκη πλέον, για απόσυρση των συμβατικών συσκευών και αντικατάσταση αυτών με καινούργιες IP συσκευές.

Εικόνα 2.3: Παράδειγμα Analog Telephone Adapter

Ο πρώτος τύπος Analog Telephone Adapter καλείται FXS to USB. FXS σημαίνει Foreign Exchange Station (τηλεφωνικές συσκευές). Κάθε ATA έχει από μία ή περισσότερες υποδοχές RJ-11. Κάθε υποδοχή αντιστοιχεί σε μία τηλεφωνική συσκευή ή μηχανή του fax. Ως έξοδο έχει USB υποδοχές που μέσω καλωδίου συνδέονται σε προσωπικούς υπολογιστές, σε κάποια θύρα USB. Ο υπολογιστής γίνεται το μέσω που θα συνδέσει το συμβατικό μηχάνημα με το Internet. Έτσι το ATA κάνει τις φωνητικές κλήσεις μέσω Internet μερικώς πιο εύκολες στο χειρισμό απ' ότι ένα μικρόφωνο με ακουστικά. Όμως δεν επικοινωνεί απευθείας με εξυπηρετητή VoIP. Η πραγματική μετατροπή αναλογικού σε ψηφιακού σήματος γίνεται από λογισμικό του υπολογιστή, γνωστό ως softphone, που πρέπει να έχει εγκατασταθεί στον υπολογιστή που το ATA είναι συνδεδεμένο.

Ο δεύτερος τύπος ATA, πραγματοποιεί απευθείας τη μετατροπή αναλογικού σε ψηφιακού σήματος φωνής. Γι' αυτό το λόγο, τέτοιου τύπου ATA δε χρειάζονται softphones για να δουλέψουν. Επικοινωνεί άμεσα με εξυπηρετητή VoIP χρησιμοποιώντας κάποιο γνωστό πρωτόκολλο όπως SIP (το πιο συνηθισμένο πρωτόκολλο για ATA), H.323, IAX ή MGCP. Τα φωνητικά δεδομένα κωδικοποιούνται και αποκωδικοποιούνται χρησιμοποιώντας GSM, a-law, u-law και άλλους φωνητικούς codecs.
Σε φυσικό επίπεδο, ένα FXS to Ethernet Gateway ATA έχει μία ή περισσότερες τηλεφωνικές υποδοχές στις οποίες μπορούν να συνδεθούν συμβατικές τηλεφωνικές συσκευές. Τα αναλογικά φωνητικά δεδομένα μετατρέπονται σε ψηφιακά δεδομένα και μεταδίδονται μέσω καλωδίου RJ-45, το οποίο με τη σειρά του είναι συνδεδεμένο σε κάποιο LAN (Local Area Network) μέσω κάποιου Ethernet hub ή switch.[17]

7.Δρομολογητές VoIP(VoIP Routers)

Η συσκευή router παρέχει τη σύνδεση του τοπικού δικτύου με τους απομακρυσμένους server, εξασφαλίζοντας μια «καθαρή» σύνδεση συσκευών πολλών ειδών. Η ύπαρξη ενός router υψηλής ποιότητας προσφέρει καλύτερη απόδοση και μεγαλύτερη αξιοπιστία σε μια VoIP σύνδεση, η οποία είναι πολύ ευαίσθητη σε καθυστερήσεις και απαιτεί γρήγορη μεταφορά πακέτων.

Ο router μεταφέρει πακέτα δεδομένων μεταξύ πολλαπλών server στο διαδίκτυο, κάνοντας πραγματικότητα τη μετάδοση δεδομένων φωνής μέσω του πρωτοκόλλου TCP/IP. Οι συσκευές router οι οποίες είναι εξειδικευμένες στις VoIP συνδέσεις διευκολύνουν την μετάδοση δεδομένων φωνής μέσα σε πακέτα δεδομένων έτσι ώστε να επιτυγχάνονται συνομιλίες μέσω του διαδικτύου σε πραγματικό χρόνο, με ικανοποιητική ποιότητα και χωρίς προβλήματα καθυστερήσεων. Εκτός αυτού οι εξειδικευμένοι VoIP routers προσφέρουν μεγαλύτερη ασφάλεια έτσι ώστε οι συνομιλίες που πραγματοποιούνται να είναι όχι μόνο καλές ποιοτικά αλλά και ασφαλείς.[26]

8. IP/VoIP PBX (Private Branch eXchange)

Ένα IP PBX είναι ένα σύστημα μεταγωγής κλήσεων (τηλεφωνικό κέντρο) το οποίο δρομολογεί κλήσεις μεταξύ VoIP χρηστών στο τοπικό δίκτυο της επιχείρησης(όχι μόνο στις επιχειρήσεις) αλλά παράλληλα τους επιτρέπει να μοιράζονται και ένα συγκεκριμένο αριθμό εξωτερικών γραμμών για κλήσεις εκτός επιχείρησης. Το IP PBX μπορεί ακόμη να συνδέσει κλήσεις μεταξύ χρηστών του απλού τηλεφωνικού δικτύου ή κλήσεις χρηστών εκ των οποίων ο ένας χρησιμοποιεί VoIP και ο άλλος το απλό τηλεφωνικό δίκτυο.

Με τα απλά τηλεφωνικά κέντρα για επικοινωνίες δεδομένων αλλά και φωνής είναι απαραίτητη η ύπαρξη ξεχωριστών δικτύων. Ένα από τα σημαντικότερα πλεονεκτήματα των IP PBX τηλεφωνικών κέντρων είναι ότι επιτυγχάνουν τη χρήση ενιαίων δικτύων για δεδομένα και φωνή. Αυτό σημαίνει ότι η πρόσβαση στο διαδίκτυο (άρα και οι κλήσεις VoIP) και η χρήση του τηλεφωνικού δικτύου μπορούν να πραγματοποιηθούν με τη χρήση μιας γραμμής για κάθε χρήστη. Το γεγονός αυτό παρέχει ευελιξία στην επιχείρηση και μπορεί επίσης να μειώσει το κόστος αλλά και τη διάρκεια αποκατάστασης βλαβών στο δίκτυο μιας επιχείρησης.

Κεφάλαιο 3

3.1 Quality of Service(QoS)

Πολλά σενάρια επικοινωνίας περιλαμβάνουν ανταλλαγή μέσων επικοινωνίας σε πραγματικό χρόνο, όπως φωνή και βίντεο. Σε τέτοιες περιπτώσεις, είναι σημαντικό τα πακέτα δεδομένων να φτάνουν στον προορισμό τους μέσα σε κάποιο συγκεκριμένο χρονικό διάστημα μετά την μετάδοσή τους από τον αποστολέα. Εάν φτάσουν μετά την λήξη του χρονικού διαστήματος τότε θα πρέπει να απορριφθούν, και αυτό γιατί τα δεδομένα που θα παραλάβει ο χρήστης δεν θα είναι κατανοητά. Για τον λόγο αυτό, σε κίνηση πραγματικού χρόνου είναι αναγκαία η παροχή υψηλής ποιότητας υπηρεσιών προς τους τελικούς χρήστες.

Μέχρι σήμερα έχει παρατηρηθεί ότι τα δίκτυα στήριξης του διαδικτύου (Internet backbones) δεν προκαλούν προβλήματα στην μετάδοση διαφόρων μέσων, όπως η φωνή. Εκατομμύρια άνθρωποι καθημερινά πραγματοποιούν τηλεφωνικές κλήσεις από το διαδίκτυο με εξαιρετικά καλή ποιότητα. Παρόλα αυτά, οι υπηρεσίες πολυμέσων που απαιτούν υψηλό εύρος ζώνης (bandwidth), όπως μετάδοση βίντεο, μπορεί να αποτελέσει πρόκληση για το κοντινό μέλλον.

Προς την κατεύθυνση αυτή, είναι σημαντική η υλοποίηση μηχανισμών που βοηθούν στην διατήρηση σταθερής ποιότητας υπηρεσιών για συγκεκριμένες ροές κίνησης και για συγκεκριμένους χρήστες. Εάν υποθέσουμε ότι οι διαθέσιμοι πόροι είναι περιορισμένοι και ότι δεν υπάρχει άπλετη χωρητικότητα στο διαδίκτυο, η εξασφάλιση ποιότητας υπηρεσιών υπονοεί κάποιους τρόπους παροχής προτεραιοτήτων σε κάποια πακέτα σε σχέση με κάποια άλλα. Αυτό απαιτεί ένα διαφορετικό μοντέλο από το παραδοσιακό best-effort μοντέλο ισότητας του διαδικτύου.

Γενικά, η διαδικασία παροχής προτεραιότητας μπορεί να υλοποιηθεί σε τύπους κίνησης σε πραγματικό χρόνο που απαιτούν πολύ αυστηρές προδιαγραφές όσον αφορά την προσφερόμενη ποιότητα υπηρεσιών. Ένας δρομολογητής μπορεί να δίνει προτεραιότητα σε πακέτα που αντιστοιχούν σε επικοινωνία σε πραγματικό χρόνο, σε σχέση με πακέτα που ανήκουν σε ροές μη πραγματικού χρόνου, όπως email. Σε τέτοιες περιπτώσεις όμως πρέπει να λαμβάνονται υπόψη και η χρέωση

για αυτές τις υπηρεσίες, καθώς ένας δικτυακός φορέας παροχής υπηρεσιών μπορεί να επιθυμεί να χρεώνει για την προσφορά επιπλέον υπηρεσιών.

Η προσφερόμενη ποιότητα υπηρεσιών για τη μετάδοση φωνής αποτελεί ένα κρίσιμο χαρακτηριστικό γνώρισμα για τις δικτυακές επικοινωνίες πραγματικού χρόνου. Για την VoIP τεχνολογία η Quality of Service (QoS) χρησιμοποιήθηκε για μεγάλο χρονικό διάστημα από τους υποστηριχτές της τεχνολογίας των συμβατικών δικτύων ως μέσο για να κρατηθούν οι χρήστες μακριά από το VoIP. Επίσης, συνήθως επικαλείται από τους φορείς παροχής δικτυακού εξοπλισμού ως βασικός λόγος αγοράς νέου δικτυακού εξοπλισμού και εξοπλισμού ελέγχου. Παρόλα αυτά, η QoS δεν απαιτείται μόνο για την αλληλεπιδραστική επικοινωνία μετάδοσης φωνής αλλά και για μετάδοση βίντεο.

3.2 Παράγοντες Ποιότητας Υπηρεσιών

Η επίτευξη επικοινωνίας μέσω του δημόσιου τηλεφωνικού δικτύου (Public Switched Telephone Network, PSTN) έχει ένα σύνολο προβλημάτων που αφορούν την μετάδοση φωνής. Κατά ανάλογο τρόπο, η VoIP τεχνολογία έχει πολλά παρόμοια προβλήματα καθώς και κάποια επιπρόσθετα. Στην συνέχεια, απαριθμούνται τα σημαντικότερα από αυτά τα ζητήματα και εξηγούνται οι επιπτώσεις που μπορούν να έχουν στα δίκτυα μεταγωγής πακέτων.

3.2.1 Καθυστέρηση (Delay/Latency)

Η VoIP καθυστέρηση (delay) ή λανθάνον χρόνος (latency) χαρακτηρίζεται ως το χρονικό διάστημα από την στιγμή που η φωνή εξέρχεται από το στόμα του ομιλητή μέχρι να φτάσει δια μέσου του δικτύου στο αυτί του ακροατή. Στα σημερινά τηλεφωνικά δίκτυα υπάρχουν τρεις τύποι καθυστερήσεων που χαρακτηρίζονται ως: καθυστέρηση διάδοσης (propagation delay), καθυστέρηση αναμονής στην ουρά (queuing delay) και καθυστέρηση διαχείρισης ή επεξεργασίας (handling or processing delay).

Καθυστέρηση Διάδοσης

Η καθυστέρηση διάδοσης μετριέται από την στιγμή που και το τελευταίο bit του πακέτου έχει μεταδοθεί από τον αρχικό κόμβο της σύνδεσης έως τον τελικό κόμβο. Το είδος αυτό της καθυστέρησης είναι ανάλογο της απόστασης ανάμεσα στον

αποστολέα και τον παραλήπτη και οδηγεί συνήθως σε μικρές καθυστερήσεις, εξαιρώντας βέβαια τις δορυφορικές συνδέσεις. Η καθυστέρηση διάδοσης εξαρτάται από τα φυσικά χαρακτηριστικά της σύνδεσης και είναι ανεξάρτητη από τον φόρτο κίνησης της σύνδεσης.

Δηλαδή, η καθυστέρηση διάδοσης εξαρτάται από το μήκος που ένα σήμα πρέπει να ταξιδέψει σε οπτικές ίνες ή σε ηλεκτρικούς παλμούς σε δίκτυα βασισμένα σε χαλκό. Το φως ταξιδεύει μέσα από το κενό με ταχύτητα 186 χιλιάδων μιλίων ανά δευτερόλεπτο, και τα ηλεκτρόνια ταξιδεύουν μέσω του χαλκού ή την οπτική ίνα με περίπου 125 χιλιάδες μίλια ανά δευτερόλεπτο. Ένα δίκτυο οπτικών ινών που εκτείνεται στα μισά του δρόμου γύρω από τον κόσμο (δηλαδή, περίπου 13 χιλιάδες μίλια) προκαλεί καθυστέρηση προς την μία κατεύθυνση περίπου 70 χιλιοστών του δευτερολέπτου (70 ms). Αν και αυτή η καθυστέρηση είναι σχεδόν ανεπαίσθητη στο ανθρώπινο αυτί, οι καθυστερήσεις διάδοσης σε συνδυασμό με τις καθυστερήσεις επεξεργασίας μπορούν να προκαλέσουν σημαντική λεκτική υποβάθμιση.

Καθυστέρηση Διαχείρισης/Επεξεργασίας

Η καθυστέρηση επεξεργασίας θεωρείται το χρονικό διάστημα ανάμεσα στη στιγμή που το πακέτο λαμβάνεται σωστά από τον αρχικό κόμβο της σύνδεσης μέχρι να ανατεθεί στην ουρά ενός εξερχόμενου κόμβου για μετάδοση. Η καθυστέρηση επεξεργασίας είναι ανεξάρτητη από τον φόρτο κίνησης που διαχειρίζεται ο συγκεκριμένος κόμβος, εφόσον βέβαια η υπολογιστική δύναμη δεν αποτελεί περιοριστικό παράγοντα.

Η καθυστέρηση διαχείρισης αναφέρεται σε πολλές διαφορετικές αιτίες της καθυστέρησης όπως: η πακετοποίηση, η συμπίεση και η μεταγωγή πακέτων, και προκαλείται από συσκευές που διαβιβάζουν τα πλαίσια (frames) μέσω του δικτύου. Οι δικτυακές συσκευές που διαβιβάζουν πλαίσια μέσω του δικτύου οφείλονται κατά κύριο λόγο για τέτοιου είδους καθυστερήσεις. Οι καθυστερήσεις επεξεργασίας μπορούν να έχουν αντίκτυπο στα παραδοσιακά τηλεφωνικά δίκτυα, αλλά αποτελούν ακόμα μεγαλύτερο ζήτημα σε περιβάλλοντα μεταγωγής πακέτων.

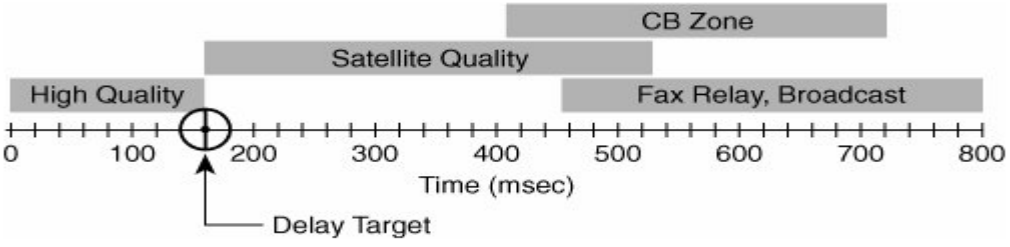
Στο σημείο αυτό μπορούμε να αναφέρουμε ότι σε IOS VoIP προϊόντα της Cisco, ο επεξεργαστής ψηφιακών σημάτων (Digital Signal Processor, DSP) παράγει ένα λεκτικό δείγμα κάθε 10ms με χρησιμοποίηση του G.729. Δύο από αυτά τα λεκτικά δείγματα (και τα δύο των 10ms καθυστέρησης) τοποθετούνται έπειτα μέσα σε ένα πακέτο. Επομένως, η καθυστέρηση των πακέτων γίνεται 20ms. Επίσης, οι

προμηθευτές μπορούν να αποφασίσουν πόσα λεκτικά δείγματα θέλουν να στείλουν σε ένα πακέτο. Επειδή στο G.729 χρησιμοποιούνται λεκτικά δείγματα των 10ms, κάθε αύξηση στα δείγματα ανά πλαίσιο αυξάνει την καθυστέρηση κατά 10ms. Στην πραγματικότητα, τα IOS προϊόντα της Cisco επιτρέπουν στους χρήστες να επιλέξουν πόσα δείγματα να βάλουν σε κάθε πλαίσιο. Τέλος, η Cisco έδωσε σε DSP ένα μεγάλο μέρος της ευθύνης για την πλαισιοποίηση και μορφοποίηση των πακέτων ώστε να κρατήσει τις συνολικές καθυστερήσεις στους δρομολογητές και τις πύλες του δικτύου χαμηλές. Για τον λόγο αυτό, η επικεφαλίδα του πρωτοκόλλου μεταφοράς σε πραγματικό χρόνο (Real-Time Transport Protocol, RTP) τοποθετείται στο πλαίσιο στο DSP αντί να αναθέτει στους δρομολογητές αυτή την ευθύνη.

Καθυστέρηση Αναμονής στην Ουρά

Η καθυστέρηση αναμονής σε ουρά αναφέρεται στο χρονικό διάστημα ανάμεσα στην στιγμή που το μήνυμα ανατίθεται σε μια ουρά για μετάδοση έως την στιγμή που αρχίζει να μεταδίδεται. Κατά την διάρκεια αυτού του διαστήματος, το πακέτο περιμένει μέχρι να μεταδοθούν άλλα πακέτα στην ουρά πριν από αυτό. Δηλαδή, ένα δίκτυο μεταγωγής πακέτων μπορεί να υφίσταται καθυστερήσεις που οφείλονται στην μετακίνηση ενός πακέτου σε μια ουρά (μεταγωγή πακέτων) και τον χρόνο αναμονής στην ουρά μέχρι να αρχίσει να μεταδίδεται.

Όταν τα πακέτα κρατιούνται σε μια σειρά αναμονής λόγω της συμφόρησης σε μια εξερχόμενη διεπαφή, τότε έχουμε ως αποτέλεσμα καθυστερήσεις αναμονής σε ουρά. Η καθυστέρηση αναμονής εμφανίζεται όταν στέλνονται περισσότερα πακέτα από όσα η διεπαφή μπορεί να χειριστεί σε ένα δεδομένο διάστημα. Επίσης, η πραγματική καθυστέρηση αναμονής της σειράς είναι μια άλλη αιτία της καθυστέρησης. Στην πραγματικότητα, αυτός ο παράγοντας πρέπει να κρατηθεί λιγότερο από 10ms με τη χρησιμοποίηση οποιουδήποτε μεθόδου αναμονής που να είναι βέλτιστη για το εκάστοτε δίκτυό.



Σχήμα 3.1 : End-to-End Καθυστερήσεις

Ο τομέας πιστοποίησης της διεθνούς ένωσης τηλεπικοινωνιών (International Telecommunication Union, ITU) για την G.114 σύσταση τομέα διευκρινίζει ότι για την επίτευξη υψηλής ποιότητας φωνής πρέπει να συμβούν έως και 150ms μονόδρομων και από άκρη σε άκρη καθυστερήσεων. Το γεγονός αυτό φαίνεται στο παραπάνω σχήμα 3.1. Επίσης από το σχήμα παρατηρούμε ότι μερικές μορφές καθυστέρησης είναι επεκταμένες χρονικά, αλλά γίνονται αποδεκτές επειδή καμία άλλη εναλλακτική λύση δεν υπάρχει. Για παράδειγμα, στη δορυφορική μετάδοση απαιτούνται κατά μέσο όρο περίπου 250ms για μια μετάδοση για να φθάσει στο δορυφόρο, και άλλα 250ms για να επιστρέψει το μεταδιδόμενο μήνυμα πίσω στην γη. Αυτό οδηγεί σε μια συνολική καθυστέρηση της τάξης των 500 ms. Αν και η ITU σύσταση σημειώνει ότι αυτό είναι έξω από την αποδεκτά όρια της ποιότητας φωνής, εντούτοις πολλές συνομιλίες εξυπηρετούνται καθημερινά από δορυφορικές συνδέσεις. Υπό αυτήν τη μορφή, η ποιότητα φωνής καθορίζεται συχνά από το είδος των χρηστών που θα την αποδεχθούν και θα την χρησιμοποιήσουν.
Σε ένα κορεσμένο δίκτυο, η καθυστέρηση αναμονής μπορεί να αθροιστεί έως και δύο δευτερόλεπτα καθυστερήσεων, αλλιώς το δίκτυο θα αρχίσει να απορρίπτει πακέτα. Αυτή η μεγάλη περίοδος καθυστέρησης είναι απαράδεκτη σχεδόν σε οποιοδήποτε δίκτυο φωνής. Η καθυστέρηση αναμονής είναι μόνο ένας παράγοντας που προκαλεί καθυστερήσεις από άκρο σε άκρο.

3.2.2 Jitter

Με τον όρο jitter εννοούμε την διακύμανση του χρόνου άφιξης πακέτων και έχει νόημα μόνο σε δίκτυα που βασίζονται στην μεταγωγή πακέτων. Παρόλο που σε ένα περιβάλλον μετάδοσης πακέτων φωνής, ο αποστολέας αναμένεται να διαβιβάσει αξιόπιστα τα πακέτα φωνής σε τακτά χρονικά διαστήματα, δηλαδή να στέλνει ένα πλαίσιο κάθε 20ms, εντούτοις τα πακέτα αυτά μπορούν να καθυστερήσουν σε όλο το δίκτυο πακέτων και να μην φθάνουν με τον ίδιο ρυθμό στο λαμβάνοντα σταθμό, δηλαδή να μην παραλαμβάνονται κάθε 20ms. Γι αυτό ακριβώς το λόγο πρέπει το σύστημα να έχει την ικανότητα να τα κρατάει κάπου μέχρι να φτάσει και το πιο αργοπορημένο, ούτως ώστε να τα συνθέσει σε στρωτή ροή όπως απαιτεί η τηλεφωνία. Αυτό προϋποθέτει την ύπαρξη επαρκών buffer στον δέκτη και συνεπάγεται φυσικά πρόσθετη καθυστέρηση.

Το πρόβλημα που προκύπτει είναι το πώς θα ελαχιστοποιηθεί κατά το δυνατόν το μέγεθος των buffer, άρα και η καθυστέρηση και ταυτόχρονα πως θα αποφύγουμε την αστάθεια καθυστέρησης.

Για την επίλυση του προβλήματος σε IP δίκτυα μετράται ο αριθμός των πακέτων που φτάνουν καθυστερημένα και υπολογίζεται έτσι ο λόγος των καθυστερημένων προς τα κανονικά πακέτα. Με τον τρόπο αυτό μπορεί να ρυθμίζεται δυναμικά το βέλτιστο μέγεθος του buffer.

Πολλοί προμηθευτές επιλέγουν την χρησιμοποίηση στατικών jitter buffers, ενώ κάποιοι άλλοι, όπως η Cisco, θεωρούν πως ένας καλά κατασκευασμένος δυναμικός jitter buffer είναι ο καλύτερος μηχανισμός που μπορεί να χρησιμοποιηθεί για τα δίκτυα πακέτων. Η χρήση στατικών jitter buffers αναγκάζουν το μέγεθος του buffer να είναι είτε πάρα πολύ μεγάλο είτε πάρα πολύ μικρό. Το γεγονός αυτό υποβαθμίζει την ποιότητα της μεταδιδόμενης φωνής λόγω των χαμένων πακέτων και των υπερβολικών καθυστερήσεων. Το μέγεθος ενός jitter buffer που αυξάνεται ή μειώνεται δυναμικά βασίζεται στην διακύμανση της καθυστέρησης μεταξύ ενδιάμεσων αφίξεων πακέτων.

3.2.3 Απώλεια Πακέτων (Packet Loss)

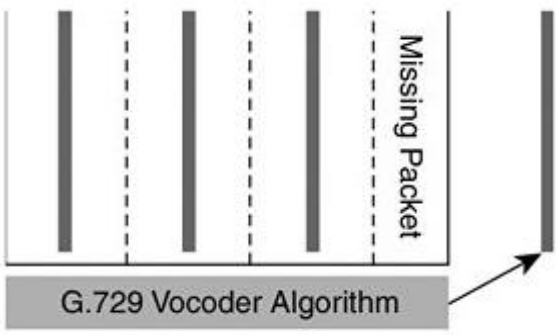
Επειδή τα δίκτυα IP δεν εγγυώνται την ορθή μεταφορά των πακέτων, υπάρχει περίπτωση κατά τη μετάδοση και ιδίως σε περιπτώσεις συμφόρησης, κάποια πακέτα να χαθούν χωρίς, στην περίπτωση της φωνής, να μπορούν να ανακτηθούν. Για την αντιμετώπιση του προβλήματος αυτού υπάρχουν διάφορες τεχνικές.

Με την πρώτη τεχνική στην πλευρά του παραλήπτη, ξαναπαίζεται το τελευταίο πακέτο για συμπλήρωση ηχητικού κενού. Αυτό λειτουργεί, χωρίς σοβαρές επιπτώσεις, σε περιπτώσεις που η απώλεια πακέτων είναι σπάνια. Σε αντίθετη περίπτωση το πρόβλημα γίνεται αντιληπτό.

Με τη δεύτερη τεχνική μαζί με κάθε πακέτο φωνής στέλνεται και το προηγούμενο. Αυτό αυξάνει την απαιτούμενη χωρητικότητα και προσθέτει καθυστέρηση, αλλά εξασφαλίζει την περίπτωση απώλειας πακέτων φωνής.

Η τρίτη τεχνική βασίζεται στην προηγούμενη με τη διαφορά ότι το πλεονάζον πακέτο που αποστέλλεται για λόγους εφεδρείας κατασκευάζεται με άλλον αλγόριθμο λιγότερο απαιτητικό, με μικρότερο μέγεθος, ώστε να μειωθούν οι απαιτήσεις σε χωρητικότητα γραμμής (bandwidth).

Η υλοποίηση πολλών VoIP συστημάτων επιτρέπει στο δρομολογητή φωνής να αποκριθεί στην περιοδική απώλεια πακέτων. Εάν ένα πακέτο φωνής δεν παραλαμβάνεται όταν αναμένεται (ο αναμενόμενος χρόνος είναι μεταβλητός), θεωρείται ότι έχει χαθεί και το τελευταίο λαμβανόμενο πακέτο. Η διαδικασία αυτή φαίνεται στο παρακάτω σχήμα 3.2. Επειδή η καθυστέρηση του πακέτου είναι μόνο 20ms, ο μέσος ακροατής δεν παρατηρεί τη διαφορά στην ποιότητα φωνής.



Σχήμα 3.2 : Απώλεια πακέτων στο G.729

Έστω ότι χρησιμοποιούμε υλοποίηση του G.729 για VoIP, και ότι κάθε μια από τις στήλες στο σχήμα 3.2 αντιπροσωπεύει ένα πακέτο. Το πρώτο, δεύτερο και τρίτο πακέτο φθάνουν στον προορισμό τους, αλλά το τέταρτο πακέτο χάνεται κάπου στη μετάδοση. Ο λαμβάνων σταθμός περιμένει μια χρονική περίοδο και έπειτα θα ξεκινήσει μια στρατηγική απόκρυψης. Αυτή η στρατηγική επαναλαμβάνει το τελευταίο λαμβανόμενο πακέτο (σε αυτήν την περίπτωση είναι το τρίτο πακέτο), και έτσι ο ακροατής δεν ακούει τα χάσματα σιωπής. Επειδή η χαμένη ομιλία είναι μόνο 20 ms, ο ακροατής πιθανότατα δεν ακούει τη διαφορά. Η στρατηγική αυτή μπορεί να δουλέψει εάν χάνεται μόνο ένα πακέτο. Εάν χαθούν πολλαπλά διαδοχικά πακέτα, η στρατηγική απόκρυψης τρέχει μόνο μια φορά μέχρι να παραληφθεί ένα άλλο πακέτο. Λόγω της στρατηγικής απόκρυψης, εμπειρικά το G.729 είναι ανεκτικό σε περίπου 5% απώλειας πακέτων κατά μέσο όρο στα πλαίσια μιας ολόκληρης κλήσης.

3.2.4 Ηχώ (Echo)

Είναι το φαινόμενο που παρατηρούμε μερικές φορές στο τηλέφωνο όταν ξανακούμε τη φωνή μας μετά από λίγο, κατά το οποίο παρατηρούνται ανακλάσεις και επιστροφές του εκπεμπόμενου σήματος σε ένα ζεύγος τηλεφωνικών γραμμών. Η

ηχώ δημιουργείται από ανακλάσεις όταν έχουμε ξαφνικές αλλαγές στη σύνθετη αντίσταση μιας γραμμής, όπως στις περιπτώσεις κακής προσαρμογής μεταξύ γραμμών. Παράδειγμα κακής προσαρμογής που είναι αιτία αυτού του φαινομένου, είναι η σύνδεση δύο γραμμών διαφορετικής σύνθετης αντίστασης, ας πούμε ενός ομοαξονικού και ενός συνεστραμμένου καλωδίου ή συνεστραμμένου διαφορετικής διαμέτρου.

Η ηχώ δημιουργείται επίσης από τα κυκλώματα μετατροπής των δισύρματων γραμμών σε τετρασύρματες όπως στα φερέσυχνα. Στην τηλεφωνία η ηχώ που δημιουργείται σε μικρή απόσταση από τον συνομιλητή δεν γίνεται αντιληπτή. Αντίθετα είναι παρατηρήσιμη και ενοχλητική αυτή που δημιουργείται σε μεγάλες αποστάσεις όπως στις υπερατλαντικές και δορυφορικές συνδέσεις.

Η ηχώ έχει δύο μειονεκτήματα. Πρώτον, μπορεί να είναι δυνατή και δεύτερον μπορεί να είναι επεκταμένη χρονικά. Είναι επόμενο πως, όσο δυνατότερη και μεγαλύτερης διάρκειας είναι η ηχώ, τόσο πιο ενοχλητική γίνεται. Τα δίκτυα τηλεφωνίας σε εκείνα τα μέρη του κόσμου όπου η αναλογική φωνή χρησιμοποιείται πρώτιστα χρησιμοποιούν τους καταπιεστές της ηχώ, οι οποίοι αφαιρούν την ηχώ με την κάλυψη της σύνθετης αντίστασης σε ένα κύκλωμα. Αυτός δεν είναι ο καλύτερος μηχανισμός που μπορεί να χρησιμοποιηθεί για να αφαιρέσει την ηχώ και, στην πραγματικότητα, προκαλεί επιπρόσθετα προβλήματα. Για παράδειγμα, δεν είναι εφικτή η χρησιμοποίηση ενός ψηφιακού δικτύου ενοποιημένων υπηρεσιών (Integrated Services Digital Network, ISDN) σε μια γραμμή που έχει καταπιεστή της ηχώ, επειδή ο καταπιεστής κόβει το φάσμα συχνότητας που χρησιμοποιεί το ISDN.

Στα σημερινά δίκτυα πακέτων, είναι δυνατή η δημιουργία καταπιεστών της ηχώ σε low-bit-rate codecs και στην συνέχεια η ενεργοποίηση τους σε κάθε DSP. Μερικοί κατασκευαστές προτιμούν υλοποιήσεις όπου η ακύρωση της ηχώ γίνεται στο λογισμικό, παρόλο που αυτή η πρακτική μειώνει δραστικά τα οφέλη της ακύρωσης της ηχώ.

Για την καλύτερη κατανόηση της λειτουργίας των καταπιεστών της ηχώ είναι καλύτερο να καταλάβει κάποιος την προέλευσή της. Έστω ένα παράδειγμα, όπου υποθέτουμε ότι ο χρήστης Α μιλά στο χρήστη Β, και ότι η ομιλία του χρήστη Α στο χρήστη Β καλείται G. Όταν το G δίνει έναν κακό συνδυασμό σύνθετης αντίστασης ή άλλα περιβάλλοντα με ηχώ, τότε αναπηδά πίσω στο χρήστη Α. Ο χρήστης Α μπορεί να ακούσει την καθυστέρηση αρκετά χιλιοστά του δευτερολέπτου αφότου μιλά πραγματικά. Για να αφαιρέσει την ηχώ από τη γραμμή, η συσκευή του χρήστης Α

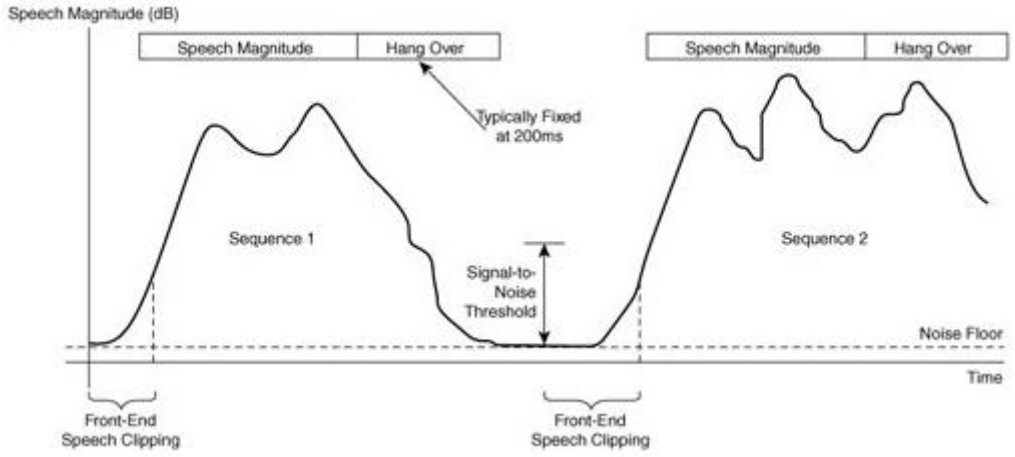
μιλά μέσω του δρομολογητή A και διατηρεί μια αντίστροφη εικόνα της ομιλίας του χρήστη A για ένα συγκεκριμένο χρονικό διάστημα. Αυτό καλείται αντίστροφη ομιλία G1. Αυτός ο καταπιεστής της ηχώ αφουγκράζεται τον ήχο που προέρχεται από το χρήστη B και αφαιρεί το G για να απομακρύνει οποιαδήποτε ηχώ. Οι καταπιεστές της ηχώ περιορίζονται από το συνολικό ποσοστό του χρόνου που περιμένουν την παραλαβή της αντανακλασμένης ομιλίας, φαινόμενο που είναι γνωστό και ως ουρά της ηχώς. Τυπικές τιμές διαμορφώσεων των ουρών της ηχώ είναι 16, 24, 32, 64, και 128 ms.

Είναι σημαντικό να διαμορφωθεί η κατάλληλη τιμή της ακύρωσης της ηχώ κατά την αρχική εγκατάσταση του VoIP εξοπλισμού. Εάν διαμορφωθεί χαμηλή τιμή της ακύρωσης της ηχώ, οι χρήστες θα ακούν ηχώ κατά τη διάρκεια των τηλεφωνικών κλήσεων. Αντίθετα, εάν διαμορφωθεί υψηλή τιμή της ακύρωσης της ηχώ, θα πάρει περισσότερο χρόνο για τον καταπιεστή της ηχώ ώστε να συγκλίνει και να αποβάλει την ηχώ.

3.2.5 Ανίχνευση Δραστηριότητας Φωνής (Voice Activity Detection)

Στις κανονικές συνομιλίες φωνής, ένα άτομο μιλά και κάποιο άλλο ακούει. Τα σημερινά δίκτυα διαθέτουν αμφίδρομο κανάλι των 64 χιλιάδων bit ανά δευτερόλεπτο (Bit Per Second, BPS), ανεξάρτητα εάν κάποιος χρήστης συνδιαλέγεται ή όχι. Αυτό σημαίνει ότι σε μια κανονική συνομιλία σπαταλάτε τουλάχιστον 50 τοις εκατό του συνολικού εύρους ζώνης (bandwidth). Μάλιστα, το ποσοστό του σπαταλημένου εύρους ζώνης μπορεί στην πραγματικότητα να είναι πολύ υψηλότερο εάν πάρουμε μια στατιστική δειγματοληψία των διαλλειμάτων και των μικρών διακοπών σε μια λεκτική συνομιλία.

Όταν χρησιμοποιείται VoIP τεχνολογία, το ποσοστό του “χαμένου” εύρους ζώνης μπορεί να χρησιμοποιηθεί για άλλους σκοπούς όταν επιτρέπεται η ανίχνευση δραστηριότητας φωνής (Voice Activity Detection, VAD). Όπως φαίνεται στο παρακάτω σχήμα 3.3, η VAD λειτουργεί με την ανίχνευση του μεγέθους της ομιλίας μετρημένης σε decibels (DB) αλλά και την απόφαση για την διακοπή της φωνής πριν τη διαμόρφωση ή πλαισιοποίηση της.



Σχήμα 3.3 : Ανίχνευση Δραστηριότητας Φωνής (AVD).

Όταν η VAD ανιχνεύει μια κάθοδο του λεκτικού εύρους, περιμένει ένα σταθερό χρονικό διάστημα προτού να σταματήσει να τοποθετεί φωνητικά πλαίσια σε πακέτα. Αυτό το σταθερό χρονικό διάστημα είναι γνωστό ως κατάλοιπο (Hangover) και έχει χαρακτηριστική τιμή περίπου στα 200 ms.

Η ανίχνευση δραστηριότητας φωνής αντιμετωπίζει ορισμένα έμφυτα προβλήματα στον καθορισμό της έναρξης και της λήξης της ομιλίας καθώς και στη διάκριση της ομιλίας από τον παρασιτικό θόρυβο. Αυτό σημαίνει ότι εάν ο χρήστης που συνομιλεί βρίσκεται σε ένα θορυβώδες δωμάτιο, η VAD είναι ανίκανη να διακρίνει μεταξύ της ομιλίας και του παρασιτικού θορύβου. Το φαινόμενο αυτό είναι γνωστό ως κατώφλι σήματος προς θόρυβο (Signal-to-Noise Threshold) και φαίνεται στο σχήμα 3.3. Σε αυτά τα σενάρια, η VAD τίθεται εκτός λειτουργίας στην αρχή της κλήσης.

Ένα άλλο έμφυτο πρόβλημα της VAD είναι η ανίχνευση της αρχής της ομιλίας. Χαρακτηριστικά η αρχή μιας πρότασης κόβεται ή ψαλιδίζεται. Το φαινόμενο αυτό είναι γνωστό ως λεκτικό ψαλίδισμα εμπροσθοφυλακής (Front-End Speech Clipping) και φαίνεται στο σχήμα 3.3. Συνήθως, το άτομο που ακούει την ομιλία
δεν παρατηρεί το προηγούμενο λεκτικό ψαλίδισμα.

3.2.6 Φτωχή Συμπίεση (Poor Compression)

Αν και η αναλογική επικοινωνία είναι ιδανική για τηλεφωνική συνομιλία, η αναλογική μετάδοση δεν είναι ούτε γερή αλλά ούτε αποδοτική όσο αφορά την ανάκτηση του σήματος από το θόρυβο. Στα δίκτυα τηλεφωνίας, όταν η αναλογική μετάδοση περνά μέσω των ενισχυτών για να ενισχύσει το σήμα, έχει σαν αποτέλεσμα όχι μόνο την

ενίσχυση της φωνή αλλά και την ενίσχυση του θορύβου. Συνήθως, αυτή η ενίσχυση στην γραμμή θορύβου οδηγεί σε μια ακατάλληλη προς χρήση σύνδεση.

Είναι πολύ πιο εύκολο για τα ψηφιακά δείγματα, που αποτελούνται από τα bit 1 και 0, να χωριστούν από την γραμμή θορύβου. Επομένως, όταν τα αναλογικά σήματα αναπαράγονται ως ψηφιακά δείγματα, διατηρείται ένας καθαρός ήχος. Τα οφέλη αυτής της ψηφιακής αναπαράστασης έγιναν εμφανή και σιγά-σιγά το δίκτυο τηλεφωνίας μετανάστευσε στη διαμόρφωση κωδικών παλμών (Pulse Code Modulation, PCM). Το PCM μετατρέπει τον αναλογικό ήχο σε ψηφιακή μορφή, με δειγματοληψία του αναλογικού ήχου 8000 φορές ανά δευτερόλεπτο και στην συνέχεια με τη μετατροπή κάθε δείγματος σε έναν αριθμητικό κώδικα. Το θεώρημα Nyquist δηλώνει ότι εάν ένα αναλογικό σήμα υφίσταται διπλάσια δειγματοληψία από την υψηλότερη συχνότητα ενδιαφέροντος, τότε το αρχικό αναλογικό σήμα μπορεί να ανακατασκευαστεί ακριβώς από τα ψηφιακά δείγματά του. Επειδή το φασματικό περιεχόμενο των συχνοτήτων της ανθρώπινης φωνής έχει εύρος στο διάστημα από 0 έως 4 KHz, τότε απαιτείται ρυθμός δειγματοληψίας της τάξης των 8000 φορών ανά δευτερόλεπτο, που αντιστοιχεί σε 125 ms μεταξύ των δειγμάτων.

Το πλήθος των δειγμάτων φωνής που πρέπει να σταλούν ανά πλαίσιο εξαρτάται από το είδος των κωδικοποιητών και αποκωδικοποιητών που έχουν επιλεγεί καθώς και από την ισορροπία μεταξύ του χρησιμοποιούμενου εύρους ζώνης και του αντίκτυπου της απώλειας πακέτων στο δίκτυο. Όσο μεγαλύτερη είναι αυτή η τιμή, τόσο υψηλότερη είναι η χρησιμοποίηση του εύρους ζώνης επειδή περισσότερα δείγματα φωνής συσκευάζονται στον τομέα ωφέλιμων φορτίων των UDP/RTP πακέτων και έτσι οι καθυστερήσεις των επικεφαλίδων του δικτύου θα είναι χαμηλότερες. Εντούτοις, ο αντίκτυπος της απώλειας πακέτων στην ποιότητα φωνής θα είναι μεγαλύτερος.

Στην πράξη χρησιμοποιούνται δύο βασικές παραλλαγές PCM των 64 Kbps που αναφέρονται ως : μ-law και α-law. Οι μέθοδοι είναι παρόμοιες δεδομένου ότι και οι δύο χρησιμοποιούν λογαριθμική συμπίεση, αλλά είναι διαφορετικές όσο αφορά λεπτομέρειες συμπίεσης. Ο μ-law έχει μικρό πλεονέκτημα στην απόδοση σήματος προς θόρυβο αναλογίας σε χαμηλά επίπεδα.

Μια άλλη μέθοδος συμπίεσης που χρησιμοποιείται αρκετά συχνά είναι η προσαρμοστική διαφορική διαμόρφωση κωδικών παλμών (Adaptive Differential Pulse Code Modulation, ADPCM). Έστω ότι χρησιμοποιούμε ADPCM στο G.726, το οποίο κωδικοποιεί χρησιμοποιώντας δείγματα των 4 bits και δίνοντας συνεπώς

ρυθμό μετάδοσης των 32 Kbps. Αντίθετα στο PCM, τα 4 bits δεν κωδικοποιούν άμεσα το εύρος της ομιλίας, αλλά κωδικοποιούν τις διαφορές στο εύρος, καθώς επίσης και το ποσοστό αλλαγής του εύρους, υιοθετώντας κάποια στοιχειώδη γραμμική πρόβλεψη.

Τα PCM και ADPCM είναι παραδείγματα των τεχνικών κωδικοποίησης κυματομορφών που εκμεταλλεύονται τα χαρακτηριστικά των τελευταίων. Τα τελευταία δέκα με δεκαπέντε χρόνια έχουν αναπτυχθεί νέες τεχνικές συμπίεσης που εκμεταλλεύονται τη γνώση των χαρακτηριστικών της πηγής παραγωγής ομιλίας. Αυτές οι τεχνικές υιοθετούν διαδικασίες επεξεργασίας σήματος που συμπιέζουν την ομιλία με την αποστολή μόνο απλουστευμένων παραμετρικών πληροφοριών για την διαμόρφωση της λεκτικής διέγερσης και των φωνητικών κομματιών, απαιτώντας το λιγότερο εύρος ζώνης για να διαβιβάσουν αυτές τις πληροφορίες. Αυτές οι τεχνικές αναφέρονται γενικά ως πηγές κωδικοποιητών-αποκωδικοποιητών και περιλαμβάνουν διάφορες παραλλαγές όπως: τη κωδικοποίηση γραμμικής πρόβλεψης (Linear Predictive Coding, LPC), τον κώδικας συμπίεσης γραμμικής πρόβλεψης (Code Excited Linear Prediction Compression, CELP), και τη κβαντοποίηση πολλαπλών παλμών και πολλαπλών επιπέδων (Multipulse Multilevel Quantization, MP-MLQ). Τα δημοφιλέστερα πρότυπα κωδικοποίησης φωνής για την τηλεφωνία περιλαμβάνουν τα πρότυπα : G.711, G.726, G.729, G.723.1 κ.α.

Η ποιότητα της φωνής μπορεί να εκτιμηθεί με δύο τρόπους: υποκειμενικά και αντικειμενικά. Οι άνθρωποι εκτελούν την υποκειμενική δοκιμή φωνής, ενώ διάφορες υπολογιστικές μηχανές είναι λιγότερο πιθανό ξεγελαστούν από την υποβάθμιση της φωνής που συνεπάγονται τα σχήματα συμπίεσης. Το σύνολο των κωδικοποιητών και αποκωδικοποιητών αναπτύσσεται και συντονίζεται με βάση τις υποκειμενικές μετρήσεις της ποιότητας φωνής. Οι τυποποιημένες αντικειμενικές ποιοτικές μετρήσεις, όπως η συνολική διαστρέβλωση φωνής και η αναλογία σήματος προς θόρυβο, δεν συσχετίζονται καλά με την ανθρώπινη αντίληψη για την ποιότητα φωνής, η οποία είναι τελικά ο στόχος των περισσότερων τεχνικών συμπίεσης φωνής.

Mean Opinion Score

Μια κοινή υποκειμενική μέτρηση επιδόσεων για την αξιολόγηση της απόδοσης των κωδικοποιητών και αποκωδικοποιητών ομιλίας είναι το Mean Opinion Score (MOS). Οι MOS δοκιμές δίνονται σε μια ομάδα ακροατών αφού η ποιότητα και ο ήχος

φωνής είναι γενικά υποκειμενικά στους ακροατές. Για τον λόγο αυτό, είναι σημαντικό οι MOS δοκιμές να διεξάγονται σε ένα ευρύ φάσμα ακροατών και υλικού των δειγμάτων. Οι ακροατές δίνουν σε κάθε δείγμα του λεκτικού υλικού μια εκτίμηση που κυμαίνεται από την τιμή ένα έως και την τιμή πέντε. Τέλος, τα αποτελέσματα υπολογίζονται κατά μέσο όρο ώστε να υπολογιστεί η τιμή MOS .
Επίσης, η δοκιμή MOS χρησιμοποιείται για να συγκρίνει πόσο καλά δουλεύει μια συγκεκριμένη διαδικασία κωδικοποίησης και αποκωδικοποίησης ομιλίας κάτω από ποικίλες περιστάσεις, συμπεριλαμβανομένων των διαφορετικών επιπέδων παρασιτικού θορύβου καθώς και του μεγάλου αριθμού κωδικοποιητών και αποκωδικοποιητών. Στην συνέχεια, τα στοιχεία αυτά μπορούν να χρησιμοποιηθούν για την σύγκριση με άλλα σχήματα κωδικοποίησης.

Perceptual Speech Quality Measurement

Αν και η προαναφερθείσα MOS είναι μια υποκειμενική μέθοδος για την αξιολόγηση της ποιότητα φωνής, εντούτοις δεν είναι η μόνη μέθοδος για τον σκοπό αυτό. Η ITU-T εισήγαγε τη σύσταση P.861, η οποία καλύπτει τους τρόπους που μπορεί να καθοριστεί η ποιότητα φωνής χρησιμοποιώντας την διαδικασία Perceptual Speech

Quality Measurement (PSQM). Η PSQM έχει πολλά μειονεκτήματα όταν χρησιμοποιείται σε συνδυασμό με κωδικοποιητές και αποκωδικοποιητές φωνής (vocoders). Ένα μειονέκτημα είναι ότι η PSQM διαδικασία καταγράφει αυτό που το ανθρώπινο αυτί δεν μπορεί να αντιληφθεί. Σύμφωνα μάλιστα με τους όρους του Layman, ένα άτομο μπορεί να εξαπατήσει το ανθρώπινο αυτί όσο αφορά την αντίληψη μιας υψηλότερης ποιότητας φωνής, αλλά ένας υπολογιστής δεν μπορεί να εξαπατηθεί. Επίσης, μειονέκτημα αποτελεί το γεγονός ότι η PSQM αναπτύχθηκε ώστε να αντιλαμβάνεται τις δυσχέρειες που προκαλούνται από τεχνικές συμπίεσης και από-συμπίεσης και όχι από την απώλεια πακέτων ή την διακύμανση του χρόνου άφιξης πακέτων.

3.3 Μηχανισμοί Ποιότητας Υπηρεσιών

Το μοντέλο best-effort υπηρεσιών του διαδικτύου δουλεύει ικανοποιητικά για τις περισσότερες εφαρμογές όταν το δίκτυο είναι σε ένα φυσιολογικό φόρτο. Εντούτοις, όταν ένα IP δίκτυο έχει μεγαλύτερο φόρτο κίνησης, η best-effort υπηρεσία μπορεί

να μην είναι επαρκής για κυκλοφορία από άκρη σε άκρη. Καθώς οι καθυστερήσεις αυξάνονται, τα πακέτα του δικτύου φτάνουν στους δρομολογητές με γρηγορότερους ρυθμούς από αυτούς που μπορούν οι δρομολογητές να τα εξυπηρετήσουν. Το γεγονός αυτό, έχει ως αποτέλεσμα την ανάπτυξη ουρών αναμονής. Όταν τα όρια μεγέθους των σειρών αναμονής ξεπερνιούνται, οι δρομολογητές αποκρίνονται με τη απόρριψη πακέτων.

Για την TCP κυκλοφορία, η απόρριψη πακέτων δεδομένων συνεπάγεται περισσότερες αναμεταδόσεις και οδηγεί σε χαμηλή απόδοση του δικτύου καθώς και σε φτωχή προσφερόμενη ποιότητα υπηρεσιών (QoS). Ο χρήστης αρχίζει να παρατηρεί καθυστερήσεις από άκρη σε άκρη ακόμη και με εφαρμογές όπως η μεταφορά αρχείων.

Εάν τα πακέτα δεδομένων που απορρίπτονται ανήκουν σε κυκλοφορία πραγματικού χρόνου, ο δέκτης δεν θα τα παραλάβει ποτέ και τα πακέτα δεν θα αναμεταδοθούν. Κατά συνέπεια, σε τέτοια δίκτυα η ποιότητα υπηρεσιών υποφέρει. Στην περίπτωση της μετάδοσης φωνής, ο ήχος μπορεί γρήγορα να γίνει ακατανόητος κατά την λήψη του στον δέκτη.

Για τις εφαρμογές που χρειάζονται υπηρεσίες καλύτερες από την προσφορά best-effort υπηρεσιών, υπάρχουν δύο διαφορετικές προσεγγίσεις: οι ενσωματωμένες υπηρεσίες (Integrated Services, intserv) και οι διαφοροποιημένες υπηρεσίες (Differentiated Services, diffserv).

3.3.1 Integrated Services

Η προσέγγιση των ολοκληρωμένων υπηρεσιών βασίζεται στο γεγονός ότι οι IP δρομολογητές δίνουν προτεραιότητα στην προνομιακή μεταχείριση κάποιων IP ροών δεδομένων σε σχέση με άλλες. Μια IP ροή θεωρείται ως ένα διακριτό ρεύμα σχετικών μεταξύ τους πακέτων δεδομένων και η οποία προκύπτει από δραστηριότητα ενός μόνο χρήστη και απαιτεί την ίδια ποιότητα υπηρεσιών. Στην πράξη, μια IP ροή διακρίνεται από το συνδυασμό : του πρωτοκόλλου, της IP διεύθυνσης της πηγής και του προορισμού, καθώς και το port της πηγής και του προορισμού.

Προκειμένου να υλοποιηθεί μια προνομιακή μεταχείριση για κάποιες συγκεκριμένες ροές, οι IP δρομολογητές θα πρέπει να ενσωματώσουν μερικές νέες λειτουργίες, όπως τους :

- **Classifier** : Πρόκειται για ένα συστατικό του δρομολογητή που επιθεωρεί τα εισερχόμενα πακέτα και τα μαρκάρει ώστε να θεωρηθούν ότι έχουν το δικαίωμα να λάβουν μια συγκεκριμένη μεταχείριση QoS από το δρομολογητή. Στην συνέχεια, ο classifier περνά το πακέτο στον scheduler.
- **Scheduler** : Αποτελεί το συστατικό του δρομολογητή που εξετάζει το σημάδι (mark) που έχει τεθεί σε κάθε πακέτο από τον classifier και διαχειρίζεται την προώθηση των πακέτων σε διαφορετικές ουρές αναμονής. Για παράδειγμα, ο scheduler, βασισμένος στο σημάδι του classifier, μπορεί να αποφασίσει ότι ένα πακέτο που ανήκει σε μια συγκεκριμένη ροή προωθείται πριν από ένα άλλο πακέτο που ανήκει σε μια διαφορετική ροή, ακόμα κι αν το τελευταίο πακέτο έφθασε νωρίτερα στη σειρά αναμονής από το πρώτο.

Η προσέγγιση των ολοκληρωμένων υπηρεσιών καθορίζει δύο διαφορετικά είδη υπηρεσιών που είναι : η υπηρεσία ελεγχόμενου φορτίου και η εγγυημένη υπηρεσία. Και οι δύο υπηρεσίες αντιπροσωπεύουν μια βελτιωμένη ποιότητα υπηρεσιών σε σύγκριση με την βασική ***best-effort υπηρεσία*** που παρέχεται από το διαδίκτυο.

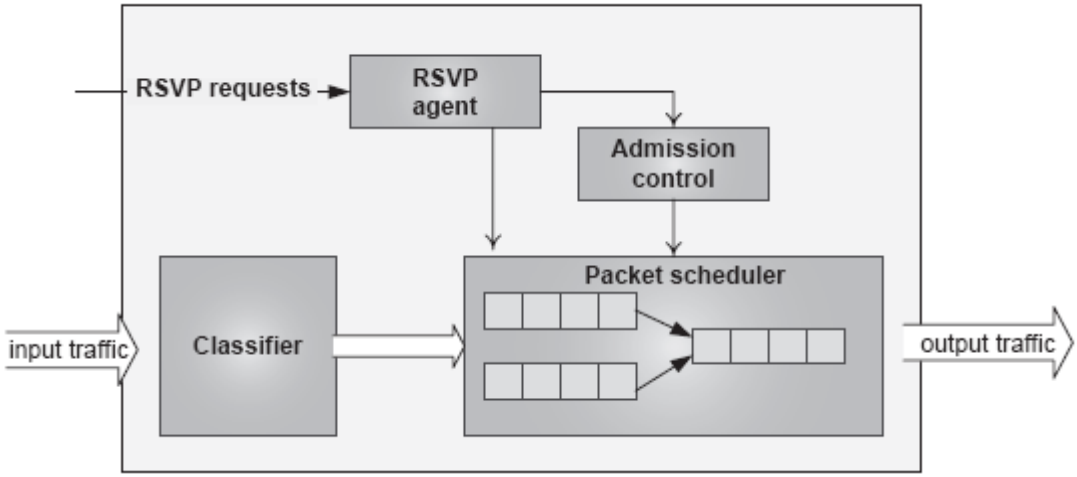
Η υπηρεσία ελεγχόμενου φορτίου (Controlled Load Service) παρέχει στους χρήστες μια ποιότητα υπηρεσίας που μοιάζει πολύ με την QoS που θα λάμβαναν στα πλαίσια ενός μη φορτωμένου δικτύου. Ακόμα και στην περίπτωση που το δίκτυο είναι κορεσμένο με παροχή best-effort υπηρεσιών, η υπηρεσία ελεγχόμενου φορτίου δίνει προτεραιότητα σε πακέτα υποκείμενα σε QoS, ως εκ τούτου μιμούμενη την συμπεριφορά ενός μη φορτωμένου δικτύου. Η υπηρεσία ελεγχόμενου φορτίου δεν προσφέρει την εγγύηση ότι η καθυστέρηση θα προορίζεται για μια συγκεκριμένη ροή, αλλά απλά, δίνει προνομιακή μεταχείριση σε μερικά πακέτα σε βάρος κάποιων άλλων.

Η εγγυημένη υπηρεσία (Guaranteed Service), αντίθετα με την υπηρεσία ελεγχόμενου φορτίου, παρέχει σε μια συγκεκριμένη ροή την διαβεβαίωση μιας οριακής καθυστέρησης. Συνεπώς, το jitter που παρατηρείται για εγγυημένη κυκλοφορία είναι μικρό έως αμελητέο.

Προκειμένου να εφαρμοστούν οι ενσωματωμένες υπηρεσίες, είναι απαραίτητα μερικά πρόσθετα στοιχεία που δεν έχουν αναφερθεί ακόμα. Κατ' αρχάς, οι πελάτες (clients) πρέπει να έχουν έναν μηχανισμό για να μπορούν να ζητούν να διατηρηθούν πόροι στους δρομολογητές, έτσι ώστε να μπορούν να τους εγγυηθούν μια καθορισμένη ποιότητα υπηρεσιών. Η λειτουργία αυτή είναι γνωστή ως δέσμευση πόρων (Resource Reservation). Δεύτερον, οι δρομολογητές (routers)

πρέπει να έχουν την ικανότητα της αποδοχής ή της απόρριψης νέων αιτημάτων δέσμευσης πόρων, βασισμένων στους υπάρχοντες διαθέσιμους πόρους των δρομολογητών. Η δεύτερη λειτουργία αναφέρεται ως έλεγχος αποδοχής (Admission Control).

Όταν ένας δρομολογητής λαμβάνει ένα αίτημα για την διαχείριση μιας νέας ροής, τότε ο δρομολογητής ελέγχει εάν έχει αρκετούς διαθέσιμους πόρους για να μπορέσει να την εξυπηρετήσει χωρίς όμως αυτό να έχει αντίχτυπο σε άλλες ροές υπό εξέλιξη. Εάν η ποιότητα υπηρεσιών που ζητείται για την εξυπηρέτηση της ροής μπορεί να χορηγηθεί, τότε ο δρομολογητής διατηρεί πόρους για την καινούργια ροή. Το παρακάτω σχήμα 3.4 αντιπροσωπεύει τις διαφορετικές λειτουργίες σε έναν IP δρομολογητή εκτεταμένο με τη προσέγγιση των ολοκληρωμένων υπηρεσιών.

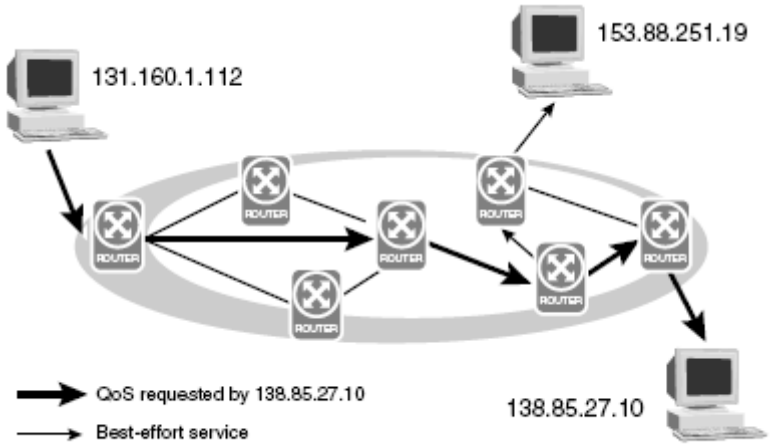


Σχήμα 3.4 : Απεικόνιση των διαφορετικών λειτουργιών σε έναν IP δρομολογητή εκτεταμένο με τη προσέγγιση των ολοκληρωμένων υπηρεσιών.

Πληροφορίες κατάστασης που αποθηκεύονται στο δίκτυο

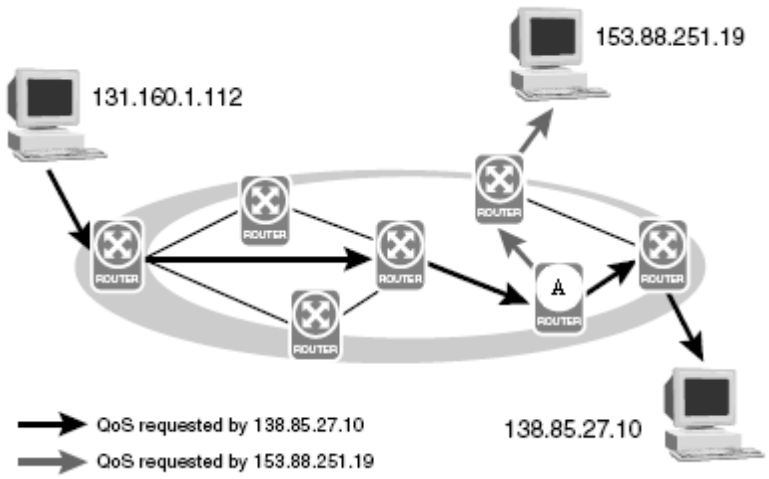
Οι δρομολογητές πρέπει να αποθηκεύουν τις πληροφορίες για τις IP ροές προκειμένου ώστε να διαφοροποιηθούν κατάλληλα τα πακέτα δεδομένων. Το γεγονός αυτό υπονοεί ότι το δίκτυο αποθηκεύει πληροφορίες κατάστασης. Ακολουθώντας την παραπάνω τακτική ερχόμαστε αντίθετοι με την IP θεώρηση, που ωθεί την νοημοσύνη στα τελικά συστήματα και αποθηκεύει όσο το δυνατόν λιγότερες πληροφορίες κατάστασης στο δίκτυο. Η ανταλλαγή αυτή για λιγότερες πληροφορίες οδηγεί σε πιο ισχυρά συστήματα που διαχειρίζονται καλύτερα τις αποτυχίες δικτύων. Αναγνωρίζοντας την αξία της IP θεώρησης αλλά και την ανάγκη να πραγματοποιηθούν εξαιρέσεις σε κάποιες περιπτώσεις, η συγχώνευση

κρατήσεων (Reservation Merging) και οι Soft States βοηθούν στην ελαχιστοποίηση των προβλημάτων που μπορούν να προκαλέσουν οι εξαιρέσεις.



Σχήμα 3.5 : Ο host 138.85.27.10 ζητά την παροχή QoS για την IP ροή του.

Τα σχήματα 3.5 και 3.6 δείχνουν τον τρόπο που εκτελείται η συγχώνευση κρατήσεων (Reservation Merging) σε μια multicast ομάδα. Ο host 131.160.1.112 είναι ο αποστολέας ενώ οι υπόλοιποι οικοδεσπότες, δηλαδή οι 153.88.251.19 και 138.85.27.10 είναι οι δέκτες. Στο σχήμα 3.5, ο δέκτης 138.85.27.10 ζητά μια ορισμένη QoS για την εισερχόμενη ροή του. Οι δρομολογητές του μονοπατιού αποθηκεύουν τις απαραίτητες πληροφορίες κατάστασης και αποδίδουν την ζητούμενη ποιότητα υπηρεσιών.

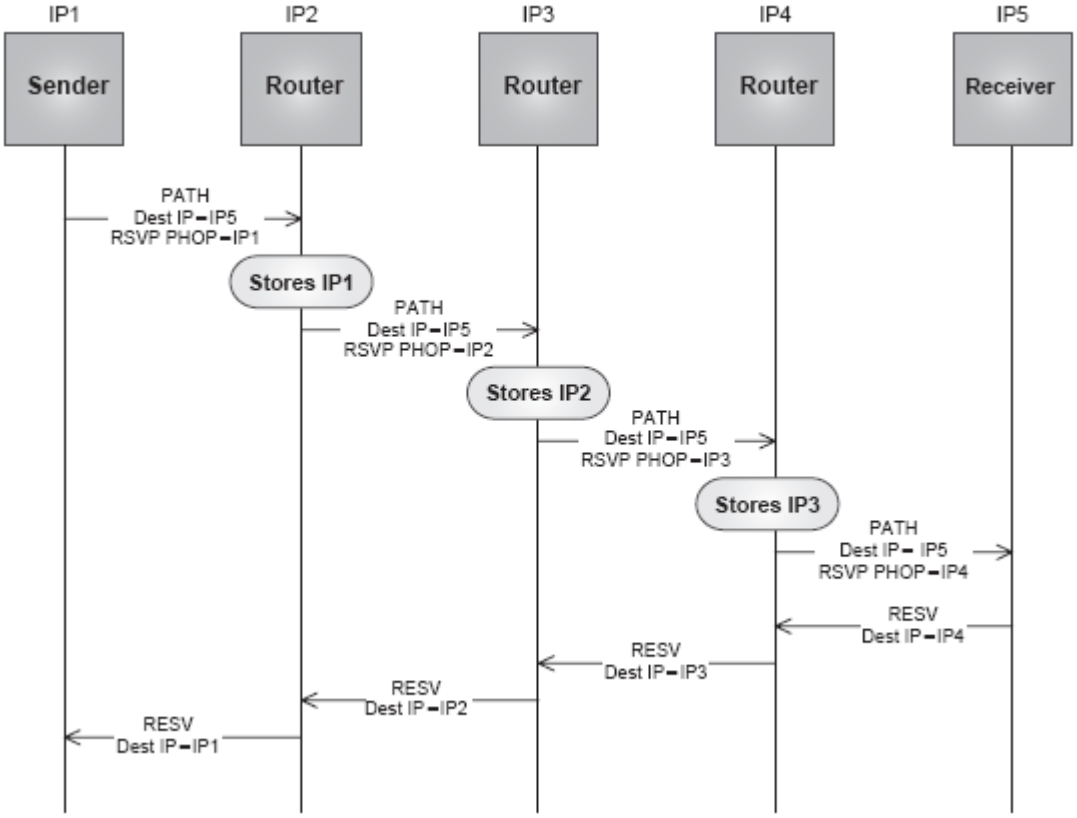


Σχήμα 3.6 : Ο host 138.85.27.19 ζητά επίσης την παροχή QoS για την IP ροή του.

Στην συνέχεια, ο δέκτης 153.88.251.19 ζητά επίσης την προσφορά ποιότητας υπηρεσιών για τη ροή που λαμβάνει. Εντούτοις, ο δεύτερος οικοδεσπότης δεν χρειάζεται να ζητήσει QoS για ολόκληρο το μονοπάτι από τον αποστολέα επειδή η QoS είναι ήδη παρούσα στο πρώτο μέρος του μονοπατιού για την ίδια ροή δεδομένων. Επομένως, όταν ο 153.88.251.19 ζητά την προσφορά QoS, οι πληροφορίες κατάστασης, που έχουν αποθηκευτεί στους δρομολογητές στο μονοπάτι που ήταν ήδη παραχωρημένο για QoS για τον πρώτο οικοδεσπότη, δεν υφίστανται καμία αλλαγή. Αντίθετα, οι νέες πληροφορίες κατάστασης περιορίζονται σε εκείνους τους δρομολογητές στο μονοπάτι από τον 153.88.251.19 έως τον τελευταίο δρομολογητή (router A) στο κύριο δέντρο διανομής. Η τελευταία διαδικασία φαίνεται στο σχήμα 3.6.
Η υλοποίηση των λεγόμενων Soft States αυξάνει την ευρωστία του συστήματος. Οι Soft States αποθηκεύουν προσωρινά τις πληροφορίες κατάστασης, και μετά τις οποίες ο δρομολογητής απομακρύνει όλες της πληροφορίες κατάστασης που διατηρούσε αποθηκευμένες. Στο πλαίσιο αυτού του συστήματος, εάν οι πληροφορίες κατάστασης δεν ανανεώνονται περιοδικά, τότε θα λήξουν και θα επιτρέψουν την απελευθέρωση όλων των πόρων που έχουν δεσμευθεί στο δρομολογητή. Οι Soft States ανανεώνονται περιοδικά με την αποστολή ενός μηνύματος στο δρομολογητή με τις κατάλληλες πληροφορίες, ενώ οι Hard States αποθηκεύονται μόνιμα στους δρομολογητές και απαιτούν μια εντολή απελευθέρωσης κατάστασης για την αποδέσμευση των πόρων.

Η διαδικασία της δέσμευσης των πόρων μπορεί να πραγματοποιηθεί με την χρησιμοποίηση του πρωτοκόλλου δέσμευσης πόρων (Resource Reservation Protocol, RSVP). Οι πελάτες μπορούν μέσω του πρωτοκόλλου RSVP να επισημάνουν στους δρομολογητές την αναγνώριση της ταυτότητας των ροών. Αυτό μπορεί να γίνει με την παροχή πληροφοριών που αφορούν πρώτον το συνδυασμό του πρωτοκόλλου, της IP διεύθυνσης της πηγής και του προορισμού, καθώς και το port της πηγής και του προορισμού και δεύτερον με τη ζητούμενη ποιότητας υπηρεσιών για την εξυπηρέτηση των πελατών. Οι δρομολογητές ελέγχουν εάν έχουν τους διαθέσιμους πόρους για να ικανοποιήσουν το αίτημα. Εάν έχουν, τότε τα πακέτα διαμορφώνονται με κατάλληλο τρόπο από τον classifier και τον scheduler

του κάθε δρομολογητή, ώστε ο δρομολογητής να δώσει ιδιαίτερη μεταχείριση και προτεραιότητα σε πακέτα που μόλις φθάνουν και αντιστοιχούν σε συγκεκριμένες ροές. Προκειμένου να δεσμευτούν οι πόροι και προς τις δύο κατευθύνσεις τότε πρέπει να εκτελεσθούν δύο διαδικασίες δεσμεύσεων.



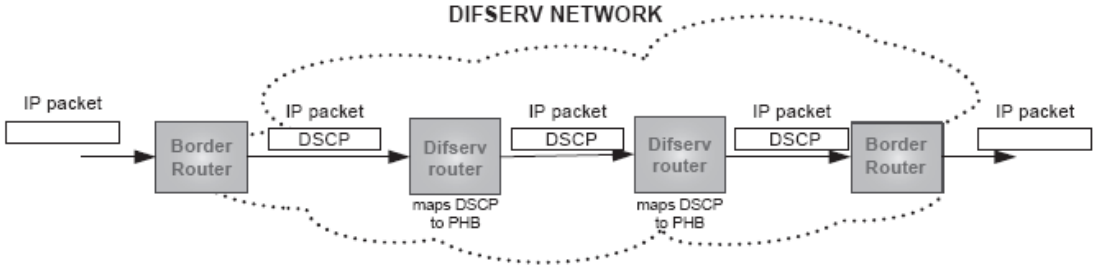
Σχήμα 3.7 : Τρόπος λειτουργίας του RSVP πρωτοκόλλου.

Η τρόπος λειτουργίας του RSVP πρωτοκόλλου είναι αρκετά απλός. Προκειμένου να δεσμευθούν πόροι προς την μια κατεύθυνση, πρέπει να ακολουθηθεί μια διαδικασία δύο σταδίων. Αρχικά, ο αποστολέας στέλνει ένα RSVP PATH μήνυμα που προορίζεται για τον δέκτη (δηλαδή, η IP διεύθυνση προορισμού του πακέτου είναι η διεύθυνση του παραλήπτη). Καθώς το μήνυμα διαβαίνει τους δρομολογητές στην πορεία προς τον παραλήπτη, θα αποθηκεύει σε κάθε δρομολογητή τη διεύθυνση του προηγούμενου δρομολογητή (που μεταβιβάζεται στην RSVP PHOP παράμετρο). Όταν το RSVP PATH μήνυμα φθάνει στον δέκτη, τότε ο δέκτης δημιουργεί ένα RESV μήνυμα που στην πραγματικότητα χρησιμοποιείται για να δεσμεύσει τους απαραίτητους πόρους στους δρομολογητές. Το μήνυμα RESV θα διαβεί προς τα πίσω όλους τους δρομολογητές που είχε προσπελάσει προηγουμένως το RSVP PATH μήνυμα. Η δρομολόγηση του RESV μηνύματος

εκτελείται με hop-by-hop τρόπο χρησιμοποιώντας τις πληροφορίες κατάστασης που είχαν προηγουμένως αποθηκευτεί σε κάθε δρομολογητή από το RSVP PATH μήνυμα. Με αυτό τον τρόπο, βεβαιώνεται ότι η δέσμευση πόρων πραγματοποιείται από τους ίδιους τους δρομολογητές που θα χειριστούν τα πακέτα από τον αποστολέα προς τον παραλήπτη, και η οποία θα ακολουθήσει την ίδια διαδρομή που λαμβάνεται από RSVP PATH μήνυμα. Η διαδικασία παρουσιάζεται στο σχήμα 3.7.

3.3.2 Differentiated Services

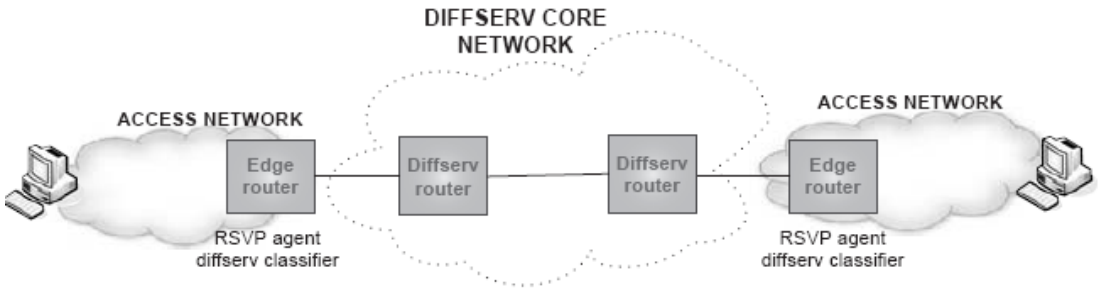
Η προσέγγιση των διαφοροποιημένων υπηρεσιών, όπως και η προσέγγιση των ολοκληρωμένων υπηρεσιών, βασίζεται στην απόδοση προνομιακής μεταχείρισης στους δρομολογητές σε μερικά πακέτα σε σχέση με άλλα. Εντούτοις, αντί της μεταχείρισης των διαφορετικών ροών με ξεχωριστό τρόπο, η προσέγγιση των διαφοροποιημένων υπηρεσιών στηρίζεται στους δρομολογητές συνόρων οι οποίοι χαρακτηρίζουν τα εισερχόμενα πακέτα με μια ετικέτα αποκαλούμενη ως σημείο κώδικα διαφοροποιημένων υπηρεσιών (Differentiated Services Code Point, DSCP). Κατόπιν, οι εσωτερικοί δρομολογητές στο δίκτυο πρέπει να εξετάσουν το DSCP στο πακέτο και βασισμένοι σε αυτό να εφαρμόζουν μια συγκεκριμένη per-hop συμπεριφορά (Per-Hop Behavior, PHB) που διαμορφώνεται σε κάθε δρομολογητή. Με άλλα λόγια, η προσέγγιση των διαφοροποιημένων υπηρεσιών βασίζεται στην εφαρμογή συγκεκριμένης μεταχείρισης προς συναθροίσεις πακέτων, παρά σε συγκεκριμένες ροές όπως στις ενσωματωμένες υπηρεσίες. Το γεγονός αυτό επιτρέπει στις διαφοροποιημένες υπηρεσίες να προσαρμόζονται πολύ καλύτερα από τις ενσωματωμένες υπηρεσίες. Το σχήμα 3.8 παρουσιάζει την προσέγγιση διαφοροποιημένων υπηρεσιών.



Σχήμα 3.8 : Η προσέγγιση των διαφοροποιημένων υπηρεσιών.

Integrated Services over Diffserv Networks

Το γεγονός ότι η προσέγγιση των ολοκληρωμένων υπηρεσιών απαιτεί οι δρομολογητές να ταξινομούν τις διαφορετικές ροές, και ως εκ τούτου να αναζητούν σε διάφορα πεδία των πρωτοκόλλων ώστε να προσδιορίσουν κάθε ροή, έχει αντίχτυπο στην επεκτασιμότητα του δικτύου. Κατά συνέπεια, δεν θεωρείται καλή προσέγγιση για τον πυρήνα του δικτύου, αν και ταιριάζει καλά με το δίκτυο πρόσβασης. Για τον πυρήνα του δικτύου η προσέγγιση των διαφοροποιημένων υπηρεσιών αποτελεί καλύτερη επιλογή. Με τον τρόπο αυτό, και οι δύο μηχανισμοί μπορεί να αποδειχθούν συμπληρωματικοί για την προσφορά από άκρη σε άκρη ποιότητας υπηρεσιών στους τελικούς χρήστες. Επιπλέον, μια καλή λύση αποτελεί η χρησιμοποίηση του PSVP, το οποίο χρησιμοποιείται για την δέσμευση των πόρων στο δίκτυο πρόσβασης, αλλά και για να ενημερώνει τους δρομολογητές συνόρων, μεταξύ του δικτύου πρόσβασης (υλοποίηση intserv) και του δικτύου πυρήνα (υλοποίηση diffserv), για τον τρόπο που πρέπει να θέσουν τη diffserv ετικέτα σε πακέτα που ανήκουν σε συγκεκριμένες ροές. Το σχήμα 3.9 παρουσιάζει το πιθανό αυτό σενάριο.



Σχήμα 3.9 : Integrated Services over Diffserv Networks

Παραλλαγές αυτής της προσέγγισης προτείνονται για τα νεώτερα IP δίκτυα της επόμενης γενιάς (3GPP IMS, TISPAN NGN), όπου αντί του RSVP τυπικά χρησιμοποιούνται άλλα πρωτόκολλα για να διεκπεραιώσουν τις QoS απαιτήσεις (π.χ., 3GPP Generic Tunneling Protocol, GTP).[20][38]

Κεφάλαιο 4

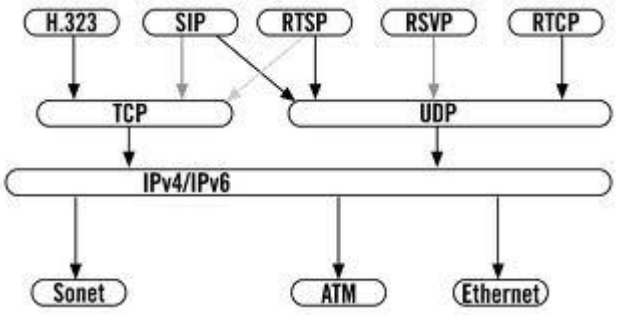
4.1 Εισαγωγή

Τα πρωτόκολλα VoIP είναι η αρχή και το τέλος αυτής της τεχνολογίας. Από τη στιγμή που κάποιος χρήστης θελήσει να πραγματοποιήσει μια κλήση ενεργοποιείται μία σειρά πρωτοκόλλων τα οποία θα αναλάβουν να την πραγματοποιήσουν.
Τα πιο συχνά αναφερόμενα πρωτόκολλα είναι τα πρωτόκολλα σηματοδοσίας (signaling protocols). Σε VoIP δίκτυα κάνουμε χρήση αυτών των πρωτοκόλλων για να εντοπίσουμε τη συσκευή στο άλλο άκρο της επικοινωνίας. Στη συνέχεια το πρωτόκολλο διαπραγματεύεται την ανταλλαγή μεταξύ των συσκευών αποστολής και λήψης. Τα δύο πιο γνωστά πρωτόκολλα σηματοδοσίας είναι:

- H.323, που ορίζεται από τη Διεθνή Ένωση Τηλεπικοινωνιών (ITU).
- Session Initiation Protocol (SIP), που ορίζεται από το Internet Engineering Task Force (IETF).

Ένα άλλο σύνολο πρωτοκόλλων, που ονομάζονται πρωτόκολλα συσκευής ελέγχου, διαχωρίζουν το κομμάτι του ελέγχου κλήσης από το κομμάτι που αλληλεπιδρά με την PSTN γραμμή στις VoIP πύλες. Παράδειγμα αυτών των πρωτοκόλλων είναι το πρωτόκολλο Media Gateway Control Protocol (MGCP).

Επίσης σημαντικό κομμάτι στην οικογένεια των πρωτοκόλλων είναι το RTP (Real Time Protocol) πρωτόκολλο που χρησιμοποιείται για την ενθυλάκωση ήχου και βίντεο σε IP πακέτα. Το RTP λειτουργεί σε συνδυασμό με το SIP ή το H.323. Μια κλήση VoIP χρησιμοποιεί δύο RTP ρεύματα, ένα προς κάθε κατεύθυνση.
Στη συνέχεια θα αναλύσουμε τα παραπάνω πρωτόκολλα με περισσότερη λεπτομέρεια αλλά θα αναπτύξουμε και κάποια άλλα που χρησιμοποιούνται σε συνδυασμό με τα βασικά πρωτόκολλα του VoIP.



Εικόνα 4.1: Πρωτόκολλα VoIP

4.2 Πρωτόκολλο H.323

Το πρωτόκολλο H.323 υλοποιήθηκε από την ITU-T αρχικά για να περιγράψει τον τρόπο που τα συστήματα πολυμέσων (multimedia systems) ήταν δυνατό να διασυνδεθούν και να επικοινωνήσουν με πολυμέσα κίνησης αποτελούμενα από φωνή πραγματικού χρόνου (real time voice), βίντεο και δεδομένων, μέσω των τοπικών δικτύων υπολογιστών (Local Area Networks LANs), χρησιμοποιώντας τερματικές συσκευές, όπως προσωπικούς υπολογιστές (PCs) και βίντεο-τηλέφωνα (videophones). Αποτελεί την επέκταση του H.320 προτύπου, το οποίο αφορούσε στην τηλεδιάσκεψη πάνω από το ISDN, με την προσθήκη της υποστήριξης των PSTN γραμμών (απλές αναλογικές γραμμές). Η εισαγωγή του H.323 ήρθε σαν αποτέλεσμα της ανάγκης για τη δημιουργία ενός πρωτοκόλλου που θα μπορούσε να υποστηρίξει ικανοποιητικά εφαρμογές πολυμέσων και φωνής, με δυνατότητα για εξουδετέρωση της ανεπιθύμητης καθυστέρησης που αποτελεί χαρακτηριστικό φαινόμενο στα κλασικά δίκτυα LAN. Σημαντικό στοιχείο αποτέλεσε επίσης η συνεχώς 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 επίσης πλατφόρμες που χρησιμοποιεί ο χρήστης για τις εφαρμογές του έχουν αποκτήσει αξιοσημείωτη ταχύτητα τόσο αποθήκευσης, όσο και προβολής και επεξεργασίας στοιχείων. Το πρωτόκολλο έλαβε υπόψη του τα παραπάνω για να διαμορφώσει μία συμπεριφορά που περιλαμβάνει τα ακόλουθα:

- 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 μία ολοκληρωμένη πρόταση για τη δημιουργία ενός δικτυακού περιβάλλοντος που ενσωματώνει πολλαπλές παλιές και νέες τεχνολογίες

από διαφορετικούς κατασκευαστές σε ένα ενιαίο πλαίσιο διαχείρισης πληροφορίας φωνής και βίντεο.

Το πρωτόκολλο αποτελείται από τρία διαφορετικά κομμάτια:

1.Terminal

Πρόκειται για τα τελικά σημεία χρηστών, που υποστηρίζουν αμφίδρομη επικοινωνία, υποχρεωτικά επικοινωνιών φωνής και προαιρετικά βίντεο και δεδομένων. Το H.323 καθορίζει τον τρόπο με τον οποίο διαφορετικοί τερματικοί σταθμοί είναι δυνατό να επικοινωνήσουν. Τα τερματικά θα πρέπει συμπληρωματικά να υποστηρίζουν το πρωτόκολλο H.245 που κατευθύνει τη χρήση των καναλιών επικοινωνίας μεταξύ τερματικών σταθμών, το πρωτόκολλο Q.931 για σηματοδοσία κλήσης, το πρωτόκολλο Registration/Admission/Status (RAS) για επικοινωνία με το Gatekeeper καθώς επίσης και το Real Time Protocol (RTP) και το Real Time Control Protocol (RTCP) για την εν σειρά αποστολή και λήψη των πακέτων φωνής. Ειδικά για την περίπτωση της επικοινωνίας με φωνή, υποστηρίζεται το πρότυπο G.711 για συμπίεση και απόδοση πακέτων με ρυθμούς 54 ή 64 kbps σε ένα τοπικό δίκτυο δεδομένων.

2. Gateway

Είναι το μοναδικό προαιρετικό στοιχείο του H.323 και παρέχει τόσο τη φυσική όσο και τη λογική διασύνδεση μεταξύ των τηλεφωνικών συσκευών και του επικοινωνιακού δικτύου. Χρησιμοποιείται συνήθως για τους παρακάτω λόγους:

- την επικοινωνία μεταξύ αναλογικών PSTN τερματικών,
- την επικοινωνία με απομακρυσμένους H.320 σταθμούς ISDN δικτύων,
- την επικοινωνία με απομακρυσμένους H.323 σταθμούς PSTN δικτύων.

Παρέχει standard interfaces προς την PSTN υπηρεσία και χρησιμοποιεί CODECs για τη μετατροπή τηλεφωνικών κυκλωμάτων σε πακέτα δεδομένων, τα οποία σε συνεργασία με τον gatekeeper μέσω του πρωτοκόλλου RAS δρομολογεί 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 και μόνο δικτύου και δεν ενδιαφέρονται για πρόσβαση εκτός αυτού.

3. Multipoint Conference Unit (MCU)

Καθορίζει και ελέγχει την ταυτόχρονη διασύνδεση (συνεδρία) περισσότερων των δύο τερματικών σταθμών. Αποτελείται από δύο διακριτά τμήματα, τον Multipoint Controller (MC), η ύπαρξη του οποίου είναι αναγκαστική και προαιρετικά ενός ή περισσοτέρων Multipoint Processors (MP). Ο MC ελέγχει την διαπραγμάτευση 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 τη ροή των δεδομένων φωνής ή βίντεο σε πραγματικό χρόνο, υλοποιώντας τεχνικές για mixing και switching.

Έλεγχος (Control)

Είναι ίσως το πλέον ουσιαστικό από τα χαρακτηριστικά γνωρίσματα κάθε πρωτοκόλλου, γιατί περιλαμβάνει μία σειρά από διαδικασίες σηματοδοσίας που αφορούν εγκαθίδρυση και τερματισμό της επικοινωνίας και διερεύνηση των δυνατοτήτων που διαθέτει κάθε ένας εκ των συμμετεχόντων μελών. Το ουσιαστικό όμως είναι ότι όλες οι υπηρεσίες ελέγχου αποτελούν ένα ανεξάρτητο στρώμα (control layer) υπό την καθοδήγηση του οποίου πραγματοποιούνται μία σειρά από αποφασιστικής σημασίας διεργασίες, όπως είναι αυτές των framing, serial numbering, error correction και error recovery. Οι παραπάνω υπηρεσίες ελέγχου, εξυπηρετούνται όπως προαναφέρθηκε από τις παρακάτω τρεις διακριτές διαδικασίες ελέγχου.

α) H.245 Control Channel: Είναι το κανάλι επικοινωνίας που συντονίζει όλες τις λειτουργίες ελέγχου μεταξύ των H.323 τερματικών με δυνατότητα εγκατάστασης και τερματισμού ενός λογικού καναλιού επικοινωνίας, μεταφορά των μηνυμάτων ελέγχου ροής πακέτων και πάνω από όλα ικανότητα για υποστήριξη της βασικής λειτουργίας "ανταλλαγής ικανοτήτων" των τερματικών, αυτό που συχνά αναφέρεται σαν "capabilities exchange".

β) Πρωτόκολλο Q.931: Χρησιμοποιείται αποκλειστικά στην πρώιμη φάση εγκαθίδρυσης της επικοινωνίας μεταξύ των τερματικών σταθμών.

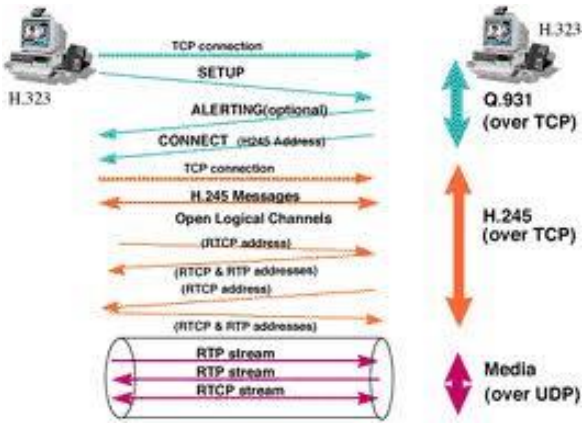
γ) Πρωτόκολλο RAS: Εκτελεί διαδικασίες που αφορούν στην εγγραφή (registration), αποδοχή (admission), περιγραφή κατάστασης (status determination) και καθορισμού μεταβολής ρυθμού αποστολής/λήψης πακέτων μεταξύ των τερματικών και του gatekeeper.

Η.323 πάνω από το Internet Protocol (IP). Η λειτουργία του Η.323 για τη μεταφορά της φωνής πάνω από ένα κλασικό IP δίκτυο θα πρέπει να πληρεί δύο απαραίτητες προϋποθέσεις. Την αξιόπιστη μεταφορά της σηματοδοσίας που μεταφράζεται σε διανομή των πακέτων ελέγχου στη σωστή τους σειρά, και την όχι απόλυτα αξιόπιστη που αφορά στη διανομή των υπολοίπων πακέτων που περιέχουν την πληροφορία φωνής. Η αξιόπιστη μετάδοση της σηματοδοσίας, όταν μεταφερθεί στο χώρο του IP πρωτοκόλλου αντιστοιχεί στο Transmission Control Protocol (TCP) και εγγυάται αξιόπιστη, ακολουθιακή, χωρίς λάθη μετάδοση των πακέτων, που αναλογεί όμως και σε χρονικές καθυστερήσεις και κατανάλωση bandwidth. Το Η.323 χρησιμοποιεί το TCP και το Η.245 end-to-end connection πρωτόκολλο. Από την άλλη πλευρά και με τη χρήση του User Datagram Protocol (UDP) που μπορεί και να μεταφραστεί σαν "η καλύτερη δυνατή προσπάθεια για μετάδοση/λήψη πακέτων", έχουμε μεν ταχεία μεταγωγή των πακέτων, συχνά όμως συμβαίνουν λάθη μετάδοσης που δεν ανακαλύπτονται και πακέτα που δε φτάνουν στον προορισμό με τη σειρά αποστολής τους. Εάν λοιπόν οι "ευαίσθητες" πληροφορίες ελέγχου μεταδίδονται πάνω από το TCP, οι υπόλοιπες χρησιμοποιούν το UDP και πιο συγκεκριμένα το IP multicast και το RTP που δρα στην κορυφή του IP multicast για τη διαχείριση των voice streams.

Ο τρόπος με τον οποίο δύο χρήστες τηλεφώνου είναι δυνατό να επικοινωνήσουν μεταξύ τους διαμέσου ενός δρομολογητή (router) έχει ως εξής :

- Ο χρήστης σηκώνει το ακουστικό σηματοδοτώντας ένα off-hook σήμα προς τη συσκευή του τοπικού τηλεφωνικού βρόγχου (local loop), όποια κι αν είναι αυτή (PBX ή router).
- Η σύνδεση που ανοίγεται, αποδίδει dial tone και περιμένει από το χρήστη να επιλέξει τον επιθυμητό αριθμό.
- Ο χρήστης επιλέγει τον αριθμό τον οποίο λαμβάνει η τηλεφωνική συσκευή του τοπικού βρόγχου.
- Ο αριθμός αντιστοιχίζεται σε ένα IP σταθμό, ο οποίος απευθύνει την κλήση κατευθείαν ή διαμέσου του PBX στο σταθμό αποστολής.

- Το H.323 χρησιμοποιείται πλέον για να εγκαταστήσει ένα κανάλι αποστολής και ένα λήψης πάνω από το IP.
- Ενεργοποιούνται οι codecs και στις δύο πλευρές, και αρχίζει η μεταφορά των πακέτων με χρήση της RTP/TCP/UDP στοίβας.
- Στο τέλος η συνομιλία τελειώνει και οι δύο πλευρές περιμένουν για νέα επαφή. [5]



Εικόνα 4.2: Ανταλλαγή μηνυμάτων πρωτοκόλλου H.323 μεταξύ δυο τερματικών σταθμών

4.3 Πρωτόκολλο Session Initiation Protocol (SIP)

Το SIP, συντομογραφία του Session Initiation Protocol (Πρωτόκολλο εκκίνησης συνόδου), είναι ένα πρωτόκολλο σηματοδοσίας τηλεφωνίας IP που χρησιμοποιείται για την πραγματοποίηση, την τροποποίηση και τον τερματισμό τηλεφωνικών κλήσεων VOIP. Δημιουργήθηκε από την Internet Engineering Task Force (IETF, συγκεκριμένα από την MMUSIC Working Group), το όργανο που είναι υπεύθυνο για τη διαχείριση και την ανάπτυξη των μηχανισμών που συνθέτουν το διαδίκτυο. Αρχικά δημοσιεύτηκε το 1996 με την ονομασία RFC 2543 και αργότερα το 2002 δημοσιεύτηκε η νέα έκδοση του ως RFC 3261. Τα τελευταία χρόνια, η VoIP κοινότητα ‘υιοθέτησε’ το SIP, ως το κύριο πρωτόκολλο σηματοδοσίας και έτσι το πρωτόκολλο αυτό συνεχίζει να εξελίσσεται και να επεκτείνεται όσο προχωρά η τεχνολογία και αρχίζει να καθιερώνεται και στην αγορά.

Το SIP είναι ένα πρωτόκολλο βασισμένο σε τεχνολογία text-based και μπορεί να λειτουργήσει είτε σε TCP ή UDP. Λόγω της τεχνολογίας του μπορεί και χρησιμοποιεί υψηλότερα επίπεδα επικοινωνίας, όπως είναι το Hypertext Transfer Protocol (HTTP) και το Simple Mail Transfer Protocol (SMTP). Έτσι μπορεί και

προσφέρει αποτελεσματικότητα, απλότητα και ευελιξία. Το SIP κατηγοριοποιείται ως ένα client-server πρωτόκολλο.

Client: Είναι μια εφαρμογή η οποία στέλνει ένα αίτημα SIP. Το ρόλο του client μπορεί να παίξει ένα software πρόγραμμα, όπως το Windows Messenger και το Skype ή μια συσκευή, πχ ένα VoIP τηλέφωνο.
Server: Ένας server γενικά απαντάει σε ένα αίτημα ενός client. Ένας server μπορεί να είναι ένα πρόγραμμα software,όπως το Live Communications Server 2003, ή μια συσκευή.

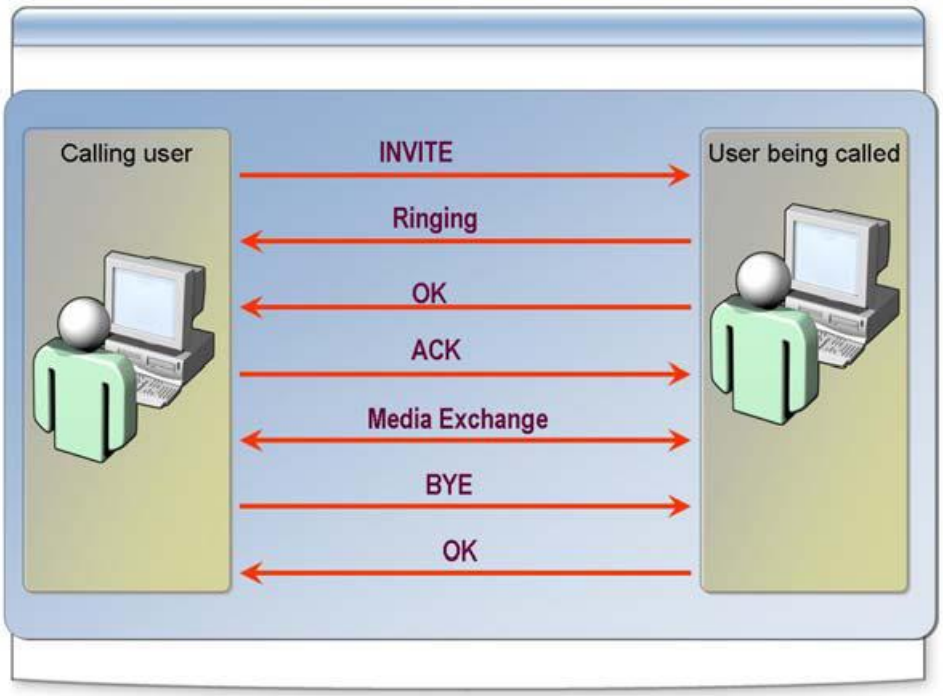
Οι SIP servers χωρίζονται σε 3 κατηγορίες:
Proxy server: Ένας SIP proxy server μοιάζει στην λειτουργεί σαν ένας HTTP proxy server. Όταν ένας client στέλνει ένα αίτημα στον proxy, ο proxy είτε το χειρίζεται ο ίδιος είτε το προωθεί σε κάποιον άλλο server.

Redirect server: Ένας SIP redirect server δέχεται ένα αίτημα SIP και μεταφέρει στον αρχικό client τον τρόπο με τον οποίο δρομολογείται η κλήση.

Registrar server. Ένας SIP registrar server δέχεται αιτήματα καταχώρισης και δημιουργεί έναν πίνακα συνδέοντας τη διεύθυνση ενός client με το user name του χρήστη που τον χρησιμοποιεί. Ένας registrar server συνήθως συνδιάζεται σε μια συσκευή με έναν proxy ή έναν redirect server.

Λειτουργία Πρωτοκόλλου SIP

Η διαδικασία για την έναρξη μιας συνομιλίας ξεκινά με ένα μήνυμα INVITE, το οποίο αποστέλλεται από τον καλών χρήστη στον καλούμενο, προσκαλώντας τον να συμμετάσχει στη συνομιλία. Ο καλών είναι πιθανόν να λάβει κάποια ενδιάμεσα μηνύματα προτού απαντήσει ο καλούμενος. Για παράδειγμα, μπορεί να υπάρχει πληροφόρηση για το αν υπάρχει χτύπος ειδοποίησης στον καλούμενο. Όταν η κλήση απαντηθεί από τον καλούμενο δημιουργείται ένα μήνυμα OK και αποστέλλεται στον καλών. Αυτός τότε στέλνει ένα μήνυμα ACK και αμέσως μετά ξεκινά η συνομιλία. Όταν κάποιος από τους χρήστες τερματίσει τη συνομιλία δημιουργείται ένα μήνυμα BYE και αποστέλλεται στον άλλο συνομιλητή ο οποίος επιβεβαιώνει το τέλος της συνομιλίας.



Εικόνα 4.3: Ανταλλαγή μηνυμάτων πρωτοκόλλου SIP μεταξύ δυο τερματικών σταθμών

Δομή μηνυμάτων SIP

Τα μηνύματα SIP χωρίζονται σε μηνύματα αίτησης και σε μηνύματα απάντησης. Αποτελούνται από την κεφαλίδα, μια κενή γραμμή και προαιρετικά ένα κομμάτι δεδομένων.

Α) τα πακέτα μηνυμάτων αίτησης έχουν την ακόλουθη δομή:

Μέθοδος	URI	Έκδοση SIP

Μέθοδος: η ενέργεια η οποία θα πραγματοποιηθεί. Πιθανές ενέργειες είναι invite, ack, options, bye, cancel, register.

ΜΕΘΟΔΟΣ	**ΕΚΤΕΛΕΣΙΜΗ ΕΝΕΡΓΕΙΑ**
INVITE	Αρχικοποίηση Κλήσης
ACK	Επιβεβαίωση Κλήσης
BYE	Τερματισμός Κλήσης
CANCEL	Ακύρωση προηγούμενης ενέργειας

OPTIONS	Features support by other side
REGISTER	Register with location service

URI: URI (Uniform Resource Identifier) είναι η διεύθυνση του χρήστη στον οποίο αποστέλλετε το μήνυμα.

Έκδοση SIP: Η έκδοση του πρωτοκόλλου που χρησιμοποιείται.

β) Τα πακέτα μηνυμάτων απάντησης έχουν την ακόλουθη δομή:

Έκδοση SIP	Κωδικός μηνύματος	Επεξήγηση κατάστασης

Έκδοση SIP: Η έκδοση του πρωτοκόλλου που χρησιμοποιείται.

Κωδικός μηνύματος: Ένας τριψήφιος ακέραιος αριθμός ο οποίος αντιστοιχεί σε ένα μήνυμα απάντησης.

ΚΩΔΙΚΟΙ ΜΗΝΥΜΑΤΩΝ	ΕΝΕΡΓΕΙΑ
1xx	αναζήτησης, κουδουνίσματος, αναμονής
2xx	Επιτυχίας
3xx	Προώθησης
4xx	λάθη Client
5xx	βλάβες Server
6xx	Κατειλημμένη γραμμή, άρνησης

Επεξήγηση κατάστασης: περιγραφή του μηνύματος

4.4 Session Description Protocol (SDP)

Το SDP (Session Description Protocol) αποτελεί ένα κομμάτι του πρωτοκόλλου SIP, έχει δημοσιευθεί από την IETF (Internet Engineering Task Force) με την ονομασία RFC 4566. Υπάρχουν επιπλέον RFC (Request for Comments) τα οποία τεκμηριώνουν επεκτάσεις καθώς και βελτιώσεις του SDP.

Το SDP είναι ένα πρότυπο που επιτρέπει σε μια συσκευή πολυμέσων να περιγράφει τα είδη των υπηρεσιών δεδομένων που έχει να προσφέρει ή που μπορεί να αποδεχθεί. Στο πλαίσιο αυτής της περιγραφής, η συσκευή αναφέρει τον τύπο των δεδομένων (audio, video, κείμενο, κ.λπ.), τις πόρτες IP και τα πρωτόκολλα που χρησιμοποιούνται (π.χ., T.120), καθώς και άλλες πληροφορίες που είναι απαραίτητες για μια συσκευή για την ανταλλαγή δεδομένων αλλά και για να μπορεί να τα χειριστεί. Οι παραλήπτες του μηνύματος SDP παίρνουν την απόφαση για το αν θα συμμετέχουν στη διάσκεψη.

Όταν ο χρήστης ενός δικτύου θέλει να πραγματοποιήσει μια διάσκεψη την «διαφημίζει» μέσω του δικτύου με την αποστολή μηνυμάτων πολλαπλής αποστολής (multicast) τα οποία περιλαμβάνουν περιγραφή της διάσκεψης, π.χ. το όνομα του δημιουργού της, το όνομα της διάσκεψης, την κωδικοποίηση, το χρονισμό, κ.λ.π. Τα μηνύματα SDP δεν μεταφέρουν δεδομένα, αλλά δημιουργούν τις συνθήκες έτσι ώστε να πραγματοποιηθεί μια διαπραγμάτευση μεταξύ των δύο τελικών σημείων (αποστολέα και παραλήπτη) και να μπορέσουν να συμφωνήσουν σχετικά με τον τύπο και τη μορφή των δεδομένων.

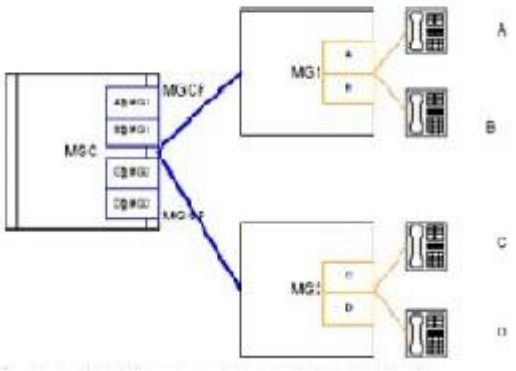
4.5 Πρωτόκολλο Media Gateway Control Protocol (MGCP)

Το MGCP (πρωτόκολλο ελέγχου πύλης μέσων) είναι ένα πρωτόκολλο που χρησιμοποιείτε στο σύστημα VoIP. Αυτό το εσωτερικό πρωτόκολλο αναπτύχθηκε αρχικά για να διευθετεί τις απαιτήσεις των δικτύων τηλεφωνίας που βασίζονται στις διευθύνσεις των φορέων. Το MGCP είναι ένα συμπληρωματικό πρωτόκολλο για το H.323 και το SIP, που σχεδιάστηκε σαν ένα εσωτερικό πρωτόκολλο ανάμεσα στον Media Gateway Controller (ελεγκτή πύλης μέσων) και στον Media Gateway (πύλη μέσων). Στο MGCP ένας Media Gateway Controller χειρίζεται όλες τις επεξεργασίες κλήσεων με το να συνδέεται με το δίκτυο IP διαμέσου συνεχής επικοινωνίας με μια συσκευή σηματοδότησης IP, για παράδειγμα ένας SIP-server ή ένας ελεγκτής πυλών(gatekeeper) H.323.

Το MGCP αποτελείται από ένα Call agent(πράκτορα κλήσεων), ένα Media Gateway το οποίο εκτελεί τη μετατροπή του σήματος μέσου ανάμεσα στα κυκλώματα και στα πακέτα, και ένα Signal Gateway όταν συνδέεται στο PSTN(Public Switched Telephone Network). Το MGCP χρησιμοποιείται ευρέως μεταξύ στοιχείων ενός αποσυνθεμένου Multimedia Gateway(πύλη πολυμέσων). Η πύλη έχει έναν Call agent ο οποίος αποτελείται από τη «νοημοσύνη» ελέγχου κλήσεων και ένα Media Gateway προσφέροντας λειτουργίες μέσων, για παράδειγμα μετατροπή από TDM voice σε voip.

Το Media Gateway χαρακτηρίζει τα τελικά σημεία για το Call agent για να δημιουργήσει και να διαχειρίζεται συνεδρίες μέσων με άλλα τελικά σημεία πολυμέσων. Τα τελικά σημεία είναι πηγές δεδομένων που μπορεί να είναι φυσικές ή εικονικές. Για τη δημιουργία των φυσικών τελικών σημείων, είναι αναγκαία η εγκατάσταση hardware ενώ εικονικά τελικά σημεία μπορούν να δημιουργηθούν χρησιμοποιώντας το διαθέσιμο λογισμικό. Οl Call agents έχουν τη δυνατότητα να δημιουργούν νέες συνδέσεις ή να τροποποιούν τις ήδη υπάρχουσες. Γενικότερα ένα Media Gateway είναι ένα στοιχείο δικτύου που δημιουργεί μετατροπή μεταξύ των πακέτων δεδομένων που μεταφέρονται μέσω του internet ή άλλων δικτύων και τα σήματα φωνής που μεταφέρονται μέσω των τηλεφωνικών γραμμών .Οι Call agents παρέχουν οδηγίες στα τελικά σημεία για να ελέγχουν για κάθε γεγονότα, και αν υπάρχουν, να δημιουργούν σήματα. Τα τελικά σημεία είναι σχεδιασμένα με τέτοιο τρόπο ώστε να μεταδίδουν αυτόματα τις αλλαγές στην κατάσταση λειτουργίας-

υπηρεσίας στον Call agent. Οι Call agents μπορούν να ελέγχουν τα τελικά σημεία και τις συνδέσεις στα τελικά σημεία.



Εικόνα 4.4: Συνδέσεις και τερματικοί σταθμοί πρωτοκόλλου MGCP

Συνδέσεις MGCP

Οι συνδέσεις MGCP μπορεί να είναι point-to-point ή multipoint. Οι συνδέσεις point-to-point μπορεί να είναι μεταξύ δύο τελικών σημείων για μετάδοση δεδομένων μεταξύ αυτών των τελικών σημείων. Όταν η σύνδεση μεταξύ δύο τελικών σημείων έχει πραγματοποιηθεί αρχίζει η μεταφορά δεδομένων μεταξύ των δύο αυτών σημείων. Σε συνδέσεις multipoint η σύνδεση δημιουργείται μεταξύ ενός τελικού σημείου και μιας συνεδρίας multipoint. Σε μια σύνδεση multipoint συνδέσεις μπορούν να δημιουργηθούν πάνω σε διάφορους τύπους δικτύων.

Αρχιτεκτονική MGCP

Το MGCP έγινε περιζήτητο μετά την εφαρμογή της τεχνολογίας voip γιατί δεν εμπλέκεται στην «εκνευριστική» δουλειά της κωδικοποίησης, αποκωδικοποίησης και μεταφοράς σήματος φωνής. Παρόλο που ο MGCP Call agent λειτουργεί ως ένα λογισμικό διαμοιραστής(switch) για ένα δίκτυο voip δεν κάνει τίποτα παραπάνω από το απλά να κατευθύνει τα Media Gateways και Signaling Gateway τα οποία κάνουν και όλη τη δουλειά. Ένα από τα κύρια καθήκοντα στο χτίσιμο ενός Call agent είναι να προσθέτει πολυάριθμες δυνατοτήτες στο πρωτόκολλο. Υπάρχουν διάφορα

πληροφοριακά RFCs τα οποία μπορούν να εξηγήσουν την προσδοκόμενη συμπεριφορά μέσα από ένα μεγάλο εύρος συνθηκών.

Στην αρχιτεκτονική MGCP, όλες οι εντολές τη χαρακτηρίζουν μια ταυτότητα συναλλαγής, παίρνουν μια επιβεβαίωση και στέλνουν μια απάντηση. Αυτό μπορεί να κατανοηθεί καλύτερα ως μια αρχιτεκτονική εγγραφής, καθώς ο Call agent πληροφορεί τα Media Gateway και τα Signaling Gateway για το ποια γεγονότα θα μεριμνήσει και ποια θα αφήσει.

Τα πακέτα MGCP, γενικά βρίσκονται στη θύρα 2427 UDP. Παρόμοια μ'αυτά που βρίσκεις στα πρωτόκολλα TCP. Ένα πακέτο MGCP μπορεί να είναι είτε εντολή είτε απάντηση. Οι εντολές αρχίζουν με ένα ρήμα τεσσάρων γραμμάτων ενώ οι απαντήσεις αρχίζουν με έναν κωδικό απάντησης τριών αριθμών.[24]

4.6 Πρωτόκολλο Real Time Transport Protocol (RTP)

Το RTP (Real-Time Transport Protocol) χρησιμοποιείται για να ενθυλακώνει VoIP πακέτα μέσα σε πακέτα UDP. Αν και χρησιμοποιείται περισσότερο ως βοηθητικό πρωτόκολλο μέσα σε άλλα (κυρίως στο SIP), έχει ορισθεί ως ξεχωριστό πρωτόκολλο για το VoIP.

Παρέχει από άκρη σε άκρη μεταφορά πακέτων κατάλληλη για εφαρμογές που μεταφέρουν δεδομένα πραγματικού χρόνου, όπως ήχο, βίντεο ή δεδομένα προσομοίωσης, πάνω από δίκτυα δεδομένων. Το RTP δεν εγγυάται quality-of service για πραγματικού χρόνου υπηρεσίες. Στη μεταφορά δεδομένων έρχεται να προστεθεί ένα ακόμη πρωτόκολλο, ελέγχου αυτή τη φορά, το RTCP που επιτρέπει την παρακολούθηση της παράδοσης των δεδομένων αλλά και να παρέχει τον υποτυπώδη έλεγχο και τη δυνατότητα αναγνώρισης. Το RTP και το RTCP έχουν σχεδιαστεί ώστε να είναι ανεξάρτητα από τα επίπεδα μεταφοράς και δικτύου (transport and network layers).[21]

4.7 Πρωτόκολλο IAX

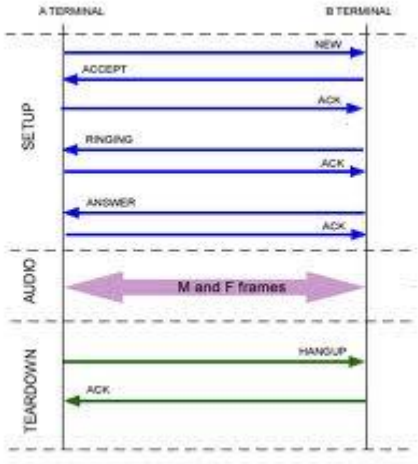
Το IAX (Inter-Asterisk eXchange) είναι ένα πρωτόκολλο ελέγχου κλήσεων για το VoIP. Το IAX σχεδιάστηκε για να αντικαταστήσει τα προηγούμενα πρωτόκολλα ελέγχου H.323 και SIP. Το IAX κάνει πολύ καλύτερη χρησιμοποίηση του bandwidth

από τα ανταγωνιστικά πρωτόκολλα επιτρέποντας του να υποστηρίζει περισσότερες ταυτόχρονες κλήσεις voip.

Η κίνηση IAX χρησιμοποιεί τη θύρα UDP 4569,η χρήση μιας κοινά γνωστής θύρας κάνει το IAX να είναι συμβατό με το NAT(Network Address Translation) κάτι το οποίο ήταν πολύ δύσκολο για τα προηγούμενα πρωτόκολλα ελέγχου.

Το IAX υποστηρίζει την αυθεντικοποίηση χρησιμοποιώντας δημόσια κλειδιά με τον αλγόριθμο SHA-1 για ψηφιακές υπογραφές.

Το IAX αναπτύχθηκε για το Asterisk PBX και αρχικά χρησιμοποιούνταν για την εσωτερική συναλλαγή στο Asterisk. Το IAX υποστηρίζεται τώρα από πολλές πλατφόρμες voip. [25]



Εικόνα 4.5: Ανταλλαγή μηνυμάτων πρωτοκόλλου IAX μεταξύ δυο τερματικών

Κεφάλαιο 5

Ασφάλεια

Πολλά από τα κίνητρα των επιθέσεων σε IP τηλεφωνία είναι τα ίδια των επιθέσεων της κλασσικής τηλεφωνίας. Οικονομικά οφέλη, υποκλοπή συνομιλίας (πληροφοριών), προσωπική φήμη, πρόκληση κολλήματος στις τηλεφωνικές εταιρίες καθώς και ενόχληση χρηστών. Εκτός των συνηθισμένων αυτών επιθέσεων της κλασσικής τηλεφωνίας, έχουμε και τις επιθέσεις πάνω σε δίκτυα υπολογιστών.

Τα VoIP τηλέφωνα και οι υπολογιστές που τρέχουν λογισμικό για IP τηλεφωνία, είναι περισσότερο υπολογιστής απ’ ότι τηλέφωνο. Έχουν λειτουργικό, αρχειακό σύστημα, χρησιμοποιούν τα γνωστά πρωτόκολλα δικτύου και τρέχουν εφαρμογές

δεδομένων, διαχείρισης αλλά και φωνής. Είναι ευάλωτοι στην αναρμόδια πρόσβαση, αλλαγή δικαιωμάτων και στην κακή χρήση συστημάτων, στους ιούς και τα σκουλήκια, στις Denial Of Service(DOS) επιθέσεις που προσβάλλουν τα πρωτόκολλα δικτύων (TCP ,IP, ICMP, arp).
Οι τρέχουσες υλοποιήσεις IP τηλεφωνίας όσον αφορά τη σηματοδοσία των κλήσεων (SIP), τη μεταφορά των μηνυμάτων φωνής (RTP) και τα πρωτόκολλα ελέγχου (RTCP), δεν παρέχουν επαρκή αυθεντικοποίηση των κλήσεων, ούτε και από άκρο εις άκρο (end-to-end) μέτρα ακεραιότητας και εμπιστευτικότητας. Μέχρι αυτά τα χαρακτηριστικά ασφαλείας να υλοποιηθούν, υπάρχουν πολλές ευκαιρίες για κακόβουλη εκμεταλλευσή τους.

Παρακάτω θα παρουσιαστούν τέσσερα σημαντικά ζητήματα ασφαλείας για το VoIP, τα οποία είναι ευρέως γνωστά και για τα δίκτυα δεδομένων:

Ιδιωτικότητα (Privacy)

Η ιδιωτικότητα σημαίνει πρόληψη μιας εξουσιοδοτημένης αποκάλυψης πληροφοριών, δηλαδή κάποιο τρίτο άτομο δεν πρέπει να είναι σε θέση να γνωρίζει πληροφορίες οι οποίες προορίζονται για τον παραλήπτη.
Στο οικείο τηλεφωνικό δίκτυο μεταγωγής κυκλωμάτων οι χρήστες γνωρίζουν τον κίνδυνο της υποκλοπής, αλλά το ζήτημα αυτό δε φαίνεται να τους προβληματίζει ιδιαίτερα, καθώς τέτοιες παράνομες τεχνικές εφαρμόζονται κυρίως στο χώρο του εγκλήματος και της κατασκοπείας. Σε αυτό το δίκτυο, για να γίνει η υποκλοπή χρειάζεται φυσική πρόσβαση στην τηλεφωνική γραμμή και συσκευή. Επίσης, μόνο μία συνομιλία μπορεί να υποκλέπτεται κάθε φορά.
Στον κόσμο του VoIP οι κίνδυνοι αυξάνονται αξιοσημείωτα. Ο εξοπλισμός ή το λογισμικό που χρειάζεται για την υποκλοπή είναι πολύ πιο εξεζητημένα, αλλά και πολύ πιο προσβάσιμα για τον κάθε υποκλοπέα. Καθώς τα πακέτα φωνής δρομολογούνται μέσω ενός δικτύου δεδομένων, περνώντας από σημεία όπου εύκολα κάποιος μπορεί να έχει πρόσβαση, θεωρητικά κάθε πακέτο μπορεί να υποκλαπεί, να αποθηκευτεί και στη συνέχεια να αναπαραχθεί, μαζί με τα υπόλοιπα πακέτα, στο τερματικό του.
Η ιδιωτικότητα των συνομιλιών VoIP μπορεί να ενισχυθεί εξαιρετικά με τη χρήση κρυπτογράφησης. Παρόλα αυτά τα περισσότερα εταιρικά δίκτυα δεν την

χρησιμοποιούν. Ο λόγος που δεν χρησιμοποιείται είναι ότι η διαδικασία κρυπτογράφησης/αποκρυπτογράφησης καταναλώνει μεγάλη υπολογιστική ισχύ και εισάγει αισθητή καθυστέρηση. Καθώς, όμως, οι ταχύτητες επεξεργασίας των υπολογιστών αυξάνονται με ραγδαίους ρυθμούς, σύντομα το πρόβλημα αυτό δε θα υπάρχει. Επίσης, η υποκλοπή πακέτων σηματοδοσίας που ανταλλάσσονται μεταξύ των SIP servers μπορεί να παρέχει στους επιτεθέμενους κωδικούς πρόσβασης χρηστών, PINs και τηλεφωνικούς αριθμούς SIP. Κάποιος που επιτυγχάνει πρόσβαση σε πληροφορίες λογαριασμών χρηστών μπορεί να επέμβει με πολλούς κακόβουλους τρόπους (να χρεώνει δικές του κλήσεις στους λογαριασμούς αυτούς, να προωθεί τις κλήσεις σε άλλο αριθμό, να αλλάξει το μήνυμα του τηλεφωνητή κ.λπ).

Ακεραιότητα

Η ακεραιότητα σημαίνει πρόληψη μη εξουσιοδοτημένης μεταβολής πληροφοριών, δηλαδή ο παραλήπτης θα πρέπει να λαμβάνει τα πακέτα που έχει στείλει ο αποστολέας χωρίς οποιαδήποτε αλλαγή στο περιεχόμενο τους. Για να μπορέσει κάποιο τρίτο άτομο να μεταβάλει οποιαδήποτε πληροφορία θα πρέπει να είναι εξουσιοδοτημένο. Για παράδειγμα, οι επιτιθέμενοι μπορούν να αλλοιώσουν συνομιλίες παρεμβάλλοντας RTP πακέτα, τροποποιώντας τα περιεχόμενα και προωθώντας τα τροποποιημένα πακέτα στον αρχικό παραλήπτη. Άλλες, παρόμοιες τεχνικές παρεμβολής, είναι δυνατές όταν δεν παρέχεται έλεγχος ακεραιότητας μέσω ασύρματων δικτύων. Για παράδειγμα, ένας εισβολέας μπορεί να παρεμβάλλει ομιλία, θόρυβο ή καθυστέρηση (κενά διαστήματα) σε ενεργές κλήσεις μέσω ενός “χτυπημένου” access point.

Ένα βήμα παραπέρα βρίσκονται οι επιθέσεις άρνησης εξυπηρέτησης (Denial of Service - DoS). Τέτοιες επιθέσεις πλημμυρίζουν έναν voice agent με αιτήσεις για εγκαταστάσεις κλήσεων, σε μια απόπειρα να εξαντλήσουν τους πόρους του, να προκαλέσουν αποσυνδέσεις και, φυσικά, τη δυσαρέσκεια των πελατών. Επίσης DoS μπορεί να προκληθεί πλημμυρίζοντας το δίκτυο με τεράστιους όγκους δεδομένων φωνής. Τέλος, μία ακόμα τεχνική πρόκλησης DoS είναι η αποστολή πλαστών σημάτων ελέγχου για αλλαγή του password του χρήστη. Έτσι, ο νόμιμος χρήστης, αγνοώντας την αλλαγή, τίθεται ανίκανος να πραγματοποιήσει κλήσεις από το λογαριασμό του.

Ένας εισβολέας μπορεί να μεταμφιεστεί ως νόμιμος χρήστης και να έχει πρόσβαση σε μια σειρά διαδικασιών του μεταγωγού. Υπάρχουν διάφορες σοβαρές απειλές στην ασφάλεια που προέρχονται από μη εξουσιοδοτημένη είσοδο στο σύστημα. Για παράδειγμα, ο εισβολέας μπορεί να χρησιμοποιήσει το επίπεδο άδειας του νόμιμου χρήστη και να εκτελέσει καταστρεπτικές λειτουργίες διαδικασιών όπως:

- Η αποκάλυψη εμπιστευτικών δεδομένων.
- Η πρόκληση επιδείνωσης διαφόρων υπηρεσιών μέσω της τροποποίησης του λογισμικού μεταγωγών.
- Η κατάρρευση του μεταγωγού.
- Η αφαίρεση όλων των ιχνών της εισβολών έτσι ώστε να μην μπορεί να είναι εύκολα ανιχνεύσιμη.[28]

Διαθεσιμότητα

Η διαθεσιμότητα αναφέρεται στην έννοια ότι οι διάφορες πληροφορίες ή υπηρεσίες πρέπει να είναι προσπελάσιμες και χωρίς αδικαιολόγητη καθυστέρηση όταν τις χρειάζεται μια εξουσιοδοτημένη οντότητα. Αυτό σημαίνει ότι οι εξουσιοδοτημένοι χρήστες των υπολογιστικών και επικοινωνιακών μέσων δεν αντιμετωπίζουν προβλήματα άρνησης εξυπηρέτησης (Denial of Service) όταν επιθυμούν να προσπελάσουν τους πόρους του συστήματος.

Η διαθεσιμότητα είναι ο προφανέστερος κίνδυνος για τους μεταγωγούς. Προκαλέι επιθέσεις οι οποίες είναι γνωστές ως «πλημμύρες» και οδηγούνται μέσω των RTP πρωτοκόλλων που είναι υπεύθυνα για τη μεταφορά της ψηφιοποιημένης φωνής. Όπως και στις UDP πλημμύρες, οι επιθέσεις αυτές προσπαθούν να εξαντλήσουν τους διαθέσιμους πόρους, βομβαρδίζοντας μια IP τηλεφωνική συσκευή με τεράστια ποσά όγκου φωνητικών δεδομένων. Ακόμη και τα μεγαλύτερα επίπεδα του OSI όπως το 7ο, που περιλαμβάνει τα λειτουργικά συστήματα, ίσως να μην είναι σε θέση να αντιμετωπίσουν τις DoS (Denial of Service) επιθέσεις.

Παρόλο που η διαθεσιμότητα συχνά αναδεικνύεται στο πιο σημαντικό χαρακτηριστικό της ασφάλειας, λίγοι μηχανισμοί υπάρχουν για να βοηθήσουν την υποστήριξή της.[28]

Αυθεντικοποίηση (Authentication)

Η αυθεντικοποίηση επιτελεί την επιβεβαίωση προς τους χρήστες ότι το πρόσωπο στην άλλη άκρη της γραμμής είναι πράγματι αυτός που ισχυρίζεται ότι είναι. Τα πρότυπα H.323, SIP και MGCP παρέχουν μηχανισμούς για την αυθεντικοποίηση των χρηστών. Οι συμμετρικές και ασύμμετρες μέθοδοι κρυπτογράφησης, οι οποίες εμπεριέχουν την ανταλλαγή μυστικών και ιδιωτικών κλειδιών, μπορούν να εξασφαλίσουν την αυθεντικοποίηση. Το μειονέκτημα της κρυπτογράφησης είναι, όπως αναφέρθηκε και προηγουμένως, ότι αποτελεί χρονοβόρα και υπολογιστικά πολύπλοκη διαδικασία. Ένα από τα ελκυστικά γνωρίσματα που φέρνει το VoIP είναι η δυνατότητα επιλογής του σημείου όπου θα φιλοξενείται ο «εγκέφαλος» της VoIP εφαρμογής από μια ποικιλία σημείων στο δίκτυο. Οι gatekeepers και οι call-manager συσκευές, οι οποίες αυθεντικοποιούν τους χρήστες και εγκαθιστούν τις κλήσεις, μπορούν να βρίσκονται σε οποιονδήποτε server του δικτύου. Αυτό όμως μπορεί να προκαλέσει και άλλο πρόβλημα, οι καταγραφόμενες πληροφορίες σχετικά με τις κλήσεις των χρηστών μπορεί να είναι χρήσιμες για τη χρέωση και τον εντοπισμό τους, αλλά αυτές οι καταγραφές μπορούν να γίνουν στόχος πειρατείας. Επομένως, η προστασία των servers που φιλοξενούν τέτοιες ευαίσθητες πληροφορίες πρέπει να είναι ακόμα πιο ισχυρή.

5.1 Τεχνολογίες Ασφάλειας

Για τους παραπάνω κινδύνους έχουν βρεθεί κάποιοι τρόποι αντιμετώπισης τους, αυτοί είναι: κρυπτογράφηση, firewalls, port scans, voip vpn.

Κρυπτογράφηση

Η κρυπτογράφηση από το κανάλι δεδομένων δεν είναι κάτι που χρησιμοποιείται αναγκαστικά από όλους τους παρόχους VoIP. Πολλοί απ' αυτούς δεν υποστηρίζουν τον μηχανισμό αυτό. Η ανάγκη όμως για κρυπτογράφηση των δεδομένων είναι μεγάλη.

Είναι λοιπόν σημαντικό να κρυπτογραφηθούν τα ίδια τα δεδομένα (RTP πακέτα) κατά την μεταφορά τους. Για τον σκοπό αυτό χρησιμοποιείται το πρωτόκολλο SRTP (Secure Real-time Transport Protocol).

Τα δεδομένα έτσι μεταφέρονται κρυπτογραφημένα στον προορισμό τους, και ο δέκτης είναι σε θέση να αποκρυπτογραφήσει τα δεδομένα αυτά. Για την

κρυπτογράφηση/αποκρυπτογράφηση των δεδομένων χρησιμοποιούνται και άλλοι αλγόριθμοι όπως SSL (Secure Sockets Layer), TLS (Transport Layer Security) κ.α.

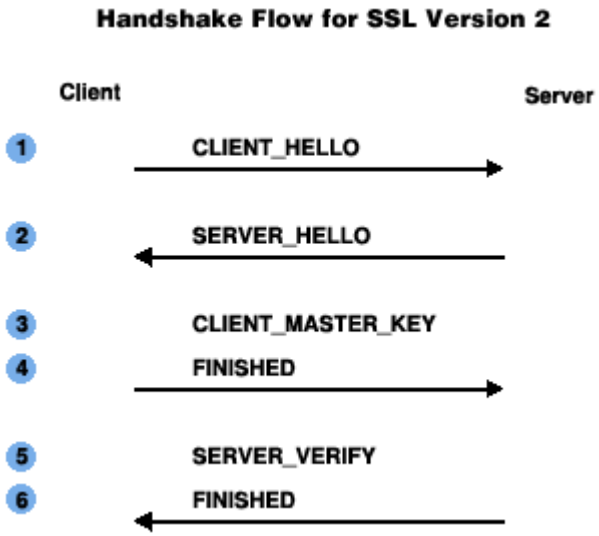
Κρυπτογράφηση RTP

Πολύ γνωστό είναι το πρωτόκολλο SSL, το οποίο χρησιμοποιείται πολύ στο Internet αλλά και στην VoIP επικοινωνία. Το SSL παρέχει ασφάλεια κατά τη μετάδοση ευαίσθητων δεδομένων (RTP πακέτων) με βάση το πρωτόκολλο TCP/IP και παρέχει υπηρεσίες:

- Κρυπτογράφησης δεδομένων
- Αυθεντικοποίηση εξυπηρετητή
- Ακεραιότητα των πακέτων που μεταδίδονται

Έτσι, μέσω του SSL μπορούμε να προστατέψουμε μια VoIP επικοινωνία από την απειλή του IP telephony call integrity(Ακεραιότητα κλήσης IP). Η έκδοση SSL 2.0 παρέχει μόνο αυθεντικοποίηση εξυπηρετητή, ενώ η έκδοση SSL 3.0 παρέχει επιπλέον και την αυθεντικοποίηση πελάτη. Το SSL χρησιμοποιεί την RSA κρυπτογράφηση. Η RSA κρυπτογράφηση χρησιμοποιεί ένα ζεύγος κλειδιών, το δημόσιο και το ιδιωτικό κλειδί. Έτσι η πληροφορία κρυπτογραφείται με το ένα κλειδί και αποκρυπτογραφείται (μόνο) με το άλλο.

Κατά τη σύνδεση ενός πελάτη VoIP (client) με τον αντίστοιχο VoIP εξυπηρετητή (server), χρησιμοποιείται και ένα άλλο κλειδί, το κλειδί συνόδου (session key), το οποίο λήγει μετά από 24 ώρες. Η ανταλλαγή του κλειδιού αυτού ανάμεσα στον χρήστη και στον εξυπηρετητή γίνεται με την κρυπτογραφία δημοσίου κλειδιού. Συγκεκριμένα, όταν ο server και ο client υποστηρίζουν SSL κρυπτογράφηση, τότε ο server στέλνει στον client μία αίτηση για την έναρξη μιας SSL περιόδου. Ο client ενημερώνει τον server στέλνοντας τον αριθμό ταυτότητας της συνόδου(session ID). Με λίγα λόγια του στέλνει το session key. Για την κρυπτογράφηση του session key ο client χρησιμοποιεί το δημόσιο κλειδί του server. Ο server με το ιδιωτικό του κλειδί αποκρυπτογραφεί και αποκτά το session key. Έτσι λοιπόν ξεκινάει η επικοινωνία.



Εικόνα 5.1 Χειραψία SSL2

Κρυπτογράφηση SIP

Το πρωτόκολλο SIP χρησιμοποιείται για να ξεκινάει, διατηρεί και τερματίζει τις κλήσεις μεταξύ δύο ή περισσοτέρων τερματικών σε μια VOIP επικοινωνία. Είναι δηλαδή πρωτόκολλο ελέγχου των κλήσεων. Μέσω του πρωτοκόλλου αυτού μεταφέρονται τα διάφορα σήματα για τον έλεγχο κάθε κλήσης, άρα αν το αφήσουμε απροστάτευτο τότε γίνεται πολύ ευαίσθητο σε κάθε είδους επίθεση.

Το Secure SIP είναι ένας μηχανισμός προστασίας του SIP πρωτοκόλλου με τέτοιον τρόπο ώστε τα SIP μηνύματα να στέλνονται κρυπτογραφημένα. Το Secure SIP χρησιμοποιεί το πρωτόκολλο TLS (Transport Layer Security) ώστε να στέλνονται τα μηνύματα SIP κρυπτογραφημένα. Έτσι, μέσω του TLS μπορούμε να προστατέψουμε μια VoIP επικοινωνία από την απειλή του eavesdropping (κρυφακούω). Το Secure SIP επίσης χρησιμοποιεί έναν μηχανισμό, τον SIPS Uniform Resource Identifier (URI) (κάτι παρόμοιο με το HTTPS) κατά τον οποίο καθορίζεται το γεγονός ότι SIP μέσω TLS θα χρησιμοποιεί τόσο ο χρήστης, όση και ο server ώστε να υπάρχει προστασία από άκρο σε άκρο. Συγκεκριμένα η διαδικασία είναι παρόμοια μ' αυτή του SSL(αλλά για το κανάλι σηματοδοσίας και όχι για το κανάλι της φωνής), δηλαδή:

Ο SIP client στέλνει στον SIP server μία αίτηση για την έναρξη μιας TLS περιόδου (TLS session). Ο server απαντάει στέλνοντας στον client ένα δημόσιο πιστοποιητικό (public certificate) και ο client με τη σειρά του ελέγχει την εγκυρότητα του πιστοποιητικού. Έπειτα αρχίζουν να ανταλλάσουν μεταξύ τους τα session keys και

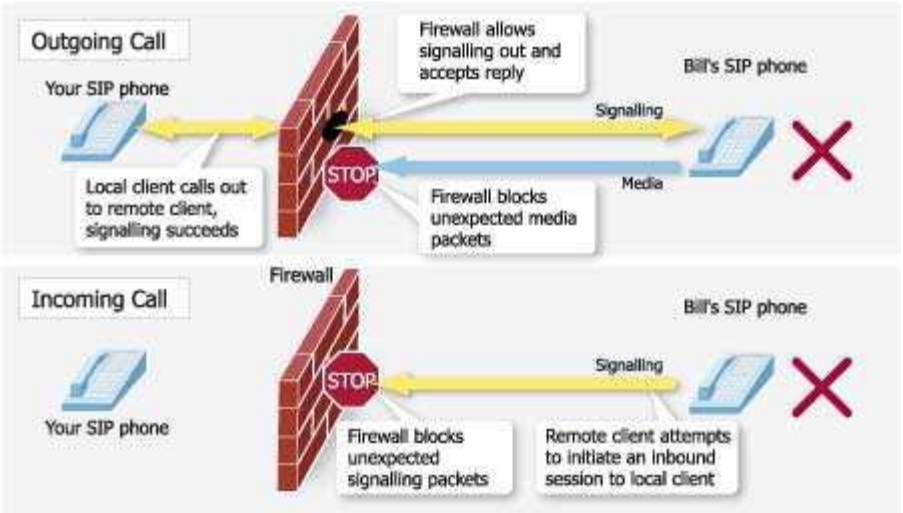
έτσι κρυπτογραφούν και αποκρυπτογραφούν τα SIP μηνύματα για κάθε session. Πολλές εταιρίες παροχής VoIP χρησιμοποιούν και τη γνωστή MD-5 hash τεχνική για την ασφάλεια του SIP. Με την κρυπτογράφηση όμως έχουμε και κάποια μειονεκτήματα. Χρησιμοποιώντας μηχανισμούς κρυπτογράφησης, αυξάνεται το ποσό των δεδομένων που διακινούνται (μεταφορά περισσότερων πακέτων) και ταυτόχρονα αυξάνεται η καθυστέρηση της μετάδοσης των πληροφοριών. Αιτίες καθυστέρησης μπορεί να είναι :

- Αρχική σύνδεση όπου ανταλλάσσονται κρυπτογραφημένες πληροφορίες
- Τα κρυπτογραφημένα δεδομένα αποτελούνται από περισσότερα bytes άρα έχουμε μεγαλύτερη καθυστέρηση κατά τη μεταφορά τους.
- Η ίδια η διαδικασία της κρυπτογράφησης η οποία απαιτεί επιπλέον υπολογιστική ισχύ.

Τα προβλήματα αυτά γίνονται εντονότερα στην VoIP επικοινωνία μιας και έχουμε να κάνουμε με μεταφορά πακέτων φωνής. Η καθυστέρηση λοιπόν κατά την ανταλλαγή πακέτων φωνής γίνεται περισσότερο αντιληπτή και μπορεί να οδηγήσει σε προβλήματα επικοινωνίας ανάμεσα στους χρήστες.[34]

Firewalls

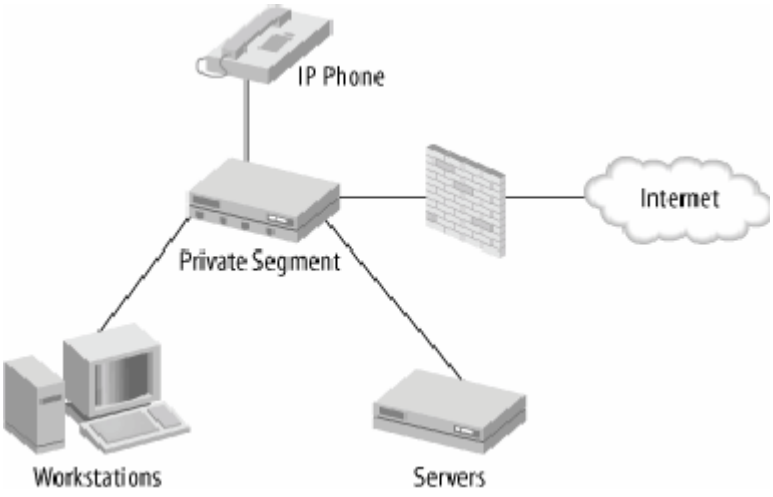
Όταν είμαστε συνδεδεμένοι στο διαδίκτυο, στέλνουμε πληροφορίες και ταυτόχρονα λαμβάνουμε πληροφορίες (πακέτα). Πρέπει επομένως η πληροφορίες αυτές να «φιλτράρονται» ώστε να στέλνουμε και να λαμβάνουμε μόνο τις απαραίτητες και αναμενόμενες πληροφορίες και να εμποδίζουμε την κίνηση των ύποπτων πληροφοριών (πακέτων). Αυτό λοιπόν γίνεται με τη βοήθεια των firewalls.



Εικόνα 5.2 : Firewalls και τηλεφωνία VoIP

Τα Firewalls (τείχη προστασίας) μπορεί να είναι είτε συσκευές είτε λογισμικό και είναι ο κύριος μηχανισμός προστασίας από τις διάφορες απειλές στην VoIP επικοινωνία. Δέχονται σαν εισόδους γνωστές (από εμάς) IP διευθύνσεις, πόρτες και υπηρεσίες (services) και με βάση τις εισόδους αυτές επιτρέπει ή αποτρέπει την κίνηση από και προς εμάς. Τα firewalls λειτουργούν με βάση το NAT (Network Address Translation) σύμφωνα με το οποίο μία εξωτερική (συνήθως wan) διεύθυνση αντιστοιχεί σε πολλές εσωτερικές(συνήθως LAN) διευθύνσεις. Αυτό προσδίδει στα firewalls μεγαλύτερη προστασία από εξωτερικές επιθέσεις (πχ MITM).

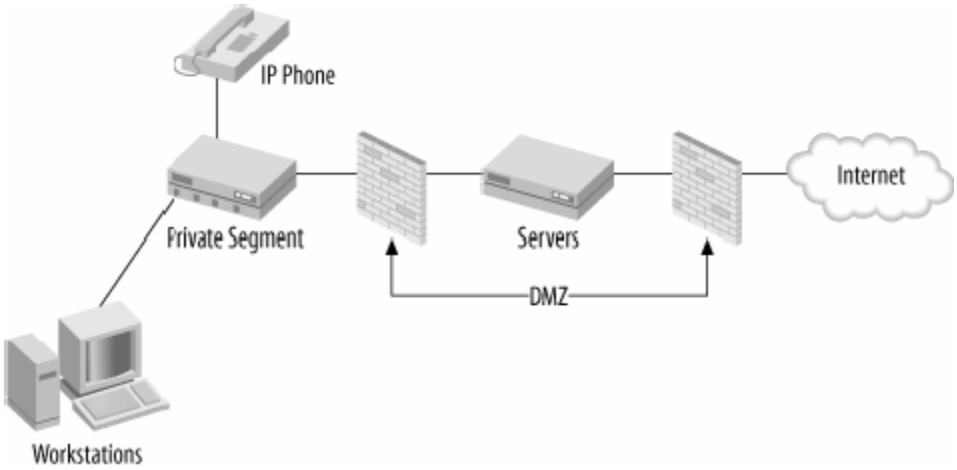
Ένα σοβαρό μειονέκτημα που παρουσιάζουν τα firewalls είναι ότι δεν μπορούν να λειτουργήσουν σωστά όταν χρησιμοποιούμε UDP πόρτες. Η VoIP επικοινωνία στηρίζεται πάνω στο UDP πρωτόκολλο. Αυτό σημαίνει ότι τα firewalls δεν είναι σε θέση να ανιχνεύσουν και να αντιμετωπίσουν διάφορες απειλές που κάνουν χρήση των δυναμικών UDP πορτών. Τέτοιες απειλές είναι το SPIT (SPAM over Internet Telephone).



Εικόνα 5.3 : Στοιχειώδη προστασία με χρήση firewall

Όπως βλέπουμε και στην εικόνα 5.3, σ' ένα μικρό τοπικό δίκτυο, αρκεί να τοποθετήσουμε το firewall μεταξύ του δικτύου μας και του Internet. Στην πραγματικότητα όμως, όταν ζητάμε μεγαλύτερη ασφάλεια στο VoIP δίκτυο μας πρέπει να εφαρμόζουμε firewalls και από τις δύο πλευρές, δηλαδή και στην πλευρά του τοπικού μας δικτύου αλλά και στην πλευρά του Internet. Τα τμήματα αυτά είναι

γνωστά και σαν DMZ segments (demilitarized zones). Ένα DMZ τμήμα είναι ένα τμήμα δικτύου (συνήθως Ethernet) που χωρίζεται από δυο τύπους firewall (συνήθως firewalled routers). Ένα firewall που προβάλει προστασία από το Internet και ένα άλλο το οποίο προβάλει προστασία από το τοπικό-ιδιωτικό δίκτυο.[34]



Εικόνα 5.4: Τμήμα DMZ

Port Scans

Port Scan είναι μια συστηματική διαδικασία που προσπαθεί να προσδιορίσει όλες τις ανοικτές πόρτες και διαθέσιμες υπηρεσίες σε έναν TCP/IP host. Οι περισσότεροι “hackers” χρησιμοποιούν το Port Scans για να μπορέσουν να προσδιορίσουν έναν χρήστη-στόχο. Ο “hacker” έτσι μπορεί να πετύχει τον πλήρη έλεγχο του χρήστη. Μια ασφαλής τεχνική λοιπόν για την αποφυγή του κινδύνου αυτού είναι το κλείσιμο-κλείδωμα των πορτών που δε λαμβάνουν μέρος στην επικοινωνία.

Σε μια TCP σύνδεση τα πράγματα είναι πολύ εύκολα. Μιας και μια TCP σύνδεση είναι connection-oriented, όταν ενεργοποιείται μια σύνδεση (established) τότε η πόρτες που λαμβάνουν μέρος στην επικοινωνία θεωρούνται ανοιχτές και διαθέσιμες. Όταν διακόπτεται η σύνδεση μεταξύ τους, τότε οι πόρτες αυτές θεωρούνται κλειστές (και μη διαθέσιμες). Έτσι με αυτόν τον τρόπο, δεσμεύοντας δυναμικά τις πόρτες ως κλειστές, εμποδίζουμε το port scan να εντοπίσει τις κλειστές πόρτες.

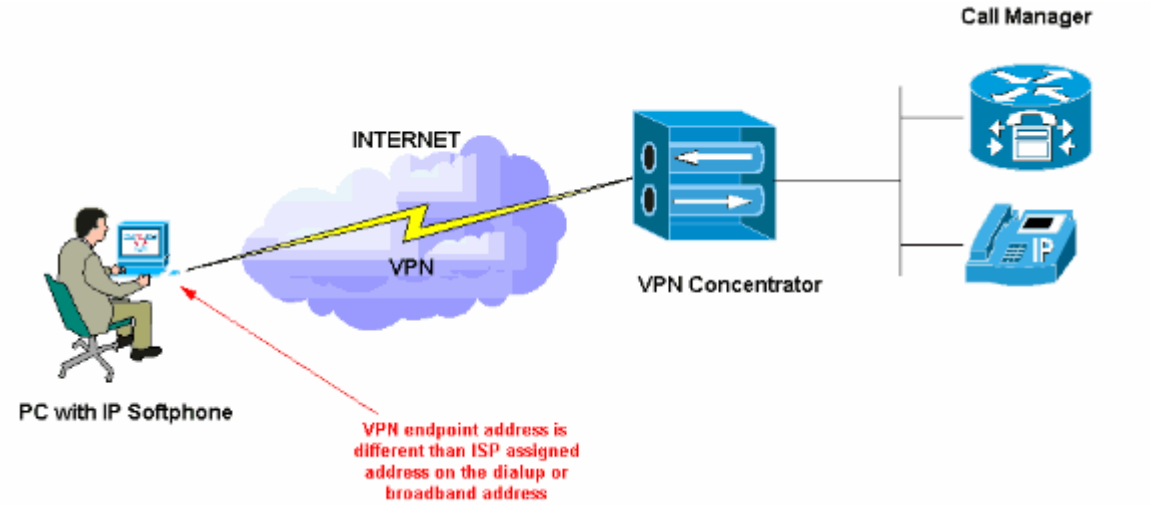
Το VoIP όμως λειτουργεί πάνω στο UDP πρωτόκολλο (connectionless). Στο UDP είναι πολύ εύκολο να εντοπιστούν ποιες πόρτες είναι ανοιχτές και ποιες είναι

κλειστές με την αποστολή δεδομένων προς αυτές και στη συνέχεια περιμένοντας για ICMP unreachable μηνύματα. Οι πόρτες οι οποίες δεν απαντάνε με κάποιο ICMP unreachable μήνυμα θεωρούνται ως ανοιχτές κ έτσι είναι πολύ εύκολο για κάποιον «hacker» να εντοπίσει τις πόρτες αυτές και να επιτεθεί μέσω των πορτών αυτών.
Η λύση στην απειλή αυτή είναι επίσης πολύ απλή. Απλά εμποδίζουμε την ICMP κίνηση στο firewall του VoIP δικτύου μας και έτσι κανένας δε θα μπορεί να εντοπίσει ποιες UDP πόρτες χρησιμοποιούνται.

VoIP VPN

Το VoIP VPN όπως μας δείχνει και το όνομά του συνδυάζει δύο τεχνολογίες, την VoIP και την VPN(Virtual Private Network) και έτσι προσφέρει μια ασφαλή μέθοδο για την μεταφορά της φωνής. Πριν περιγράψουμε την μέθοδο αυτή θα κάνουμε μια συνοπτική περιγραφή της VPN τεχνολογίας.

Είναι ένα ιδιωτικό δίκτυο επικοινωνίας το οποίο χρησιμοποιείται συχνά μέσα σε εταιρίες ή και μεταξύ εταιριών για ασφαλή και εμπιστευτική επικοινωνία μέσω του δημόσιου δικτύου (vpn tunnel). Έτσι η κίνηση των δεδομένων σ' ένα VPN δίκτυο γίνεται μέσω ενός δημόσιου δικτύου (πχ Internet).
Ο όρος Tunnelling χρησιμοποιείται όταν ενθυλακώνονται τα δεδομένα και οι πληροφορίες ενός ιδιωτικού δικτύου (frames) σε δεδομένα δημόσιου δικτύου (IP packets). Έτσι με το VPN-Tunnel οι χρήστες του δημόσιου δικτύου μπορούν να ανταλλάσουν δεδομένα με τέτοιον τρόπο, σαν να βρίσκονται στο ίδιο τοπικό ιδιωτικό δίκτυο.



Εικόνα 5.5: VPN

Το VoIP όπως είπαμε χρησιμοποιεί το κανάλι μεταφοράς των δεδομένων (RTP) για να μεταφέρει τα πακέτα της φωνής και είναι δυνατόν να εφαρμοστεί πάνω στο κανάλι αυτό κρυπτογράφηση πχ SSL (Secure voice) όπως αναφέρουμε και πιο πάνω.

Εδώ λοιπόν γνωστοποιούμε ότι η κρυπτογράφηση εφαρμόζεται μέσω του VPN. Συγκεκριμένα ο VoIP gateway-router πρώτα μετατρέπει το αναλογικό σήμα της φωνής σε ψηφιακό, ενθυλακώνει το σήμα σ' ένα IP πακέτο και στη συνέχεια εφαρμόζει κάποια κρυπτογράφηση. Έπειτα δρομολογεί το πακέτο μέσω του VPN tunnel.

Ο αποστολέας (κάποιος άλλος VoIP router στην άλλη άκρη του VPN tunnel) αποκωδικοποιεί/αποκρυπτογραφεί το πακέτο και στη συνεχεία μετατρέπει το ψηφιακό σήμα σε αναλογικό, το οποίο και μεταδίδεται από το ακουστικό του VoIP τηλεφώνου.[35]

5.2 Πολιτικές Ασφάλειας

Από την ανάλυση που πραγματοποιήθηκε στις παραπάνω ενότητες γίνεται κατανοητό ότι υπάρχει ένα σύνολο απειλών της ασφάλειας αλλά ταυτόχρονα υπάρχουν και οι τεχνολογίες για την αντιμετώπιση τους. Βέβαια, από πρακτική άποψη είναι αδύνατο να αναπτυχθούν τεχνολογίες ασφάλειας για την αντιμετώπιση κάθε πιθανής απειλής. Συνεπώς, απαιτείται από κάθε χρήστη ή κάθε εταιρεία η αξιολόγηση των κινδύνων της ασφάλειας που είναι συγκεκριμένες για το δίκτυό τους

καθώς και η διευθέτηση αλλά και αξιολόγηση των απειλών υψηλής προτεραιότητας.

Στο σημείο αυτό, κρίνεται απαραίτητος ο σχεδιασμός ενός λειτουργικού σχεδίου που να περιγράφει τις κρίσιμες εφαρμογές, τις συσκευές, και τους κινδύνους της ασφάλειας κατά σειρά προτεραιότητας. Αυτό το σχέδιο πρέπει να καθοδηγεί τις τεχνολογίες ασφάλειας που πρέπει να αναπτυχθούν και να καθορίζει την προτεραιότητα των μελλοντικών εφαρμογών. Επίσης, πρέπει να περιλαμβάνει ένα συναφές σχέδιο περιγράφοντας τα βήματα που πρέπει να ακολουθηθούν σε περίπτωση παραβίασης της ασφαλείας. Το σχέδιο πρέπει να τεκμηριώνει τις εσωτερικές πολιτικές όπως οι πολιτικές κωδικού πρόσβασης, ο έλεγχος προσπέλασης, οι στρατηγικές ελέγχου και να κοινοποιείται στους ανθρώπους που είναι υπεύθυνοι για την εφαρμογή, επιβολή και επίλυση θεμάτων ασφαλείας. Στην συνέχεια, ακολουθεί μια σύντομη περιγραφή των εκτιμήσεων που πρέπει να ληφθούν υπόψη για την υλοποίηση ενός τέτοιου σχεδίου.

Μεταβατική εμπιστοσύνη

Με τον όρο “μεταβατική εμπιστοσύνη” αναφερόμαστε στην εμπιστοσύνη που διαβιβάζεται μέσω ενός άλλου συμβαλλόμενου μέλους. Για παράδειγμα, σε ένα VoIP σύστημα με πολλαπλούς servers, ένας πελάτης μπορεί να επικυρωθεί με έναν server, ενώ οι υπόλοιποι servers δεν χρειάζεται να επικυρώσουν ξανά τον πελάτη. Αυτό το πρότυπο εμπιστοσύνης είναι κοινό σε πολλά κατανεμημένα συστήματα. Όταν χρησιμοποιείται αυτό το πρότυπο, οι servers πρέπει να ευθυγραμμίσουν τις πολιτικές ασφαλείας τους για να διαφυλάξουν αδύναμες συνδέσεις οι οποίες αποτελούν εύκολο στόχο εκμετάλλευσης από κακόβουλες συσκευές ή επιτιθέμενα άτομα.

Ζητήματα Σχετικά με VoIP Πρωτόκολλα

Η επιλογή συγκεκριμένων VoIP τεχνολογιών και υπηρεσιών διαδραματίζει έναν σημαντικό ρόλο στον προγραμματισμό σχεδίων ασφάλειας. Για παράδειγμα, μπορούμε να αναφέρουμε το τρέξιμο softphones σε PCs που οδηγεί σε πολύπλοκη τμηματοποίηση δεδομένων και φωνής.

Ανταλλαγές πολυπλοκότητας (Complexity Tradeoffs)

Είναι απαραίτητο να εξεταστεί η πολυπλοκότητα και η αναλογία κινδύνου-ανταμοιβής από την εφαρμογή μιας τεχνολογίας εξασφάλισης της ασφάλειας σε ένα σύστημα. Παραδείγματος χάριν, οι τεχνικές κρυπτογράφησης δημοσίου κλειδιού περιλαμβάνουν αρχικά γενικά έξοδα με την ανάπτυξη των συστατικών της υποδομής όπως οι αρχές πιστοποίησης (CAs), τα πιστοποιητικά και ούτω καθεξής. Επίσης, μια υποδομή δημοσίου κλειδιού (Public Key Infrastructure ,PKI) απαιτεί μόνο την ελάχιστη καθημερινή συντήρηση.

NAT/Firewall Traversal

Τα Firewalls είναι γνώστες της VoIP σηματοδοσίας των πρωτοκόλλων και τυπικά η λειτουργία τους βασίζεται στην επιθεώρηση του περιεχομένου των μηνυμάτων σηματοδοσίας. Με βάση το περιεχόμενο των μηνυμάτων σηματοδοσίας, ανοίγουν διεξόδους για την διέλευση των φωνητικών μέσων. Τα είδη αυτά των Firewalls τα οποία σχετίζονται με τις εφαρμογές φωνής αναφέρονται συνήθως ως πύλες του επιπέδου εφαρμογής (Application-Layer Gateways, ALG) του δικτύου.
Η ικανότητα όμως αυτή των Firewalls να είναι ενήμερα για την VoIP σηματοδοσία των πρωτοκόλλων παύει να υφίσταται εάν τα μηνύματα σηματοδοσίας είναι κρυπτογραφημένα. Επειδή τα ενδιάμεσα Firewalls δεν μπορούν να εξετάσουν το περιεχόμενο των μηνυμάτων σηματοδοσίας, τα μέσα μπορεί να εμποδιστούν κατά την διέλευσή τους μέσα από το δίκτυο. Επομένως, είναι ενδεδειγμένο να χρησιμοποιηθεί ένα ιδιωτικό διάστημα διευθύνσεων που είναι συγκεκριμένο για VoIP αντί της χρησιμοποίησης της μετάφρασης διευθύνσεων δικτύων (Network Address Translation, NAT) μέσα στο διάστημα των VoIP διευθύνσεων.

Κωδικός Πρόσβασης και Έλεγχος Προσπέλασης

Οι περισσότερες συσκευές έρχονται με τους κωδικούς πρόσβασης προεπιλογής που είναι εύκολο να ανακαλυφθούν. Όπως με όλους τους κωδικούς πρόσβασης, πρέπει οι χρήστες να πάρουν προφυλάξεις αλλάζοντας το password και διατηρώντας το μυστικό. Για παράδειγμα, σε ένα VoIP περιβάλλον, οι διοικητικές

υπηρεσίες καθώς και οι υπηρεσίες απλών πρωτοκόλλων διαχείρισης του δικτύου (Simple Network Management Protocol, SNMP) πρέπει να κρατηθούν ασφαλείς.
Επίσης, οι συσκευές μπορεί να επιτρέπουν επανεκκίνηση του κωδικού πρόσβαση εάν οι χρήστες έχουν φυσική πρόσβαση σε αυτές (επανεκκίνηση αποκατάστασης του κωδικού πρόσβασης σε IOS συσκευές). Ταυτόχρονα, η μακρινή διαχείριση των συσκευών είναι επίσης κοινή. Λαμβάνοντας υπόψη αυτό και μια ευρεία ποικιλία άλλων λόγων, είναι σημαντικό να περιοριστεί η φυσική πρόσβαση στις συσκευές και να χρησιμοποιηθεί ένα περιορισμένο εκτός ζώνης σύστημα διαχείρισης.

Κεφάλαιο 6

6.1 Πλεονεκτήματα VoIP

Σύμφωνα με όσα έχουμε δει παραπάνω παρατηρούμε ότι το VoIP παρέχει κάποια οφέλη προς τους χρήστες και αυτά τα οφέλη οδηγούν όλο και περισσότερο κόσμο στο να γίνουν χρήστες αυτής της τεχνολογίας. Τα πλεονεκτήματα αυτά αναφέρονται και αναλύονται παρακάτω.

6.1.1 Χαμηλό κόστος κλήσεων

Ένα από τα πιο σημαντικά πλεονεκτήματα είναι το χαμηλό κόστος κλήσεων. Στις περιπτώσεις όπου χρησιμοποιείται το ίντερνετ για τηλεφωνικές κλήσεις το κόστος είναι πολύ μικρότερο από τη χρήση του δημοσίου τηλεφωνικού δικτύου. Πολλές VoIP υπηρεσίες όπως είναι το Skype και το iCall δεν κοστίζουν τίποτα αρκεί οι κλήσεις να γίνουν από τον ένα υπολογιστή στον άλλο.
Όταν η τεχνολογία VoIP χρησιμοποιείται για κλήσεις αριθμών του δημοσίου τηλεφωνικού δικτύου το κόστος παραμένει χαμηλό γιατί η φωνή μεταδίδεται με μορφή πακέτων δεδομένων μέσω του ίντερνετ. Αυτή η μέθοδος επιτρέπει στον πάροχο να παρέχει την υπηρεσία στον καταναλωτή σε χαμηλότερη τιμή.

6.1.2 Κόστος κλήσεων

Η τεχνολογία VoIP δεν έχει χρεώσεις υπεραστικών κλήσεων για κλήσεις που γίνονται εντός της ίδιας χώρας. Για παράδειγμα ενώ μια κλήση από την Αθήνα στη Θεσσαλονίκη κανονικά θα χρεωνόταν σαν υπεραστική σύμφωνα με τις χρεώσεις του δημοσίου τηλεφωνικού δικτύου, με την τεχνολογία VoIP η κλήση χρεώνεται σαν αστική. Με άλλα λόγια παύουν να υπάρχουν διαφορετικές χρεώσεις για αστικές και υπεραστικές κλήσεις.

Πολλοί πάροχοι επεκτείνουν αυτή τη λογική περιλαμβάνοντας στις κοινές χρεώσεις ολόκληρες ηπείρους, πχ την Ευρώπη. Αυτό επιτρέπει στους κατοίκους της Ελλάδας, της Γαλλίας και των άλλων Ευρωπαϊκών χωρών να επικοινωνούν με κοινές χρεώσεις.

6.1.3 Φορητότητα

Σε αντίθεση με τις τηλεφωνικές γραμμές οι οποίες πρέπει να είναι μόνιμα εγκατεστημένες, οι συνδέσεις VoIP πραγματοποιούνται εικονικά. Αυτό σημαίνει ότι οι χρήστες τους μπορούν να πραγματοποιούν κλήσεις από οπουδήποτε υπάρχει διαθέσιμη σύνδεση στο ίντερνετ. Αυτή εξυπηρετεί ιδιαίτερα όσους μετακινούνται συχνά.

Η φορητότητα αυτή δεν εξαντλείται στις VoIP συνδέσεις αλλά επεκτείνεται και στους VoIP αριθμούς. Σε αντίθεση με τους τηλεφωνικούς αριθμούς που περιορίζονται μέσα σε κάποια γεωγραφικά όρια, οι VoIP αριθμοί δεν χρειάζεται να αλλάξουν και επιτρέπουν στον χρήστη τους να τους χρησιμοποιεί βρισκόμενος σε οποιοδήποτε μέρος του κόσμου.

6.1.4 Πρόσθετες υπηρεσίες

Οι πάροχοι VoIP επιτρέπουν στους χρήστες να έχουν πρόσβαση σε πολλές υπηρεσίες χωρίς επιπρόσθετο κόστος. Αυτές οι υπηρεσίες μπορούν συνήθως να εφαρμοστούν χρησιμοποιώντας κάποιο λογισμικό υπολογιστή. Παραδείγματα υπηρεσιών που βασίζονται σε λογισμικό είναι η προώθηση κλήσεων, αναμονή κλήσεων, τηλεδιάσκεψη κ.α.

Επίσης η τεχνολογία VoIP από τη φύση της, λόγω της χρήσης των πρωτοκόλλων του internet για αποστολή δεδομένων, επιτρέπει την αποστολή δεδομένων τηλεομοιότυπου (fax) με χαμηλό κόστος, με κάποιο πρόγραμμα λογισμικού να

αντικαθιστά την παραδοσιακή μηχανή του fax. Με τον ίδιο τρόπο μπορούν να αποσταλούν ηλεκτρονικά εικόνες και έγγραφα. [14]

6.2 Μειονεκτήματα VoIP

Όπως σε κάθε τεχνολογία έτσι και στη VoIP εκτός από τα πλεονεκτήματα υπάρχουν και κάποια μειονεκτήματα που για κάποιους είναι αρκετά σημαντικά ώστε να μην το προτιμάνε ως μέσο για την επικοινωνία τους.

6.2.1 Χρήση ηλεκτρικής ενέργειας

Κατά τη διάρκεια μιας διακοπής ρεύματος ένα απλό τηλέφωνο παραμένει σε λειτουργία γιατί τροφοδοτείται με ρεύμα μέσω της τηλεφωνικής γραμμής. Αυτό δεν συμβαίνει με τα τηλέφωνα VoIP καθώς όταν κόβεται η παροχή ρεύματος παύει και η λειτουργία τους. Μια λύση σε αυτό το πρόβλημα είναι η χρήση εναλλακτικών πηγών παροχής ενέργειας, όπως μια γεννήτρια ρεύματος. Μια ακόμη λύση είναι η χρήση μιας κανονικής γραμμής τηλεφώνου σαν εφεδρική. Βέβαια η λύση αυτή οδηγεί σε σπατάλη των χρημάτων που εξοικονομούνται από τη χρήση της τεχνολογίας VoIP, παρόλα αυτά μπορεί να φανεί χρήσιμη σε περιπτώσεις επιχειρήσεων όπου πραγματοποιούνται πολλές υπεραστικές κλήσεις και όπου μια απώλεια της τηλεφωνικής γραμμής θα αποτελούσε σοβαρό πρόβλημα.

6.2.2 Κλήσεις έκτακτης ανάγκης

Άλλο ένα βασικό μειονέκτημα χρήσης της VoIP τηλεφωνίας αφορά τις κλήσεις έκτακτης ανάγκης. Με την παραδοσιακή τηλεφωνία μια κλήση έκτακτης ανάγκης ‘οδηγείται’ στο πλησιέστερο τηλεφωνικό κέντρο της υπηρεσίας που καλείται, όπου γίνεται εντοπισμός της κλήσης ακόμα και αν αυτός που καλεί δεν είναι σε θέση να μιλήσει. Με την τεχνολογία VoIP ο κάθε αριθμός δεν συνδέεται γεωγραφικά με μια περιοχή (όπως είδαμε κ παραπάνω) και έτσι μια κλήση είναι απλά μια μεταφορά δεδομένων μεταξύ δύο IP διευθύνσεων. Αυτό έχει ως αποτέλεσμα να μην υπάρχει τρόπος να εντοπιστεί από πού προήλθε η κλήση.

6.2.3 Ποιότητα κλήσης και αξιοπιστία

Εξ' αιτίας της εξάρτησης της τεχνολογίας VoIP με μια σύνδεση Internet η ποιότητα και η αξιοπιστία και των δύο είναι άρρηκτα συνδεδεμένες. Προβλήματα στη σύνδεση Internet θα οδηγήσουν και σε προβλήματα στην ποιότητα την κλήσεων. Αλλά ακόμα και να μην υπάρχουν προβλήματα στη σύνδεση ο τρόπος μετάδοσης των πακέτων μέσω του διαδικτύου μπορεί να δημιουργήσει προβλήματα. Τα πακέτα δεδομένων που αποστέλλονται στο διαδίκτυο πολλές φορές φτάνουν στον προορισμό τους με διαφορετική σειρά από αυτή που έφυγαν από τον αποστολέα τους. Αυτό δεν αποτελεί μεγάλο πρόβλημα για αποστολές email ή εγγράφων γιατί τα δεδομένα μπορούν να επανασυναρμολογηθούν στη μεριά του παραλήπτη χωρίς κανένα πρόβλημα. Στην περίπτωση πακέτων που περιέχουν δεδομένα VoIP κλήσεων το πρόβλημα είναι λίγο μεγαλύτερο γιατί η καθυστέρηση για την επανασυναρμολόγηση των πακέτων προκαλεί σημαντικές καθυστερήσεις στην επικοινωνία. Ένας τρόπος να αποφευχθούν οι καθυστερήσεις είναι να απορρίπτονται πακέτα τα οποία φτάνουν με καθυστέρηση. Αυτό έχει ως αποτέλεσμα να δημιουργούνται κενά ήχου στην επικοινωνία. Το πόσο μεγάλα θα είναι αυτά τα κενά και το κατά πόσο θα δημιουργήσουν πρόβλημα στην επικοινωνία εξαρτάται από το πόσα είναι τα πακέτα τα οποία φτάνουν καθυστερημένα στον προορισμό τους.[15]

6.3 Προοπτικές εξέλιξης

Το VoIP αν και χρησιμοποιείται ήδη από πληθώρα ανθρώπων σε όλο τον κόσμο μελέτες και έρευνες δείχνουν πως και το μέλλον της τεχνολογίας αυτής θα συνεχίσει να είναι λαμπρό αφού οι προοπτικές που αναφέρονται θα προσελκύσουν ακόμα περισσότερο κόσμο. Αν γυρίσουμε λίγα χρόνια πίσω θα δούμε πως θέλοντας να πραγματοποιήσουμε κάποια κλήση στο εξωτερικό και για λίγα λεπτά συνομιλίας ο λογαριασμός του τηλεφώνου θα ήταν πολύ υψηλός. Σήμερα με τη χρήση του VoIP, μπορούμε να κάνουμε απεριόριστες κλήσεις σε οποιαδήποτε χώρα θέλουμε σχεδόν σε τοπικά ποσοστά χρεώσεων.

Παρόλο που η τεχνολογία αυτή έχει κάνει πολλά βήματα προς τα εμπρός η χρήση της δεν είναι ευρέως γνωστή σε πολλές χώρες, αλλά με την ανάπτυξη της τεχνολογικής προόδου, στο άμεσο μέλλον, σχεδόν κάθε λαός στον κόσμο θα

χρησιμοποιεί την υπηρεσία VoIP για επικοινωνία. Οι εξελίξεις και οι προοπτικές αυτές αναφέρονται παρακάτω.[32]

6.3.1 Κινητή τηλεφωνία VoIP (Mobile VoIP)

Η Mobile VoIP (Mobile Voice over Internet Protocol) είναι η εφαρμογή της φωνής μέσω της τεχνολογίας IP σε φορητές συσκευές (PDA, Pocket PC ή Smartphone).
Η Mobile VoIP απαιτεί μια φορητή συσκευή που υποστηρίζει, υψηλής ταχύτητας επικοινωνίες IP. Συνήθως αυτό συμβαίνει χρησιμοποιώντας τη φωνή μέσω Wi-Fi (VoWiFi) , αλλά τα ίδια πρωτόκολλα συνήθως SIP ή Jabber μπορεί να χρησιμοποιηθούν σε οποιαδήποτε ευρυζωνικής δυνατότητας IP ασύρματη σύνδεση δικτύου, όπως τα διάφορα 3G πρότυπα, EVDO rev A. (η οποία συνδέεται με σύγχρονη υψηλή ταχύτητα – ταχύτητες από το δίκτυο προς το χρήστη (downlink), ταχύτητες από το χρήστη προς το δίκτυο (uplink)), HSDPA ή εντέλει με WiMax.
Η Mobile VoIP θα απαιτήσει έναν συμβιβασμό μεταξύ της οικονομίας και της κινητικότητας. Για παράδειγμα, Voice over Wi-Fi προσφέρει δωρεάν υπηρεσία, αλλά είναι διαθέσιμη μόνο εντός της περιοχής κάλυψης του Wi-Fi Access Point. Οι υπηρεσίες υψηλής ταχύτητας από φορείς εκμετάλλευσης κινητών επικοινωνιών χρησιμοποιούν EVDO rev A. ή HSPDA, με πιθανώς καλύτερη ποιότητα ήχου και δυνατότητες για τις μητροπολιτικές-ευρείας κάλυψης, (συμπεριλαμβανομένων των υψηλών ταχυτήτων μεταβιβάσεων από κινητό που βρίσκεται στο βασικό σταθμό σε άλλο), αλλά θα κοστίζουν περισσότερο από τα τυπικά Wi-Fi που βασίζονται σε υπηρεσίες VoIP.
Η Mobile VoIP, θα καταστεί μια σημαντική υπηρεσία τα επόμενα χρόνια, καθώς οι κατασκευαστές συσκευών αξιοποιούν πιο ισχυρούς επεξεργαστές και λιγότερο δαπανηρή μνήμη για να ικανοποιήσουν τις ανάγκες των χρηστών με μικρότερο κόστος γι'αυτούς. Τα Smartphone από τα μέσα του 2006 είναι σε θέση να στέλνουν και να λαμβάνουν email, να περιηγούνται στο internet και σε ορισμένες περιπτώσεις, επιτρέπουν στους χρήστες να παρακολουθούν τηλεόραση.

Η πρόκληση για τον κλάδο του φορέα κινητής εκμετάλλευσης είναι να παραδώσει τα οφέλη και τις καινοτομίες της IP, χωρίς απώλεια ελέγχου της υπηρεσίας δικτύου. Όπως η χρήση του Internet να είναι δωρεάν και να παρέχονται υψηλές ταχύτητες χωρίς επιπλέον χρεώσεις για την επίσκεψη συγκεκριμένων περιοχών σε σχέση με

άλλους δικτυακούς τόπους. Η παροχή κινητού VoIP είναι μια υπηρεσία που αμφισβητεί τις πιο πολύτιμες υπηρεσίες στον τομέα των τηλεπικοινωνιών - Voice. Υπάρχουν τρεις κύριες τεχνολογίες που χρησιμοποιούνται για την κινητή VoIP:

- UMA - Η Unlicensed Mobile Access Generic Access Network, σχεδιάστηκε για να επιτρέψει στο VoIP να ξεπεράσει το GSM

- SIP - Το πρότυπο που χρησιμοποιείται από τις περισσότερες υπηρεσίες VoIP, και τώρα υλοποιείται σε κινητά τηλέφωνα

- Skype πρωτόκολλο - μια ιδιόκτητη έκδοση του Jabber[29]

Εικόνα 6.1:Mobile VoIP

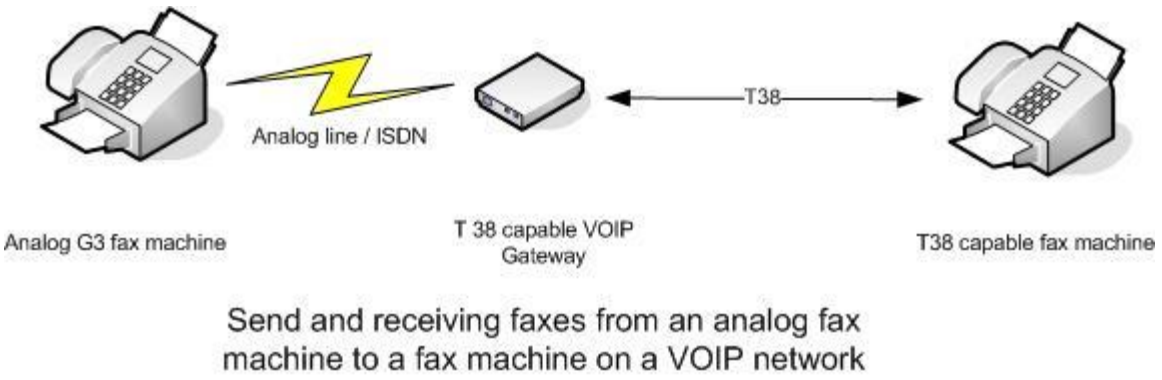
6.3.2 Fax over IP

Τι είναι το fax over ip;

Το Fax over IP(FOIP) αναφέρεται στη διαδικασία αποστολής και λήψης φαξ μέσω δικτύου VOIP. Το Fax over IP λειτουργεί μέσω T38 και απαιτεί πύλη VOIP ικανή για T38, καθώς και συσκευή φαξ, κάρτα φαξ και λογισμικό φαξ ικανά για T38. Οι σύγχρονες πολυλειτουργικές συσκευές φαξ υποστηρίζουν T38.

Το λογισμικό διακομιστή φαξ που μιλάει τη γλώσσα «T38» μπορεί να στείλει και να λάβει φαξ απευθείας μέσω της πύλης VOIP και έτσι δεν χρειάζεται κάποιο

πρόσθετο λογισμικό φαξ. Στις μέρες μας, οι περισσότεροι διακομιστές φαξ απαιτούν τη χρήση χωριστών αδειών για προγράμματα οδήγησης EICON SoftIP ή Cantata FOIP για αποστολή και λήψη φαξ.



Εικόνα 6.2

Τι είναι το T38;

Το T38 είναι ένα πρωτόκολλο που περιγράφει τον τρόπο αποστολής φαξ μέσω ενός δικτύου δεδομένων υπολογιστών. Το T38 είναι απαραίτητο γιατί τα δεδομένα φαξ δεν μπορούν να αποσταλούν μέσω ενός δικτύου δεδομένων υπολογιστών με τον ίδιο τρόπο όπως η φωνητική επικοινωνία.

Το T38 περιγράφεται στο RFC 3362 και ορίζει τον τρόπο με τον οποίο μια συσκευή θα πρέπει να διαβιβάζει τα δεδομένα φαξ. Στην παραπάνω εικόνα (εικόνα 6.2) τόσο η πύλη όσο και η συσκευή φαξ πίσω από την πύλη θα πρέπει να είναι ικανές για T38. Για τη συσκευή φαξ G3 σε αναλογική γραμμή, η διαδικασία αυτή θα είναι σαφής. Η αναλογική συσκευή φαξ δεν χρειάζεται να γνωρίζει τη γλώσσα T38.

Πώς λειτουργεί το Fax σε περιβάλλοντα VOIP;

Το Fax σχεδιάστηκε για αναλογικά δίκτυα και δεν συνεργάζεται καθόλου καλά με δίκτυα VOIP. Αυτό οφείλεται στο γεγονός ότι η επικοινωνία με Fax χρησιμοποιεί το σήμα με διαφορετικό τρόπο από τη συνήθη φωνητική επικοινωνία.
Όταν οι τεχνολογίες VOIP συμπιέζουν και μετατρέπουν σε ψηφιακή την αναλογική φωνητική επικοινωνία, βελτιστοποιείται για φωνή και όχι για Fax. Επομένως, αν συνδέσετε μια συσκευή Fax μέσω προσαρμογέα ATA στο δίκτυο VOIP, θα λειτουργήσει αλλά το πιθανότερο είναι να αντιμετωπίσετε προβλήματα στη διάρκεια των μεταδόσεων φαξ. Αν αυτό είναι επιβεβλημένο, θα πρέπει να διασφαλίσετε ότι χρησιμοποιείτε τον codec G 711, που έχει ελάχιστη συμπίεση.

Για τη χρήση του φαξ έχετε τις ακόλουθες επιλογές:
1. Ο ευκολότερος τρόπος για να χρησιμοποιήσετε τη συσκευή φαξ είναι να τη συνδέσετε απευθείας στην υπάρχουσα αναλογική τηλεφωνική γραμμή και να παρακάμψετε εντελώς το περιβάλλον VOIP σας.
2. Να αντικαταστήσετε τη συσκευή φαξ με κάποιον πάροχο υπηρεσιών φαξ. Υπάρχουν πολλές υπηρεσίες διαθέσιμες με πολύ χαμηλό μηνιαίο κόστος (φθηνότερες από τη συνδρομή της τηλεφωνικής γραμμής)
3. Την εφαρμογή T38, που απαιτεί πύλη συμβατή με T38 και συσκευή φαξ, κάρτα φαξ ή λογισμικό φαξ συμβατά με T38.[30]

ΒΙΒΛΙΟΓΡΑΦΙΑ

1.http://www.3cx.gr/voip-sip/h323.php
2.http://www.worldlingo.com/ma/enwiki/el/Mobile_VoIP
3.http://www.netvoice.gr/index.php/-voip
4.http://www.interga.gr/index.php/el/interga-blog/34-voip/65-voip-telephony-systems
5.http://www.technicalreview.gr/index.php?option=com_content&task=view&id=487
6.http://www.hau.gr/resources/publications/hau_voip_ipcc_article1.pdf
7.http://www.infosum.net/el/communication/new-ways-of-communication-the-voip-technology-a.html
8.https://www.omnivoice.eu/index.cfm/doc/2/cat/5
9.http://www.adslgr.com/forum/showthread.php?t=105763
10.http://www.viva.gr/numbers/knowledgebase
11.The definition Guide to VOIP
12.VoIP for Dummies
13.http://www.en.wikipedia.org
14.http://www.ehow.com/list_6021371_benefits-voip-technology_.html
15.http://www.why-switch-to-voip.com/Advantages_Disadvantages_VoIP.html
16.http://el.wikipedia.org/wiki/%CE%99%CF%83%CF%84%CE%BF%CF%81%CE%AF%CE%B1_%CF%84%CF%89%CE%BD_%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CF%8E%CE%BD
17.http://www.tech-faq.com
18.IP Telephony,The integration of Robust VoIP services by Bill Douskalis(2000)
19.Voice,Video,and Data Network by Juanita Ellis,Charles Pursell,Joy Rahman(2003)
20.Τηλεπικοινωνίες και Δίκτυα Υπολογιστών 6η έκδοση,ΑΡΗΣ ΑΛΕΞΟΠΟΥΛΟΣ,ΓΙΩΡΓΟΣ ΛΑΓΟΓΙΑΝΝΗΣ(1η εκδοση 1991,6η 2003)
21.http://www.iptelephony.gr/news.php?item.118.8
22.http://www.tech-faq.com/rtp.html
23.http://technology.pubkicks.com/el/how-exactly-does-a-voip-phone-work/565/
24.http://www.tech-faq.com/mgcp.html
25.http://www.tech-faq.com/iax.html
26.http://www.voipmentor.com/voip-guide/how-voip-router-works/
27.http://searchunifiedcommunications.techtarget.com/definition/IP-PBX

28.Ασφάλεια πληροφοριακών συστημάτων και δικτύων, Γ.ΠΑΓΚΑΛΟΥ, Ι.ΜΑΥΡΙΔΗ(εκδόσεις ΑΝΙΚΟΥΛΑ)

29.http://knol.google.com/k/mobile-voip#

30.http://www.3cx.gr/voip-sip/foip.php

31.http://www.voipnow.org/protocols/sdp

32.http://ezinearticles.com/?Evolution-and-Future-of-VoIP-Technology&id=3922491

33. http://tinyurl.com/448muyd

34.Porter, Thomas. Practical VoIP Security. 1597490601

35.VoIP-VPN. VPNTOOLS. [Online] [Cited: 4 10, 2007.] http://www.vpntools.com/vpntools_articles/ssl-voip-vpn.htm.

36.http://www.packetizer.com/ipmc/papers/understanding_voip/voip_protocols.html

37.http://www.protocols.com/pbook/voipfamily.htm

38.http://www.ciscopress.com/articles/article.asp?p=606583&seqNum=7